Digital Twins

Yacine Ayachi, Frédéric Kesselring, Idir Hadjari and Enzo Causse

January 10, 2024

Abstract

Advancement of digital twins in research

1 Introduction

In an era where the internet of things (IoT) is used more and more in multiple sectors like healthcare and industries, it has become very important to secure its functioning. Digital twins are an innovative perspective that will revolutionize the security in IoT.

1.1 Definition

They act like a virtual replica of a physical system and are a great ally for risk management and security improvement.

This technology was introduced over a decade ago, but it is more recently that its definition which could cover the different application domains was precised: the debate continued about considering the digital twins as the final product, or as the entire product's life cycle; nowadays, the agreement states them as both. [SKZ+22]

In fact, they are linked to real data sources from the environment, which means that the twin updates in real time to reflect the original version.

There are a few different types of digital twins:

- First, there's a **product** twin, which is a representation of a product at various stages of its life cycle. As an example, Google Maps is a digital twin of the Earth's surface: it links real-time data on traffic to help optimize your commute.
- Other types of twins include **production plant** twins, which represent an entire manufacturing facility, or procurement and supply chain twins, also called network twins.
- Additionally, twins can represent **physical infrastructure** such as a highway, a building, or even a stadium. [BH22]

1.2 Functioning

For a substantial use, it's possible to advance a twin from simply representing assets, people, or processes to providing simulations through the use of AI and advanced modeling techniques. [ACC+22] However, digital twins still differ from those simulations and agent-based modeling in the fact that they are updated in real-time. [SKZ+22]

1.3 Application Sectors

Digital twins can help a lot in modeling buildings, bridges or ships, and in simulating tests for them. For instance, a digital twin of sailing environments, boats, and crew members enables Emirates Team New Zealand to test boat designs without actually building them. This has allowed the champion sailing team to evaluate thousands, rather than just hundreds, of hydrofoil designs. [ACC+22]

1.3.1 The Application of Digital Twins in Incident Response for Cyber-Physical Systems (CPSs)

The following outlines the application of Digital Twins (DTs) to enhance incident response for Cyber-Physical Systems (CPSs). The primary focus is on integrating DTs into different phases of the Incident Response (IR) life cycle for critical infrastructures. The proposed framework categorizes DTs into three modes of operation: Data Analysis and Optimization, Simulation, and Replication.

Preparation and Identification

- Data-driven DTs can be utilized for analyzing system inter dependencies and providing real-time anomaly detection.

Containment, Eradication, and Recovery

- Simulation-based DTs serve as a tool for side-by-side comparison with the real-world system and projecting its future states. They can be used for testing interventions in a safe environment.
- Replication-based DTs provide a baseline for comparing the real-world system, allowing testing interventions in a safe environment, including digital forensics.

Management and Oversight

Management and oversight involve:

- Documentation using DT platforms to automatically update playbooks, incident reports, and other documents with information gained from the DT.

Digital Forensics and Incident Response (DFIR) Assistance

DFIR assistance includes:

- Status Query: DTs can be queried to provide real-time status updates of the system during incident response activities.
- Associative Query: Utilizing the associative capabilities of DTs, investigators can explore associations and relationships between different components of the system.
- Interventional Query: DTs support testing interventions in a safe digital environment, allowing for proactive measures during incident response.
- Counterfactual Query: Investigating alternate scenarios and exploring what-if situations to understand the potential consequences of different actions.

Communication

DTs facilitate communication by providing a common platform for sharing real-time information among multi-disciplinary teams involved in incident response. In conclusion, the integration of DTs in incident response for CPSs offers a holistic approach, addressing the challenges posed by the digitization of critical infrastructures. The proposed framework provides a structured and comprehensive analysis of DT applications across various phases of the IR life cycle, enhancing the effectiveness and resilience of incident response teams.

1.4 Benefits

One of the areas where digital twins can bring the most value is the reduction in time to market. [BCC+22] Digital twins can allow for rapid iterations and optimizations of product designs, far faster than physically testing every single prototype, just like Solidworks software help in industry's conception [Bor22]: by simulating the product throughout the manufacturing process, it's possible to identify flaws in the design much earlier. [BCC+22]

These digital twins can even help organizations reduce the material used in a product's design, as well as improve the traceability of a product to reduce environmental waste. [BH22, SKZ+22]

2 Relation to cybersecurity

2.1 Prevent cyberattacks

The digital twins need many components to be completely functional, especially ones coming from various computer science's domains.
Such instances of those are mainly:

- IoT
- Big data
- machine learning
- real-time synchronization
- automation algorithms
- security systems

As lots of data are likely to transit between those different components, not only before but also during use, it is a necessity to protect them from cyberattacks. [SKZ+22]

2.1.1 Physical detection

Breaches can be incredibly subtle and thus difficult to detect or differentiate from other, sometimes more routine, system anomalies; to implement this, operational data describing what is occurring within machines could support cyberattack detection (sensor data, error signals, digital commands being issued or executed, for example). [ABR21]

However, directly accessing that kind of data in near real-time from operational technology devices could put the performance and safety of the process on the factory floor at risk, which is precisely what we do want to avoid as much as possible. [SKZ+22, BFP+18] So, when it's not possible to inspect a physical machine while it's in operation, its digital twin is the next best thing.

Because manufacturing processes produce such rich data sets (temperature, voltage, current...), and they are so repetitive, there are opportunities to detect anomalies that stick out, including cyberattacks. [SKZ+22, ABR21]

2.1.2 Software processing

Secondly, even with the wealth of information at hand, how do the computer programs distinguish a cyber threat from something more routine?

In fact, it is possible to employ pattern-recognizing machine learning models trained on normal operating data. Doing that, the models can be adept at recognizing what the real product looks like under normal conditions, also meaning they can tell when things are out of the ordinary. [ABR21, BFP+18]

If these models detect an irregularity, they pass the baton off to other computer models that check whether the strange signals are consistent with anything in a library of known issues, such as a computer's CPU overheating or its memory overload slowing the operating system for example. Then the twin's system categorizes the irregularity as an expected anomaly or a potential cyber threat.

Of course, in the last step, a human expert is meant to interpret the system's finding and then make a decision. [BFP+18]

2.1.3 Machine learning

The framework can also provide tools to systematically formalize the subject matter expert's knowledge on anomaly detection; if the framework hasn't seen a certain anomaly before, a subject matter expert can analyze the collected data to provide further insights to be integrated into and improve the system. [SKZ+22]

Generally speaking, the expert would either confirm the cybersecurity system's suspicions or teach it a new anomaly to store in the database. And then as time goes on, the models in the system would theoretically learn more and more, and the human expert would need to teach them less and less. [ABR21]

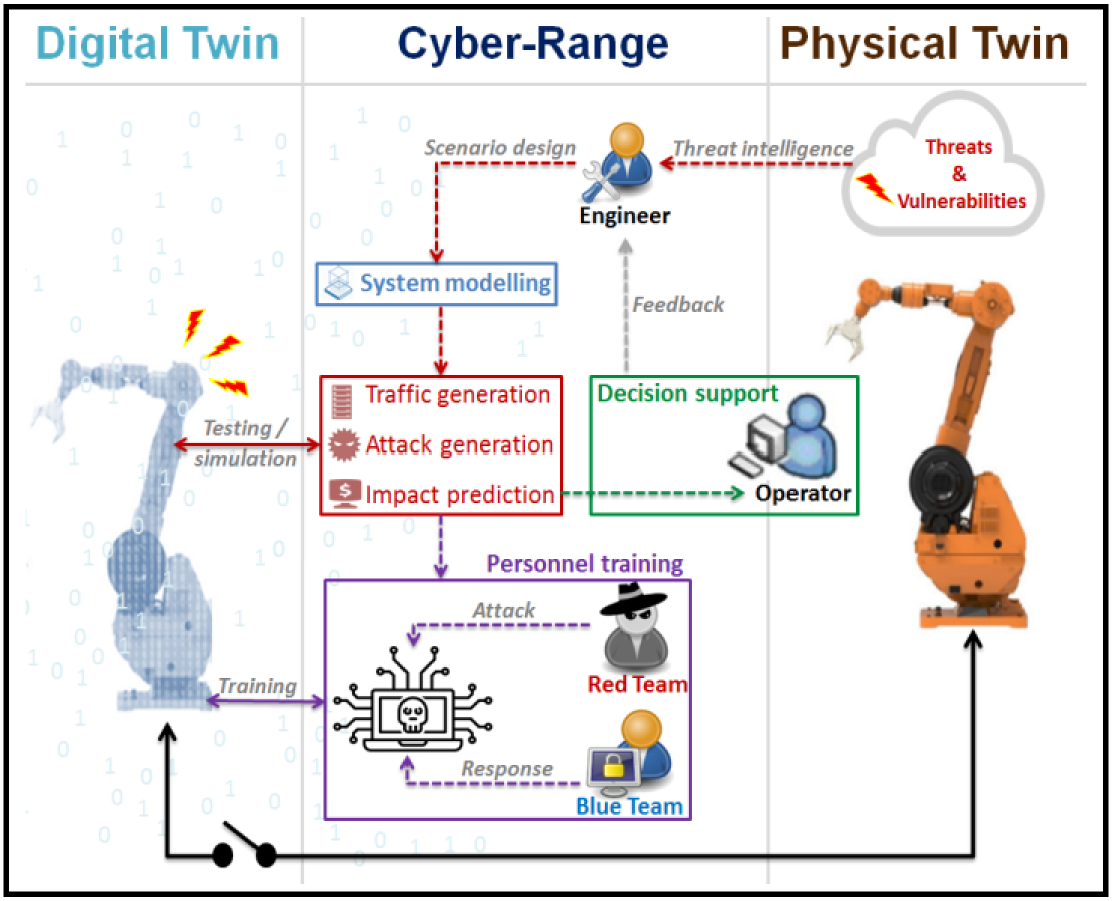

Figure 1: **Cyberattack detection schema.** [BFP+18]

2.2 Usage in cybersecurity

2.2.1 Real-Time Monitoring and Analysis:

Digital twins excel in real-time monitoring and analysis by continuously mirroring the behavior of their physical counterparts. Leveraging advanced sensors, they collect data on network traffic, system performance, and user activities. This real-time monitoring is crucial for the prompt detection of anomalies and potential security threats. Machine learning algorithms and advanced analytics are often employed to analyze the vast amount of data generated.

2.2.2 Vulnerability Assessment:

The capability of digital twins to simulate various attack scenarios is a key aspect of vulnerability assessment. By emulating potential cyber threats, digital twins help organizations identify vulnerabilities within their digital infrastructure. This proactive approach allows for the timely application of patches and security updates, mitigating the risk of exploitation by malicious actors.

2.2.3 Incident Response Simulation:

Digital twins provide a controlled environment for realistic incident response simulations. This involves creating scenarios mimicking different types of cyber threats, enabling cybersecurity teams to practice and refine their response strategies.

2.2.4 Dynamic Risk Management:

Dynamic risk management is a crucial function enabled by digital twins in cybersecurity. By continuously collecting and analyzing data, digital twins allow organizations to dynamically assess and adapt their risk management strategies. This adaptive approach ensures that cybersecurity measures evolve in response to emerging threats.

2.2.5 Behavioral Analytics and Anomaly Detection:

Digital twins leverage behavioral analytics to establish baseline patterns of normal behavior within the digital infrastructure. Any deviation from these established patterns is flagged as an anomaly, signaling potential security threats.

2.2.6 Automated Threat Response:

Integrating digital twins with automated threat response mechanisms enhances cybersecurity capabilities. By pre-defining response actions based on identified threats, digital twins can autonomously mitigate certain types of attacks. This aspect of automated threat response is crucial in minimizing response time and limiting the impact of cyber incidents.

2.2.7 Predictive Analysis:

Digital twins, with their historical data and continuous monitoring, enable predictive analysis in cybersecurity. By analyzing trends and patterns, digital twins can anticipate potential security issues, allowing organizations to take preventive measures. This predictive analysis contributes to a more proactive cybersecurity posture.

2.2.8 Regulatory Compliance Monitoring:

Digital twins aid in ensuring regulatory compliance by continuously monitoring and documenting security-related activities. This is particularly crucial in industries where compliance with data protection and privacy regulations is mandatory.

3 Digital Twins and the Internet of Things (IoT)

The convergence of digital twins and the Internet of Things (IoT) represents a paradigm shift in the way we perceive and interact with the physical world. Digital twins, virtual replicas of physical entities or systems, find a natural synergy with the vast network of interconnected devices that form the IoT ecosystem. [SAB+21]

3.1 The Rise of the Internet of Things

The Internet of Things refers to the network of interconnected devices that communicate and share data, enabling a seamless flow of information and automation. IoT devices, ranging from sensors and actuators to smart appliances, collect and transmit data to centralized systems for analysis and decision-making.

3.2 Synergies between Digital Twins and IoT

The link between digital twins and the IoT lies in their complementary capabilities. IoT devices generate vast amounts of data, providing real-time insights into the physical world. Digital twins, on the other hand, utilize this data to create virtual representations that can be analyzed, simulated, and optimized. [QTH+21, CBGS21]

3.2.1 Enhanced Monitoring and Control

By integrating digital twins with IoT devices, organizations gain enhanced monitoring and control over physical assets. Real-time data from sensors can be used to update digital twins, ensuring that the virtual representation accurately reflects the current state of the physical entity. This synchronization facilitates better decision-making and responsiveness.

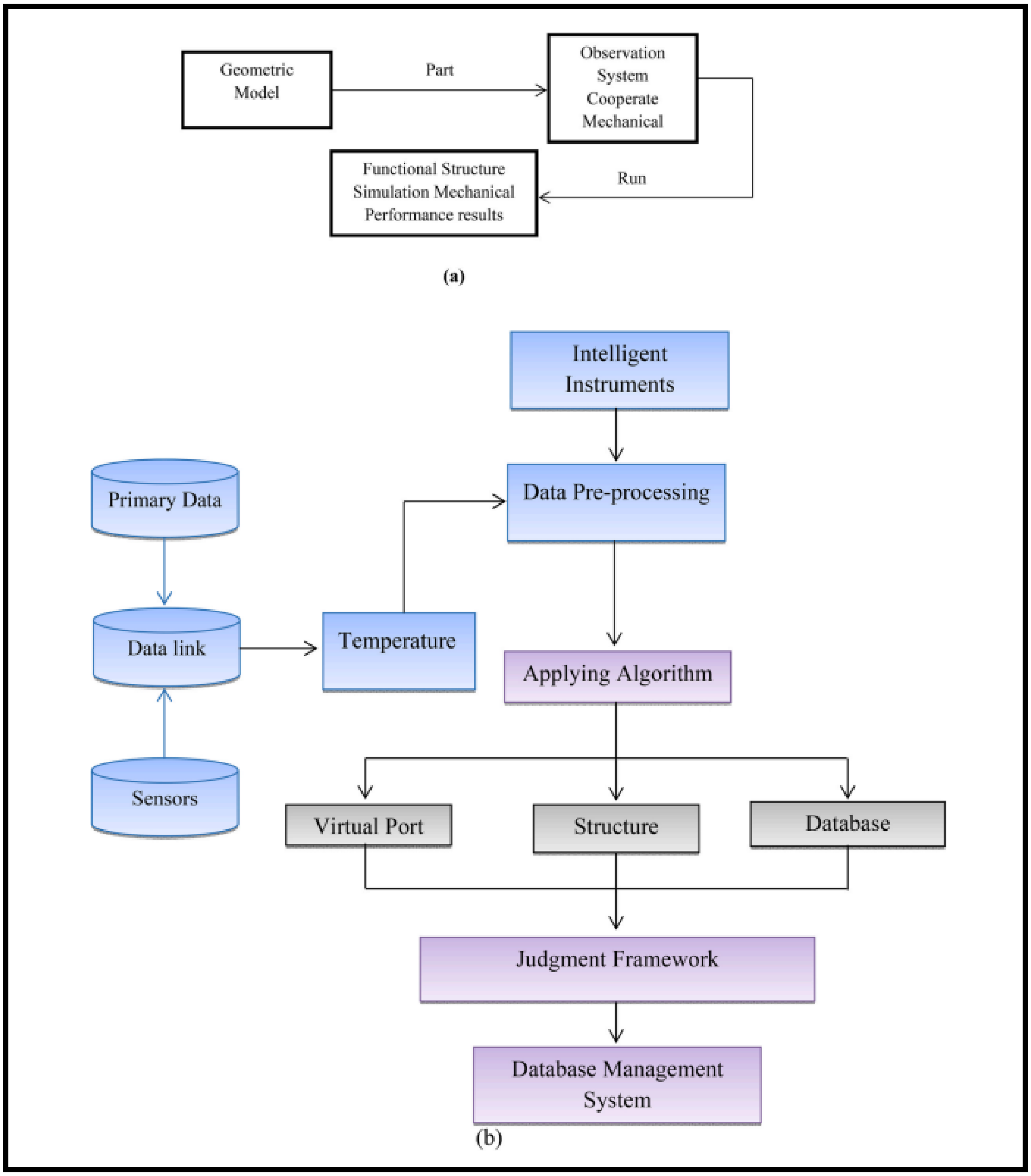

Figure 2: **Machines construction structure (a) Basic structure (b) Smart DT structure**

3.2.2 Predictive Analytics and Maintenance

Digital twins, fueled by data from IoT sensors, enable predictive analytics and maintenance strategies. Organizations can anticipate potential issues, optimize performance, and schedule maintenance activities based on real-time conditions. This proactive approach minimizes downtime and extends the lifespan of physical assets. [SAB+22]

3.2.3 Optimization of Processes and Systems

The combination of digital twins and IoT allows for the optimization of processes and systems. Data-driven insights from IoT devices inform the continuous refinement of digital twin models, leading to improved efficiency, resource utilization, and overall performance. [WKC22]

3.2.4 Challenges and Future Directions

While the integration of digital twins and IoT offers promising advantages, it also poses challenges related to data security, interoperability, and standardization. Future research will likely focus on addressing these challenges and further exploring the potential of this synergistic relationship.

4 Conclusion

This research has provided a comprehensive overview of digital twins, exploring their definition, application sectors, functioning, benefits, their crucial role in cybersecurity and their intersection with the Internet of Things.

Digital twins, defined as virtual representations of physical entities or systems, have found applications in diverse sectors, including manufacturing, healthcare, smart cities, and more. Their ability to mirror real-world entities and processes facilitates improved decision-making, optimization, and innovation across various industries.

The functioning of digital twins involves the continuous exchange of data between the physical entity and its digital counterpart. This dynamic synchronization allows for real-time monitoring, analysis, and simulation, contributing to enhanced operational efficiency and performance.

The benefits of digital twins are multifold, ranging from predictive maintenance and reduced downtime to improved product development and innovation. The ability to simulate various scenarios and analyze data in real-time empowers organizations to make informed decisions and respond proactively to emerging challenges.

Moreover, the integration of IoT with digital twins strengthens the ability to simulate and analyze diverse scenarios, providing a more holistic understanding of the physical entities being replicated. This expanded capability is invaluable in sectors like smart cities, where the interconnectedness of various systems, such as transportation, energy, and infrastructure, can be accurately mirrored and analyzed for improved decision-making and operational efficiency.

Of particular significance is the intersection of digital twins with cybersecurity. The proactive nature of digital twins makes them valuable tools in identifying vulnerabilities within digital infrastructure. By emulating potential cyber threats, organizations can conduct thorough vulnerability assessments, enabling timely application of patches and security updates. This approach significantly mitigates the risk of exploitation by malicious actors and strengthens overall cybersecurity postures.

In conclusion, the research underscores the transformative potential of digital twins and emphasizes the critical need for organizations to embrace these technologies in their pursuit of enhanced efficiency, innovation, and, most importantly, robust cybersecurity practices.

References

[ABR21] Kaznah Alshammari, Thomas Beach, and Yacine Rezgui. Cybersecurity for digital twins in the built environment: current research and future directions. *Journal of Information Technology in Construction*, 26:159–173, 2021. Link.

[ACC+22] Joshan Abraham, Guilherme Cruz, Sebastian Cubela, Tomás Lajous, Kayvaun Rowshankish, Sanchit Tiwari, and Rodney Zemmel. Digital twins: The foundation of the enterprise metaverse. 2022. Link.

[BCC+22] Mickael Brossard, Sebastien Chaigne, Jacomo Corbo, Bernhard Mühlreiter, and Jan Paul Stein. Digital twins: The art of the possible in product development and beyond. 2022. Link.

[BFP+18] Adrien Bécue, Yannick Fourastier, Isabel Praça, Alexandre Savarit, Claude Baron, Baptiste Gradussofs, Etienne Pouille, and Carsten Thomas. Cyberfactory1 - securing the industry 4.0 with cyber-ranges and digital twins. 2018. Link.

[BH22] Kimberly Borden and Anna Herlt. Digital twins: What could they do for your business? 2022. Link.

[Bor22] Kimberly Borden. Digital twins: Flying high, flexing fast. 2022. Link.

[CBGS21] G. Cathey, J. Benson, M. Gupta, and R. Sandhu. Edge-centric secure data sharing with digital twins in smart ecosystems. In *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, page 70–79. IEEE, December 2021. link.

[QTH+21] Q. Qi, F. Tao, T. Hu, N. Anwer, A. Liu, Y. Wei, and A.Y.C. Nee. Enabling technologies and tools for the digital twin. *Journal of Manufacturing Systems*, 58:3–21, 2021. link.

[SAB+21] R. Sahal, S.H. Alsamhi, K.N. Brown, D. O'Shea, C. McCarthy, and M. Guizani. Blockchain-empowered digital twins collaboration: Smart transportation use case. *Machines*, 9(9):193, 2021. link.

[SAB+22] R. Sahal, S.H. Alsamhi, K.N. Brown, D. O'Shea, and B. Alouffi. Blockchain-based digital twins collaboration for smart pandemic alerting: Decentralized covid-19 pandemic alerting use case. *Computational Intelligence and Neuroscience*, 2022, 2022. link.

[SKZ+22] 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. Link.

[WKC22] Y. Wang, X. Kang, and Z. Chen. A survey of digital twin techniques in smart manufacturing and management of energy applications. *Green Energy and Intelligent Transportation*, 2022. link.