Digital Twin for Cybersecurity: Towards Enhancing Cyber Resilience

Rajiv Faleiro, Lei Pan(✉), Shiva Raj Pokhrel, and Robin Doss

School of IT, Deakin University, Geelong, VIC 3220, Australia
{rfaleiro,l.pan,shiva.pokhrel,robin.doss}@deakin.edu.au

Abstract. Digital Twin (DT) impacts significantly to both industries and research. It has emerged as a promising technology enabling us to add value to our lives and society. DT enables us to virtualize any physical systems and observe real-time dynamics of their status, processes, and functions by using the data obtained from the physical counterpart. This paper attempts to explore a new direction to enhance cyber resilience in the perspective of cybersecurity and Digital Twins. We enumerate definitions of the Digital Twin concept to introduce readers to this disruptive concept. We then explore the existing literature to develop a holistic analysis of the DT's integration into cybersecurity. Our research questions develop a novel roadmap for a promising direction of research, which is worth exploring in the future and is validated by an extensive and systematic survey of recent works. Our research has aimed to properly illustrate the current research state in this area and can benefit both community and industry to further the integration of Digital Twins into Cybersecurity.

Keywords: Digital Twin · Cybersecurity · Cyber resilience

1 Introduction

Every company is now concerned about cybersecurity and the resilience of their infrastructure, and we anticipate that new technology like digital twin may contribute significantly to a robust online defense. Therefore, we envision creating a virtual framework of our information technology (IT) network to identify security flaws, create attack scenarios, avoid expensive attacks, and improve resilience before our security infrastructure is deployed into the real network system.

We start with the basic idea and concept of Digital Twin. First, what is a Digital Twin (DT)? In general, "*Digital Twin*" [25] refers to developing a highly complex computer image that is the replica (or twin) of a physical object. For example, a physical object can be an automobile, a house, a bridge, or a jet engine. DT's underlying idea employs the virtual computer image model to project the sensor data gathered from the connected physical objects.

Different industry verticals define DT in a slightly different fashion. IBM defines DT as[1] "*a virtual representation of an object or system that spans its life*

[1] https://ibm.co/3vCiwl5.

W. Xiang et al. (Eds.): BROADNETS 2021, LNICST 413, pp. 57–76, 2022.
https://doi.org/10.1007/978-3-030-93479-8_4

cycle, is updated from real-time data, and uses simulation, machine learning, and reasoning to help decision-making." Gartner[2] defines DT as "*a software design pattern that represents a physical object with the objective of understanding the asset's state, responding to changes, improving business operations and adding value.*" Furthermore, Gartner says that 13% of industry verticals undertaking Internet of Things (IoT) projects are using DTs in 2021, and 62% are in the process of doing so or intend to do so soon. Our study indicates that DTs can best complement Cyber Security as an Intrusion Detection System due to the bi-directional flow of real-time data. We have elaborated more on this in Sect. 2, according to the chart provided below:

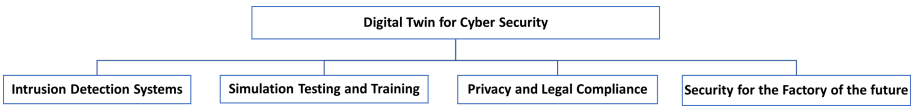

Fig. 1. Digital Twin for cybersecurity use cases

With the increasing application of DT in manufacturing and industry 4.0 [25], organizations have realized that developing a digital replica of their resources, processes, and, most importantly, cybersecurity systems is always advantageous. The cases of cyber attacks increased at an unprecedented pace during the epidemic, prompting some to call it a *cyber pandemic*. As soon as more businesses migrate their digital assets to the web and their IT network becomes increasingly prevalent, cyber criminals are becoming more interested in exploiting unprotected nodes, systems, and repositories. Being a relatively new topic, DTs' importance to enhance cybersecurity has been poorly understood. By using simulated attacks over the DT, companies can identify security gaps that are currently neglected [25].

Considering one of the critical infrastructure sectors such as power homes, schools, critical infrastructures, healthcare, energy sectors, and their data from physical assets' sensors and/or cyber assets' controllers used to efficiently operate them in a low-risk domain [51,60]. Distributed control systems are highly vulnerable to cyber threats. The need to protect them has risen due to ongoing malicious damages. In such systems, data encryption, certificate authentication, and control system resiliency can be used to improve the resilience. However, extensive research has been lacking to monitor, manage, and mitigate the multiple coordinated attacks on such distributed systems [55]. A conceptual framework proposed in [55] hints at the potential of DTs for improving the level of cyber resilience.

This paper's primary objective is to explore and exploit the current state of DT research for cybersecurity to investigate whether resilience has been completely covered. To start with, we use the Scopus database and search for the

[2] https://gtnr.it/337j7Py.

term "Digital Twin", which hits over 1,500 papers in 2020. Next, we search for the two terms "cybersecurity" and "Digital Twin," which found only 13 papers of 2020. These statistics demonstrate that DTs are explored for several applications in different industry verticals, but not enough has been investigated regarding cybersecurity. This observation provides us the confidence to analyze the following two research questions: i) *How DT contributes to cybersecurity and Resilience?*, ii) *What is the state of cybersecurity in DT?*

2 Digital Twin for Cybersecurity

Our first main research question is: "**How does DT currently contribute to cybersecurity?**"

We witnessed several notorious cyber attacks over the past decade targeting ICS. In 2010, the Stuxnet computer worm successfully compromised an Iranian nuclear plant. The Ukrainian power grid was compromised by the black energy malware attack. Recent cyber-attacks on U.S. natural gas pipelines took place in 2020 [37]. The introduction of DTs as digital counterparts of physical assets could prevent a repeat of the above attacks by continuously monitoring the DTs to improve the detection of malicious threats and actors. In 2017, the use of DTs was proposed in [66] to enhance cybersecurity. More papers have been published on DTs since 2017. As of early 2021, 21 publications related to the topic were found.

Intrusion Detection Systems. The intrusion detection system (IDS) is commonly used to protect a network from malicious external attacks [36]. The use of an IDS improves the reliability and resilience of a system by detecting and reacting to behaviors that might endanger the system [73]. An IDS system has two varieties: 1) Anomaly or profile-based detection uses heuristics and behavior-based patterns to identify the activities that deviate from the normal usage. 2) In contrast, signature-based detection identifies threats in a system by matching known attack scenarios and subsequently raises an alert [4,36]. Intrusion detection systems are leveraging artificial intelligence to pinpoint system deviations and detect anomalies within a system's normal functioning from the collected data.

DTs enable us to mirror the internal environment and behavior of physical systems through creating exact virtual replicas [23]. DT's property allows us to implant an intrusion detection algorithm within the DT and test this virtual counterpart instead of the physical system without interrupting the live environment [3]. The latter can be considered a separate enhancement to cybersecurity. The DT can collect data from the physical twin and compare any deviations from the expected values, which can help determine failures within the system [35].

Rubio *et al.* [54] advocated to use DTs to provide IDS services in the context of Industry 4.0. Eckhart *et al.* [21] demonstrated how to implement a knowledge-based IDS using a DT together with knowledge-based rules, as shown in Fig. 2.

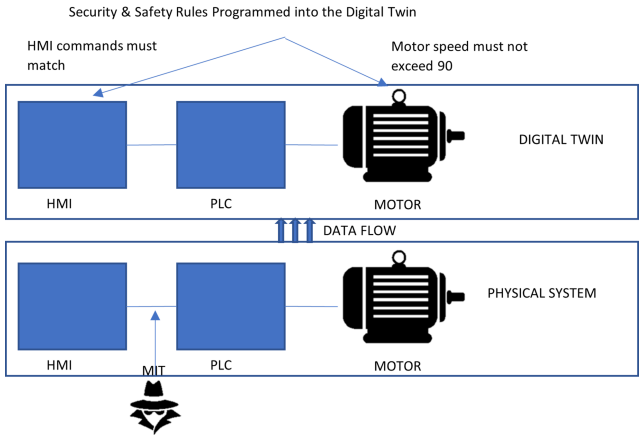

Fig. 2. Rule-based IDS for a DT

These rules were specified using AML and encompassed safety and security rules that the DT must follow. The safety rule ensured that the maximum velocity of the motor controlled by a PLC stayed within a specified threshold; and the security rule checked for consistency between the human-machine interface that sets the motor's velocity and the PLC that controls the motor velocity. These two rules were checked continuously for any violations. This experiment was more concentrated on simulating the system rather than incorporating real-time data into the DT. The operator will be alerted for any MITM attack that injects malicious commands, if it deviates from the defined rules.

A passive state replication approach was proposed in [20], where the DT virtually mirrored the behavior of the physical asset during its operation. It helped realize the intrusion detection use case. Here, the IDS was a behavior specification-based IDS that relied on the system's normal functioning to be predefined, which always yields a low false-negative rate and detects unknown attacks when the predefined system behavior was set. It was assumed that the system's correct behavior has already been created during the engineering phase. This method allows for identifying an intrusion by comparing the inputs and outputs of the physical asset to their counterparts of the DT. However, this approach can only copy a limited amount of data of the physical twin, resulting in a gap between the state of the physical twin and the DT. An improved architecture was proposed to allow a DT to constantly mirror the physical twin's behavior. This architecture is further equipped with a novel intrusion detection algorithm that can detect attacks on the ICS promptly in [3] and proposes a method to diagnose the detected attack type via classification using a Kalman filter.

Saad *et al.* [55] have introduced an IoT-based DT for cyber-physical networked microgrids to increase their cyber resiliency on physical sensors and control agents. A cloud-based platform was proposed in [49] to provide a central view for a networked microgrid system. This DT generates a digital replica for

the interactions between the physical and cyber layers. The proposed DT framework by the authors detects false data injection (FDIA) and denial of service (DoS) attacks on the control system in case of a single or a coordinated attack and allows for corrective action to be taken by the user.

Dietz *et al.* [19] propose and demonstrate how a DT can be integrated into a Security Operation Centre (SOC) and Security Incident and Event Management (SIEM) to enhance cybersecurity. The SOC is responsible for providing a visualization of the procedures, technologies, and people within an enterprise [56] by integrating all security-relevant systems and events in a single point. Its main task is to identify and handle alerts while taking corrective actions to protect the organization's assets and data. A SIEM collects data like logs and network flows from different heterogeneous sources and collates them into a single view [68] and apply transfer learning with multipath communication [47] for accelerating the performance of DT along with the SIEM system.

SOCs face an increase in responsibility with the integration of industrial systems with corporate security. The current security strategies cannot keep pace with the growing attack surface of convergence of IT infrastructure and industrial systems that use sensors connected to enterprise networks [19]. Dietz *et al.* [19] have developed a process-based security framework to support SOCs using DT security and create a proof of concept. Using a Man-in-the-Middle attack simulation, they demonstrate how this integration can generate system logs provided to SIEM systems to build rules and take corrective action against attacks. Enterprises use a SOC supported by a SIEM to leverage capabilities ranging from security analysis to enforce rules and detect patterns to manage security-relevant data.

Authors in [17] apply simulations of security incidents in the DT and pass on the collected information to the SOC and a test SIEM system. The test SIEM is used to avoid negatively affecting the production environment during the simulation. SIEM security monitoring rules are created in advance by the experts who are assumed to be present in the SOC. The experts decide on the simulation parameters (e.g., a man-in-the-middle attack) within the DT, and the simulations settings. The output is the incident information artifact used within the test SIEM to verify whether it detects the security incident. Once this is verified, the logic/patterns identified can be passed onto the real SIEM and added into its monitoring rules to prevent similar real-world attacks in the future. Hence, DT focuses more on a particular asset than the attack itself [17]; see the identification of patterns—signature-based, behavior-based, specification-based, or hybrid [32], and a realistic attack demonstrated in [19] using ARP spoofing.

Simulation, Testing and Training. The authors in [17,20,21] propose various DT applications to enhance security in terms of historical data analysis and emulated environments to simulate attack testing. Testbeds help provide the security assessment of planned infrastructure, and cyber ranges help develop IT systems or infrastructures in a virtual environment for vulnerability assessment. Both testbeds and cyber rangers can serve as a training environment to improve the security, stability, and performance of the targeted infrastructure [44]. While

testbeds are used to avoid damage or interruptions to the physical systems, this exercise can be costly and time-consuming to accurately represent the CPS in operation [9,21].

More importantly, another interest in using the DT with the above technologies is that it covers the entire life cycle of its physical twin. It begins with the planning and design phase to gather data as early as possible, even before the physical component exists. The inclusion of a DT enables the secure-by-design paradigm where the DT simulates the functioning of its physical counterpart and identifies security-related vulnerabilities before the physical asset is manufactured and begins to operate [59]. DT can incorporate security testing from the design phase onwards to fix any early identified vulnerabilities and continue into the following stages of the product life cycle to enable the secure by design paradigm to be a part of the CPS [22].

All CPS and IoT devices need to be tested to capture their effects on the underlying DT architecture. A complete rigorous testing should involve hundreds and maybe thousands of devices being a part of the test simulation. It is expensive in terms of the IoT test and evaluation costing and management but is a crucial aspect to study their large-scale effects [41]. In [40], the authors discussed how DTs can be used to replicate the behavior of IoT devices by multiplying them in a simulation environment to study large-scale effects of the IoT devices. A cyber-attack is modeled on a cluster of smart devices (smart thermostats) and examines their effects on a simulated environment.

Mittal *et al.* [40] conducted experiments on a NEST thermostat embedded in a local environment. This environment consists of multiple input sources such as the house environment, its occupancy, weather, and remote operations via a mobile application. The remote operations in this scenario open the possibilities of the thermostat being hacked. By observing how an attack influences the connected smart system, the DT owner incorporates simulations to enhance the infrastructure security during its deployment in the physical environment.

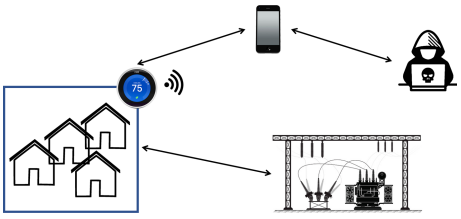

Fig. 3. An example of exploiting of SMART thermostat

As shown in Fig. 3, a SMART nest thermostat is connected to multiple households and can also be accessed via a mobile app, which opens the possibility of a hacker gaining access credentials and causing malicious damage. While a single app being hacked could cause a minor energy spike in the connected power grid,

a hack involving multiple households' thermostats to be simultaneously switched on can be disastrous.

The DT generated from specification can simulate plant operation and generate the network traffic flows. This activity can allow an analyst to discover unused and unnecessary services within the system, thereby minimizing the attack surface of the plant [21]. This simulation can be complemented with logic and network features that allow security testing in a layer-wise fashion, which could indicate how an attacker can pivot through different system components and help realize a defense in depth strategy [21].

DT can be geared towards hardware and software misconfiguration. Since the DT is a replica of its physical twin, the DT should mimic the functionality of the physical asset (e.g., in terms of its communications interface, I/O modules in the hardware layer, and execution of control logic in the case of a PLC). We can expect to observe common features between both twins. Any deviation from the configurations in the hardware or software layer implies malicious activity. This use case is similar to implementing a behavior-specification-based IDS from DTs, which checks for differences in the functioning of the physical twin from the DT. Software manipulations can be detected by comparing configuration data between the twins [21]. In this case, the twin would need to be set up in an isolated environment to ensure that a malicious actor cannot make changes to the twin and mask their exploit if they could access the DT in the worst case.

To minimize the managing cost of a DT that mirrors its physical counterpart at all times, an economical method is proposed in [9]. A cost-effective DT within a budget only accounts for specific security tests that fit within the specified budget. Alternatively, DTs are integrated into a cyber range to test defense tactics and train users on cyber incident responses before the product's release into the production environments [7]. In this case, attacks could be launched against the DT from the cyber range itself. The cyber range can serve a range of use cases aside from training cybersecurity professionals. New cyberattack detection algorithms are developed before being released to production by using virtual hosts to showcase new security products [67]. DT serves as a source of data generation that is realistic enough to train AI algorithms [26], provides a testing environment for security equipment [69] and performs as environments to test out incident response plans before they are finalized.

The primary purpose of a CR is for cyber defense, focusing on network and information security [63]. CRs are adapting their offerings to support an OT and ICS use case [8]. Upon integrating a DT into a cyber range, we can obtain the performance of a DTs application to safety and the CRs application to security together. The DT will provide information to the CRs about the chain of impacts of an incident, and the CR can provide the source of the incident along with its nature (malicious/accidental) for a detected anomaly. In simpler terms, DTs can provide information about the physical processes and function of the system while the CR can report on the network traffic and bridge the gap between the digital and physical layers [8].

System testing is a part of their proposed DT framework in [21]. For testing purposes, real devices can be interfaced with the DT. Eckhart *et al.* [21] introduce the concept of CPS Twinning, which can allow testing of the network and logic layer of the CPS. The network layer of the CPS is emulated on Mininet, which allows the emulation of logic specific to a variety of devices like PLCs, HMIs, and motors. According to [22], DTs can be used as training exercises for Red and Blue teams for security testing purposes. The red team can uncover flaws and vulnerabilities from the current system configuration and state. The blue team would improve upon their incident response capabilities in response to the Red team. The data collected over these kinds of simulations and events can contribute to risk assessments to motivate cybersecurity uplift activities.

Cyber resilience is described in [71] as the ability of a system to maintain a stable level of control of physical processes while under attack. A four-step method is proposed to improve cyber resilience—risk assessment, resilience engineering, resilience operation, and resilience enhancement. This method lowers the probability of an attack, its impacts, and the recovery time needed to recover from an attack. The DT can actively support this process by providing an isolated environment to test for process control [22]. This iterative simulation on the DT can also identify potential losses during an attack and facilitate the creation of a containment and response plan tailored to different attacks.

Privacy and Legal Compliance. Recently, monitoring the CPS's security and safety posture during operation is regarded as a critical task in [62]. The monitoring activity could provide evidence of meeting security standards like IEC 62443, which would assist organizations in complying with legal requirements. According to [62], the DTs may provide an accurate reflection of CPSs throughout their entire lifecycle for continuous monitoring and documentation of security and safety aspects. The NIS directive (European Parliament and the Council of the European Union 2016) has brought about an increase of regulatory requirements for operators of CPS, which requires integrating security and legal compliance support into DTs.

DTs were used in [16] to enable automated privacy assessments and protect the privacy of smart car drivers, as shown in Fig. 4. A DT of the car continually receives data from the different sensors within the smart vehicle.

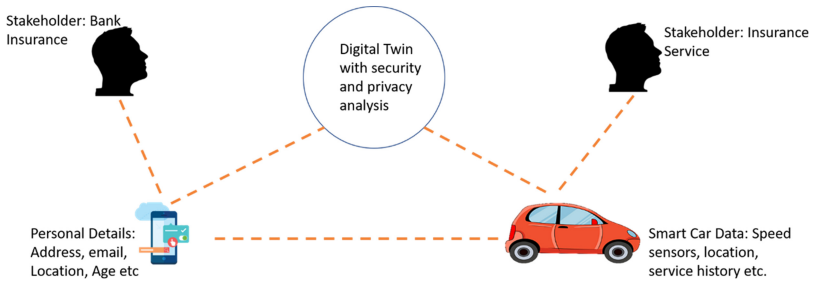

Fig. 4. Privacy protection and compliance via DTs

An example of anonymizing customer data was provided in [16], where DT can assist controllers and processors in fulfilling the general data protection regulation (GDPR) requirements. The customers' data is anonymized to preserve the customers' privacy rights before being sent to insurers.

This approach can be extended to other types of CPSs such as [48]. Privacy-enhancing techniques based on DTs for smart grids, medical CPSs, and smart transport are areas that need to be further explored due to the large volume of the produced data [22].

Security for the Factory of the Future (FoF) and a System of Systems (SoS). A factory of the future (FoF) DT technology was proposed in [8] to enhance cybersecurity resilience. DTs can be integrated into cyber ranges. Cyber range products are used for cybersecurity simulation and training [7], but using DTs will help better understand how cyber events are represented between the physical asset and the digital counterpart. Hence, combining DTs and cyber ranges benefits safety monitoring, predictive decision making, and SoS architecture decision support. Moreover, human behavior can be integrated into the DT for security testing. Nearly 60% of all cyber-attacks involve a human (intentionally or unintentionally), the inclusion of human behavior modeling will enhance the cyber resilience capability of the FoF [74].

3 Cybersecurity of Digital Twin

The second important research question in this work is: "**What is the current state of cybersecurity for the DT?**

With the growing convergence of information technology (IT) and operation technology (OT) [46], the evolution of intelligent manufacturing and industry 4.0 automation have increased the cyber attack surface dramatically. As manufacturing assets become increasingly interconnected, decision-making will be more reliant on DTs, and the increasing use of cloud manufacturing services increases the attack surface [8], a new attack fractal.

DTs have been considered by organizations to add to the current fractal and they must be subject to security measures to prevent an entry point for cyber attackers [7]. When machines are unprogrammable and relied mostly on electric power, the security issue is not important because they were isolated from the organizational infrastructure. However, with the introduction of the internet to the manufacturing industry has opened many security challenges [46,47]. Therefore, it is worth considering that the introduction of the DT will enlarge the attack surface. Therefore its weakened security requires additional measures and enhancements. Our main finding is that the decision to adopt and deploy DT in organization and industries poses additional challenges in security and privacy [43], which is the main focus of this section.

Along with all of the benefits and opportunities that DT brings, new attack vectors are also exposed. Adopting DT is a promising performance enhancement, and there has been an impeding demand from academic and industrial research.

But, quantification of security challenges and potential solutions should be investigated thoroughly before the adoption of DT [39]. When an attacker gets access to a DT of the system, great care should be taken to prevent the attackers getting into the physical twin and compromising them [39]. As mentioned earlier, we can consider DTs of cars and/or remote surgery, which requires bidirectional communication links, therefore security needs are to be given equal attention to that of performance improvements for improved seamless migration to DTs.

Data Security Involving Personally Identifiable Information. DTs present privacy issues. Due to a large amount of data collected from users, especially in AVs or digital healthcare, the information may allow insights into people's behavior and usage patterns without their consent. The data could help target specific advertising at the users or even inflate insurance and healthcare. Similar to security and privacy regulations present in most of the standards followed in IT and OT, regulatory mechanisms need to enable usage of DT while preventing its misuse [10].

While the DT aims to represent its physical counterpart as accurately as possible, it raises the possibility of the collected data related to individuals' life, behavioral patterns, intellectual property, or combined. Currently, no regulations explicitly govern the ownership of data within a DT. As this paradigm further evolves and permeates into sectors like smart cars and smart health, data ownership will become increasingly important since the participant is part of the DT with significant data contribution in both cases—health and AVs. However, third parties are involved in the administration and management. Further questions include—who owns the data, who are allowed to access it, and when the access is granted [28]?

The DT environment must be developed with a strong resilience towards viruses and malicious activities. Compromising the private, sensitive, and confidential information within the DT can damage all sources of the physical twin that are communicating with the DT. A focus needs to be given to the DTs in the medicine and healthcare sectors regarding data security and privacy [6]. A security layer was introduced to a DT model in [18] for secure data sharing in the DT environment. And the security layer is used to protect the sensitive data transmitted between the DT and its physical counterpart.

Intellectual Property Protections. DTs raise the need for intellectual property protections. Intellectual property protection mechanisms like watermarking [29] and digital rights management (DRM) [53] can protect the DT and its organizational specific knowledge. However, watermarking and DRMs can be bypassed.

Trusted Platform Module Use. Further security protections for a DT may limit its use to a specific set of hardware or specific machines using a trusted platform module (TPM). The secure execution of DT is ensured via a successful cryptographic exchange between the hardware and software.

Software Security within the DT. An end-to-end scheme for cyber resilience was proposed in [75] to enable the security of DT software. The scheme identifies

vulnerable functions in DT software projects for healthcare. A deep code attention technique was employed to explore the context code relationships between vulnerability-related keywords. The results of empirical studies showed superior performance to some state-of-the-art deep learning methods.

4 Challenges and Future Directions

The proliferation of IoT-enabled CPS induces multiple complexities. Since CPS are key components of a DT, the associated risks and vulnerabilities need to be better understood. The security-by-design is achieved through considering security and incorporating it from the design phase of a technology. While technology is moving at an accelerated rate and the transmission and supervision of vast quantities of data is supported by a sturdy infrastructure, the standards which govern data transactions are outpaced by the rise of smart technologies and their inclusion into different smart sectors [15]. The inter-connectivity of different smart sectors increases the threat surface and may lead to a severe security breach [1].

IDS Challenges. SIEMs are too complex for us to create intrusion detection and correlation rules [19]. Future research is needed to define complex rules in simple code to reduce the requirements of SIEM experts' familiarity with the SIEM syntax. Thus, more and more security personnel may contribute to the improved lightweight framework.

Physical Twin Vulnerabilities Affecting the DT. Cybersecurity risks present themselves to the DT paradigm [27]. Since the DT becomes a repository for enormous amounts of data via collection from sensors, a successful compromise of the system can result in the loss of sensitive data and financial damage. As DTs are used to predict and provide suggestions based on the acquired information, the compromise can also lead to the loss of business secrets and processes. When a hacker has attained access to the DT, the attackers may find a rich data asset, including a blueprint of the entire system and the possessed data on the DT, and a viable method of influencing the real twin in the case of a bidirectional twin [27].

Security gaps between DT and real twin were identified with examples of failing to replicate a microcontroller's security protection in the real twin within the DT. While there has been an increasing amount of research on the DT paradigm, there is little research on the actual security of the DT itself.

Security issues of a DT are similar to the security concerns observed in IoT, since they are connected as key components to a DT. The security issues include data encryption, access privileges, principle of least privilege, labelling known device, and vulnerabilities.

Threat modeling of the different components that make up a DT needs to be carried out to enable a secure by design DT that can mitigate the cyber risks currently present within it [1]. Within the smart healthcare sector, security threats were identified in [72] on smart devices, including hardware exploitation, backdoors, software exploitation, and many more.

CPS can attract compromised-key attacks due to authenticity requirements among different sensors using the handshake protocols. It can be problematic since CPS are key components of the DTs, especially since the supporting infrastructure can be manipulated to enable a backdoor [31] to the system for future access or potential intellectual property (IP) theft.

Data and Information Privacy Challenges. In [76], a DT was used to protect human safety in an airport cargo scenario. This work can be extended to include individual health status like blood pressure and heart rate, which can develop normal patterns of human behavior to check for anomalies and challenges.

Healthcare DTs applications will require massive development in terms of cyber resilience [14] due to the volume of patient data that is collected, moving in transit, and processed between the digital and physical twin. The information like personal data about a patient and their current state of health, needs to be handled with the utmost care, so hospitals and organizations must ensure the data security and integrity [75]. Vulnerability detection is a crucial requirement for cyber resilience in healthcare DTs [34] since an exploited vulnerability in the medicine DT can pose threats to its many users.

In [10], the privacy concerns were explored for DT in healthcare. Since a DT in medicine can be used to create the 'virtual patient', governance and due diligence will need to be used to safeguard the rights of a DT user. The governance can use processes from how biobanks or medical banks are inspected, designed, and regulated. Data protection will be a vital concern of the DT paradigm being used in medicine due to the sensitive nature of the data.

Human Errors. The human factor in any technology is currently overlooked as an inherent weakness and underestimated in the cyber-physical networks. The increasing number of phishing attacks to exploit this vulnerability are a severe threat, given that smart devices and the emerging use of IoT are targeted extensively. Another vector to be considered is the threat of the malicious insider [2], resulting in non-compliance, fraud, industrial espionage, or even plain human error. A baseline needs to be established to distinguish normal and malicious behaviors and integrated into the DT IDS [13]. Since a DT forms part of an organization's proprietary technology, it requires stringent IP protection.

Integration of Legacy Systems with a DT. With CPSs having a long life cycle, implementing the DT on brownfield sites will be a large area of interest [22]. Older systems are often insufficiently documented, which may affect the DT model's accuracy. It can lead to a dysfunctional DT representation of the system. The challenge will be to determine the use case of the DT. According to [12,22], a specification mining approach was proposed to implement an IDS of automation systems. Further research needs to be conducted on how legacy systems and DTs can be integrated to enhance the cyber resilience.

Enabling a Factory of the Future DT. Currently, the scope of DT is tied to a single asset. According to [8], the narrow scope is a limitation with current DTs. More research is needed to release the DT beyond the limits of an individual

physical asset and eventually span the complete System of Systems [61]. The System of Systems is not a sum of isolated assets but a complete network of factories [38].

4.1 Potentials of DTs with Cybersecurity

Cybersecurity professionals shall establish an online digital clone for each physical device in the world through cyber DTs. As mentioned, such automated emulation simulates cyber attacks, circumvent vulnerabilities and spots possible threats before the actual production environment is effected. To this end, we have identified the following avenues for future research.

Attacks to/from DTs. When machines were not programmable and only relied on electricity powering them, there was little concern about their security since they were isolated from the organizational infrastructure. The introduction of the internet to the manufacturing industry has opened many challenges in terms of security and the many opportunities it presents. More research is required on the attacks against DTs or even attacks that can be carried out using the DT itself [22]. Since the DT is a replica of the system and is used to provide a digital replica of the physical counterpart, a capable attacker can manipulate the data in the DT to hide their traces within the physical counterpart go undetected. Alternatively, if the DT can issue automated commands based on the actions of the physical system, a compromised DT can be used by an attacker to issue malicious commands back to the physical asset and cause it to go to an unsafe state. The security and privacy concerns will be a key discussion factor in the future development of DTs. Its current level of maturity indicates a strong presence in industry 4.0 and the automation of manufacturing [33].

To thoroughly examine the security for a manufacturing system, five levels were proposed in [30] for the CIM model [64]. The five levels of the CIM model can be applied to the DT since it replicates the physical twin. By ensuring that security rules are defined, established, and implemented at each level, security within an organization could be addressed from a high-level view to more granular aspects of the system. The five levels are: i) **Enterprise or Corporate level:** Decision related to workflows and operational management are defined that span the complete process from production to the finalised product; ii) **Plant Management level:** The decisions that affect management of a single plant; iii) **Supervisory level:** The decisions that affect the manufacturing cells that come under a single supervisory process; iv) **Cell Control level:** This decision at this level effect a single process and its performed actions; v) **Sensor Actuator level:** This level consists of the most granular aspects of the system which could consist of the sensors, actuators and controllers that integrate to perform the physical process

Protocols used to support the manufacturing infrastructure like modbus, distributed network protocol (DNP3), industrial Ethernet, PROFIBUS, building automation, and control networking (BACnet) are mainly used for supervisory controls and not security. They cannot provide authentication, confidentiality,

integrity, non-repudiation, and the ability to detect anomalies [30]. Manufactures are exposed to cyber liabilities like non-availability of systems, data breaches, intellectual property theft, and third-party damage.

Securing DTs with Authentication Measures. With the authors in [31] using DTs as a use case in remote control for surgery, they emphasize a strong need for authentication on each site where the DT is operating. Using state-of-the-art techniques like multi-factor authentication (MFA) and biometric authentication [65,70] should be made mandatory in addition to the application of physical access controls to the DT system. Any physical access to the facilities should be restricted and supported by strong multi-factor or biometric authentication [1]. A malicious actor could wreak havoc if they were to gain access to the system and affect all the connected systems and those that are linked to the DT. While there is very little research in authentication measures for a DT, research into this would provide an added layer of security that would make the DT harder to compromise and add to the defense-in-depth approach taken to secure it.

Knowledge-Based IDS for DTs. Multiple articles attempted to identify and mitigate cyber-attacks by using DTs as an IDS system. In [52,57], many IDSs have revolved around behavior-based systems because knowledge-based systems need historical data of realistic previous exploits to establish rules. DTs can be used as testbeds to obtain the required system behavior and data and can also be used as testbeds to simulate realistic incidents.

Scope and Optimality of DT. While the DT is meant to be a digital mirror image of its physical counterpart, it should only provide support to its physical twin and not be a redundancy backup that replicates the CPS in its entirety [22]. While a cost-effective method for operating a DT is proposed in [9], there is no current standard for how accurately a DT is supposed to mirror its physical twin. It is challenging to build a DT with sufficient capabilities [20]. Due to this pursuing the balance between budget and twin similarity is a direction worth pursuing.

DT-Based Honeypots. Honeypots are employed as baiting mechanisms to attract hackers by emulating a real-world environment. The primary use of honeypots is to serve as deception devices and discover attackers' tactics, techniques, and procedures. The use of hardware automation can enhance their similarity to real-time systems to enhance the credibility [45]. While we found no publication in this area, the results and learnings from integrating a DT with a cyber range can help create an accurate representation of the physical environment as a honeypot.

Secure Decommissioning with DT. Simulation has not been used for decommissioning an asset, even at the peak of its research [42] except for when it is an asset of high risk like a nuclear power plant [50]. Any high-risk asset requires to be securely decommissioned. It also holds for the DT that is accompanying a high-risk asset through its production life cycle. The DT needs to be decommissioned securely and avoid any instances of unauthorized access [22]. Since the DT has

been leveraged in different phases of the systems' life cycle, Eckhart *et al.* [22] advocate to include the DT in the last stage of the life cycle (the decommissioning stage). Moreover, the inclusion of DT in the prior stages will allow a holistic view of how a DT can be used to its full capacity.

Human Behavior with DT for IDS. Human behavior modeling is in a very early stage of development within the DT concept [11,24]. Human behavior may have a massive impact on any manufacturing process since interfaces that require human input can be error-prone. A tired worker can lose focus and cause a problem with a machine [58], and it is challenging to distinguish as a malicious act or an accident. Nevertheless, it requires an understanding of human intention compared to normal behavior addressed by techniques like User and Entity behavior Analysis (UBEA) [5]. It has not been explored across cyber ad physical spheres yet. The authors in [8] propose that interactions with equipment (systems, applications, mouse, and keyboard) can be used to build a worker's profile which will establish a normal baseline of their activities and patterns of work and isolate any anomalies that might arise from the safety and security point of view; see a DT-enabled tracking framework [76] and the reference therein.

DT, SOC, and SIEM Integration. In [19], a DT was integrated with a SOC and SIEM to detect a MITM attack. It created new rules for the SIEM to assist with attack detection. This paradigm could be extended further by the data provided to the SOC from the DT or even the addition of cyber threat intelligence (CTI) and the common vulnerabilities and exposures (CVE)s. The integration of these could be used to simulate various scenarios in the DT and make it as realistic as possible. It could also be supplemented using data that has been obtained from honeypots about the attacker's TTPs. A point of convergence between the DT and CRs was forecasted in [7]. However, no research publication has been found for connecting security tests and simulations in a DT setup in early 2021 [8].

5 Conclusion

Over the past decade, fast advances in machine learning, artificial intelligence, IoT, and others have played a part in the emergence of the DT and will continue to do so for the upcoming decade. The advancement of technologies has led to the DT applied in broad fields, including manufacturing, aviation, automobiles, medicine, the design of cities, and many more. This paper has explored how the DT can be utilized further by enhancing cybersecurity measures.

This paper answered the two research questions: *How does a DT currently contribute to cybersecurity? What is the current state of cybersecurity for the DT?* We have examined some promising frameworks in the literature and have provided insights into the different use cases where DTs can enhance cybersecurity. Regarding the DT's security, some methods are used to prevent access of the DT from falling into malicious hands, but further research is required. In conclusion, this study has provided challenges faced by the use of DT and open research areas worth exploring to further this concept.

References

1. Ahmadi-Assalemi, G., et al.: Digital twins for precision healthcare. In: Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J. (eds.) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. ASTSA, pp. 133–158. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-35746-7_8
2. Ahmadi-Assalemi, G., Al-Khateeb, H.M., Epiphaniou, G., Cosson, J., Jahankhani, H., Pillai, P.: Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace. In: Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 1–9. IEEE (2019)
3. Akbarian, F., Fitzgerald, E., Kihl, M.: Intrusion detection in digital twins for industrial control systems. In: Proceedings of the 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–6. IEEE (2020)
4. Aldwairi, T., Perera, D., Novotny, M.A.: An evaluation of the performance of restricted Boltzmann machines as a model for anomaly network intrusion detection. Comput. Networks **144**, 111–119 (2018)
5. Babu, S.: Detecting anomalies in Users-An UEBA approach. In: Proceedings of the International Conference on Industrial Engineering and Operations Management, pp. 863–876 (2020)
6. Barricelli, B.R., Casiraghi, E., Fogli, D.: A survey on digital twin: definitions, characteristics, applications, and design implications. IEEE Access **7**, 167653–167671 (2019)
7. Becue, A., et al.: Cyberfactory# 1-securing the industry 4.0 with cyber-ranges and digital twins. In: Proceedings of the 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), pp. 1–4. IEEE (2018)
8. Becue, A., Maia, E., Feeken, L., Borchers, P., Praca, I.: A new concept of digital twin supporting optimization and resilience of factories of the future. Appl. Sci. **10**(13), 4482 (2020)
9. Bitton, R., et al.: Deriving a cost-effective digital twin of an ICS to facilitate security evaluation. In: Lopez, J., Zhou, J., Soriano, M. (eds.) ESORICS 2018. LNCS, vol. 11098, pp. 533–554. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99073-6_26
10. Bruynseels, K., Santoni de Sio, F., van den Hoven, J.: Digital twins in health care: ethical implications of an emerging engineering paradigm. Front. Genet. **9**, 31 (2018)
11. Buldakova, T., Suyatinov, S.: Hierarchy of human operator models for digital twin. In: Proceedings of the 2019 International Russian Automation Conference (RusAutoCon), pp. 1–5. IEEE (2019)
12. Caselli, M., Zambon, E., Amann, J., Sommer, R., Kargl, F.: Specification mining for intrusion detection in networked control systems. In: Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), pp. 791–806 (2016)
13. Cheh, C., Keefe, K., Feddersen, B., Chen, B., Temple, W.G., Sanders, W.H.: Developing models for physical attacks in cyber-physical systems. In: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and Privacy, pp. 49–55 (2017)
14. Chen, X., et al.: Android HIV: a study of repackaging malware for evading machine-learning detection. IEEE Trans. Inf. Forensics Secur. **15**, 987–1001 (2019)
15. Coppinger, R.: Design through the looking glass [digital twins of real products]. Eng. Technol. **11**(11), 58–60 (2016)

16. Damjanovic-Behrendt, V.: A digital twin-based privacy enhancement mechanism for the automotive industry. In: 2018 International Conference on Intelligent Systems (IS), pp. 272–279. IEEE (2018)
17. Dietz, M., Pernul, G.: Unleashing the digital twin's potential for ICS security. IEEE Secur. Priv. **18**(4), 20–27 (2020)
18. Dietz, M., Putz, B., Pernul, G.: A distributed ledger approach to digital twin secure data sharing. In: Foley, S.N. (ed.) DBSec 2019. LNCS, vol. 11559, pp. 281–300. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22479-0_15
19. Dietz, M., Vielberth, M., Pernul, G.: Integrating digital twin security simulations in the security operations center. In: Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1–9 (2020)
20. Eckhart, M., Ekelhart, A.: A specification-based state replication approach for digital twins. In: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, pp. 36–47 (2018)
21. Eckhart, M., Ekelhart, A.: Towards security-aware virtual environments for digital twins. In: Proceedings of the 4th ACM Workshop on Cyber-physical System Security, pp. 61–72 (2018)
22. Eckhart, M., Ekelhart, A.: Digital twins for cyber-physical systems security: state of the art and outlook. In: Security and Quality in Cyber-Physical Systems Engineering, pp. 383–412. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25312-7_14
23. Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H.: Digital Twin Technologies and Smart Cities. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-18732-3
24. Graessler, I., Pöhler, A.: Integration of a digital twin as human representation in a scheduling procedure of a cyber-physical production system. In: Proceedings of the 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 289–293. IEEE (2017)
25. Grieves, M., Vickers, J.: Digital twin: mitigating unpredictable, undesirable emergent behavior in complex systems. In: Kahlen, F.-J., Flumerfelt, S., Alves, A. (eds.) Transdisciplinary Perspectives on Complex Systems, pp. 85–113. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-38756-7_4
26. Hallaq, B., Nicholson, A., Smith, R., Maglaras, L., Janicke, H., Jones, K.: CYRAN: a hybrid cyber range for testing security on ICS/SCADA systems. In: Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 622–637. IGI Global (2018)
27. Hearn, M., Rix, S.: Cybersecurity considerations for digital twin implementations. IIC J. Innov. 107–113 (2019)
28. Jones, D., Snider, C., Nassehi, A., Yon, J., Hicks, B.: Characterising the digital twin: a systematic literature review. CIRP J. Manuf. Sci. Technol. **29**, 36–52 (2020)
29. Katzenbeisser, S., Petitcolas, F.: Digital Watermarking. Artech House, London 2 (2000)
30. Kaur, M.J., Mishra, V.P., Maheshwari, P.: The convergence of digital twin, IoT, and machine learning: transforming data into action. In: Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H. (eds.) Digital Twin Technologies and Smart Cities. IT, pp. 3–17. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-18732-3_1
31. Laaki, H., Miche, Y., Tammi, K.: Prototyping a digital twin for real time remote control over mobile networks: application of remote surgery. IEEE Access **7**, 20325–20336 (2019)

32. Liao, H.J., Lin, C.H.R., Lin, Y.C., Tung, K.Y.: Intrusion detection system: a comprehensive review. J. Network Comput. Appl. **36**(1), 16–24 (2013)
33. Lim, K.Y.H., Zheng, P., Chen, C.H.: A state-of-the-art survey of digital twin: techniques, engineering product lifecycle management and business innovation perspectives. J. Intell. Manuf. **31**(6), 1–25 (2019)
34. Liu, L., De Vel, O., Han, Q.L., Zhang, J., Xiang, Y.: Detecting and preventing cyber insider threats: a survey. IEEE Commun. Surv. Tutorials **20**(2), 1397–1417 (2018)
35. Liu, M., Fang, S., Dong, H., Xu, C.: Review of digital twin about concepts, technologies, and industrial applications. J. Manuf. Syst. **58**, 346–361 (2020)
36. Lv, L., Wang, W., Zhang, Z., Liu, X.: A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. Knowl. Based Syst. **195**, 105648 (2020)
37. Malik, N.S., Collins, R., Vamburkar, M.: Cyberattack pings data systems of at least four gas networks (2018)
38. Mennenga, M., Cerdas, F., Thiede, S., Herrmann, C.: Exploring the opportunities of system of systems engineering to complement sustainable manufacturing and life cycle engineering. Procedia CIRP **80**, 637–642 (2019)
39. Minerva, R., Lee, G.M., Crespi, N.: Digital twin in the IoT context: a survey on technical features, scenarios, and architectural models. Proc. IEEE **108**(10), 1785–1824 (2020)
40. Mittal, S., Tolk, A., Pyles, A., Van Balen, N., Bergollo, K.: Digital twin modeling, co-simulation and cyber use-case inclusion methodology for IoT systems. In: Proceedings of the 2019 Winter Simulation Conference (WSC), pp. 2653–2664. IEEE (2019)
41. Mittal, S., Zeigler, B.P., Tolk, A., Õren, T.: Theory and practice of M&S in cyber environments. In: The Profession of Modeling and Simulation: Discipline, Ethics, Education, Vocation, Societies and Economics. Wiley Online Library (2017)
42. Mourtzis, D., Doukas, M., Bernidaki, D.: Simulation in manufacturing: review and challenges. Procedia CIRP **25**, 213–229 (2014)
43. Parmar, R., Leiponen, A., Thomas, L.D.: Building an organizational digital twin. Bus. Horiz. **63**(6), 725–736 (2020)
44. Pham, C., Tang, D., Chinen, K.i., Beuran, R.: CYRIS: a cyber range instantiation system for facilitating security training. In: Proceedings of the Seventh Symposium on Information and Communication Technology, pp. 251–258 (2016)
45. Piggin, R., Buffey, I.: Active defence using an operational technology honeypot (2016). https://bit.ly/3njohBz
46. Pokhrel, S.R., Garg, S.: Multipath communication with deep Q-Network for industry 4.0 automation and orchestration. IEEE Trans. Ind. Inform. **17**(4), 2852–2859 (2020)
47. Pokhrel, S.R., Pan, L., Kumar, N., Doss, R., Le Vu, H.: Multipath TCP meets transfer learning: a novel edge-based learning for industrial IoT. IEEE Internet Things J. **8**(13), 10299–10307 (2021)
48. Pokhrel, S.R., Qu, Y., Gao, L.: QoS-aware personalized privacy with multipath TCP for industrial IoT: analysis and design. IEEE Internet Things J. **7**(6), 4849–4861 (2020)
49. Pokhrel, S.R., Vu, H.L., Cricenti, A.L.: Adaptive admission control for IoT applications in home wifi networks. IEEE Trans. Mob. Comput. **19**(12), 2731–2742 (2019)
50. Polenghi, A., Fumagalli, L., Roda, I.: Role of simulation in industrial engineering: focus on manufacturing systems. IFAC Pap. OnLine **51**(11), 496–501 (2018)

51. Poon, J., Jain, P., Konstantakopoulos, I.C., Spanos, C., Panda, S.K., Sanders, S.R.: Model-based fault detection and identification for switching power converters. IEEE Trans. Power Electron. **32**(2), 1419–1430 (2016)
52. Roosta, T., Nilsson, D.K., Lindqvist, U., Valdes, A.: An intrusion detection system for wireless process control systems. In: Proceedings of the 2008 5th IEEE International Conference on Mobile ad hoc and Sensor Systems, pp. 866–872. IEEE (2008)
53. Rosenblatt, B., Trippe, B., Mooney, S., et al.: Digital Rights Management. New York (2002)
54. Rubio, J.E., Alcaraz, C., Roman, R., Lopez, J.: Analysis of intrusion detection systems in industrial ecosystems. In: SECRYPT, pp. 116–128 (2017)
55. Saad, A., Faddel, S., Youssef, T., Mohammed, O.A.: On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks. IEEE Trans. Smart Grid **11**(6), 5138–5150 (2020)
56. Schinagl, S., Schoon, K., Paans, R.: A framework for designing a security operations centre (SOC). In: Proceedings of the 2015 48th Hawaii International Conference on System Sciences, pp. 2253–2262. IEEE (2015)
57. Shin, S., Kwon, T., Jo, G.Y., Park, Y., Rhy, H.: An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. IEEE Trans. Ind. Inform. **6**(4), 744–757 (2010)
58. Shultz, K.S., Wang, M., Olson, D.A.: Role overload and underload in relation to occupational stress and health. J. Int. Soc. Investig. Stress **26**(2), 99–111 (2010)
59. Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H., Sui, F.: Digital twin-driven product design, manufacturing and service with big data. Int. J. Adv. Manuf. Technol. **94**(9), 3563–3576 (2018)
60. Tao, F., Zhang, H., Liu, A., Nee, A.Y.: Digital twin in industry: state-of-the-art. IEEE Trans. Ind. Inform. **15**(4), 2405–2415 (2018)
61. Tao, F., Zhang, M.: Digital twin shop-floor: a new shop-floor paradigm towards smart manufacturing. IEEE Access **5**, 20418–20427 (2017)
62. Tauber, M., Schmittner, C.: Enabling security and safety evaluation in industry 4.0 use cases with digital twins. ERCIM News (2018)
63. Tian, Z., et al.: A real-time correlation of host-level events in cyber range service for smart campus. IEEE Access **6**, 35355–35364 (2018)
64. Tuptuk, N., Hailes, S.: Security of smart manufacturing systems. J. Manuf. Syst. **47**, 93–106 (2018)
65. Tuyls, P., Akkermans, A.H.M., Kevenaar, T.A.M., Schrijen, G.-J., Bazen, A.M., Veldhuis, R.N.J.: Practical biometric authentication with template protection. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 436–446. Springer, Heidelberg (2005). https://doi.org/10.1007/11527923_45
66. Uhlemann, T.H.J., Lehmann, C., Steinhilper, R.: The digital twin: realizing the cyber-physical production system for industry 4.0. Procedia CIRP **61**, 335–340 (2017)
67. Urias, V.E., Stout, W.M., Van Leeuwen, B., Lin, H.: Cyber range infrastructure limitations and needs of tomorrow: a position paper. In: Proceedings of the 2018 International Carnahan Conference on Security Technology (ICCST), pp. 1–5. IEEE (2018)
68. Vielberth, M., Menges, F., Pernul, G.: Human-as-a-security-sensor for harvesting threat intelligence. Cybersecurity **2**(1), 1–15 (2019)
69. Vykopal, J., Ošlejšek, R., Čeleda, P., Vizvary, M., Tovarňák, D.: Kypo cyber range: design and use cases. In: Proceedings of the 12th International Conference on Software Technologies, pp. 310–321. SciTePress (2017)

70. Wayman, J., Jain, A., Maltoni, D., Maio, D.: An introduction to biometric authentication systems. In: Wayman, J., Jain, A., Maltoni, D., Maio, D. (eds.) Biometric Systems, pp. 1–20. Springer, London (2005). https://doi.org/10.1007/1-84628-064-8_1
71. Wei, D., Ji, K.: Resilient industrial control system (RICS): concepts, formulation, metrics, and insights. In: Proceedings of the 2010 3rd International Symposium on Resilient Control Systems, pp. 15–22. IEEE (2010)
72. Wurm, J., et al.: Introduction to cyber-physical system security: a cross-layer perspective. IEEE Trans. Multi Scale Comput. Syst. **3**(3), 215–227 (2016)
73. Yahalom, R., Steren, A., Nameri, Y., Roytman, M., Porgador, A., Elovici, Y.: Improving the effectiveness of intrusion detection systems for hierarchical data. Knowl. Based Syst. **168**, 59–69 (2019)
74. van Zadelhoff, M.: The biggest cybersecurity threats are inside your company. Harvard Bus. Rev. **19** (2016)
75. Zhang, J., Li, L., Lin, G., Fang, D., Tai, Y., Huang, J.: Cyber resilience in healthcare digital twin on lung cancer. IEEE Access **8**, 201900–201913 (2020)
76. Zhao, Z., Shen, L., Yang, C., Wu, W., Zhang, M., Huang, G.Q.: IoT and digital twin enabled smart tracking for safety management. Comput. Oper. Res. **128**, 105183 (2021)