I.J. Wireless and Microwave Technologies, 2026, 3, 290-304
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.03.19

Review on Intelligent Security Models for Digital Twins

Raghavendra Babu T. M.*
School of Computer Science Engineering and Information Science, Presidency University, Yelahanka, Bangalore-560064, Karnataka, India
E-mail: raghavendra.20223cse0034@presidencyuniversity.in
ORCID iD: https://orcid.org/0009-0003-0956-2931
*Corresponding Author

Harish Kumar K. S.
School of Computer Science Engineering and Information Science, Presidency University, Yelahanka, Bangalore-560064, Karnataka, India
E-mail: harishkumarks@presidencyuniversity.in
ORCID iD: https://orcid.org/0000-0001-6438-5606

Received: 20 June, 2025; Revised: 13 November, 2025; Accepted: 24 March, 2026; Published: 08 June, 2026

Abstract: Digital twins are revolutionizing various industries by enabling real-time monitoring, simulation, and optimization of physical entities through their virtual counterparts. However, the increased interconnectivity between the physical and digital realms introduces significant security and privacy challenges, necessitating the development of intelligent security models. This paper explores the architecture of digital twins and identifies the key characteristics of effective security solutions, such as adaptability, real-time response, data integrity, and privacy preservation. Through a comprehensive literature review, we highlight existing intelligent security frameworks that leverage machine learning and artificial intelligence technologies to address the growing range of cyber threats in digital twin environ-ments. Key observations indicate a trend toward integrating advanced analytics for threat detection and response, as well as the application of block chain technology to enhance data integrity and trust. Furthermore, this paper outlines future research directions, emphasizing the potential of innovations like federated learning, graph neural networks, and transfer learning to bolster security in digital twin systems. By examining these aspects, this work underscores the critical importance of developing robust security frameworks to protect digital twins and ensure their safe deployment across various applications.

Index Terms: Digital Twin Security, Artificial Intelligence, Machine Learning, Cyber Threat Detection, Privacy Preservation

1. Introduction

Digital Twins (DT) have emerged as a transformative technology, bridging the gap between the physical and digital realms across various industries. Digital Twins enable real-time monitoring, predictive analytics, and improved decision-making by creating virtual replicas of physical assets, processes, or systems. As organizations increasingly rely on these sophisticated models for operational efficiency and innovation, securing Digital Twins has become paramount. Integrating intelligent security models into Digital Twins is essential for safeguarding sensitive data and ensuring system integrity. The unique characteristics of Digital Twins—such as their dynamic nature, real-time data processing, and reliance on interconnected IoT devices—present new security challenges. Traditional security approaches often fall short in addressing the evolving threats faced by Digital Twins, necessitating the development of advanced security frameworks that leverage artificial intelligence (AI) and machine learning (ML) techniques.

Recent advancements in AI and ML have paved the way for innovative security solutions that can proactively identify and mitigate risks associated with Digital Twins. These intelligent security models can analyze vast amounts of data, detect anomalies, and adapt to new threats, providing a robust defense against cyberattacks. However, despite the progress made in this field, several challenges persist, including the complexity of integration, data privacy concerns, and the need for continuous adaptation to emerging threats.

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

1.1. Architecture

In (Fig. 1.) depicting the architecture of security for digital twins outlines a multi-layered approach to safeguarding the integrity, confidentiality, and availability of digital representations of physical entities. This architecture ensures that digital twins operate securely within their ecosystems, protecting them from various cyber threats. The security architecture of Digital Twins is divided into four separate layers: physical, virtual, data integration, and analysis/decision, where each layer is clearly associated with its respective threat sources and AI/ML-based security solutions. In the physical layer, threats like device spoofing and sensor hijacking are countered by using ML-based anomaly detection and block chain-based provenance tracking to guarantee the authenticity of devices. In the virtual layer, threats like unauthorized access and model manipulation are countered by using strong identity management, digital signatures, and secure containerization. In the data integration layer, threats like data poisoning and replay attacks are countered by using federated learning, encrypted APIs, and integrity validation to ensure the confidentiality and integrity of data. Finally, in the analysis and decision layer, adversarial machine learning attacks and model drift are countered by using adversarial training, differential privacy, and explainable AI, thus ensuring transparent and trustworthy decision-making in Digital Twin systems.

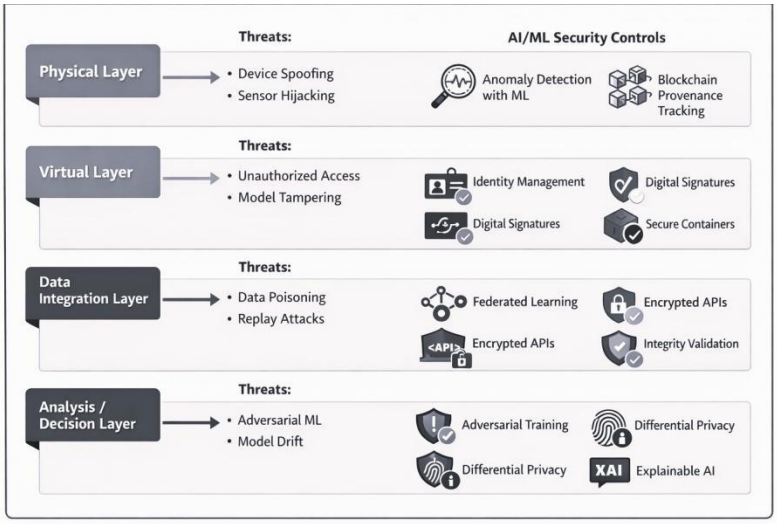


Fig. 1. Architecture of Security for Digital Twins

Unlike traditional layered security architectures, the Digital Twins concept integrates strong cyber-physical coupling, which means that cyber threats can directly lead to unsafe physical behaviors. As such, the security architecture of Digital Twins needs to be analyzed with respect to threat-to-control mapping.

Table 1. Threat-Aware Security Architecture for Digital Twins

DT Layer	Primary Assets	Threat Classes	Representative Attacks	Security Controls
Physical Layer	Sensors, actuators	Tampering, spoofing	Sensor injection, re-play attacks	Secure boot, device at-testation
Data Integration Layer	Data streams, APIs	MITM, data poisoning	Data manipulation, concept drift	Encryption, integrity checks
Virtual Layer	DT models	Model inversion, IP theft	State manipulation	Access control, model watermarking
Analysis & Decision Layer	AI/ML models	Adversarial ML	Evasion, poisoning attacks	Robust training, XAI validation
Actuation Loop	Control signals	Safety violations	Malicious control commands	Runtime policy enforcement

The effectiveness regarding security in Digital Twins correlates not only with detecting cyberattacks but also preventing dangerous physical behavior.

1.2. Characteristics of Intelligent Security for Digital Twins

- **Real-Time Monitoring**: Intelligent security systems provide continuous surveillance of Digital Twins, enabling the immediate detection of anomalies or suspicious activities.
- **Adaptive Threat Detection**: Leveraging machine learning algorithms, these models can learn from historical data and adapt to new threats, enhancing their ability to identify previously unknown attack vectors.
- **Data Integrity and Confidentiality**: Ensures that the data exchanged between physical and digital environments remains accurate and secure, safeguarding sensitive information from unauthorized access or tampering.

- **Anomaly Detection**: Utilizes advanced algorithms to identify deviations from expected behavior in Digital Twins, which may indicate potential security breaches or system malfunctions.
- **Automated Response Mechanisms**: Integrates automated protocols that respond to detected threats in real-time, minimizing response times and mitigating potential damage.
- **Multi-Layered Security Architecture**: Implements a comprehensive security framework that encompasses various layers, including network security, application security, and physical security, providing a holistic defense strategy.
- **Interoperability**: Supports seamless integration with existing security infrastructures and technologies, allowing for enhanced security measures without significant disruption to operations.
- **Predictive Analytics**: Employs predictive modeling techniques to foresee potential security threats and vulnerabilities based on historical data, enabling proactive measures.
- **User-Centric Access Control**: Incorporates robust authentication and authorization mechanisms to ensure that only authorized users have access to sensitive data and functionalities within Digital Twins.
- **Scalability**: Designed to scale with the growth of Digital Twin environments, allowing for the integration of additional devices and systems without compromising security.
- **Compliance with Regulatory Standards**: Adheres to industry regulations and standards related to data protection and cyber security, ensuring that organizations maintain compliance while using Digital Twins.
- **Holistic Risk Assessment**: Provides tools for evaluating the overall security posture of Digital Twins, including identifying potential vulnerabilities and recommending improvements.
- **Context-Aware Security Policies**: Develops security measures that take into account the context in which the Digital Twins operate, ensuring that security protocols are appropriate for specific use cases or environments.
- **Collaboration and Information Sharing**: Facilitates communication and information sharing among various stakeholders to improve situational awareness and collaborative defense strategies.
- **Use of Artificial Intelligence and Machine Learning**: Integrates AI and ML technologies for advanced security analytics, improving the system's ability to learn from threats and enhance its security measures.

These characteristics illustrate the complexity and dynamism required in intelligent security models for Digital Twins. By focusing on these aspects, organizations can better safeguard their Digital Twin environments, ensuring operational continuity and protecting sensitive information from emerging threats. Further, the features are grouped into three strategic dimensions. Each dimension embodies a set of trade-offs between performance, latency, and explainability.

- Operational: Real-time analysis, adaptive detection, latency resilience.
- Analytical: Predictive modeling, federated collaboration, drift adaptation.
- Governance: Compliance (GDPR/HIPAA), auditability, explainability.

Thus, this work aims to explore the current landscape of intelligent security models for Digital Twins, examining the methodologies, technologies, and applications that define this evolving domain. By providing a comprehensive literature review, this work identifies key observations and challenges in the field, ultimately proposing future research directions that can guide the development of more secure and resilient Digital Twin environments. The rest of the paper is organized as follows: Section 2 presents a comprehensive Literature Review of existing research on security models for Digital Twins (DT). Section 3 discusses the process of Developing an Intelligent Security Model for Digital Twins, highlighting the essential stages. Section 4 examines various ML and AI Models applicable to securing Digital Twins, emphasizing their role and relevance. Section 5 provides an Overview of Open Source and Proprietary Tools available for Digital Twin development. Section 6 offers Observations and Future Research Directions, addressing current challenges and proposing future avenues for investigation. Finally, Section 7 concludes the paper and outlines potential areas for Future Work in this domain.

2. Literature Review

Recent advancements in Digital Twins (DT) have been extensively documented in the literature, showcasing a variety of methodologies, applications, and challenges. This section reviews significant contributions to the field, categorized into various subsections.

2.1. Foundational Studies

Klaus Droder et al. [1] present a method that combines machine learning with robot control to enable obstacle avoidance and human protection, emphasizing the need to improve data processing and response times in the demonstration system. Adnan Khan et al. [2] describe implementing a digital twin for legacy systems using model-based testing. They used conformance testing in addition to visual examination to confirm the correct input-output assignments, leading to a more reliable simulation model.

2.2. Modeling and Simulation Advances

Soumya Singh et al. [3] introduce a toolbox that enhances modeling and simulation practices to implement domain-specific Digital Twins (DT). The approach is demonstrated through the development of a battery system Digital Twin in a robotic mini-car. Aderrahim Ait-Alla et al. [4] propose a method that focuses on the number of synchronization points and sensors required to realize dedicated control by the digital twin while analyzing the connection between a physical production system and its digital twin. Simulation results indicate that the key to achieving cost savings through digital twins (DT) implementation lies in measuring parameters that reflect uncertainties in production systems, such as machine breakdowns and order arrival times. Elisa Negri et al. [5] build a simulation module called the FMUs to simulate particular behaviors of the manufacturing equipment. The digital twins (DT) can be utilized to comprehend various elements of what is occurring on the shop floor in real time and to update the actual system with any enhancements made to the digital model. Suewellyn Kruger et al. [6] conduct a bibliometric analysis of Digital Manufacturing, specifically focusing on Digital Twins and real-time system monitoring, using the ProKnow-C method for knowledge development and systematically analyzing the research portfolio. To ensure a strong theoretical foundation for this research, the ProKnow-C method was employed to systematically, effectively, and comprehensively search and select relevant articles from various databases.

2.3. Frameworks and Methodologies

Hasan Latif et al. [7] suggest a framework for implementing digital twins. They explore how digital twins (DT) might be used as a tool in the manual assembly process, review the state of the art, and identify research gaps. An appropriate industrial case study is examined to illustrate the suggested framework. Kirill Semenkov et al. [8] Analyze and compare different modeling approaches for Cyber-Physical Systems, highlighting the significance of a hybrid model that incorporates virtual machines, emulators, and real hardware for testing and verifying complex systems while ensuring consistent time scales. Manolya Atalay et al. [9] highlight the risks to different layers of smart grid environments and provide an overview of smart grid cybersecurity standards. They propose digital twins (DT)-based strategy for smart grid security testing, emphasizing its potential as a crucial tool for standardization. Mamadou K. Traore [10] proposed a three-layered model that provides a technology-independent and comprehensive framework for defining and understanding digital twins, offering a modular architecture for developing specific solutions.

2.4. Application and Implementation

Muhammad Fajrul Falah et al. [11] describe a platform that integrates Digital Twin concepts with immersive experiences, utilizing free and open-source software and hardware, to link physical devices with their virtual models. The platform showcases the successful integration of physical devices with their virtual models through Digital Twins, empowering industry stakeholders to independently develop their digital twins. Behrang Ashtari Talkhestani et al. [12] Present the implementation of the Anchor-Point-Method based on an assistance system and evaluate its functionality. For the reconfiguration of a manufacturing system, a synchronized Digital Twin's benefits are evaluated both qualitatively and quantitatively. Cristina Alcaraz and Javier Lopez [13] conducted an in-depth analysis of how various security threats impact the confidentiality, integrity, and availability of Digital Twins (DTs). They emphasize incorporating security measures throughout the DT lifecycle, from design and development to deployment and operation. The study highlights that security threats to DTs can result in financial losses, operational disruptions, and safety hazards, while current mitigation strategies remain in early stages, necessitating further research and development. Peter Bauer et al. [14] introduced a virtual replica of Earth to monitor environmental changes and human impacts, assisting in the EU's green transition by supporting decision-making in sectors such as energy, agriculture, and disaster management. The potential to enhance disaster preparedness, monitor biodiversity, and protect ecosystems is also emphasized. Hailin Feng et al. [15] proposed a scheme utilizing attribute-based encryption (ABE) to safeguard data privacy, ensuring that only authorized users access sensitive information in IoT communication systems. While effective for securing communication in various twin systems, scalability and interoperability challenges may arise in large-scale and heterogeneous IoT networks. Aidan Fuller et al. [16] stressed the need for clear definitions and applications of Digital Twins, particularly leveraging IoT and machine learning (ML). They see DTs as essential to Industry 4.0, with expanding interest in healthcare and smart cities, but advocate for precise definitions, efficient technology integration, and the need to address the challenges. Mina Jafari et al. [17] emphasized the advantages of using DTs in smart grids and transportation systems, noting reductions of 10-20% in transportation time and cost savings of 5-10%, with power grid reliability improvements of up to 99.5%. They call for enhanced data security and privacy mechanisms to protect sensitive information in these sectors. Maninder Jeet Kaur et al. [18] reviewed the essential components for successful IoT-based Digital Twin products, highlighting the integration of DTs, IoT, and ML for actionable insights. They demonstrated various ML model performances but emphasized addressing IoT security threats like cyberattacks to ensure comprehensive implementation. Kostiantyn Maksymenko et al. [19] introduced a novel approach simulating surface electromyography (sEMG) signals using a digital twin model, facilitating smart assembly processes for complex products. By leveraging workflow technology, this framework traces assembly processes to detect errors and deviations, with a focus on personalized human-machine interfaces. Hanqing Qiu et al. [20] proposed a conceptual framework for a Forest Digital Twin (FDT), organized into three layers: data, simulation, and application. The paper highlights the

importance of ethical considerations in the use of FDTs in forest management and calls for practical case studies to demonstrate real-world implementation. Csaba Ruzsa [21] proposed a standardized framework to classify Digital Twins by complexity, purpose, and data sources. The study emphasizes the need for robust mechanisms to ensure accurate integration of external data and evaluates ML model performances, with SVM achieving 0.78 and KNN 0.85. Michael Jacoby and Thomas Uslander [22] identified similarities and differences among IoT and DT standards. They proposed a classification scheme for resource description, discovery, and access applied to six existing standards. The study highlights the need for performance and scalability evaluations of these standards, alongside addressing security and privacy challenges. The key features of manufacturing digital twins have been presented by the authors Anis Assad Neto et al. [23] based on a literature review. For behavior simulations and performance evaluations, the Digital Twin permits physical resource abstraction in the virtual environment. Industrial experts examined the identified features and found them to be vital to the implementation of digital twins. Ananda Chakraborti et al. [24] propose a model reduction method based on spectral clustering and graph centrality to optimize high-importance variables and minimize the total number of variables in a multi-dimensional digital twin model. A model reduction method is presented for the multidimensional graphical representation of variables in VE models, utilizing spectral clustering to identify and eliminate less sensitive variables, thereby improving the speed and efficiency of the DT representation.

2.5. Recent Advances

Chiara Cimino et al. [25] highlight the benefits of using Dynamic Models (DMs) in a Digital Twin (DT) by discussing their integration, data interchangeability, and providing an illustrative example using an object-oriented modeling language. Leonard Overbeck et al. [26] outline a method for bridging the gap between models and reality through continuous, iterative upgrades made possible by connecting simulation models with IT systems and smart data analysis. The effectiveness of the approach was demonstrated by a real-world automobile sector, where an average variation between output and reality per week of 0.1% was attained. Using the Alpha Algorithm, the material flow was identified. Lucrezia Morabito et al. [27] propose a method to implement a digital twin in manufacturing by using a virtual simulator connected in real time to the actual system, with two industrial use cases showcasing its benefits for the manufacturing sector. Vladimir Kutscher et al. [28] propose a method for virtualizing cyber-physical system tests using digital twins (DT), aiming to reduce time and cost by leveraging Industry 4.0 methods and focusing on the interaction between simulated hardware and embedded software, which is demonstrated through a prototype implementation. Yin Z H et al. [29] suggest the technology of digital twins (DT) in the aerospace field, highlighting their benefits such as shorter design cycles, increased reliability, reduced overhauls, and lower maintenance costs. The importance and current applications of digital twins in the aerospace industry are discussed. Dionisio Rocha et al. [30] present a methodology that combines self-organized distributed control system design with DT to anticipate the system's evolution and, if necessary, modify it. DTs can be used to predict the execution of devices and systems in industrial environments. Benjamin Maschler et al. [31] present case studies from the field of industrial manufacturing that are provided and qualitatively analyzed to highlight the potential of intelligent Digital Twins reinforced with cross-phase transfer learning capabilities. To illustrate the benefits, a real cyber-physical manufacturing system composed of an automated welding machine and an automated guided vehicle with a robot arm is used. Wider adoption of the proposed concept would greatly benefit intelligent digital twins, enabling expanded functionality, reduced training requirements, and increased robustness. The Deep-Q Network is used by Zai Mueller-Zhang et al. [32] to present a digital twin-based self-learning process planning technique that can discover the best process plans and workflows for the simultaneous manufacture of personalized products. The approach is evaluated for the BaSys 4 project in relation to the SMS Group's aluminum cold milling factory. The evaluation's objective was to show conclusively that the suggested method can handle a large problem space.

Benjamin Rohm et al. [33] present a conceptual approach to the SDM-Digital Twins (DT), emphasizing the process and information model. A case study is used to explain the suggested concept. Tsega Y. Melesse et al. [34] demonstrate a method for developing a machine learning-based digital twin of a banana fruit using a thermal camera as a data collection device to monitor the product quality. A promising method for the creation of fruit digital twins has been demonstrated with a prediction accuracy of 99%. Manuel S. Muller et al. [35] propose an approach aimed at bridging the gap between reality and simulation to create self-improving models for an intelligent Digital Twin. The method is evaluated using autonomous mobile robots that connect CPMS workstations. The synchronization mechanism learned to compensate for nonlinearities in the system, resulting in a 30% increase in the accuracy of the movement model. Feng Xiang et al. [36] define and build a manufacturing service network for a digital twin system, providing insights into optimizing its configuration. Additionally, it reviews the main technologies used in developing the manufacturing service network. Geoffrey Tissot et al. [37] create a digital twin architecture based on a simulation optimization model. This architecture will be demonstrated using a scheduling problem as a case study, but its applicability can be extended to other decision-making levels. A cloud-based digital twin has been developed by Sam Weckx et al. [38] to monitor a clamping technique used in machine composite parts. The cloud-based digital twins (DT) examine the drilled holes quality using computer vision, track drill wear, and find instances where the active clamping mechanism is operating improperly. The entire deployment takes place on the cloud platform Microsoft Azure. Alessandro Chiurco et al. [39] recommend an architecture-based methodology to help ML practitioners choose the best ML algorithms for creating

intelligent DTs for Production Planning & Control (PPC) applications. The framework is illustrated through an industrial case study employing Neural Networks, k-Nearest Neighbor, and Symbolic regression algorithms to validate its effectiveness. Ehsan Badakhshan et al. [40] present a framework that combines simulation and machine learning to optimize inventory replenishment strategies in supply chain digital twins, highlighting the significant impact of the upstream member in mitigating the bullwhip effect. Zhengmin Zhang et al. [41] proposed a clearing function-based simulation optimization (CFSO) methodology for addressing product release planning issues in a digital twin wafer fabrication system, introducing specific procedures for creating and revising product release plans. The proposed method for product release planning in a digital twin wafer fabrication system is validated through a benchmark test, demonstrating its effectiveness in saving at least 26% of production costs compared to other methods, particularly suitable for digital twin platforms utilizing discrete event simulation technology. Lixiang Zhang et al. [42] Present twins learning (TL), a real-time scheduling technique based on reinforcement learning and digital twins that combines the physical, digital, and learning optimization spaces to simultaneously accomplish responsiveness and optimization efficiency requirements. The twins learning (TL) method proposed in this study demonstrates enhanced adaptability compared to other methods. Chanjei Vasanthan et al. [43] describe an autonomous path-planner. The model's limitations were developed using COLREG rule 14 in conjunction with the standards put forward by DNV GL for an autonomous path planner. Based on a control plant model, a digital twin of the own vessel was created. The digital twin (DT) was also incorporated into the path-planner to detect probable collisions and start the re-planning process as a result. Sylvain Chabanet et al. [44] suggest the use of a self-adaptive digital twin (DT) for stream-based Active Learning, demonstrating a sawmill sector use-case to handle variations in data flow and enable the DT's active participation in selecting training samples for supervised Machine Learning (ML) models. The approach presented by N. Kolibarov et al. [45] utilizes supervised deep learning techniques to extract roof edges from a single orthophoto for generating parametric LoD2+ models of buildings. The proposed method achieves good performance in semantic segmentation of roofs, even with a small amount of training data and in the presence of noise, with mean IOU and Dice metric scores of approximately 56% and 71%, respectively, for the extracted roof elements in the test area. Omer San [46] presented a mathematical framework using probabilistic graphical models to enhance intelligent automation and decision-making in asset-twin systems. This framework supports real-time control and dynamic decision-making, although its reliance on synthetic data limits its representation of real-world complexities.

Concetta Semeraro et al. [47] provided a detailed overview of Digital Twin research, emphasizing the synchronized virtual representation of reality. They highlighted the need for cognitive digital twins capable of seamless interaction with other twins and humans to maximize the technology's potential.

Angira Sharma et al. [48] provided a comprehensive definition of Digital Twins, distinguishing them from related concepts such as simulations and autonomous systems. They suggest further exploration of DT applications across various domains and a deeper discussion on their potential benefits and limitations.

Maulshree Singh et al. [49] consolidated definitions of Digital Twins and related concepts such as 'prod-uct avatar' and 'digital thread.' They emphasized the role of DTs in reducing operational costs and improving system productivity, maintenance, and safety. The study advocates for better data quality and security mechanisms for DTs.

Sabah Suhail et al. [50] tackled security challenges by providing a gamified platform supported by explainable AI (XAI) for training security analysts and assessing the security of DTs. While effective in simulations, the platform's long-term adaptability to new cyber security challenges remains a key concern. Xuemin Sun et al. [51] explored the integration of 3D design, process parameters, and runtime data in Digital Twins to support simulation and issue prediction during assembly-commissioning processes. The use of AI and ML for automation was also examined, specifically in industries like aerospace and marine. Thomas H-J Uhlemann et al. [52] highlighted the potential of real-time data acquisition and simulation-based data processing in production systems, demonstrating substantial improvements in production efficiency, downtime, and data processing. However, the need for robust security measures in handling sensitive data was emphasized. Xiaochen Zheng et al. [53] proposed the Cognitive Digital Twin (CDT) as an evolution of the traditional Digital Twin, aimed at providing a more intelligent and comprehensive representation of complex systems throughout their lifecycle. However, challenges remain in developing the cognitive capabilities of CDT. Cunbo Zhuang et al. [54] introduced a Digital Twin model for improving the management of assembly data in complex products. This model enhances data management efficiency and traceability accuracy, but the authors emphasize the need for strong data protection mechanisms to secure assembly data. Tian et al. [55] present a comprehensive survey on poisoning attacks in machine learning, examining various attack types and mechanisms, as well as effective countermeasures to improve system security and robustness against adversarial threats. Joern Ploennigs et al. [56] explore the use of semantic graphs to automate Digital Twins (DT), including the introduction of benchmark datasets and reference architecture, addressing scaling challenges and providing insights for configuring Artificial Intelligence (AI) models in Digital Twins (DT). Zhihan Lv et al. [57] review the application and challenges of digital twins combined with Artificial Intelligence (AI) in different fields, aiming to provide a theoretical foundation for their implementation across industries and inspire future research. Mariana Segovia et al. [58] focus on the methodology of constructing digital twins, including the design, creation, and connection of physical objects with their virtual counterparts by covering various phases from functional requirement selection to model integration and verification. The research addresses modeling physical objects, structuring Digital Twins (DT) architecture, synchronizing real-time

data, and identifying challenges in developing DTs. Dong Zhong et al. [59] examined the use of Digital Twins for predictive maintenance (PdM), which aims to reduce equipment downtime and maintenance costs while extending machine lifespan. The accuracy of predictive models is crucial for the success of PdM, and ensuring data quality is paramount. Lisa Gopal et al. [60] focus on cost-effective defect diagnosis methods, efficient data acquisition through Micro-Electro-Mechanical (MEM) devices, Zigbee wireless transmission, and secure manufacturing systems. This investigation explores damage management in precision instrument components, develops a defect prediction module using Digital Twins (DT) techniques, and establishes system architecture for damage detection and model optimization in manufacturing systems. Sabah Suhail et al. [61] discuss attacks on digital twins, propose security solutions, and introduce a gamification approach for assessing and enhancing the security level of digital twins while providing a virtual training environment for security analysts. The proposed gamification approach is effective for evaluating the security level of both digital modes, i.e., replication and simulation.

The important unanswered questions found in the current literature are:

- Lack of DT-specific threat modeling that links attack vectors to physical consequences and safety impact.
- Lack of security classification scale aligned with the data flow from DT sensing to actuation: integration → analytics→ actuation.
- Lack of synthesis between AI/ML-related methods for security and models of adversaries, criticality of assets, and system-level resilience.
- Insufficient treatment of the topic of criterion evaluation for intelligent security models in terms of robustness, latency overhead, and explainability.

Objective of this review The challenges described create a gap that this article will fill by tackling these challenges through: (i) organizing existing security research regarding DTs from a threat-aware architectural layer perspective, (ii) conceptualizing AI/Machine Learning security solutions based on adversaries' intentions and security implications, and lastly, by pointing to research directions with security evaluation benchmarks applicable to Digital Twin settings.

3. Developing an Intelligent Security Model for Digital Twins

The (Fig. 2.) represents key steps involved in developing an intelligent security model for Digital Twins. The process begins with Risk Assessment and Threat Modeling, where potential security risks and vulnerabilities are identified, and an understanding of possible threats is established. Following this, the security model is architected in the Architect Security Model phase, where a comprehensive framework for securing the Digital Twin environment is designed.

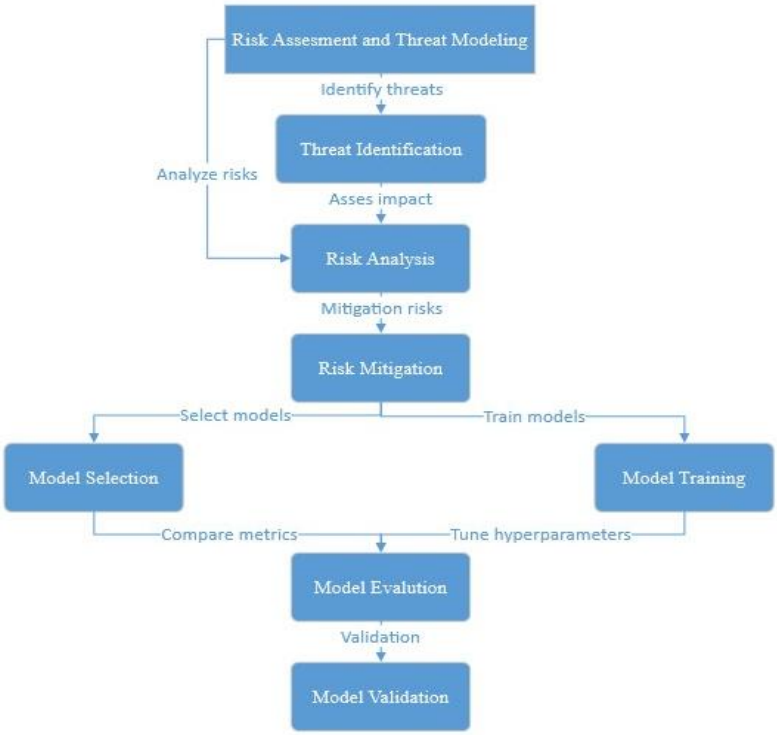


Fig. 2. Process for Developing an Intelligent Security Model for Digital Twins

Once the architecture is defined, the focus shifts to selecting and training machine learning (ML) and artificial intelligence (AI) models in the Select & Train AI/ML Models stage. These models are critical for providing real-time insights and adapting security mechanisms. After the models are prepared, the Implementation of Security Mechanisms takes place, where the necessary security controls and protocols are deployed within the system.

Subsequently, Secure Communication Channels are developed to ensure that data transferred between the physical and virtual layers remains encrypted and protected from cyberattacks. This is followed by the Testing and Validation phase, where the security model is rigorously tested for vulnerabilities and its effectiveness is validated.

Once testing is complete, the security model is deployed in a real-world setting to ensure that it functions as intended. The system is then subject to Real-time Monitoring and Adjustments, where security performance is continuously tracked and any necessary adjustments are made to address new threats. Finally, the process enters a Continuous Monitoring and Updates phase, ensuring that the system stays secure and resilient over time as new vulnerabilities are discovered and addressed.

Table 2. Summary of Articles on Digital Twins

Paper	Type	Actual Twin	Broad Area	Technology
Droder et al. (2018) [1]	Concept	Yes	Robotics	Machine Learning
Khan et al. (2018) [2]	Case Study	Yes	Legacy Systems	Model-Based Testing
Singh et al. (2021) [3]	Case Study	No	Battery Systems	Simulation Toolbox
Ait-Alla et al. (2019) [4]	Concept	No	Production Systems	Simulation
Negri et al. (2019) [5]	Concept	No	Manufacturing	Simulation Modules
Kruger et al. (2019) [6]	Review	No	Digital Manufacturing	Literature Review
Latif et al. (2020) [7]	Case Study	No	Manual Assembly	Framework Development
Semenkov et al. (2020) [8]	Concept	No	Cyber-Physical Systems	Hybrid Modeling
Atalay et al. (2020) [9]	Concept	No	Smart Grids	Cyber security
Traore (2021) [10]	Concept	No	Digital Twins	Framework Development
Falah et al. (2020) [11]	Case Study	Yes	Digital Twin Platforms	Immersive Technology
Talkhestani et al. (2020) [12]	Case Study	Yes	Manufacturing Systems	Anchor-Point Method
Neto et al. (2020) [23]	Review	No	Digital Twins	Review of Features
Chakraborti et al. (2020) [24]	Concept	No	Model Reduction	Spectral Clustering
Cimino et al. (2020) [25]	Concept	No	Dynamic Modeling	Object-Oriented Modeling
Overbeck et al. (2021) [26]	Case Study	Yes	Automotive Sector	Data Analysis
Morabito et al. (2021) [27]	Case Study	Yes	Manufacturing	Real-Time Simulation
Kutscher et al. (2021) [28]	Concept	No	Cyber-Physical Systems	Virtualization
Yin Z H et al. (2020) [29]	Review	No	Aerospace	Digital Twin Technology
Rocha et al. (2021) [30]	Concept	No	Control Systems	Self-Organized Design
Maschler et al. (2021) [31]	Case Study	Yes	Manufacturing	Transfer Learning
Mueller-Zhang et al. (2021) [32]	Case Study	Yes	Process Planning	Deep-Q Network
Ro¨hm et al. (2022) [33]	Concept	No	SDM-Digital Twins	Process Model
Melesse et al. (2022) [34]	Case Study	No	Agriculture	Machine Learning
Muller et al. (2022) [35]	Case Study	Yes	Autonomous Systems	Self-Improving Models
Xiang et al. (2022) [36]	Concept	No	Manufacturing Service Network	Optimization Techniques
Tissot et al. (2022) [37]	Concept	No	Simulation Optimization	Scheduling Problem
Weckx et al. (2022) [38]	Case Study	Yes	Composite Parts	Cloud Technology
Steinmetz et al. (2022) [62]	Case Study	No	DT-Based Systems	Simulation Environment
Chiurco et al. (2022) [39]	Concept	No	Production Planning	ML Algorithms
Zhengmin Zhang et al. (2022) [41]	Concept	No	Wafer Fabrication	Simulation Optimization
Lixiang Zhang et al. (2022) [42]	Concept	No	Scheduling	Reinforcement Learning
Vasanthan et al. (2021) [43]	Case Study	No	Autonomous Systems	Path Planning
Chabanet et al. (2022) [44]	Concept	No	Active Learning	Stream-Based Learning
Kolibarov et al. (2022) [45]	Case Study	No	Building Models	Deep Learning
Tian et al. (2023) [55]	Review	No	Machine Learning	Poisoning Attacks

4. ML and AI models for Intelligent Security model for Digital Twins

Table 3. categorizes various machine learning and AI models used for enhancing security in Digital Twins. It includes supervised learning models like SVMs and decision trees for threat detection, unsupervised models for anomaly detection, and deep learning models like CNNs and RNNs for complex pattern recognition. Reinforcement learning models, hybrid models, and emerging techniques like federated learning and block chain-based security solutions are also listed for secure communication, predictive accuracy, and tamper-proof logging.

Table 3. ML and AI Models for Intelligent Security in Digital Twins

Category	Model	Use Case
Supervised Learning Models	Support Vector Machines (SVM) Decision Trees (DT), Random Forests k-Nearest Neighbors (k-NN)Naive Bayes	Anomaly detection, classification of threats Identifying security breaches by learning decision paths Detecting patterns and anomalies Real-time classification of cyber attacks
Unsupervised Learning Models	K-Means Clustering Gaussian Mixture Models (GMM) Autoencoders	Clustering patterns to detect outliers Identifying unusual activities or attacks Anomaly detection in high-dimensional data
Deep Learning Models	Convolutional Neural Networks (CNN) ,Recurrent Neural Networks (RNN), LSTM Generative Adversarial Networks (GANs) Deep Belief Networks (DBN)	Intrusion detection in network traffic, pattern recognition Time-series data for detecting sequential security patterns Simulating attack scenarios, generating threat data Detecting high-level anomalies in large datasets
Reinforcement Learning Models	Q-Learning Deep Q-Networks (DQN) Proximal Policy Optimization (PPO)	Adaptive security policies for dynamic environments Autonomous learning for threat detection Continuous security monitoring
Hybrid & Ensemble Models	Boosting Algorithms (Ada Boost, XGBoost) Stacked Generalization (Stacking) Random Forests	Improved classification for security threats Enhanced predictive accuracy by combining multiple models Hybrid models for security threat classifications
Anomaly Detection Models	Isolation Forest One-Class SVM Local Outlier Factor (LOF)	Detecting outliers in large datasets Identifying rare events or security outliers Detecting localized security threats
Federated Learning (FL)	Distributed Machine Learning	Collaborative model training while maintaining data privacy
Graph Neural Networks (GNNs)	Graph-based Learning	Network-based threat detection, learning from dependencies
Transfer Learning	Reuse of Pre-trained Models	Adapting existing models to DT security contexts
Bayesian Networks	Probabilistic Decision Making	Predicting likelihood of security breaches
Time-Series Analysis Models	ARIMA Holt-Winters Exponential Smoothing	Time-series forecasting to detect anomalies Detecting anomalies in time-series data
Blockchain-based Security Models	Blockchain & Smart Contracts	Tamper-proof logging, decentralized verification

5. Overview of Open Source and Proprietary Tools for Digital Twin Development

Table 4 presents a comparative overview of open-source and proprietary digital twin tools, highlighting their descriptions, key features, and applications across various industries. This table categorizes the tools into two distinct groups, providing insights into their functionality and usage contexts. Open-source tools are designed to foster collaboration and flexibility, often facilitating integration with other software and enabling customization to meet specific user needs. In contrast, proprietary tools offer robust, commercially supported solutions tailored for industry-specific applications, ensuring reliability and advanced capabilities.

Review on Intelligent Security Models for Digital Twins:

Table 4. Digital Twin Tools: Open Source and Proprietary

Tool Name	Description	Key Features	Applications
Open Source Tools			
Unity Reflect	Real-time 3D visualization tool for architecture, construction, and engineering, integrating with design software like Revit and BIM tools.	- Real-time collaboration - BIM visualization - AR/VR integration	- Architecture - Engineering - Construction
SimScale	Cloud-based physics simulation platform offering CFD, FEA, and thermal analysis for engineers.	- Cloud simulation - Physics tools (CFD, FEA) - Collaboration features	- Mechanical engineering - Fluid dynamics
AWS IoT TwinMaker	AWS platform for creating digital twins with integrated real-time data and analytics.	- Scalable cloud platform - Real-time data processing	- IoT infrastructure - Smart buildings
Altair Digital Twin	HPC simulation tool integrating AI/ML for optimizing designs and predictive maintenance.	- AI/ML integration - HPC simulations	- Automotive - Aerospace
ThingWorx (PTC)	IoT platform integrating AR/VR for digital twins with real-time monitoring.	- IoT connectivity - Predictive analytics	- Smart manufacturing - Supply chain management
Proprietary Tools			
Siemens Mindsphere	Industrial IoT platform for cloud-based data analytics and predictive maintenance.	- Cloud analytics - Edge computing support	- Smart manufacturing - Energy management
Ansys Twin Builder	Simulation-driven platform to build and optimize digital twins for product development.	- Multi-physics simulation - Predictive maintenance	- Aerospace - Energy sectors
Azure Digital Twins	Microsoft IoT platform for creating comprehensive models of physical environments.	- Cloud model - Real-time integration	- Smart buildings - Industrial IoT
Dassault Systemes 3DEXPERIENCE	Platform for 3D modeling and digital twin creation used in various industries.	- 3D design - Collaborative cloud	- Aerospace - Manufacturing
GE Digital Predix	Industrial platform for asset Performance management with predictive analytics.	- Asset monitoring - AI insights	- Industrial automation - Power generation
IBM Digital Twin Exchange	Platform for virtual representations of assets integrated with IoT and AI.	- AI integration - Real-time monitoring	- Energy - Manufacturing

6. Observations and Future Research Directions

6.1. Observations

The integration of intelligent security models within Digital Twins (DT) represents a transformative shift in safeguard-ing complex systems. As industries increasingly adopt Digital Twin technology for real-time monitoring and predictive analytics, the importance of robust security measures cannot be overstated. Observations in this domain reveal that the application of machine learning algorithms enhances the ability to identify anomalies and potential threats within digital environments. Traditional security methods are often insufficient due to the dynamic nature of digital twins, which require adaptive and intelligent systems to respond to evolving threats.

Recent advancements in artificial intelligence (AI) and machine learning (ML) have paved the way for the development of intelligent security models that leverage data-driven insights for proactive threat detection. These models utilize various learning methods, including supervised, unsupervised, and reinforcement learning, to train algorithms on historical data, enabling them to recognize patterns associated with malicious activities.

Moreover, tools and frameworks that facilitate the simulation and evaluation of security measures in Digital Twins have gained traction. Technologies such as virtualization and cloud computing provide environments for testing security protocols and evaluating their effectiveness without risking real-world systems. The use of secure communication protocols, along with decentralized architectures, enhances the resilience of Digital Twins against unauthorized access and data breaches.

6.2. Challenges

Despite the progress made in developing intelligent security models for Digital Twins, several challenges persist. One of the primary obstacles is the complexity of integrating security measures within existing DT frameworks without compromising their performance and efficiency. Ensuring that security protocols do not introduce latency or hinder the functionality of Digital Twins is critical, particularly in real-time applications such as manufacturing, healthcare, and smart cities.

Data privacy and regulatory compliance also pose significant challenges. As Digital Twins often handle sensitive data, ensuring that security models comply with legal frameworks such as GDPR and HIPAA is paramount. The need for transparency in how data is used and secured further complicates the development of intelligent security models.

Additionally, the variability in the architecture and components of Digital Twins creates difficulties in implementing standardized security solutions. Different industries may have distinct security requirements based on their operational contexts, making it challenging to develop universally applicable models.

Finally, the adversarial nature of cybersecurity threats means that intelligent security models must continuously evolve. Threat actors employ sophisticated techniques, such as machine learning adversarial attacks, to exploit vulnerabilities. Therefore, developing models that can adapt and learn from new threats in real-time remains a formidable challenge.

The challenges are systematically mapped to the three-stage Digital Twin pipeline of sensing, integration, and actuation, where each stage is described by typical threats and compliance metrics.

6.3. Future Research Directions

To address the current challenges and enhance the security of Digital Twins, several future research directions can be pursued:

- **Development of Adaptive Security Models:** Research should focus on creating security models that can dynamically adapt to changing environments and emerging threats. Incorporating real-time learning capabilities will allow systems to evolve alongside the threats they face.
- **Integration of Blockchain Technology:** Exploring the use of blockchain for securing Digital Twins can provide immutable records of transactions and interactions, enhancing data integrity and authenticity. Future research could investigate the effectiveness of decentralized trust models in the context of Digital Twins.
- **Enhanced Threat Detection Mechanisms:** There is a need for advanced anomaly detection systems that utilize deep learning techniques. By leveraging neural networks and other sophisticated algorithms, these systems can identify complex patterns indicative of potential security breaches.
- **Interdisciplinary Approaches:** Collaborating across fields such as AI, cybersecurity, and systems engineering can lead to innovative solutions. Future research could benefit from insights gained from related domains, such as IoT security and industrial control systems.
- **Simulation and Testing Frameworks:** Developing comprehensive testing frameworks that simulate various attack scenarios can help evaluate the resilience of intelligent security models. These frameworks should incorporate automated tools for continuous security assessment.
- **Focus on Regulatory Compliance:** Future studies should explore methodologies for ensuring that intelligent se-curity models are compliant with data protection regulations. This includes developing best practices for data handling, storage, and sharing in the context of Digital Twins.
- **User-Centric Security Solutions:** Investigating the role of human factors in the security of Digital Twins can enhance the effectiveness of security models. Future research could explore how user behavior impacts security and how adaptive interfaces can improve user engagement with security measures.
- **User-Centric Security Solutions:** Investigating the role of human factors in the security of Digital Twins can enhance the effectiveness of security models. Future research could explore how user behavior impacts security and how adaptive interfaces can improve user engagement with security measures.

By pursuing these research directions, the field of intelligent security models for Digital Twins can advance significantly, contributing to safer and more resilient digital environments.

Table 5. Data Flow Phase-wise Risk Analysis and Proposed Controls

Data Flow Phase	Key Risk	Proposed Controls / Compliance Metrics
Sensing	Sensor spoofing, unauthorized access	Latency < 100 ms, hardware attestation, encrypte
Integration	Poisoned data streams, Man-in-the-Middle (MITM) attacks	Secure multiparty computation, API trust scoring
Actuation	Model drift, unsafe outputs	Explainable ML validation, real-time monitoring

7. Conclusion and Future Work

This paper presents a comprehensive review of the current advancements and methodologies related to intelligent security models for Digital Twins (DTs). The literature highlights the increasing need for robust and adaptable security mechanisms as DTs become more integral to modern industries. We explored the essential components for developing intelligent security models and identified relevant Machine Learning (ML) and Artificial Intelligence (AI) models that can enhance the security framework. The analysis shows that supervised, unsupervised, deep learning and reinforcement learning models are particularly effective for identifying, classifying, and mitigating various security threats in DT environments. Furthermore, the study outlined existing tools, both open source and proprietary, which are vital for researchers and developers to experiment and implement secure DTs. Despite the progress in securing DTs, several challenges remain. These include the complexity of integrating ML models in real-time environments, addressing privacy concerns, and ensuring continuous monitoring and adaptability of the security models. Scaling these solutions to handle large, distributed systems introduces new performance bottlenecks and attack vectors. The use of blockchain, federated learning, and graph neural networks shows promise but requires further research to optimize their deployment in secure DT environments.

Future work focuses on the continued development of adaptive security frameworks that can dynamically adjust to evolving threats while maintaining the integrity and performance of the digital twin system. Integrating quantum-resistant encryption techniques and advanced decentralized approaches, such as blockchain for immutable logging, could play a significant role in future DT security models.

All the Declarations and Statements

Author Contributions Statement
All authors have read and agreed to the version of the manuscript.

Conflict of Interest Statement
Authors declare no conflict of interest.

Funding Declaration
No external funding.

Data Availability Statement
None.

Ethical Declarations
This study does not invoke any human participants or animals. Hence, ethical approval is not required.

Acknowledgments
The authors would like to express their sincere gratitude to domain experts and reviewers for their valuable feedback and constructive suggestions, which significantly improved the quality.

Declaration of Generative AI in Scholarly Writing
During the preparation of this work, the author used AI-assisted tools for language refinement and formatting purposes only.

Abbreviations
AI – Artificial Intelligence
ML – Machine Learning
DT – Digital Twins

Appendix A\B\C…, with appendix tile
None.

References

[1] Klaus Droder et al. Machine learning with robot control. Procedia CIRP, 76:187–192, 2018.
[2] A. Khan, M. J. Dahl, P. Falkman, and M. Fabian. Digital twin for legacy systems: Simulation model testing and validation. In 2018 IEEE International Conference on Automation Science and Engineering (CASE), 2018.
[3] S. Singh, M. Weeber, and K. P. Birke. Advancing digital twin implementation: a toolbox for modelling and simula-tion. Procedia CIRP, 99:567–572, Jan 2021.
[4] A. Ait-Alla, M. Kreutz, D. Rippel, M. Lutjen, and M. Freitag. Simulation-based analysis of the interaction of a physical and a digital twin in a cyber-physical production system. IFAC-Papers OnLine, 52(13):1331–1336, Jan 2019.
[5] E. Negri, L. Fumagalli, C. Cimino, and M. Macchi. Fmu-supported simulation for cps digital twin. Procedia Manufacturing, 28:201–206, Jan 2019.
[6] S. Kruger and M. Borsato. Developing knowledge on digital manufacturing to digital twin: a bibliometric and systemic analysis. Procedia Manufacturing, 38:1174–1180, Jan 2019.
[7] H. Latif and B. Starly. A simulation algorithm of a digital twin for manual assembly process. Procedia Manufacturing, 48:932–939, Jan 2020.
[8] K. Semenkov, V. Promyslov, and A. Poletykin. Verification of large scale control systems with hybrid digital models and digital twins. In 2020 IEEE International Conference on Automation Science and Engineering (CASE), 2020.
[9] M. Atalay and P. Angin. A digital twins approach to smart grid security testing and standardization. In 2020 3rd International Conference on Measurement, Instrumentation and Electronics (ICMIE), 2020.
[10] M. K. Traore. Unifying digital twin framework: Simulation-based proof-of-concept. IFAC-Papers on Line, 54(1):886–893, Jan 2021.
[11] M. F. Falah, S. Sukaridhoto, M. U. H. A. Rasyid, and H. Wicaksono. Design of virtual engineering and digital twin platform as implementation of cyber-physical systems. Procedia Manufacturing, 52:331–336, Jan 2020.
[12] B. A. Talkhestani, D. Braun, W. Schloegl, and M. Weyrich. Qualitative and quantitative evaluation of reconfiguring an automation system using digital twin. Procedia CIRP, 93:268–273, Jan 2020.
[13] Cristina Alcaraz and Javier Lopez. Digital twin: A comprehensive survey of security threats. IEEE Communications Surveys & Tutorials, 24(3):1475–1503, 2022.
[14] Peter Bauer, Bjorn Stevens, and Wilco Hazeleger. A digital twin of earth for the green transition. Nature Climate Change, 11(2):80–83, 2021.
[15] Hailin Feng, Dongliang Chen, and Haibin Lv. Sensible and secure iot communication for digital twins, cyber twins, web twins. Internet of Things and Cyber-Physical Systems, 1:34–44, 2021.
[16] Aidan Fuller, Zhong Fan, Charles Day, and Chris Barlow. Digital twin: Enabling technologies, challenges and open research. IEEE Access, 8:108952–108971, 2020.
[17] Mina Jafari, Abdollah Kavousi-Fard, Tao Chen, and Mazaher Karimi. A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future. IEEE Access, 11:17471–17484, 2023.
[18] Maninder Jeet Kaur, Ved P Mishra, and Piyush Maheshwari. The convergence of digital twin, iot, and machine learning: transforming data into action. In Digital twin technologies and smart cities, pages 3–17. Springer, 2020.
[19] Kostiantyn Maksymenko, Alexander Kenneth Clarke, Irene Mendez Guerra, Samuel Deslauriers-Gauthier, and Dario Farina. A myoelectric digital twin for fast and realistic modelling in deep learning. Nature Communica-tions, 14(1):1600, 2023.
[20] Hanqing Qiu, Huaiqing Zhang, Kexin Lei, Huacong Zhang, and Xingtao Hu. Forest digital twin: A new tool for forest management practices based on spatio-temporal data, 3d simulation engine, and intelligent interactive environment. Computers and Electronics in Agriculture, 215:108416, 2023.
[21] Csaba Ruzsa. Digital twin technology—external data resources in creating the model and classification of different digital twin types in manufacturing. Procedia Manufacturing, 54:209–215, 2021.
[22] Michael Jacoby and Thomas Uslander. Digital twin and internet of things—current standards landscape. Applied Sciences, 10(18):6519, 2020.
[23] A. A. Neto, E. R. Da Silva, F. Deschamps, and E. P. De Lima. Digital twins in manufacturing: An assessment of key features. Procedia CIRP, 97:178–183, Jan 2021.
[24] A. Chakraborti, A. Heininen, K. Koskinen, and V. S. Lamsa. Digital twin: Multi-dimensional model reduction method for performance optimization of the virtual entity. Procedia CIRP, 93:240–245, Jan 2020.
[25] C. Cimino, G. Ferretti, and A. Leva. The role of dynamics in digital twins and its problem-tailored representation.
[26] IFAC-Papers online, 53(2):10556–10561, Jan 2020.
[27] L. Overbeck et al. Continuous adaptation through real data analysis to turn simulation models into digital twins.
[28] Procedia CIRP, 104:98–103, Jan 2021.
[29] L. Morabito et al. A discrete event simulation based approach for digital twin implementation. IFAC-Papers OnLine, 54(1):414–419, Jan 2021.
[30] V. Kutscher, T. F. Martins, J. Olbort, and R. Anderl. Concept for interaction of hardware simulation and embedded software in a digital twin based test environment. Procedia CIRP, Jan 2021.
[31] L. Wang. Application and development prospect of digital twin technology in aerospace. IFAC-Papers OnLine, 53(5):732–737, Jan 2020.
[32] A. D. Rocha and J. Barata. Digital twin-based optimiser for self-organised collaborative cyber-physical production systems. Manufacturing Letters, 29:79–83, Aug 2021.
[33] B. Maschler, D. Braun, N. Jazdi, and M. Weyrich. Transfer learning as an enabler of the intelligent digital twin.
[34] Procedia CIRP, 100:127–132, Jan 2021.
[35] Z. Mueller-Zhang, P. O. Antonino, and T. Kuhn. Integrated planning and scheduling for customized production using digital twins and reinforcement learning. IFAC-Papers OnLine, 54(1):408–413, Jan 2021.

[36] B. Rohm and R. Anderl. Simulation data management in the digital twin (sdm-dt) – evolution of simulation data management along the product life cycle. Procedia CIRP, 105:847–850, Jan 2022.
[37] T. Y. Melesse, M. Bollo, V. Di Pasquale, F. Centro, and S. Riemma. Machine learning-based digital twin for monitoring fruit quality evolution. Procedia Computer Science, 200:13–20, Jan 2022.
[38] M. M. Muller, N. Jazdi, and M. Weyrich. Self-improving models for the intelligent digital twin: Towards closing the reality-to-simulation gap. IFAC-Papers OnLine, 55(2):126–131, Jan 2022.
[39] F. Xiang, P. Zhou, Y. Zuo, F. Tao, and D. Zhang. Manufacturing service network of digital twin systems under cloud computing environment. Procedia CIRP, 109:460–465, Jan 2022.
[40] G. Tissot, G. Alpan, F. Mangione, and F. Noel. A hybrid simulation/optimization architecture for developing a digital twin. In IFAC-Papers OnLine, volume 55, pages 532–537, 2022.
[41] S. Weckx et al. A cloud-based digital twin for monitoring of an adaptive clamping mechanism used for high performance composite machining. Procedia Computer Science, 200:227–236, Jan 2022.
[42] A. Chiurco, M. Elbasheer, F. Longo, L. Nicoletti, and V. Solina. Data modeling and ml practice for enabling intelligent digital twins in adaptive production planning and control. Procedia Computer Science, 217:1908–1917, Jan 2023.
[43] E. Badakhshan, P. Ball, and A. Badakhshan. Using digital twins for inventory and cash management in supply chains. IFAC-Papers OnLine, 55(10):1980–1985, Jan 2022.
[44] Z. Zhang, G. Yeming, and G. Zailin. Clearing function-based simulation optimization for release planning under digital twin wafer fabs. IFAC-Papers OnLine, 55(10):2539–2544, Jan 2022.
[45] L. Zhang, Y. Yan, Y. Hu, and W. Ren. Reinforcement learning and digital twin-based real-time scheduling method in intelligent manufacturing systems. IFAC-Papers OnLine, 55(10):359–364, Jan 2022.
[46] C. Vasanthan and D. Nguyen. Combining supervised learning and digital twin for autonomous path-planning. IFAC-Papers OnLine, 54(16):7–15, Jan 2021.
[47] S. Chabanet, B. El-Haouzi, and P. Thomas. Toward a self-adaptive digital twin based active learning method: an application to the lumber industry. IFAC-Papers OnLine, 55(2):378–383, Jan 2022.
[48] N. Kolibarov, D. Wastberg, V. Naserentin, D. Petrova-Antonova, S. Ilieva, and A. Logg. Roof segmentation towards digital twin generation in lod2+ using deep learning. IFAC-Papers OnLine, 55(11):173–178, Jan 2022.
[49] Omer San. The digital twin revolution. Nature Computational Science, 1(5):307–308, 2021.
[50] Concetta Semeraro, Mario Lezoche, Herve Panetto, and Michele Dassisti. Digital twin paradigm: A systematic literature review. Computers in Industry, 130:103469, 2021.
[51] Angira Sharma, Edward Kosasih, Jie Zhang, Alexandra Brintrup, and Anisoara Calinescu. Digital twins: State of the art theory and practice, challenges, and open research questions. Journal of Industrial Information Integration, 30:100383, 2022.
[52] Maulshree Singh, Evert Fuenmayor, Eoin P Hinchy, Yuansong Qiao, Niall Murray, and Declan Devine. Digital twin: Origin to future. Applied System Innovation, 4(2):36, 2021.
[53] Sabah Suhail, Mubashar Iqbal, Rasheed Hussain, and Raja Jurdak. Enigma: An explainable digital twin security solution for cyber–physical systems. Computers in Industry, 151:103961, 2023.
[54] Xuemin Sun, Jinsong Bao, Jie Li, Yiming Zhang, Shimin Liu, and Bin Zhou. A digital twin-driven approach for the assembly-commissioning of high precision products. Robotics and Computer-Integrated Manufacturing, 61:101839, 2020.
[55] Thomas H-J Uhlemann, Christoph Schock, Christian Lehmann, Stefan Freiberger, and Rolf Steinhilper. The digital twin: Demonstrating the potential of real-time data acquisition in production systems. Procedia Manufacturing, 9:113–120, 2017.
[56] Xiaochen Zheng, Jinzhi Lu, and Dimitris Kiritsis. The emergence of cognitive digital twin: Vision, challenges and opportunities. International Journal of Production Research, 60(24):7610–7632, 2022.
[57] Cunbo Zhuang, Jingcheng Gong, and Jianhua Liu. Digital twin-based assembly data management and process traceability for complex products. Journal of Manufacturing Systems, 58:118–131, 2021.
[58] Z. Tian, L. Cui, J. Liang, and S. Yu. A comprehensive survey on poisoning attacks and countermeasures in machine learning. ACM Computing Surveys, 55(8):1–35, 2023.
[59] J. Ploennigs, K. Semertzidis, F. Lorenzi, and N. Mihindukulasooriya. Scaling knowledge graphs for automating ai of digital twins. In Springer eBooks, pages 810–826. 2022.
[60] Z. Lv and S. Xie. Artificial intelligence in the digital twins: State of the art, challenges, and future research topics.
[61] Digital Twin, 1:12, Nov 2022.
[62] M. Segovia and J. Garcia-Alfaro. Design, modeling and implementation of digital twins. Sensors, 22(14):5396, Jul 2022.
[63] Dong Zhong, Zhelei Xia, Yian Zhu, and Junhua Duan. Overview of predictive maintenance based on digital twin technology. Heliyon, 2023.
[64] L. Gopal, H. Singh, P. Mounica, N. Mohankumar, N. P. Challa, and P. Jayaraman. Digital twin and iot technology for secure manufacturing systems. Measurement: Sensors, 25:100661, Feb 2023.
[65] Suhail S., Jurdak R., and Hussain R. Security attacks and solutions for digital twins. arXiv preprint, 2202.12501, 2022.
[66] C. Steinmetz et al. Digital twins modeling and simulation with node-red and carla. IFAC-Papers OnLine,55(19):97–102, Jan 2022.

Authors' Profiles



Raghavendra Babu T. M. is currently an Assistant Professor in the Department of Computer Science and Engineering at PES College of Engineering, Mandya, Karnataka, India. He is pursuing a Ph.D. at Presidency University, Bengaluru. He has published more than 10 papers in peer-reviewed journals and conferences.



Harish Kumar K. S. is currently serving as an Assistant Professor (Senior Scale) at the School of Computer Science and Engineering, Presidency University, with over eight years of teaching experience at both undergraduate and postgraduate levels. He holds a Ph.D. in Data Science, and his research interests include Artificial Intelligence, Machine Learning, and Deep Learning. He has authored more than 20 research papers published in reputed peer-reviewed journals and conferences indexed by Elsevier, IEEE, Springer, and Scopus. His research contributions focus on the application of AI to real-world problems such as air quality prediction and plant disease detection. His work has received over 317 citations on Google Scholar (H-index: 4) and 218 citations on Scopus (H-index: 3). He is currently guiding five research scholars, with one scholar already awarded the Ph.D. He has also contributed as an editor and author, with a book chapter and an edited volume on emerging trends in Artificial Intelligence.

How to cite this paper

Raghavendra Babu T M, Harish Kumar K S, "Review on Intelligent Security Models for Digital Twins", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.3, pp. 290-304, 2026. DOI:10.5815/ijwmt.2026.03.19