Received: 29 November 2023 | Revised: 28 February 2024 | Accepted: 20 March 2024

DOI: 10.1002/spy2.396

SURVEY PAPER

WILEY

Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications

Mohammed El-Hajj | **Taru Itäpelto** | **Teklit Gebremariam**

SCS, EEMCS, University of Twente, Enschede, The Netherlands

Correspondence
Mohammed El-Hajj, SCS, EEMCS, University of Twente, Enschede, The Netherlands.
Email: m.elhajj@utwente.nl

Abstract

Connectivity and data exchange are key features of Industry 4.0. In this paradigm, (Industrial) Internet of Things ((I)IoT) devices are a vital component facilitating the collection and transmission of environmental data from the physical system to the central station for processing and analysis (digital twin [DT]). However, although (I)IoT devices play a critical role in this process, they are not inherently equipped to run strong encryption mechanisms to secure the data they transmit over wired or wireless channels. This research aims to explore the potential of DTs in securing Industry 4.0 applications and the security mechanism employed to ensure confidentiality, integrity, and authentication of data communicated between (I)IoT and DT through a systematic literature review (SLR). This SLR, based on the analysis of 67 papers published between 2018 and 2023, underscores the evolving significance of DT technology, particularly within the ambit of Industry 4.0. The findings illuminate the pervasive influence of DT technology across multiple industrial sectors. The result SLR revealed that DT is growing and being widely adopted as a security tool particularly in Industry 4.0 using enabling technology like machine learning, data analytics, blockchain, and 5G networks to provide security solutions such as intrusion detection, vulnerability assessment, cyber range, and threat intelligence.

KEYWORDS

digital twins, DT, IIoT, Industry 4.0, Security, SLR, systematic literature review

1 | INTRODUCTION

Industry 4.0, characterized by cyber-physical systems (CPSs), IoT, cloud computing, and big data analytics, has heightened system connectivity, making industrial systems more susceptible to cyber threats.[1] The intricate nature of these systems presents challenges in vulnerability assessments, where even basic scans can cause disruptions.[2]

Digital twin (DT) technology offers a virtual environment for secure vulnerability assessments and penetration testing, mitigating risks without operational disruptions.[2,3] DTs contribute to security enhancement through IoT-based

All authors are contributed equally to this study.

monitoring, anomaly detection, access control, and the enforcement of security policies.[4,5] DT and IoT integration span across industries, utilizing IoT devices for data collection and DTs for analysis and insights.[6] This research investigates DTs' role in securing Industry 4.0 applications while proposing lightweight secure communication solutions for constrained devices integrated with DTs.

1.1 | Motivation

The driving force behind this research lies in the extensive adoption of DT technology within the realm of Industry 4.0 and its integration with the Industrial Internet of Things (IIoT).[7] DT implementation extensively relies on interconnected IIoT devices such as sensors and actuators, often constrained in resources necessary to support conventional security measures. The significance of conducting a systematic literature review (SLR) emerges as a fundamental step to comprehensively understand the landscape of integrating DT to fortify security within the domain of IIoT. This review aims to consolidate existing knowledge, highlight successful methodologies, and pinpoint the prevailing challenges encountered in previous studies concerning DT and IIoT integration for enhanced security measures. Within this context, the secure communication between DT and resource-constrained IIoT devices stands out as a crucial aspect. The communication channel plays a pivotal role in transmitting critical data, demanding a robust and resource-efficient lightweight encryption scheme to ensure the integrity and confidentiality of the exchanged information. As the fusion of DT and IIoT becomes increasingly pervasive in critical infrastructures, ensuring the security of their interaction channels is paramount. By exploring prior studies through a SLR, it becomes feasible to identify effective methodologies and potential gaps in current security practices. This comprehensive understanding is pivotal in devising novel approaches to tackle security challenges and bridge existing gaps in DT and IIoT integration. This research endeavors to contribute significantly by consolidating and analyzing existing knowledge through a SLR. By harnessing the insights gleaned from previous studies, it aims to pave the way for innovative solutions that enhance the security of DT and IIoT integration in the realm of Industry 4.0.

1.2 | Methodology

This research seeks to perform a SLR to investigate the utilization of DT technology for enhancing security within Industry 4.0 applications. Additionally, it aims to scrutinize the security methodologies proposed in previous studies for securing communication between DT and (I)IoT devices. To achieve the primary objective, this study follows the three-phase SLR process outlined by Kitchenham and Charter.[8] The systematic approach encompasses planning the review protocol, executing the review process, and comprehensively reporting the obtained results. For streamlining the literature review procedure and enhancing information retrieval, two valuable tools were employed. First, *Parsifal*, an online tool explicitly designed to automate SLRs, facilitated the structured collection of relevant literature. Second, *Logseq*, a note-taking application renowned for its capacity to interlink ideas and efficiently retrieve stored information, was utilized to streamline data organization and synthesis. This systematic methodology aims to provide a comprehensive understanding of the existing literature about DT's role in enhancing security within Industry 4.0 scenarios. Moreover, it strives to identify and analyze the effectiveness of security methods proposed in prior studies for securing the communication interface between DT and resource-constrained (I)IoT devices.

1.3 | Research questions

This SLR aims to address two primary research questions within the domain of DT integration for enhancing security in Industry 4.0. First, the review endeavors to explore and analyze the utilization of DT technology in bolstering security measures within Industry 4.0 applications. Specifically, it seeks to examine the various ways in which DT has been employed to enhance security, encompassing aspects such as monitoring, threat detection, access control, and vulnerability assessment. Second, the review intends to investigate and evaluate the efficacy of security methods proposed in previous studies for securing communication channels between DT and resource-constrained (I)IoT devices. This includes assessing the strengths and limitations of existing security approaches, identifying gaps in current practices, and exploring potential advancements in securing the interaction between DT and (I)IoT devices. The research questions of the study are listed as follows:

- **RQ1: How DT is used to enhance the security of Industry 4.0 applications?** This research question aims to identify in what way DT is used to provide security services such as intrusion detection, vulnerability assessment and so on to enhance the security aspect of the Industry 4.0 process.
- **RQ2: What are the security mechanisms presented in the literature to ensure the confidentiality, integrity, and authenticity of data (message) communicated between DT and its mapped physical devices?** This research question focuses on the identification of cryptographic or any other security solutions that are used to improve the security of digital channels for data communication between DT and (I)IoT devices.

1.4 | Contribution

This research primarily contributes to advancing knowledge regarding the role of DT technology in bolstering security within Industry 4.0 processes. Through a SLR, the study extensively explores and elucidates the diverse applications of DT in enhancing security measures within the realm of Industry 4.0. By synthesizing existing literature, the research aims to offer a comprehensive understanding of how DT is utilized to fortify security aspects such as monitoring, threat detection, access control, and vulnerability assessment in industrial settings. Additionally, the study identifies and highlights gaps in the existing research related to security mechanisms employed in securing data communication within DT applications. This contribution underscores the research's significance in not only comprehensively documenting the role of DT in enhancing security but also in pinpointing areas for further investigation and improvement in securing DT applications within Industry 4.0 contexts.

1.5 | Outline

The remaining sections of this paper are structured to provide a comprehensive exploration of the research landscape concerning the integration of DT technology to fortify security within Industry 4.0. In Section 2, a detailed design for the SLR will be delineated, outlining the approach employed to reveal the current academic landscape. This section aims to clarify the complexities entailed in formulating a comprehensive framework for conducting the SLR, offering insights into the methodologies tailored to analyze the existing literature.

Subsequently, Section 3 will encapsulate the comprehensive execution and subsequent reporting of all stages within this SLR. This section serves as the nucleus where every facet of the SLR will be expounded upon. Notably, it will focus on addressing the two main research questions highlighted in Section 1.3. Through categorization and evaluation, the selected papers will be dissected into distinct categories, each contributing uniquely to the augmentation of security within Industry 4.0 through DT implementation.

Section 4 will delve into the analysis of the papers obtained from the conducted SLR. This analysis will be segmented, aiming to address the research questions highlighted in Section 1.3.

Moving forward to Section 5, the synthesized results will be comprehensively discussed, facilitating the identification of research gaps and charting future directions for further study. This section will also candidly present the limitations inherent in this study, providing a transparent reflection on the constraints.

Finally, the conclusive insights drawn from this comprehensive review will be presented in Section 6. This conclusive section aims to encapsulate the essence of the study, offering a succinct summary of the derived insights, key findings, and recommendations.

2 | DESIGNING THE SYSTEMATIC LITERATURE REVIEW

A SLR is a methodical investigation of existing research within a defined domain, employing systematic approaches to identify, select, and evaluate relevant articles while scrutinizing the data they provide. Our objective goes beyond merely summarizing existing literature; we aim to pinpoint specific gaps in the current research landscape. To achieve this, we adopt a rigorous SLR approach, outlined in this study. Initially, we formulate a precise search string and query predetermined online databases, followed by a meticulous screening process to discard irrelevant articles. The retained corpus undergoes comprehensive analysis to identify knowledge gaps and propose future research directions. Adhering to the three-phase approach delineated by Kitchenham and Charter[8] ensures the systematic review is conducted transparently and methodically. Figure 1 illustrates the flow of this process. The figure illustrates the systematic steps undertaken for the SLR. Initially, research questions were formulated to guide the inquiry. Based on these questions, key search terminologies were identified for use across various online databases. The results obtained from these searches were collected using Zotero software. Subsequently, a series of filtering rules were applied, starting with the removal of duplicates and then applying inclusion/exclusion criteria along with initial screening. The refined results were then inputted into Parsifal software, an online tool designed to support researchers in conducting SLRs. Parsifal assists in planning the review by aiding with objectives, PICOC (Population, Intervention, Comparison, Outcome, Context), search strings, keyword selection, source selection, and defining inclusion/exclusion criteria. Additionally, it provides tools for building quality assessment checklists and data extraction forms. Finally, a metadata analysis of the extracted data was conducted, and the findings were reported. The figure visually depicts this entire process, providing a comprehensive overview of the systematic approach employed in the SLR. The SLR serves as a formal and structured process for synthesizing relevant research studies to address predetermined inquiries, providing a comprehensive overview of existing literature and identifying research gaps. By following established guidelines and supplementary resources, we ensure transparency and replicability throughout the review process. Our review protocol, detailed in the subsequent section, includes defining the PICOC

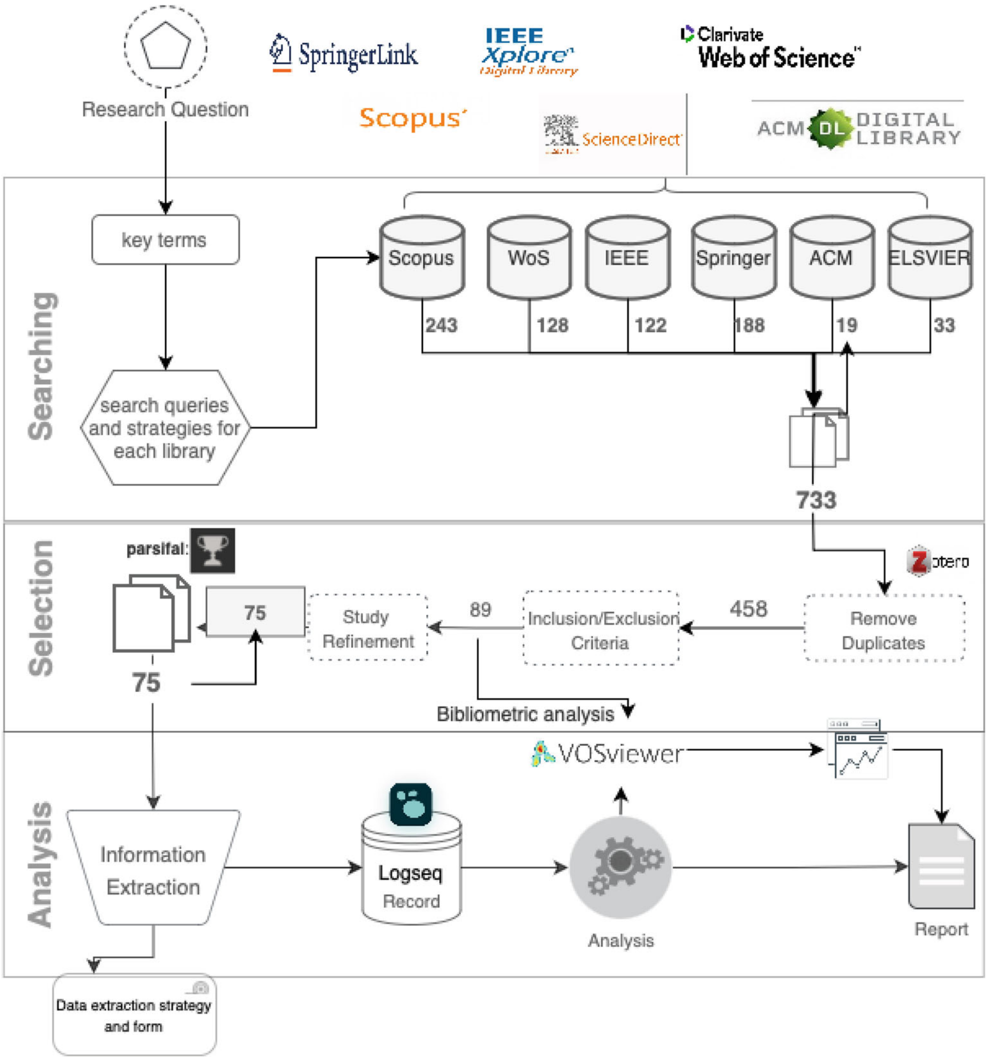

FIGURE 1 Systematic literature review process diagram.

TABLE 1 Inclusion and exclusion criteria.

Criteria type	Inclusion	Exclusion
Period	Studies published between 2018 and 2023	Before 2018
Language	English	Not English
Accessibility	Accessible in full-text	Not accessible in full-text
Type of source	Journal articles, conference proceedings	Books, book chapter
Type of literature	Of type black literature	Grey literature
Relevance	Study related to computer science	Not related to computer science

TABLE 2 Data extraction form.

Data point	Options/explanation
Aim of research	Summarized version of the aim of the paper
Targeted sector	The studied or targeted Industry 4.0 sector
DT purpose	The function or purpose the proposed digital twin
Enabling technology	Technology integrated with digital twin to provide security service
Security mechanism	The security mechanism employed to secure communication channel
Contribution category	Framework, algorithms, architecture, model, platform
Study type	Paper with case-study, experiment based, theoretical concept, review paper science

framework, research questions, search queries, digital library sources, and inclusion/exclusion criteria. The PICOC framework guides our exploration of literature, focusing on population, intervention, outcome, and context within the realm of DT technology and IoT security mechanisms in Industry 4.0 applications.

To conduct a comprehensive review, we formulate search strings based on PICOC criteria and research questions, utilizing key terms and variants summarized in Table 1. These queries are applied to selected electronic databases, including ScienceDirect, Scopus, IEEExplore, and ACM. Inclusion and exclusion criteria are employed to filter research studies, ensuring relevance and quality. A well-designed data extraction form, presented in Table 2, facilitates the collection of pertinent information from selected articles, categorizing contributions and study types to identify prevalent patterns within the literature. Overall, this systematic approach ensures a thorough and rigorous examination of the research landscape, enabling us to identify key insights and areas for future investigation.

3 | PERFORMING THE SYSTEMATIC LITERATURE REVIEW

In Section 2, we provided an overview of the SLR process. Here, we delve into the practical execution of the methodology outlined, detailing the outcomes of each stage. A thorough search was conducted across well-known digital databases including ScienceDirect, SpringerLink, Scopus, IEEExplore, ACM, and Web of Science, renowned for their publication of computer science-related research. Inclusion criteria focused on papers published between 2018 and 2023, limited to articles from journals and conference proceedings. Each database employed distinct search queries and strategies due to their varied mechanisms, detailed further in subsequent sections. This detailed approach ensured a comprehensive retrieval of relevant literature within the defined scope of computer science, facilitating a systematic and exhaustive review from esteemed digital repositories.

3.1 | Search queries and search strategy

In order to maintain a systematic approach to our search process, we considered the distinct methods of advanced searching offered by different databases, each with its own unique search fields and filtering options. With this in mind, we adhered to the following protocol for conducting our search. Initially, we focused on locating papers that included the primary key term *DT* or *Digital Replica* or *Digital Model* within their titles. Subsequently, we refined our search results by introducing security-related terms such as *authentication*, *security*, *encryption*, and *cryptography* into the abstracts of the papers. Lastly, to further narrow down the search results, we integrated industry and IoT-related terms found within the full text of the research papers.

Web of science To search for DT and Internet of Things (IoT) terms within the Web of Science database, we used the “Topic” field, which includes titles, keywords, and abstracts. As for security-related terms like authentication, encryption, cryptography, and industry-related terms, we performed searches across all available fields. We excluded document types such as book chapters, early access, and editorials to refine the search results and focused solely on articles and conference papers. Executing the search query under the “Computer Science” category and “Engineering” categories resulted in a total of 128 articles, which all were published later than 2018.

Query

((((((TI=("digital twin*" OR "digital replica" OR "digital model)) AND AB=("authenticat*" OR "cryptography" OR "security" OR "encrypt*"))) AND ALL=("internet of thing*" OR "industr*" OR "factor*" OR "manufactur*" OR "cyber physical system*" OR "infrastructure*" OR "smart device*")) AND LA=(English)) AND DT=(Proceedings Paper OR Article)) AND SU=(Engineering OR "Computer Science")

Filter: Inclusion - Document Types: Article or Proceeding Paper. Languages: English. Web of Science Categories: Engineering and Computer Science-related papers were selected.

Scopus: Similarly, the search mechanism in Scopus is equivalent to that of the Web of Science. We used the “Article Title”field to search for articles containing the term “digital twin” in their title. This initial search yielded 3330 references after applying the exclusion criteria. We used the “Abstract”field to search papers that have terms related to security, which included “authentication,”“encryption,”“cryptography,” and “security.” We further refined the search by incorporating keywords related to industry and the IoT and searching within the “All Fields.” We only selected articles and conference papers and excluded documents such as book chapters and editorials, as well as early access results. The search in the subject area of “Computer science” and “Engineering” resulted in 242 articles, all published in 2018 or later.

Query

(TITLE ("digital twin" OR "digital replica" OR "digital model) AND ABS ("authenticat*" OR "cryptography" OR "security" OR "encrypt*") AND ALL ("internet of thing" OR "industr*" OR "factor*" OR "manufactur*" OR "cyber physical system" OR "infrastructure" OR "smart device")) AND (LIMIT-TO (SRCTYPE, "j") OR LIMIT-TO (SRCTYPE, "p")) AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI")) AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "re"))

Filter: The filters were within the search query.

IEEExplore: We searched for “digital twin*” within the document title field. Then, we looked for security-related terms like authentication, cryptography, security, and encryption in the “Abstract” field. We then expanded our search to include industry and IoT-related terms within the “Full text and Metadata” fields. The search result in IEEExplore led to the retrieval of 121 papers, including conference and journal articles.

Query

("Document Title":"digital twin*" OR "digital replica" OR "digital model) AND ("Abstract":"authenticat*" OR "Abstract":"cryptography" OR "Abstract":"security" OR "Abstract":"encrypt*") AND ("Full Text & Metadata":"internet of thing*" OR "Full Text & Metadata":"industr*" OR "Full Text & Metadata": "factor*" OR "Full Text & Metadata": "manufactur*" OR "Full Text & Metadata": "cyber physical system" OR "Full Text & Metadata": "infrastructure*" OR "Full Text & Metadata":"smart device*")

Filters: Conferences Journals and Journals filters were applied.

ACM:Among the six databases, ACM returned the lowest number of papers (17). First, we searched for papers with "digital?twin*" in the title. We further refined our search by searching for security-related terms in the abstract and industry and IoT-related terms in the "All" field. This search query resulted in 17 papers matching the inclusion criteria, that is, all papers were accessible and published in English between 2018 and 2023.

Query

[Title: "digital?twin*" OR "digital?replica" OR "digital?model] AND [[Abstract: "authenticat*"] OR [Abstract: "cryptography"] OR [Abstract: "security"] OR [Abstract: "encrypt*"]] AND [[All: "internet of thing*"] OR [All: "industr*"] OR [All: "factor*"] OR [All: "manufactur*"] OR [All: "cyber?physical system*"] OR [All: "infrastructure*"] OR [All: "smart device*"]]

Filter: No filter was applied

ScienceDirect(Elsevier): We tested different search phrase combinations to find the maximum search results. Then we selected the most well-performing search phrase consisting of a combination of keywords and a maximum of eight logical operators.

We conducted the advanced search with the keyword "digital twin" in the "Title"-input field, the security-related terms within the "Title, abstract or author-specified keywords"-input field, and the industry and IoT-related keywords within the "Find articles with these terms"-input field.

As a result of the above search result, we retrieved 31 papers from ScienceDirect.

Query

Title: ("digital twin" OR "digital replica" OR "digital model).
Title, abstract, keywords: ("authentication" OR "cryptography" OR "security" OR "encrypt")
Find articles with these terms: ("internet of things" OR "industry" OR "factory" OR "manufacturing" OR "cyber physical system" OR "infrastructure" OR "smart device")

Filter: Review and Research Article types, together with Engineering and Computer Science Subject areas, were selected as filters.

SpringerLink: One notable difference between SpringerLink and other databases is the absence of a separate field for searching queries in "abstract" and "full content." This limitation inhibited us from using the similar strategy we used for the other databases. As a result of this limitation, we used alternative search mechanisms, briefly described in the box below.

Query General search: ("digital twin*"OR "digital replica" OR "digital model) AND ("authenticat*" OR "cryptography" OR "security" OR "encrypt*") AND ("internet of thing*" OR "industr*" OR "factor*" OR "manufactur*" OR "cyber physical system*" OR "infrastructure" OR "smart device*")

Filter: We used the following filters: Discipline: Computer Science and Engineering; Content-Type: Conference Paper and Article; Language: English
We filtered papers with "digital twin" in their title using a few lines of Python scripts. Finally, we were able to find 188 papers from the SpringerLink database.

3.2 | Search result and bibliometric analysis

After completing the selection process, which involved applying inclusion and exclusion criteria and eliminating duplicate studies, 73 research papers were considered eligible for further review and analysis. The accompanying pie chart (see Figure 2) reveals that IEEE was the primary publisher of the selected papers, accounting for 45 of them. SpringerLink was the second largest contributor, with 12 publications, while Elsevier (7), ACM (6), and MDPI (3) each account for the lowest contribution of publications. The second right side of the pie chart 2 also demonstrates that the majority of the selected papers were sourced from Web of Science and Scopus, followed by IEEE and SpringerLink. It is important to note how the selected papers are distributed in terms of publishing kinds. Of these papers, that is, 67% -or 45-were published as conference papers, whereas the remaining 32% -or 22-were in the form of journal articles.

Analysis of the distribution of selected papers based on publication year revealed that the majority of articles were published in 2022 and 2021 (see Figure 3). Furthermore, the bar chart illustrates a general upward trend in the number of publications addressing security concerns for industries utilizing DT and (I)IoT applications. This trend indicates a growing interest and concern among researchers in the DT and (I)IoT security field and highlights the relevance of this SLR.

Note that the data in the figure of search results obtained on May 14, 2023 contain only 6 papers for the year 2023. Since this number covers less than half a year and considering the trend of published articles from the last 5 years, we expect a further increase in the number of papers by the end of 2023.

3.2.1 | Keyword frequency analysis

To gain a deeper understanding of the trending topics within the 67 selected papers published between 2018 and 2023, a frequency analysis of keywords was conducted. This analysis was performed by extracting keywords that appeared more than three times in the keyword sections of the articles using the VOSviewer* tool. Further filtering and sensitization were applied to create a shortlist of keywords using a thesaurus text file (a text file used by VOSviewer with one column for keywords and another column for replacing words). Keywords that have similar meanings with different spellings and variations were merged. For instance, we replaced "artificial intelligence" and "deep learning" with "machine learning,"

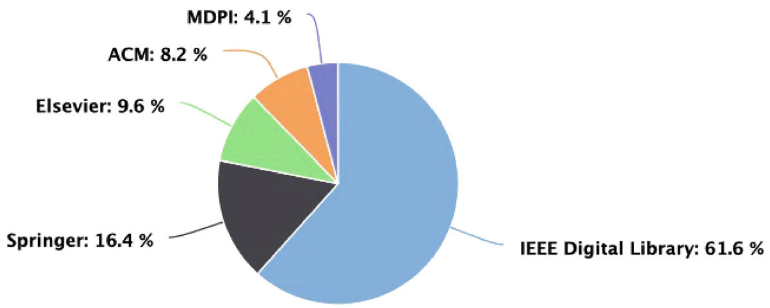

FIGURE 2 An analysis of paper distribution based on publisher.

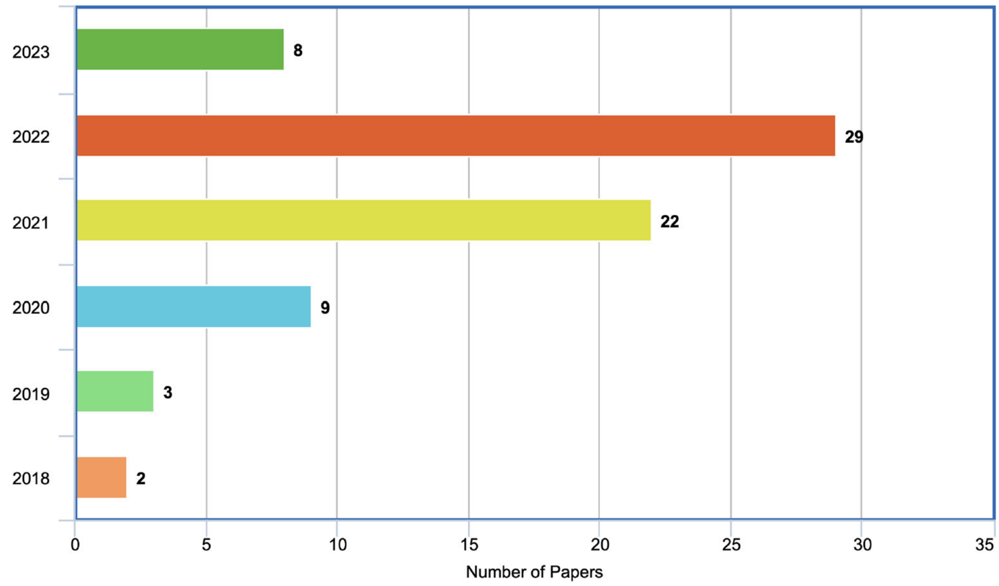

FIGURE 3 Distribution of papers published per year.

and “intrusion detection” with anomaly detection. We also replaced the occurrence of “security” with “cybersecurity.” We combined “control systems” under the term “industrial control system.” “Smart grid” and “power grid” are considered similar concepts. Additionally, we have replaced the term “real-time” with “real-time system.” We considered “emulation” and “simulation” as related concepts hence we used the “simulation” keyword as a representative for “emulation.” The resulting frequency analysis of keywords, illustrated in Figure 4, provides insight into the key themes and concepts that are prevalent in the research topic of DT and cybersecurity. In addition, this analysis can help guide future research by identifying areas where there is a need for further investigation and providing a sense of the current state of the field.

“digital twin” with 55 occurrences indicates the centrality of this concept in this review. “cybersecurity” is the second most frequently mentioned word, indicating the selected papers focus on using DT to provide security services. “iot” is the third a frequent mention word with 19 times mention. This highlights the significant role of this enabling technology in sending and receiving data to and from the DT environment. This analysis identified several key enabling technologies, namely “blockchain(9),” “machine learning(9)” “cloud computing(4)” and “analytics(3).” These technologies are the main driving force of DT to be used as a security tool. Our frequency analysis also revealed the prevalent adoption of DT within Industry 4.0, as evidenced by terms such as “cyber-physical systems(12),” “smart grid(7),” and “industrial control systems(7).” These industry sectors highlight the integration and utilization of DT in critical infrastructure, indicating its role in providing various services including security-related functions. The main security and non-security functions of DT identified from the analysis were “anomaly detection(8),” “network security(6),” and “simulation(9).” This indicates the growing interest in leveraging DT frameworks for proactive security measures (anomaly detection), monitoring and detecting security problems in interconnected networks, and utilizing simulation techniques for testing security measures before they are deployed to real operation environments to avoid accidental failure.

3.2.2 | Keyword co-relationship network

In order to gain further insights into the evolution of research in the field of DT and cybersecurity, a keyword co-relationship network analysis was extracted from the VOSviewer tool. This analysis aimed to identify clusters of related items and visualize the relationships between keywords over time. The results of this analysis revealed that in the early days of research on DT, keywords such as “computational modeling,” “embedded system,” “situational awareness,” “safety,” and “simulation” were frequently mentioned, which suggests that the primary focus of the research at that time

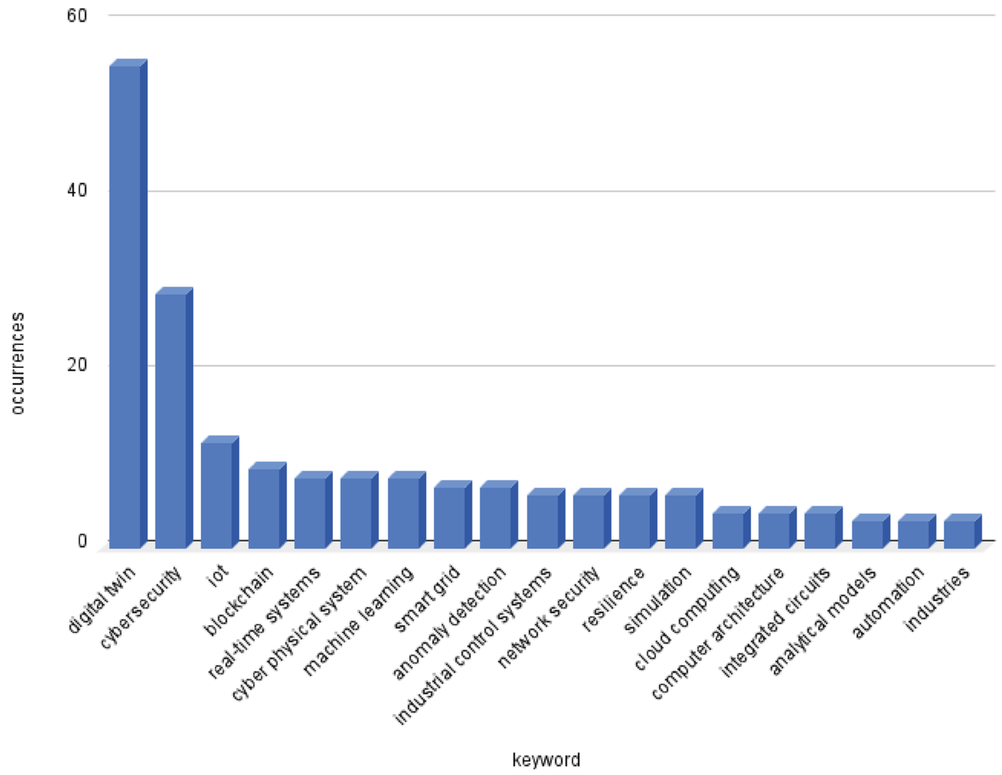

FIGURE 4 Frequency of keywords from keyword section of 67 papers.

was on utilizing DT as a visual aiding tool. On the other hand, more recent research was characterized by the frequent mention of emerging technologies such as "blockchain," "machine learning," "e-learning" "5G," and "emulation" This indicates that the development of DT has shifted towards utilizing these technologies and augmenting DT to provide more service other than used as a model. The analysis of the co-occurrence of keywords in the selected articles, as represented in Figure 5, identified eight clusters. As defined by the VOSviewer documentation, these clusters are groups of terms that exhibit a high degree of relatedness.

- **Cluster one:** This cluster focuses on various aspects related to the industrial and digital domains. It includes topics such as authentication, autonomous vehicles, cloud computing, costs, DT, IIoT, microgrids, real-time systems resilience, and smart manufacturing. The common theme in this cluster appears to be the integration of digital technologies in industrial settings, emphasizing security, efficiency, and advanced manufacturing processes.
- **Cluster two:** This cluster revolves around computer-related topics, computational modeling, computer architecture, and embedded systems. It also includes subjects like CPSs, Industry 4.0, network security, situational awareness, and smart grids (SG). The primary focus here seems to be the intersection of computer science and engineering, with an emphasis on the integration of smart technologies into physical systems and networks.
- **Cluster three:** Cluster three is centered around security and privacy concerns in the digital landscape. It encompasses topics such as blockchain, cyber DT, cybersecurity, data privacy, safety, smart cities, smart contracts, soft sensors, and traffic control. The key theme here is the exploration of secure and privacy-preserving solutions in digital ecosystems, including blockchain technology and data protection measures.
- **Cluster four:** This cluster focuses on topics related to access control, automation, data security, and smart homes within the IoT context. The cluster includes items such as access control, automation, data security emulation, and IoT smart homes. The primary theme revolves around securing and managing access to IoT devices and systems, as well as exploring automation and smart home technologies.
- **Cluster five:** Cluster five centers on industrial control systems (ICS) and security. It includes topics such as ICS, integrated circuits, intelligent control, intrusion detection, machine learning, predictive models, and security-by-design.

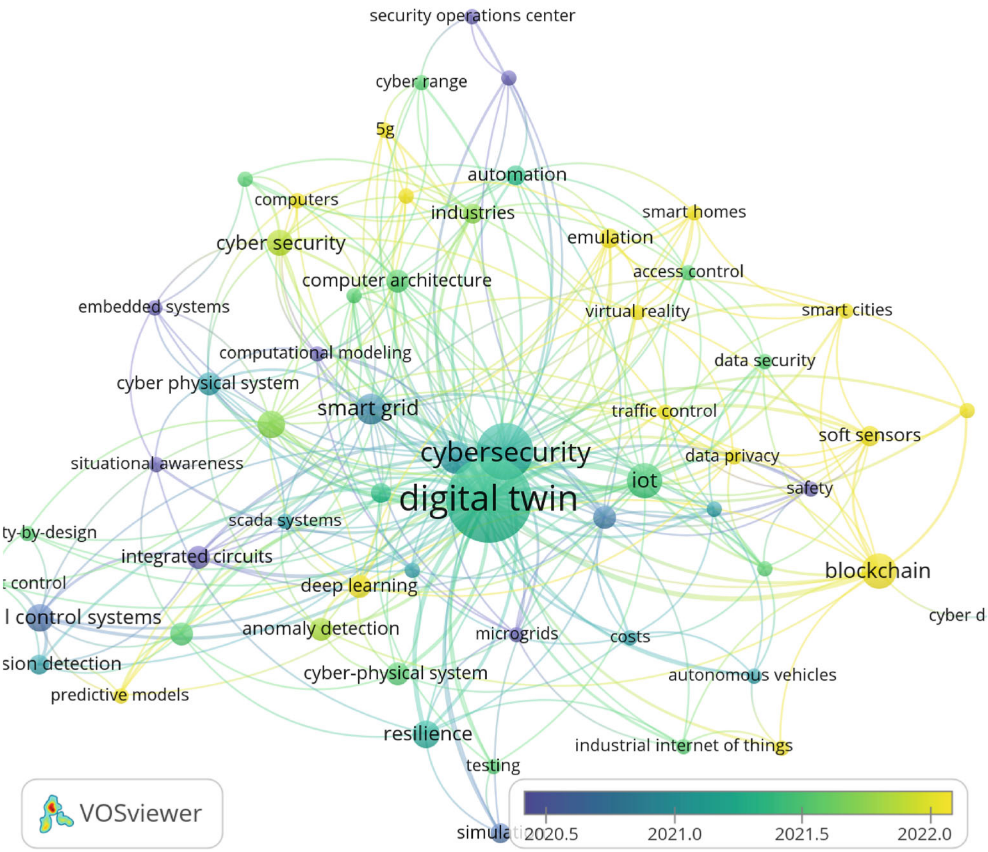

FIGURE 5 Keyword co-relationship from VOSviewer.

The focus here is on ensuring the security and reliability of ICS, incorporating intelligent control algorithms, and leveraging machine learning for intrusion detection and predictive maintenance.

- **Cluster six:** This cluster encompasses topics related to communication networks and security frameworks. It includes items such as 5G, cyber range, industries, pipelines, security framework, security operation center, and wireless communication. The primary theme is the exploration of cyber range for training employees in sectors such as 5g network and security operation center.
- **Cluster seven:** Cluster seven revolves around anomaly detection, CPSs, deep learning, monitoring, and SCADA systems. The focus here is on leveraging advanced techniques such as deep learning and anomaly detection for monitoring and securing CPSs, particularly in the context of SCADA systems.
- **Cluster eight:** Cluster eight is centered around analytical models, simulation, and testing. The focus is on the development and application of analytical models and simulation techniques for testing and evaluating various systems or scenarios.

3.3 | Study selection and refinement

In our SLR targeting DT security in Industry 4.0, our initial electronic database search yielded 727 papers. After applying the inclusion and exclusion criteria outlined in Table 1, we refined this pool to 452 papers. Screening the titles and abstracts led us to include papers specifically addressing the DT's role in securing Industry 4.0, resulting in 83 papers for full-text review. Among these, 16 papers were excluded for various reasons: some lacked relevance to (I)IoT and Industry 4.0, others presented duplicate content or were sourced from non-conference materials like book chapters. Additionally, some studies didn't align with our research questions or lacked an industry use case connection. Following this refinement process, we identified a final set of 67 papers for in-depth data extraction and analysis. Subsequently, we present a comprehensive review of these papers, addressing the two research questions outlined in Section 1.3.

4 | LITERATURE REVIEW RESULT AND ANALYSIS

The primary aim of this literature review is to address two pivotal research inquiries concerning the utilization of DT technology to augment security measures within Industry 4.0. The initial research question sought to identify extant solutions harnessing DT to fortify security within Industry 4.0 use cases, while the subsequent question aimed to discern the mechanisms employed in securing communication between DT and (I)IoT devices. Following the methodology established by Kitchenham and Charter,[8] a three-phase approach was adopted to systematically review the literature. Leveraging automated tools such as Parsif.al for crafting the review protocol, VOSviewer for bibliometric analyses, and Logseq for data collation and facilitating the review process streamlined the execution of this methodology. The initial search spanned across six distinct digital libraries, yielding a total of 727 papers. Subsequently, the application of stringent inclusion and exclusion criteria, complemented by a study refinement phase, meticulously winnowed this corpus down to a final selection of 67 pertinent items germane to addressing the initial research inquiries. To ensure methodological coherence throughout the review process, a structured data extraction form, elucidated in Table 2, was developed. This systematic approach facilitated comprehensive scrutiny of each selected paper, enabling detailed insights into the deployment of DT technology within Industry 4.0 contexts. This systematic approach aimed to offer a comprehensive and meticulous examination of the pertinent literature, providing nuanced insights into the application of DT technology within the purview of Industry 4.0, specifically focusing on augmenting security measures.

4.1 | RQ1: Digital twin as security tool in Industry 4.0

This section aims to answer the first research question of this paper: **How digital twin technology enhances security within Industry 4.0 contexts?** While the integration of operational technology and IT systems in Industry 4.0 heightens cyber attack risks,[9] DT applications offer promising solutions.[10] Our literature review confirms the potential of DTs to strengthen security across various Industry 4.0 sectors, as summarized in Table 3. We classified and analyzed research papers based on target sectors, *digital twin purposes*, *enabling technologies*, *contributions*, and *study types*, revealing a wide range of applications spanning satellite, energy, transport, agriculture, and manufacturing. Enabling technologies such as big data, AI, cloud computing, and blockchain empower researchers to develop security-equipped DT systems tailored for diverse use cases. Contributions were categorized as frameworks, platforms, or architectures, depending on the level of detail provided.[†] Study types varied from theoretical proposals to case-based solutions and experimental evaluations, with experiments often validating practical applicability.[‡] This analysis underscores the versatility and effectiveness of DTs in fortifying security within Industry 4.0 environments.

Note that, the data extracted using extraction form from Table 2 and presented in Table 3 doesn't include data from papers that focus only on securing the data used by DT technology.

4.1.1 | Power grid

Authors in Reference 43 proposed the "Automatic Network Guardian for Electrical Systems (ANGEL)" framework aimed at bolstering the security and resilience of microgrids through real-time data visualization. This framework integrates both cyber and physical layers of microgrids, enabling detection of disparities between simulated and physical systems across various operational scenarios. The bidirectional coupling between simulation and the physical system facilitates continuous improvement of simulations, identification of anomalous changes, and assessment of meter data accuracy, thereby enhancing security measures. The authors suggest that ANGEL could incorporate machine learning algorithms to attain self-healing capabilities, mitigating component failures and cyber-attacks. Despite its potential, the ANGEL framework exhibits limitations such as potential false positives and challenges in detecting certain malicious attacks. Furthermore, it remains under development and has yet to undergo testing on real-world microgrid systems for comprehensive evaluation

In Reference 5 authors introduced an IoT-based DT framework for microgrids, aiming to enhance their resilience against cyber attacks. This framework, implemented as a cloud-based platform, serves as a central hub for networked microgrid systems, modeling both their physical and cyber layers. It employs observer-based What-If scenarios to detect and respond to false data injection (FDIA) and denial of service (DoS) attacks promptly, ensuring

TABLE 3 Digital twin: Use cases, purpose, enabling technology, contribution category, and study type in references.

Reference	Use case	Purpose	Enabling technology	Contribution	Study type
11	Smart manufacturing	Botnet detection	ML and blockchain	Framework	Experiment
12	Smart home	Intrusion detection and prevention	Deep learning (deep Q-network)	Platform	Experiment
4	Healthcare	Vulnerability assessment/testing	-	Framework	Theoretical
13	Automotive	Black-box testing	-	Framework	Theoretical
14	ICS	Attack testing	Analytics	Framework	Experiment
15	CPS	Risk assessment/testing	Cloud computing, network function virtualization (NFV)	Architecture	Theoretical
16	Nuclear plant	Testing	3D modeling, software defined network (SDN)	-	Theoretical
17	Satellite	Simulation	Big data and AI	Platform	-
18	Smart grid	Anomaly detection	Machine learning	Architecture	Experiment
19	Energy	Testing	-	Platform	Case-study
5	Power grid	Anomaly detection	Cloud computing and data analytics	Framework and algorithms	Experiment based
20	ICS	Simulating and testing	Machine learning	Framework	Experiment
10	ICS	Simulation	-	Framework	Experiment
3	CPS	Monitoring, incident handling, testing	-	Framework	Theoretical
21	Water, agriculture	Simulation and testing	Data analytics	Architecture	Case study and experiment
22	Smart grid	Device policy enforcement	-	Architecture	Theoretical
23	ICS	Testing and security assessment	-	Framework	Experiment
2	ICS	Intrusion detection	Machine learning	Architecture	Experiment
24	Automotive industry	-	-	Framework	Theoretical
25	ICS	Testing	-	Framework	Experiment
26	Intelligent transportation	Access control	Edge computing	Architecture	Case-study
27	Enterprise network	Simulation	NFV, big data processing	Platform	Experiment
28	ICS	Testing, vulnerability assessment	-	-	Experiment
29	Smart grid	Detection	Blockchain	Architecture	Theoretical
30	Aerospace	Simulation (attack)	-	-	Case-study
31	Automotive industry	Predictive analytics	-	Platform	-
32	-	-	-	-	Review paper
33	ICS	Intrusion detection	Machine learning	Framework	Experiment
9	-	-	-	-	Review paper
34	Power grid	Model	-	Algorithm	Experiment
35	Intelligent transport system	Testing and simulating	-	Platform	Case-study and experiment
36	Automotive industry	-	Analytics	Framework	Case-study

(Continues)

TABLE 3 (Continued)

Reference	Use case	Purpose	Enabling technology	Contribution	Study type
37	Manufacturing	Simulation testing-training	-	Theoretical	
38	CPS of drones	Simulation	AI—deep learning	Architecture	Experiment
39	Power grid	Situational awareness	Data analytics	Framework	Theoretical
40	Agriculture sector	Anomaly detection	Machine learning	Framework	Experiment
41	Enterprises	-	Analytics	-	Experiment
42	IIoT Network	Simulation, intrusion detection	Blockchain, deep learning	Framework	Experiment
43	Smart grid	Data visualization	-	Framework	Experiment
44	Intelligent transport systems	-	-	Architecture	-
45	Smart grid	Training	-	Platform	Case-study
46	ICS	Intrusion detection	Cloud computing	Framework	Experiment
47	Smart grid	Testing	-	Framework	Theoretical
48	Satellites and space	Penetration testing	-	Framework	Theoretical
49	5G network	Simulation—training and testing	Machine learning	Architecture	Experiment
50	ICS	Data sharing	-	Architecture	Case study
51	Transportation	-	Cloud	-	-
52	CPS	Training	-	Platform	Experiment
53	Automotive industry	Testing	Blockchain	Framework	Use-case
54	Automotive	Threat modeling, testing	Analytics	-	Experiment
55	Transportation	Detection	Machine learning	Framework	-
56	5G network	Detection	-	Framework	-
57	CPS	Anomaly detection	Machine learning	Framework	Case study
58	ICS	Simulation, testing	-	-	-
59	CPS/IoT	Security assessment	AI and modeling and simulation tools	-	Experiment through proof of concept
60	Smart power grid	Vulnerability assessment	MATLAB-SIMULINK, Node-RED	Architecture	Experiment through test-bed
61	Power grid	Security management	Edge computing	Architecture	Theoretical
62	IoT	Vulnerability assessment	Automated adversary emulation *(Caldera)*	Architecture	Experiment
63	Vehicular network/automotive	Anomaly detection	Machine learning, edge computing	Architecture	Experiment
64	CPS	Security-awareness learning training	Machine learning/eXplainable AI	FrameWork	Experiment
65	CPS	Systematic literature review	-	-	Review paper
66	CPS	Simulation	MiniNet	Platform	Experiment
67	CPS	Simulation/anomaly detection	Siemens PLC	Model	Experiment
68	CPS	Survey	Intrusion detection system	Framework	Review paper
69	CPS	Systematic literature review	Augmented reality	Architecture	Review paper

the safe and uninterrupted operation of microgrids. Validation of the proposed framework was conducted using a distributed control system setup and Amazon Web Services (AWS), demonstrating its effectiveness in swiftly detecting and mitigating various cyber attacks. The authors assert that the integration of deep learning and Luenberger observer (LO) techniques enhances the speed, accuracy, and predictability of attack detection. Overall, the IoT-based DT framework offers a practical solution for bolstering the resilience of microgrids against cyber threats. In Reference 34 paper, Hossen et al. propose a knowledge-based self-security algorithm that leverages the inverter's steady-state and dynamic behaviors, determined experimentally, to create a DT. This DT acts as a virtual replica of the inverter and is employed to evaluate incoming power set points for safety before their implementation. The approach's main objective was to safeguard SG from man-in-the-middle attacks. By thoroughly examining incoming commands via the DT before involving the local controller, the method effectively prevents unsafe set points from being implemented.

The study undertaken by authors in Reference 47 focused on providing an overview of smart grid cybersecurity standards and reviews major threats to smart grid environments at the physical, network, and application layers. In this study, the authors argued that despite the prevalence of SG in energy distribution networks, there was a lack of standards for comprehensive security assessment, which is a critical shortcoming. To address this gap, the authors proposed a DTs-based approach for the security testing lifecycle of SG, by accurately modeling the functioning of the physical grid and running security testing on the model without causing disruption. The authors claimed that this approach has the potential to become an important tool for standardization. While the paper presented an innovative framework for security testing, it lacks experimental validation and implementation details for real-event scenarios.

In their study, authors in Reference 22 proposed a methodology to build a cybersecurity DT of a smart grid based on its architectural blueprint. The methodology aims to enable the adoption of Zero Trust Architecture (ZTA) and dynamic enforcement of security policies for devices connected to the grid. The authors presented a novel approach to dynamically align the DT with its real-world counterpart, creating a maintenance-aware model for the smart grid. This was achieved by adopting an architectural view that gets dynamically aligned with the state of the real-world counterpart during deployment and operation time. The authors laid the foundation for a DT model that allows dynamic enforcement of security policies that reflect smart grid topology changes over time. In Reference 39, authors targeted the electrical energy sector to increase the cyber-resilience of critical control infrastructures (CCIs) using a DT implementation to address risks associated with the integration of computational, communication, and physical aspects of CCIs. It seeks to provide increased situational awareness, a common understanding of incidents, and enhanced response capacity to minimize response time and reduce the impact of cyber-attacks on organizations and society. However, the study is limited by the fact that it only focused on the conceptual model, rather than the implementation of the DT, which may require further validation through proof of concepts in different CCI contexts. Nevertheless, this research addressed the needs expressed by key stakeholders in the electrical energy sector and presented design principles that can be applied in disaster management contexts.

A study in Reference 18 presented a deep-learning convolutional neural network (CNN) as a module within the Automatic Network Guardian for Electrical Systems (ANGEL) DT environment to detect physical faults in a power system. The approach uses high-fidelity measurement data from the IEEE 9-bus and IEEE 39-bus benchmark power systems to detect if there is a fault in the power system and to classify which bus contains the fault. The anomaly detection CNN algorithm was able to identify the existence of a fault with near-perfect accuracy and classify the location of the fault with an accuracy of nearly 95% for both systems. The long-term goal of this project was to have the DT with the anomaly detection CNN running alongside the physical smart grid. However, the study's limitation is that, due to the small timescales present in power systems, the inference speed of the network will be of critical importance. For real-time implementation, more powerful hardware would be beneficial to the overall performance of the integrated system. Despite this limitation, deep learning algorithms show significant promise in the detection and location of power system faults and can improve performance and reduce the cost of power distribution. To overcome limitations in security studies of SG in physical test beds, authors in Reference 45 built a digital power twin that enables the deployment of real-world attacks and countermeasures while allowing easy modification of components and configurations. The tool presented by the authors, named EPICTWIN, a DT for a power physical test-bed, allows users to validate the security and safe operation of critical components in a more realistic environment, reducing the gap between physical and simulated test-bed environments. They claim their tool provides an attacker designer (AD) and attack launcher (AL), that enable researchers to validate and improve defense mechanisms even without expertise in offensive security testing. Finally, the authors highlighted the uniqueness of their contributions in building a DT of an existing cyber-security test bed, presenting a procedure that can be extended to any type of system, and providing unique tools for launching systematic attacks on the twin.

In Reference 61, the author's contribution lied in proposing a security management and control model for the power grid DT using edge computing technology. They highlighted the increasing demand for power grid security and the vulnerabilities posed by edge computing and DT technologies and constructed a power grid DT security control model, consisting of five layers: application layer, function layer, model layer, data layer, and physical layer. This model aims to ensure all aspects of the power grid are protected, allowing for efficient and safe operation in a technology-driven environment. The authors emphasized the importance of data layer security due to the risk of data loss and tampering in the power grid context. They also discussed the mutual coupling between physical entities and virtualized objects in the power grid DT's physical layer, supporting practical applications like equipment detection, fault alarm, and maintenance planning. The authors in Reference 60 proposed a hybrid digital twin (HDT) system for cyber security analysis in SG and other CPSs. The HDT system comprises a MATLAB-SIMULINK digital model representing the physical system and multiple single-board computers representing the cyber components. The DT was used in this research to identify the cyber-security vulnerabilities in SG and other CPSs. The HDT can replicate real industrial hardware and network components by establishing highly configurable, low-cost, and scalable prototypes. The paper describes the HDT architecture and communication system design, including network segmentation using a configurable network switch and communication protocols using Node-RED. Performance evaluations showed acceptable results for communication between digital and physical models and among network components. The HDT offers a platform for conducting cyber-security analyses in complex CPSs, addressing the challenges in securing power grids and other critical infrastructure.

4.1.2 | Smart factory

In their paper,[29] authors aimed to investigate the evolution of DTs within smart grid infrastructures and their role in implementing intelligent authorization policies. The authors explore the application of AI technologies, such as machine learning and blockchain, in DTs to manage dynamic information flows and detect real-time cybersecurity issues. They conduct a comprehensive analysis of mid-term and long-term challenges facing DTs, delineating a three-stage evolution process from basic monitoring systems to advanced, self-learning platforms. This study's contribution lies in forecasting the future of SG through DT evolution, highlighting significant challenges ahead. The authors predict that DTs will play a pivotal role in advancing electricity grids towards decentralized and autonomous models governed by intelligent authorization systems. However, they emphasize the need for standardization, information security efforts, and in-depth research into machine learning applied specifically to critical infrastructures and smart cities. In Reference 19 authors aimed to develop a low-cost real-time DT (RTDT) of an interconnected and distributed residential energy storage system (RESS) controlled and monitored via cloud-based energy management system (CEMS). They aimed to analyse the cyber-security of such systems and develop appropriate intrusion detection systems against cyber attacks. The proposed RTDT allowed for flexibility in modifying, scaling, and replicating the system without compromising its real-time fidelity. The development procedure could be easily replicated to develop RTDT of any CPS or micro-grid test-beds. The paper presented a systematic procedure for the development of the RTDT and verified its performance through an experimental case study. The RTDT was developed using a low-cost single-board computer with Simulink Desktop Real-Time, which reduced overall development costs. Overall, the paper presented a reliable and economical solution for cyber security studies on RESS through the development of an RTDT.

Authors in Reference 11 proposed a secure blockchain-enabled digital framework for the early detection of botnet formation in a smart factory environment. The proposed framework integrates a DT, a packet auditor (PA), deep learning models, blockchain, and smart contracts (SC) for securing the data flow of a smart factory environment. The DT was designed to collect device data and inspect packet headers for connections with external unique IP addresses with open connections. Data is synchronized between the DT and the PA for detecting corrupt device data transmission. Smart contracts-based DT and PA authentication were used to ensure malicious nodes do not participate in data synchronization. Botnet spread was prevented using DT certificate revocation. A comparative analysis with existing research showed that the proposed framework provides data security, integrity, privacy, device availability, and non-repudiation. In Reference 37 proposed innovations in cognitive modeling and co-simulation to address limitations in existing DT approaches within the context of Industry 4.0. While current methods often focused on specific manufacturing assets and overlooked human factors and interdependencies, the authors advocated for a holistic DT approach. This approach tried to model the entire manufacturing process, including external network dependencies, rather than individual assets. Additionally, the authors introduced methods for integrating models of human behavior and capabilities for security testing with DTs. They argued that this holistic approach enabled new services for optimizing and enhancing the resilience of factories of the future.

4.1.3 | Health

Authors in Reference 4 proposed an automated framework aimed at enhancing cybersecurity in IoT-based healthcare applications using DT technology. The framework incorporates innovative healthcare security techniques such as system modeling, traffic and attack generation, impact assessment, attack response strategies, and cyber-attack prevention processes. The authors explore the feasibility of DT for preventing cyber-attacks and present a strategic approach to cybersecurity enhancement. Their framework facilitates the updating of access control policies, resolves known vulnerabilities and threats, and offers an automated cybersecurity solution. However, it is important to note that this research is theoretical and requires validation through experiments and simulations. The authors concluded that DT is a valuable tool for enhancing cybersecurity in healthcare systems, as it enables analysis, design, and optimization of systems to enhance accuracy, speed, and effectiveness. Additionally, it can simulate security breaches and develop decision-making strategies and mitigative responses to simulated cyber-attacks.

4.1.4 | Smart home

Authors in Reference 12 proposed a novel digital-twin-based security framework, CommandFence, to protect smart home systems from malicious and benign apps with design flaws or logical errors that may cause harm to the user when executed. The framework used an interposition layer to interpose app commands and an emulation layer to execute these commands in a virtual smart home environment and predict whether they can cause any risky smart home state when correlating with human activities and environmental changes. If a sequence of app commands can potentially lead to a risky consequence, they are treated as dangerous, and the framework drops them before any insecure situation can occur. The authors fully implemented the CommandFence framework and tested it on 553 official SmartApps on the Samsung SmartThings platform, 10 malicious smartApps,[70] and 17 non-malicious SmartApps with logic errors.[71] The experiment successfully identified 34 potentially dangerous SmartApps out of 553 official SmartApps, and 7 out of 10 malicious SmartApps, and achieved 100% accuracy for the 17 non-malicious SmartApps with logic errors. CommandFence is orthogonal to the well-received permission-based access control mechanisms and can be implemented as plug-in software without any hardware upgrades.

4.1.5 | Transportation

The authors in Reference 26 proposed an innovative edge-centric access control framework tailored for IoT environments, leveraging Tag Based Access Control (TBAC) techniques. This architecture utilizes DTs to dynamically assign tags, thereby segregating data and restricting access exclusively to authorized users and applications. Notably, the architecture prioritizes lightweight implementation, facilitating low-latency and real-time security measures while enhancing system security and efficiency by minimizing data sharing and providing individualized access to data subsets. The study showcased the efficacy of TBAC in smart settings like manufacturing and internet-connected vehicles. Additionally, a DT-based tool named Testing and Simulation (TaS) was introduced in Reference 35 to streamline testing and simulation processes in IoT environments, aiming to enhance testing methodologies and assess the potential impact of IoT systems on the physical domain. TaS facilitates both functional and nonfunctional testing, enabling the detection and prediction of failures in evolving IoT ecosystems. Validation experiments within the H2020 ENACT project demonstrated the tool's utility. A notable contribution of the paper is the design of a tool enabling real-time linkage between the physical system and a new software version deployed in the DT, ensuring that code modifications do not compromise existing software functionality. While TaS automates various testing procedures, the study acknowledged limitations in testing scenario generation that warrant further improvement. The authors in Reference 55 proposed a framework that utilizes DT in the context of a Vehicular Ad-hoc Network (VANET) to identify and prevent malicious nodes. They employed machine learning techniques to distinguish between normal and attack traffic. The physical road side unit (RSU) parsed IP addresses from incoming packets and compared them against a blacklist. The packet was considered malicious and discarded if its IP address matched the blacklist. The approach demonstrated a high F-1 score, indicating its effectiveness in detecting malicious nodes in VANET. Thus, the combination of DT, machine learning, and blacklist-based filtering proved valuable for the detection and prevention of malicious nodes in the VANET infrastructure.

4.1.6 | Automotive industry

In Reference 36, authors proposed a standard framework for the creation of vehicular DTs that streamlines data collection, processing, and analytics. The authors also highlighted the importance of DT security through a case study that showcases how hackers, potentially leading to collisions, can alter radar sensor readings. The paper concludes by providing insights into the implementation of DTs in the autonomous vehicle industry and addressing privacy, safety, security, and cyber attack mitigation. Authors in Reference 31 presented research focusing on autonomous vehicles to address safety and security concerns in connected cars and autonomous driving. Within the scope of IoT4CPS, they provided guidelines for securely integrating IoT into autonomous driving. The authors outlined three primary steps for designing DTs to mitigate security vulnerabilities in autonomous driving. First, they proposed identifying assets, modeling them, and defining security and safety objectives. Second, they suggested designing security and safety evaluation metrics. Lastly, they recommended performing threat modeling and test case demonstrators based on security and safety risk assessment and forecasting. A study by Marksteiner et al.[13] which was funded by the Austrian Research Promotion Agency (FFG) and the ECSEL Joint Undertaking, with support from the European Union's Horizon 2020 program, proposed an automated approach for cybersecurity testing in a black box setting. The methodology combines pattern-matching-based binary analysis, translation mechanisms, and model-checking techniques to generate meaningful attack vectors with minimal prior knowledge of the tested system. It is designed to meet the security requirements outlined by UNECE regulation R155[72] for vehicular systems. In Reference 24 authors introduced a conceptual framework called the vehicular DT (VDT), designed to aid in the fusion, calculation, and communication of data in autonomous vehicles (AVs). The VDT, which is stored on the cloud, is constantly updated in real-time to match the AV it represents. It can also connect with other DTs to obtain necessary information. To maintain secure communication between the AV and the DT, the authors proposed an authentication protocol that combines the secret handshake scheme and group signature. This protocol provides anonymity for honest members while allowing for traceability if necessary, and also ensures the authenticity of messages sent between the AV and the DT. The result of the performance analysis showed that the authentication protocol had less computational cost while satisfying necessary security requirements effectively. The authors introduced a framework named trusted twins for securing cyber-physical systems (TTS-CPS) in Reference 53. This framework utilizes blockchain-based DTs to enhance the security of CPSs. The primary objective of the TTS-CPS framework is to ensure the trustworthiness of data generated according to DT specifications by employing integrity checking mechanisms (ICMs). The authors contend that this framework contributes to establishing a deeper understanding and confidence in the decisions made by underlying systems by storing and retrieving Safety and Security (S&S) rules from the blockchain. The feasibility of the TTS-CPS framework was demonstrated in the paper through its implementation in an assembly line within the automotive industry. This prototype supported simulated network topology, programmable logic controllers (PLCs), human machine interfaces (HMIs), and physical devices. While authors in Reference 63 proposed a new approach called digital twin vehicular edge networks (DITVEN) to enhance security in vehicular networks. They suggested using DTs, to capture their characteristics and detect anomalies. To ensure network safety, the approach includes a distributed trust evaluation system (to ensure the credibility of DTs), mutual trust evaluation, and anomaly detection techniques, and it considers the cooperative context for interaction between physical and digital twin vehicles. In Reference 54 authors from Siemens addressed the challenges posed by the increasing connectivity and complexity of modern vehicles as they progress towards full autonomy level 5.[73] The paper emphasized the importance of cyber security and threat modeling in this dynamic landscape, where security threats are constantly evolving. To facilitate effective cybersecurity testing, the author presented an automotive cybersecurity testbed that includes a car simulator, onboard network simulator, FPGA system, and real car's instrument cluster. Additionally, the Siemens PAVE 360 Platform was introduced as a DT environment for comprehensive testing of vehicle systems under various conditions. The ultimate goal was to achieve full autonomy and ensure both safety and security against present and future cyber attackers.

4.1.7 | Water treatment

The authors in Reference 21 introduced an approach for the integration, verification, and validation of security in IoT devices. The approach is based on the DT concept and involves creating a comprehensive virtual representation of a physical device, composed of black box and white box models at different abstraction levels. By using this approach, the cost impact of adding security to physical devices is reduced, while still ensuring the security and functionality of the device. This approach provides a new way to think about integrating security in the IoT and has the potential to improve the overall security and efficiency of connected devices. To validate their approach they conducted two use case studies based on the H2020 critical infrastructure of water management project.

In Reference 66, the authors presented a novel DT solution named the Digital HydrAuLic SIMulator (DHALSIM) designed for water distribution systems. They addressed the limitations observed in existing DT solutions, which often focused on individual aspects such as physical processes, control logic, or network communication. DHALSIM set itself apart by offering a comprehensive representation that simulates hydraulic processes, control protocols, and network communication simultaneously. The key innovation lied in the integration of the Water Network Tool for Resilience (WNTR) hydraulic simulator and MiniCPS—an industrial network emulator—within a co-simulation environment. This integration enabled DHALSIM to provide a realistic emulation of water distribution systems, incorporating both the physical and cyber elements. Notably, DHALSIM was demonstrated on the C-Town benchmark case study, where the authors conduct cyber-attack experiments to validate its capabilities.

4.1.8 | Space industry

In Reference 30, the authors emphasized the application of DTs in the aerospace manufacturing sector, particularly within Airbus Defence and Space factories integrating the IIoT. Through a case study, they illustrated how simulation solutions based on DTs could simulate attacks and devise countermeasures without disrupting manufacturing operations. The study demonstrated that DTs could effectively contribute to enhancing cybersecurity while implementing connected and collaborative manufacturing practices. while in Reference 48 authors proposed a method to enhance the detection of cybersecurity issues in satellite communication using runtime verification based on DTs. The method involves monitoring and evaluating software or hardware systems against user-defined properties, employing state synchronization and encryption for secure communication between the physical and DT. However, the framework has some limitations, such as insufficient discussion on security protocols for secure communication and the absence of security and performance analysis. In Reference 17, the authors introduced the concept of characteristic hyper-large scientific infrastructures and evaluation indicators for traditional large scientific infrastructures. To address security risks in the space Internet, they proposed constructing a hyper-large scientific infrastructure called Space Spider, simulating the entire life cycle of the space internet and establishing a system for space internet attack and defense. Additionally, they introduced Spiderland, an open experimental platform for studying space internet applications and security.

4.1.9 | Enterprise network

Authors in Reference 27 suggested a digital twin cyber platform based on NFV (DTCPN) address the challenges in developing large-scale networks, such as complex network management and operation, and high risk and overhead of on-the-fly optimization of product network. The DTCPN combines the advantages of DT and NFV technology to eliminate complex and inaccurate modeling processes, support real-virtual interaction, and provide high fidelity. The platform was designed to facilitate the design, analysis, testing, and evaluation of network technologies and devices in a rapid, accurate, and efficient way. The article concluded that DTCPN has technical advantages that can play a significant role in network security, network management, and network applications. Further optimization and enrichment of the DTCPN's design and functions were planned for the future.

In Reference 41, the authors proposed a novel method for automatically gathering and prioritizing security control requirements (SCRs) for rapid risk reduction in active networks. It introduced a cyber DT, based on attack graph analytics, that associates network information with attack tactics, evaluates the efficiency of implemented SCRs, and automatically detects missing security controls. The paper presented a framework and methodology to construct a contextual cyber DT, rank the risk impact of security controls, and prioritize SCRs to reduce risk impact as quickly as possible. The paper also provided visualizations of a field experiment conducted via an active network, demonstrating successful results in reducing cyber impact and identifying missing security controls for future implementation. The proposed cyber DT simulator offers several new risk reduction methods for automatically selecting SCRs and can be used as a valuable tool for existing cybersecurity evaluation and future cybersecurity budget proposals.

4.1.10 | ICS/CPS environment use case

Research in Reference 33 introduced a DT-based security framework for ICS that can simulate attacks and defense mechanisms. Four process-related attack scenarios were tested on an open-source DT model of an industrial filling plant. The study proposed a real-time intrusion detection system based on a stacked ensemble classifier that combines predictions from multiple algorithms. This model outperformed previous methods in terms of accuracy and F1 score, detecting intrusions in close to real-time (0.1 s). The proposed framework extends the capabilities of an existing ICS DT framework with an ML-based IDS module and provides a platform for developing intrusion detection and prevention systems. In Reference 44 authors discussed the use of DT technology to improve the cybersecurity of critical infrastructures. The paper presented a cybersecurity view that can be derived from an enterprise architecture (EA) approach to cybersecurity. This view facilitates the identification of adequate cybersecurity measures for the system while improving the overall system design. The methodology proposed in this paper can be applied to the whole system life-cycle: from design/construction to production/exploration and phaseout. The paper addressed two main challenges: the custom-built nature of industrial automation and control systems (IACS) and the impedance between the EA models used in industrial automation and the models used in visual threat modeling. To address these challenges, the paper proposed the adoption of a reference architecture framework suitable for IACSs and uses a set of rules to build a cybersecurity view of IACS that is amenable to translation into a visual threat modeling language. The practical usefulness of the proposed methodology was demonstrated through two real-world use cases: the Cooperative Intelligent Transport System (C-ITS) and the Road tunnel scenario.

While in Reference 23, authors discussed the security issues of ICSs and proposed an approach for introducing security-by-design system testing with the help of a DT. The authors argued that proper system testing can reveal the system's vulnerabilities and provide remedies and that security measures should be carried out as early as possible, especially to render systems secure by design. The authors implement a DT representing a pressure vessel and demonstrate how to carry out each step of their proposed approach, identifying vulnerabilities and showing how an attacker can compromise the system by manipulating the values of the pressure vessel with the potential to cause over-pressure, which, in turn, can result in an explosion of the vessel. Overall, the DT presented in this study is a tool for security-by-design system testing in ICS. In another study,[58] the same authors discussed the challenges and opportunities presented by Industry 4.0 (I4.0) concerning industrial security. As traditional operational technology (OT) systems are increasingly integrated with general-purpose IT systems, which creates novel attack vectors in industrial ecosystems, the author argued that I4.0 technologies, such as DTs, can contribute to industrial security by providing virtual entities that represent physical industrial systems. They also added that the DTs offer opportunities for security, such as simulation and replication of system behavior, and can play an important role in mitigating and avoiding risks associated with critical infrastructures. They also claimed that DTs can provide comprehensive information about the asset's status, history, and maintenance needs, and can support an immediate reaction to security incidents. In conclusion, the author suggested that DTs can be an important tool to strengthen industrial security in the context of I4.0.

To enhance cyber-situation awareness for operators, authors in Reference 3 proposed a digital-twin cyber situational awareness framework for CPSs. The paper built upon and extended the previous research on leveraging the digital-twin concept for securing CPSs. The proposed framework provides advanced monitoring, inspection, and testing capabilities that support the operations staff in gaining situation perception, comprehension, and projection. In addition, the proposed framework enables real-time visualization and a repeatable, thorough investigation process on a logic and network level. The technical use cases illustrated the added value of the proposed framework for improving cyber situational awareness regarding CPSs, such as risk assessment, monitoring, and incident handling. However, the paper acknowledged that further development effort is required to improve the visualization of DTs and to complete the record-and-replay feature.

Also authors in Reference 14 proposed a security framework that leverages DT-based security simulations to enhance Security Operations Center (SOC) and Security Information and Event Management (SIEM) systems in mitigating the expanding attack surface in industrial environments. The authors demonstrated how the framework can simulate attacks, analyze their impact on virtual counterparts, and create technical rules for implementation in SIEM systems. The framework generally comprises five activities: asset modeling, attack modeling, simulation execution, result analysis, and action implementation. The paper concludes by highlighting the contribution of the proposed framework to SOC security strategies and suggests future work to evaluate its effectiveness and performance. Additionally, the authors recommended extending the framework to integrate with cyber threat intelligence (CTI) to provide more utility to SOC analysts. The work in Reference 15 presented the implementation of a DT for industrial networks to facilitate cyber-security testing and validation without interfering with the real CPS. The proposed methodology involves the use of technologies such as Cloud Computing and Network Function Virtualization (NFV) and is supported by the ETSI NFV Management and Orchestration (MANO) framework to automate the deployment of the DT. The authors described the different steps involved in the lifecycle management of the DT, which included the preparation phase, commissioning phase, operation phase, and de-commissioning phase. The paper also included a quantitative evaluation of the time needed to perform these actions. Overall, the paper highlighted the potential of DT technology in addressing cyber-security concerns in CPSs. Authors in Reference 2 introduced an off-premises approach to designing and deploying DTs for securing critical infrastructures. The proposed solution involved the use of high-fidelity replicas of programming logic controllers (PLCs), which provide a faithful environment for security analysis and evaluation of potential mitigation strategies. The authors highlighted that while on-premises implementation can be costly, DTs offer a reliable option for security analysis and evaluation. However, adapting security and safety monitoring mechanisms to synchronize with the DT replica can be challenging. To address this issue, the paper presented an off-premises approach that uses real-time, high-fidelity emulated replicas of PLCs along with scalable and efficient data collection processes. The approach included the development and validation of Machine Learning models to mitigate security threats such as Denial of Service (DoS) attacks. The results of the experiments demonstrated that DTs provide a faithful environment for security analysis and evaluation of potential mitigation strategies against high-impact threats such as distributed DoS attacks.

The use of DTs as security enablers and data sharing for Industrial Automation and Control Systems (IACS) was discussed in detail by authors in Reference 50. They identified design-driving security requirements for DT-based data sharing and control and proposed a state synchronization model to meet these requirements. They also evaluated the security and performance of the proposed architecture through a proof-of-concept implementation with a programmable logic controller (PLC) software upgrade case. The paper concluded that a DT-based security architecture can be a promising way to protect IACS while enabling external data sharing and access, but further research is needed to fully implement and evaluate the proposed architecture. Motivated by the increasing connectivity of ICS which makes them more vulnerable to cyber attacks, authors in Reference 20 proposed a DT-based solution consisting of two parts: attack detection and attack classification. The intrusion detection mechanism uses a combination of a Kalman filter is used to estimate the correct signals of the system and remove the destructive effects of attacks and noises, which helps detect the occurrence of attacks. Support vector machine is then used for the classification of the system's state as normal, scaling attack, or Ramp attack. The proposed anomaly detection algorithm was evaluated through Matlab simulation. authors in Reference 46 proposed a similar security framework to prior work[20] for ICS to address the vulnerability of these systems to cyber attacks, particularly when controlled over the cloud. Like their prior work, their proposed framework consisted of two parts: attack detection and attack mitigation. The detection part was an intrusion detection system that was deployed in the digital domain, which can detect attacks in a timely manner. To mitigate the effects of attacks, a local controller was added to the factory floor close to the plant. The research paper also evaluated the proposed security framework using a real test bed, which showed that it can detect attacks on a real system in a timely manner and keep the system stable with good performance even during attacks. A study in Reference 28 proposed the use of DTs in ICS to enhance security testing, vulnerability assessment, and penetration testing at low cost and without disrupting operational physical systems. The authors identified key challenges to ICS security, including the convergence of IT and OT, supply chain insecurity, and the difficulty of OT security testing due to operational disruption. The study presented a proof-of-concept system involving a programmable logic controller (PLC)-based bottle-filling system. The authors suggested future directions such as creating additional modular DTs for various environments, expanding the DT testbed for more elaborate ICS integrations and security testing, and automating the process of creating security scenarios for the effective utilization of DTs in security training and education.

A framework that utilizes DT as a simulation tool to generate cyber threat intelligence (CTI) which can provide valuable threat information for organizations to improve their security postures, is presented in this study.[10] By combining a general CTI process with DT security simulation capabilities, the authors demonstrated the successive steps using the

STIX2.1 standard and provided utility tools to assist the CTI generation process. They also conducted an attack simulation with a prototypical DT application to evaluate the framework and provide tool-based guidance on the CTI process steps. The experimental results show that STIX2.1 CTI reports can be systematically constructed and customized according to the use case.

A paper in Reference 25 suggested a method for creating a cost-effective DT for testing ICS environment. The proposed method consisted of two modules: a problem builder that takes facts about the system under test and converts them into a rule set that reflects the system's topology and digital twin implementation constraints; and a solver that takes these inputs and uses 0–1 nonlinear programming to find an optimal solution (i.e., a DT specification), which satisfies all of the constraints. The proposed method maximizes the impact of the DT within budgetary limitations by evaluating the number and types of security penetration tests that it supports. The cost of a test is determined by the costs of the participating components (i.e., the direct cost of implementing them in the DT), as well as the test's execution costs (e.g., security expert's time/salary). The output of the proposed method specified the DT configuration, that is, which components of the ICS should be implemented and at which implementation level. Authors in Reference 57 proposed anomaly detection digital twin based on LATTICE[§] approach, which is an extension of the ATTAIN[¶] method proposed in the authors' previous work. LATTICE introduces curriculum learning to optimize the learning paradigm of ATTAIN. It attributes each sample with a difficulty score and feeds it into a training scheduler, which samples batches of training data based on these difficulty scores. This allows the model to learn from easy to difficult data. The authors also used five publicly available data sets collected from five real-world CPS test beds including water treatment and gas pipeline to evaluate LATTICE and compare it with three baselines and ATTAIN. Additionally, the authors built the digital twin model (DTM) as a timed automaton machine and used GAN as the backbone of the digital twin capability (DTC) to provide ground truth labels to improve the anomaly detection capability of LATTICE. While the work in Reference 52 demonstrated the development and implementation of a DT-based cyber range for Security Operations Center (SOC) analysts. The cyber range provides a virtual training environment where analysts can engage in a realistic simulation of an industrial system and practice detecting various attacks using a SIEM system. The study included a user evaluation, which shows a significant increase in knowledge about SIEM-related topics among the participants, along with positive feedback on the learning experience. The proposed cyber range concept utilized a modular architecture and microservice infrastructure, offering flexibility for future extensions and component replacements. This work addresses the demand for skilled cybersecurity analysts by providing an effective training solution. In Reference 59, the authors proposed and recommended the utilization of DT to enhance the cyber resilience of CPSs in Critical National Infrastructure (CNI). They suggested that DT could be combined with a cyber range to analyze how the system behaved under attack. The DT was also able to execute attacks to demonstrate resilience metrics, aiding in designing security and safety mechanisms for CPSs. The authors also presented a proof-of-concept for holistic cyber resilience testing using DT at the port of Southampton, integrating cyber standards and security descriptors with emerging modeling techniques to effectively represent the impact of cyber-attacks and resilience efforts. Consequently, the paper proposed that integrating cyber modeling and simulation with DTs and methodologies for characterizing threat sources could result in cost-effective security and resilience assessments. Authors in Reference 64 developed the sEcuriNg dIgital twins through GaMification Approach (ENIGMA) offers a gamification-based solution to DTs security challenges. The main contribution is the development of the ENIGMA framework, utilizing gamification principles for DT security assessment. This framework incorporates artificial intelligence/machine learning (AI/ML) and eXplainable AI (XAI) with SHAP values for transparency. While recognizing limitations in replicating DT functionality, limited validation datasets, and reliance on simulated data, the authors propose potential future directions. These include exploring hybrid attack scenarios, enhancing gameplay in a multi-stage environment, transitioning to a metaverse-supported platform, integrating with Industry 5.0 vision, evolving into an adaptive gamification platform, and investigating variable fidelity DTs for proactive security.

In Reference 67 the authors of this paper address the issue of cyber attacks on industrial plants and propose a solution utilizing a DT for detection and localization. The DT encompasses a representation of the nominal plant behavior, employing differential-algebraic equation systems or discrete state models. Through online simulation of the nominal behavior concurrently with the actual process, deviations are identified, and attacks are detected. Localization is achieved through root-cause analysis based on the plant model. The demonstrated implementation on a small-scale industrial prototype highlights the feasibility of using simulation-based DTs to detect manipulations in automation and control systems, communication networks, field devices, and processes. The contribution can be categorized as a model, specifically a physics-based, scalable behavior model for cyber attack detection, with a focus on the dynamic aspects of the system. The method offers advantages over traditional detection schemes by capturing both static and dynamic aspects and providing robust detection at the process level. However, practical issues, such as the lack of cyclic state updates from the real process, scalability limitations in root cause analysis, and securing the DT against attacks, are acknowledged. Future research directions include distinguishing attacks from malfunctions, assessing appropriate countermeasures, and extending commercial virtual commissioning environments for algorithm execution and real-time updates. In Reference 68 the authors delved into the challenges posed by the Industry 4.0 paradigm, emphasizing the exponential growth of cyber-attacks as physical systems become interconnected with the cyber world. The paper reviewed existing cybersecurity research on CPS in virtual environments and identifies four challenges in the current state-of-the-art research. Recognizing the potential of DT technology in addressing these challenges, the authors proposed its use in creating virtualized systems with high fidelity, thereby lowering the entry barrier for cybersecurity research on CPS. The contribution is characterized as a framework, as the authors plan to develop a DT system to address the identified challenges. The proposed framework involves three components: DT, representing plant components and the control system; a physical system; and a security brain. The DT operates in simulation and synchronization modes, allowing the flow of data between the real and virtual worlds. The authors envision future work focusing on developing a high-fidelity DT framework and implementing a DT-based intrusion detection system using Tecnomatix from Siemens. while in the authors explored the combined application of augmented reality (AR) and DT in the context of the industrial revolution driven by the IoT and CPSs. Analyzing academic literature, the authors identified monitoring, education, and analysis as key areas where AR was applied with DT, with the manufacturing sector leading in implementation, followed by education and other sectors like energy. Existing approaches predominantly used proprietary architectures but could be generalized using a layered architecture comprising a physical layer, DT, an application layer, and AR. The study suggested the potential of AR-powered DTs in improving cybersecurity, particularly in the context of CPSs. The combination facilitated real situational awareness by integrating physical situations with insights derived from DT data, enhancing human domain knowledge integration into security measures. The authors proposed a conceptual architecture for integrating AR and DT with existing security mechanisms. However, they emphasized the importance of securing AR for DTs, as unauthorized access could have posed serious threats to confidentiality and become an existential threat for companies. Despite being in its early stages, the research indicated significant potential for progress in cybersecurity through the combination of AR and DT.

4.1.11 | 5G and communication network

Authors in Reference 56 introduced and proposed the application of DT technology to establish essential security functions and develop an automated solution for provisioning security capabilities within 5G network slices. The objective was to attain adaptable and KPI-driven provisioning of security measures for network slices. Utilizing DT technology, the study advocated for the creation of a virtual replica of the network slice, facilitating the monitoring and administration of security functions. This methodology enabled the autonomous provisioning of security capabilities that matched the distinct requirements and key performance indicators (KPIs) of each network slice. Ultimately, the intention was to enhance the security of 5G network slices by dynamically adjusting security measures according to their performance objectives and attributes.

To address the shortage of skilled cybersecurity experts in the context of 5G networks, authors in Reference 49 introduced a cyber range called SPIDER. It was based on three main pillars: cyber security assessment, training of cyber security teams to defend against complex cyber-attack scenarios, and the evaluation of cyber risk. The cyber range replicated a customized 5G network and allowed hands-on interaction, information sharing, and feedback gathering from network equipment. Its aim was to assist 5G security professionals in enhancing their ability to collectively manage and predict security incidents, complex attacks, and vulnerabilities. The platform utilized advanced network orchestration, log-processing data pipelines, cyber risk assessment frameworks, and applied machine learning techniques to support its learning objectives.

4.1.12 | IoT/IIoT network

To improve communication security and data privacy for the DT powered IIoT network, Kumar et al.[42] introduced a framework that combined blockchain and deep learning. They presented a new DTM that could simulate and replicate security-critical processes in a virtual environment, alongside a blockchain-based data transmission scheme that used smart contracts to ensure data integrity and authenticity. They also presented a Deep Learning scheme that utilized the Long Short-Term Memory-Sparse AutoEncoder (LSTMSAE) technique to extract spatial-temporal representation and the Multi-Head Self-Attention (MHSA)-based Bidirectional Gated Recurrent Unit (BiGRU) algorithm to detect attacks. The practical implementation of the framework demonstrated a significant enhancement in communication security and data privacy for the DT empowered (I)IoT network.

A study by Ewout Willem and Mohammed El-Hajj[62] showed the potential use of DTs and Automated Adversary Emulation (AAE) to enhance the privacy and security of data in IoT applications. The study didn't target a specific industry sector. However, they proposed a framework to improve IoT device security by integrating DTs and AAE, which could be relevant to various industries that utilized IoT devices. The authors provided a proof of concept for this framework and described their methodology for setting up a DT of an IoT device, using the AAE tool MITRE CALDERA and the *precomp* plugin to execute repeatable, autonomous attacks. They demonstrated the potential of automated penetration testing on a cyber digital twin of an IoT device, showcasing the creation of automated attack patterns targeting software configuration weaknesses.

4.1.13 | Drone network

To improve the security of the CPS drone network, Wu et al.[38] studied the utilization of DT as a simulation aid with deep learning. The authors presented an attack prediction model using improved long short-term memory (LSTM) networks and differential privacy frequent subgraph (DPFS) to ensure data privacy. The constructed model was simulated using the Tennessee Eastman process, and the results showed higher prediction accuracy and better robustness compared to other models. DT technology was employed to map the drone's operating environment in physical space, comprehensively analyze the information security concerns of the drone system in the virtual space, and detect multiple attacks and intrusions. However, the study had limitations as only three types of attacks (FDIA, replay attacks, and DoS) were taken into consideration. Additionally, only the temperature sensor was targeted in the attack, and other factors like location, time, and intensity of the drone system were not considered.

4.1.14 | Agriculture

In Reference 40, Chukkapalli et al. introduced a security surveillance system for a smart farm that tracked the data generated by sensors and alerted the farm owners. The system included the collected sensor data, a smart farm ontology for creating knowledge graphs, and DT modules for anomaly detection. The researchers initially used the collected data to generate knowledge graphs with the smart farm ontology and then employed the DT to train the anomaly detection model using principal component analysis. The authors demonstrated that the DT-based anomaly detection model could detect various anomalies in the smart farm.

4.1.15 | Nuclear power plants

The authors of Reference 16 proposed the utilization of DT technology to enhance the security of physical protection systems (PPS) in nuclear power plants. They developed a cyber security test platform based on DT technology, enabling the evaluation of security measures without affecting the actual physical system. The DT technology combined multi-dimensional information perception, intelligent algorithms, and other tools to enable intelligent cognition and iterative optimization of real objects. The paper identified threats from external and internal factors, referring to the national standard for classified protection of cybersecurity. 3D modeling was employed to digitize each physical object of the PPS, offering an intuitive display and enabling the association of important system information. The use of DT technology resulted in the creation of a cyber security test platform that facilitated the verification of various protection measures. Only measures that passed the test platform could be deployed in the real environment. Additionally, the test platform could be used for training purposes related to PPSs and cyber security.

TABLE 4 Security mechanism for protecting the communication between DT and its mapped physical asset.

Reference	Security mechanism(s)	Goal(s)
50	Central access control system based on OAuth and XACML	Secure access control
24	Anonymous communication based on secret-handshake scheme and group signature	Unforgeability and conditional traceability (privacy)
38	Differential privacy techniques	Privacy and confidentiality of data
42	Blockchain and smart contract-based Proof-of-Authentication (PoA)	Validate the legitimacy and integrity of data collected from (I)IoT nodes
11	Blockchain, smart contract and deep learning	Integrity of data, detect botnet behavior
74	Quantum communication technologies	Improve overall security of communication between DT and IIoT
75	Trusted execution environment and unclonable functions (PUFs)	Security and trustworthiness of communication
51	Attribute-based access control	Secure data storage
76	Blockchain	To authenticate data generated from the cluster before they are used in DT
77	Authorization blockchain and storage blockchain	Secure data sharing through authorization
78	Blockchain and SHA-256 hash for chained checksum	To increase the security and trustworthiness of sensor reading for digital twin application
79	Blockchain, access control secure transmission protocol	Improve the communication security of Internet of Vehicles (IoV)
80	Framework based on verifiable data register (VDR) and credentials	Secure and protect the privacy of data exchange in digital twin ecosystem
81	Attribute-based encryption (ABE) and symmetric encryption scheme	To ensure the secure communication of digital twin and IoT

4.2 | RQ2: (I)IoT-DT security—Literature's security mechanisms

This subsection addresses the second research question of the paper, focusing on identifying security mechanisms for ensuring secure data communication between (I)IoT and DT systems. Establishing secure communication between physical (I)IoT components and their digital counterparts is crucial for the reliability and security of DT-based systems, considering the limitations in computational power and storage of physical components. Our analysis of 14 papers delved into discussions on data confidentiality, integrity, and privacy within the DT ecosystem. Table 4 offers a comprehensive summary of the security mechanisms discussed in the literature. The reviewed studies encompass various topics, including access control systems, cryptography, authentication protocols, privacy protection mechanisms, quantum networking, and blockchain-based data sharing. This overview provides insight into the current research landscape regarding communication security in CPSs integrating DT and (I)IoT components. Authors in Reference 50 discussed the implementation of a single central access control system based on policies defined using standard frameworks such as XACML and tokens like SAML and OAuth. These policies helped regulate who had access to what information and ensured the security of the communication. To address security problems such as communication trust and privacy protection, the authors in Reference 24 proposed a secured vehicular digital twin communication framework that utilized anonymous authentication. To achieve this, the authors presented a concrete authentication protocol based on a secret-handshake scheme and group signature, which solved the issues of unforgeability and conditional traceability. The proposed framework provided secure communication between iTwins (DT) and their physical lords, as well as between iTwins(DT) themselves, ensuring the privacy and security of the information transmitted. The proposed protocol was validated and found to meet basic security requirements while having low computation costs. In Reference 38 authors presented a method that focused on the privacy and confidentiality of data used for training detection models in drones of CPSs. The authors used differential privacy-enhancing techniques to improve the accuracy and efficiency of the analysis of drone data while ensuring the protection of sensitive information. While in Reference 42 authors suggested a blockchain-based data transmission scheme that employed a Proof-of-Authentication (PoA) mechanism, which was implemented through the use of smart contracts. This helped to validate the legitimacy and integrity of data collected from Internet of Things (IIoT) nodes, improving communication security and data privacy within a decentralized IIoT network. In Reference 11 Salim's work involved securing the communication between IoT devices and DTs using a private blockchain, smart contracts, and deep learning for network traffic monitoring. The private blockchain and smart contracts helped ensure the data flow between physical devices and DTs was secure and tamper-proof. The deep learning model helped detect early signs of botnet behavior and alerted the security vendor to take action to isolate infected devices, maintaining the security of the communication and the integrity of the data. Another study conducted by authors in Reference 74 aimed to enhance the communication security between IIoT devices and DTs by using quantum communication technologies. The authors introduced a channel encryption scheme based on quantum communication using entanglement states and quantum teleportation. Further, they proposed an Adaptive Key Residue algorithm based on a quantum key distribution mechanism. The goal was to improve the security of communication between IIoT devices and DTs. In Reference 51, authors presented a scheme for secure and privacy-preserving traffic control data sharing using DTs. The scheme incorporated a group signature with time-bound keys for data source authentication and efficient member revocation during the data uploading phase, ensuring secure data storage on the cloud service provider. Moreover, the scheme included an attribute-based access control technique for flexible and efficient data sharing during the data sharing stage. The primary objective of this scheme was to guarantee effective and secure data sharing for traffic control purposes. In Reference 75, author addressed the security and trustworthiness of the communication between the DT and physical device through various technologies and HW and SW solutions such as Trusted Execution Environment platforms and Physically Unclonable Functions (PUFs) for device authentication. In addition, blockchain technology, which provided secure, immutable, and auditable data storage for the exchanged critical data, was investigated by the authors. While the authors in Reference 76 proposed a secure smart manufacturing framework through the integration of DT and blockchain technologies. The framework aimed to facilitate efficient and secure multi-party collaborative information processing in heterogeneous IIoT environments. Notably, the paper demonstrated that the proposed authentication mode outperformed the standard protocol in terms of time efficiency. Although the paper did not provide detailed information on other methods employed in the framework, it highlighted simulation results. In conclusion, the authors suggested the future inclusion of quantum computing technology to further enhance the overall efficiency and security of the proposed framework. In Reference 77, authors proposed a data security sharing architecture based on a dual blockchain network to solve the security problems of the IoT. The first blockchain called the authorization blockchain, was used for permission control and consensus, and the other, called the storage blockchain, was used for the storage of data bodies. The proposed architecture was applied to the IoT system based on DT to address the data security transmission between the physical system, DT system, and IoT application system. However, the authors in this study provided only data authentication. They assumed the data from IoT devices was encrypted on transmission. In Reference 78, a novel use of the lightweight SHA-256 hash algorithm was proposed to create a blockchain of sensor readings, ensuring trustworthy communication between the control center and remote sensors. By chaining the checksums of current and previous readings, the implementation established trust based on the unbroken linked list length. The authors in this paper claimed that this approach strengthened the security and trustworthiness of sensor data in DT applications, particularly in high-value domains such as the power grid. Authors in Reference 79, authors proposed BC-Based IoV Secure Communication Framework, presenting an architecture designed to enhance secure communication in the context of the Internet of Vehicles (IoV). By leveraging blockchain technology, the authors claimed the framework securely stored vital data such as public keys and communication history. It consisted of five key modules: BC network, access control, secure transmission protocol, vehicle Ad Hoc, and a Sybil attack detection mechanism. To combat the rising prevalence of Sybil attacks in IoV scenarios, the framework utilized regular location certificates issued by base stations, which served to validate vehicle location accuracy. This proposed framework offered a viable solution to enhance communication security in IoV environments. In Reference 80, the authors introduced a framework called SIGNED, which aimed to enable a secure and verifiable exchange of DT data in a smart city context. The framework focused on data ownership, selective disclosure, and verifiability principles using verifiable credentials. It consisted of five functional components: Cyber & Physical Layer, Workflow Designer, Analysis Layer, Traceability Layer, and Digital Wallet. The Traceability Layer, integrated with a blockchain-based Verifiable Data Registry, maintained the public credentials and tracked registered assets. The authors presented a proof of concept using a smart water management use case to demonstrate the effectiveness of SIGNED in ensuring trusted and verifiable data exchange, with minimal performance impact. Overall, the framework provided enhanced security and privacy when sharing data between different functional units in a smart city. A contribution by authors in Reference 81 presented work to enhance IoT communication security in DT networking. They proposed an interference source location scheme with a mobile tracker to reduce attacks, improve resistance, and enhance attribute-based encryption (ABE). They use access control policy and symmetric encryption to secure key exchange. To address observation noise through an unscented Kalman filter, the paper modifies interference source location. The authors in this work concluded that utilizing jamming signal strength information with the untracked Kalman filter algorithm can effectively estimate the interference source location and other related state information.

4.3 | Insights into digital twin technology in Industry 4.0

As part of a SLR, this analysis focuses on the use of DT technology in Industry 4.0. We explored the enabling technologies used, the adoption of DT across different sectors, and the security services provided by DT. By examining these aspects, this analysis aims to provide insight into the current landscape of DT in terms of key technologies used, industry sectors targeted, and security functionalities associated with this technology.

4.3.1 | Digital twin adoption by sector

Figure 6 provides insights into the adoption of DTs based on their use cases or targeted industry sectors. The data are the results of data collected from the reviewed papers. The CPS/ICS (cyber-physical systems/industrial control systems) sector emerges as the main area for DT adoption. It is worth noting that, CPS/ICs is an umbrella term that includes other specific industries like smart cities, oil and gas and so forth. Regarding specific industries, the power grid sector stands out as the most extensively researched area for the deployment of DTs. It was observed that DT technology is primarily utilized in this sector to enable anomaly detection. It is worth noting that other services such as vulnerability assessment, access control, simulation, security management, and situational awareness have also been explored. The automotive and intelligent transport sectors also widely have adopted DT to protect and secure vehicles, transportation systems, and traffic management. Other sectors, such as the 5G network, aerospace, agriculture, satellite, enterprise network, and water, show smaller but notable percentages, reflecting the diverse range of industries using DT technology.

4.3.2 | Digital twin as security tool

The first research question (**RQ1**) of this paper seeks to explore the utilization of DT as a security tool. Indeed, DT proves to be an integrated platform capable of delivering a wide range of security services, as evidenced by the papers reviewed in this work. Given its nature as a replica of assets and processes, DT can provide security-related operations without causing

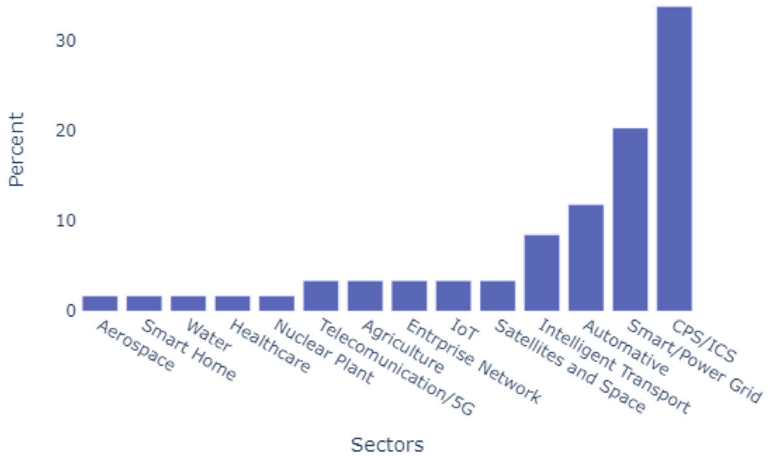

FIGURE 6 Use case of digital twin.

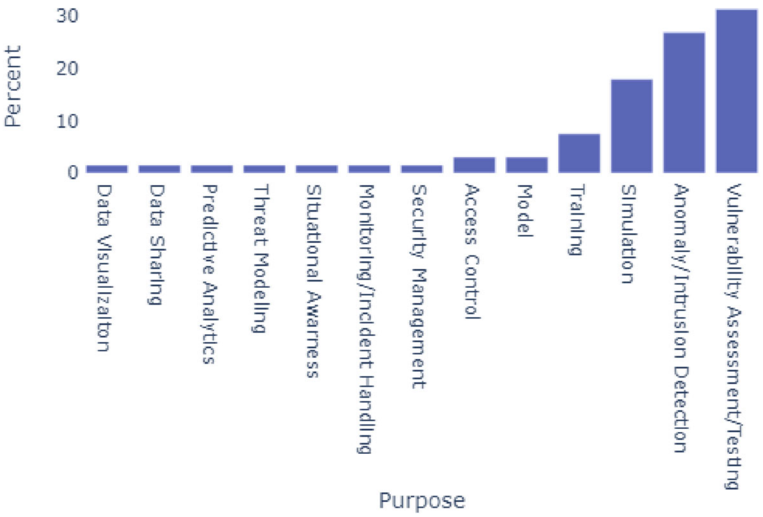

FIGURE 7 Distribution of papers based on security service provided by digital twin.

any disruptions to the ongoing processes. Hence, DT as a security tool can provide a simulation environment to enhance security skills (cyber range), predictive analytics capability in terms of forecasting attacks and security weaknesses, a testing environment for conducting vulnerability assessment penetration testing, anomaly, and intrusion detection by processing data generated from the DT and actual environment and an environment for access control. In addition, a limited number of papers highlighted that DT can provide functionality such as data visualization, threat modeling, situational awareness, and data sharing, all of which can be leveraged for security purposes. The security services provided by DT technology within various industries are presented in Figure 7. Testing, encompassing activities such as vulnerability assessment and penetration testing emerged as the most widely adopted practice, which might be due to the inherent capability of DTs to facilitate rigorous testing procedures without disrupting the ongoing operations of a business was seen as beneficial. Anomaly and Intrusion detection were the next most prominent security services provided. Specifically, it is the primary motivation behind deploying the DT in the power grid and smart grid sector.

4.3.3 | Enabling technologies integrated with digital twin

Based on the literature review, the most prominent technologies that power DTs are AI, blockchain, cloud and edge computing, analytics, and big data. AI is an umbrella term to represent various technologies including ML and deep learning (DL). In general, machine learning encompasses analytical operations; however, analytics, by itself, lacks the inherent learning capability exhibited by machine learning. In other words, analytics is a “Data Science” field for collecting and representing data to identify patterns and insight.[82] On the other hand, big data technology is used to store and process large-scale data. To avoid bias, we categorize the papers when any of the enabling technologies are explicitly mentioned as being used within the DT to augment its capabilities. Figure 8 shows the distribution of enabling technologies used or implemented with DT technology to provide various functionalities and services. Among the enabling technologies, machine learning (ML) emerged as the most dominant DT functionality augmenter. Different ML algorithms and models were proposed in the literature to equip DT with the capability of data analysis, predictive insight, anomaly, and intrusion detection. Cloud computing along with edge computing played a key role in supporting the storage, and processing of large amounts of data. Additionally, blockchain technology is used with DT mainly to enhance the security and privacy of shared data.

4.4 | Security mechanisms analysis from literature

Securing the communication channel between DT and (I)IoT deployment is a critical concept that should not be neglected especially in the critical infrastructure of Industry 4.0. To address this, a few research efforts on various security

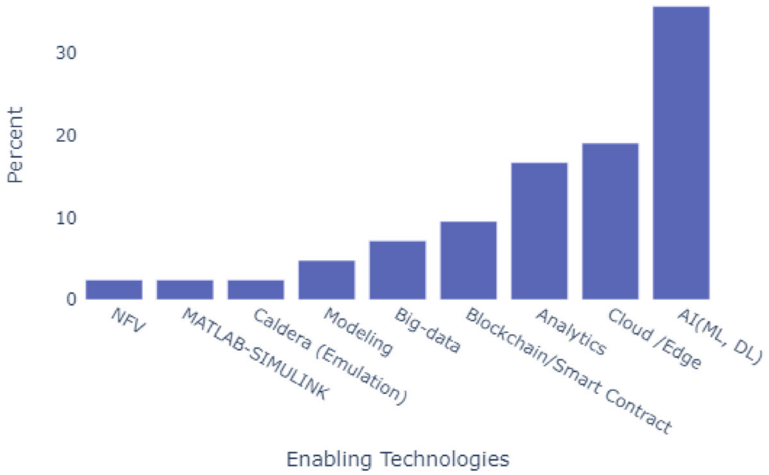

FIGURE 8 Distribution of papers based on enabling technology integrated with digital twin.

mechanisms were presented in the literature. In this subsection, we present a comparative analysis of security mechanisms for secure data communication in terms of practicality resource efficiency, and deployment. The most widely used approach to provide privacy and security in the DT ecosystem in the existing literature is blockchain (smart contract) technology. In References 11,42,76–79 blockchain-based data transmission scheme for data integrity are proposed. Due to the inherent nature of Blockchain, the proposed solution based on this technology has a limitation in providing data confidentiality. Blockchain-based security approaches offer data integrity in a distributed environment, but they may have computationally demanding underlying technology, impacting their suitability for resource-constrained IoT devices. Three studies[24,38,51,80] focused on providing privacy using techniques such as secret-handshake scheme, group signature and differential privacy techniques. While enhancing privacy, these two approaches may require significant computational resources for cryptographic operations on resource-constrained (I)IoT devices. Furthermore, we encountered security mechanisms that focus on access control and trust.[50,51,75] The first paper suggests a centralized access control system using XACML policies and tokens like SAML and OAuth to regulate access and ensure communication security. In another paper, the authors proposed a scheme for secure data sharing using attribute-based access control. In the third paper, the authors propose secure data exchange between DT and (I)IoT using technologies namely PUF (Physical Unclonable Functions) and TPM (Trusted Platform Module). Though these solutions are resource efficient, it might not be economically practical to use them as the special hardware setup and complex key management involved. Finally, a distinctive study by authors in Reference 74 delved into the realm of quantum communication and quantum entanglement. It is a theoretical proposed solution that may not even be possible soon as this technology has not yet developed. Therefore, quantum communication might provide very efficient and strong security but it might also require sophisticated hardware, which makes its practical implementation challenging.

5 | DISCUSSION AND RESEARCH GAP

In this literature review part of the project, we conducted a systematic way of reviewing the literature on the use of DT technology in the Industry 4.0 domain to enhance security requirements. The study was carried out using the three-phase approach of conducting a SLR that included designing a review protocol, conducting the review, and analyzing. The aim was to investigate how DT is used to enhance security Industry 4.0. Besides, we explored the literature on what security scheme or mechanism is used to protect the integrity and confidentiality of data flow between (I)IoT devices and DT. In this SLR, we first performed a search on six electronic databases (ScienceDirect, SpringerLink, Scopus, IEEExplore, ACM, and Web of Science) yielded 727 papers. We then applied the inclusion and exclusion criteria, which resulted in 452 papers. Part of these criteria were already applied during the database search, such as the language, publication type, subject categories, and publication year. Then we manually screen the titles, keywords, and abstracts of the 452 papers. This resulted in 83 papers that were eligible for full-text review. We then conducted a full-text review of the 83 papers and excluded 16 papers that were not relevant to our research question. The final set of 67 papers was included in our analysis.

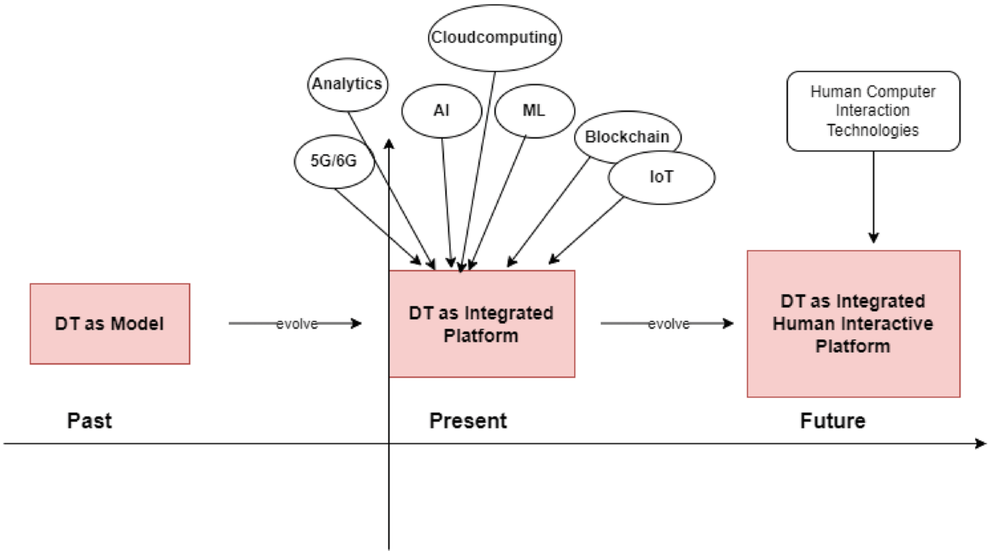
Cloudcomputing
Analytics
AI
ML
5G/6G
Blockchain
IoT
Human Computer Interaction Technologies
DT as Model
evolve
DT as Integrated Platform
evolve
DT as Integrated Human Interactive Platform
Past
Present
Future

FIGURE 9 Evolution of digital twin over time.

We observed that publishing research studies on using DT as a security solution began in 2018, and the adoption of DT technology has been growing rapidly in various Industry 4.0 sectors leading to a significant surge in research articles over the past 6 years, particularly in years 2021 and 2022. The contributions of the analyzed literature varied from theoretical concepts to DT-based security platforms. However, the majority of the studies focused on providing a framework with theoretical concepts. In the following section, first, we discuss the past, present, and future status of DT. Then, we briefly look into how DT is used as a security tool. Finally, we reflect on security mechanisms discussed in the literature for protecting data flow between DT and (I)IoT.

5.1 | Observation and findings

As a result of a thorough review of the literature on the use of DT technology for securing (I)IoT applications and securing digital communication between DT and IoT devices, we have identified a few findings.

5.1.1 | Past, present, and future of digital twin

In its early days, the DT concept was used primarily as a model in the manufacturing industry. However, with the advent of enabling technologies such as (I)IoT, AI, and cloud computing, it has evolved into an integrated platform capable of providing a range of services beyond just modeling. Today, it is used in various industries to enhance the security of complex environments in addition to improving productivity and efficiency. In the future, DTs are expected to incorporate even more technologies and integrate more deeply with humans through research on Human-Computer Interaction technology. From the review, we identified DT as an integrated platform of a virtual model and enabling technologies to process collected data from the operating environment through (I)IoT sensors to gain insight for monitoring, optimization, and security purposes. One crucial aspect emphasized by authors for deploying a properly functioning DT is the necessity for real-time and uncorrupted data. A solution based on a lightweight and authenticated encryption algorithm might ensure that this requirement is met by ensuring that the data communicated between DT and the resource-constrained (I)IoT device is secured, meaning that the integrity of data is secured with authentication and the confidentiality of data with encryption (Figure 9).

5.1.2 | Digital twin as security tools

DTs have been developed for various purposes and use cases, including security. Our review indicated that it has mostly been used as a simulation platform for conducting testing and training. Next to using DT as a simulation, several solutions were proposed to detect anomalies[40] and intrusions in CPSs and ICSs.[20,33] In this regard, the potential threats are DDoS, botnet activities, network breaches, and anomaly processes. The majority of papers discussed setting up a DT in a standalone environment to enhance the security of a targeted industry.[30,31,36,40] However, we found a few papers that presented the idea of sharing cyber threat intelligence (CTI)[10,36] data generated using DT across industries to improve security collectively, which is a unique approach to using DT technology potentially having a significant impact on tackling big security problems, such as ransomware through sharable CTI. However, for this to be effective, we argue that the data-sharing process must happen in real time with privacy in mind. In terms of enabling technologies, machine learning, and data analytics are the core technologies used to power up DT to function as a security-enhancing tool. In other words, detection and protection security services are realized mainly using machine learning and data analytics that operate on extensive data collected through sensors.

5.2 | Research gap

In our review of selected papers, it became evident that most of the papers placed little emphasis on ensuring the authenticity and integrity of the sensor data that is fed into the DT. Even though a handful of papers discussed securing the data transmission channel, their recommendations relied on traditional encryption and authentication mechanisms such as AES, SHA-256, and RSA. This research gap and these proposals are concerning because in most use cases, the field sensors are power constraints where it is not feasible to deploy traditional encryption algorithms to secure them. Hence, it is important in future research to focus on lightweight algorithms to protect data confidentiality, integrity, and authenticity of data used in DT-based solutions.

5.3 | Future directions

The application of DTs for security in Industry 4.0 is at its early stage. While researchers have made significant contributions to its development, there are remaining research gaps that still require exploration and improvement. In this section, we identify and discuss three potential research areas.

Efficient lightweight encryption algorithms: As the development of DT technology progresses, it is expected that it will become accurate in replicating physical objects and processes. To achieve this level of accuracy, a large number of tiny, resource-constrained IoT sensors will need to be deployed on a massive scale to measure every aspect of the physical status being replicated. This presents future research directions for designing and implementing efficient encryption algorithms that can be deployed on resource-constrained devices.

Remote access control for DT: One area of research that we have identified as a gap in the literature is the secure remote access control to the virtual counterpart of an ICS component for vendors to perform troubleshooting and testing. In the traditional real-world industry setup, vendors of ICS components have remote access control to the physical object of the industry for various reasons. However, it is not clear how this is going to be handled on the DT yet. One potential direction for research is to explore and investigate how secure remote access can be achieved to one or more components of the DT.

Human computer interaction: Finally, future research could explore the human–computer interaction (HCI) aspect of DT technology. This could involve examining how users interact with DT models and exploring new and innovative ways to improve the user experience. By improving the HCI aspect of DT technology, it may be possible to enhance the accuracy and reliability of the models by ensuring that human error is minimized.

5.4 | Limitations of the study

This study has two main categories of limitations: those related to collecting searching papers and those related to reviewing them.

Limitations related to searching: Regarding the limitations related to collecting papers, the first issue is with the methodology used to select papers. Only papers with the exact phrase "[Dd]igital [Tt]win[s]?" in their title were collected for review. While the authors argue that research focused on DTs will likely use this term in the title, this is not always the case. However, this approach also had the benefit of limiting the number of papers reviewed to those specifically discussing DTs in security, instead of a potentially much larger set of papers.

Limitation related to reviewing: There were multiple limitations associated with reviewing papers. First, most papers did not provide a complete and comprehensive definition of DT. Specifically, while the "state" component, encompassing both the virtual and physical states, was often explicitly described, the intended purpose and interconnectivity between these states were not consistently included in the definition.

Another limitation within this category relates to the misunderstanding of DT as simulation software. Few papers, particularly within the healthcare sector, propose solutions utilizing simulation software under the consideration of DT. This view of DT as merely a simulation model or tool without bidirectional data flows between the DT and the mirrored real system may lead to confusion and potentially incorrect conclusions regarding the potential benefits and drawbacks of DT technology.

Lastly, we observed that there needs to be more consistency in using the terms Framework, Methodology, and Architecture, which are often used interchangeably without a clear understanding of their definitions and distinctions. We argue that this could be due to a lack of consensus on how these terms should be used to categorize the contributions of authors. The inconsistency of the contribution categorizations in the analyzed papers is particularly evident in cases where different terms are used to refer to the same things within a single paper, causing further ambiguity and hindering the accurate classification of the author's contributions.

To address these limitations, reviewers had to carefully evaluate the definitions and concepts presented within papers by considering the broader context of the research to ensure a thorough understanding of the DT concept. In addition, researchers must establish clear definitions and appropriate usage of terms like framework, methodology, and architecture to facilitate effective communication and reliable classification of research contributions. By doing so, we have enhanced the quality and reliability of not only this research but might also enhance the quality and reliability of all future research related to DTs.

5.5 | Specific implementation challenges

Addressing the multifaceted challenges associated with the implementation of DT in industrial settings is essential for ensuring their effectiveness and security. One critical concern revolves around cybersecurity, where compromise can have far-reaching consequences on the physical systems mirrored by the DTs. To mitigate this, it is imperative to develop robust encryption techniques, secure communication protocols, and authentication mechanisms, safeguarding the integrity and confidentiality of the data[#]. Another challenge lies in the integration complexity of DT technology with existing legacy systems, given variations in communication protocols, data formats, and standards. Overcoming this challenge involves the development of standardized interfaces and middleware solutions, enabling seamless integration with diverse industrial systems. Moreover, the accuracy of the digital representation in DT relies heavily on the quality of input data. To address inaccuracies and inconsistencies that may lead to erroneous predictions, implementing data validation processes, continuous monitoring, and feedback loops becomes crucial. Additionally, scalability issues can arise when implementing DT across large industrial environments, resulting in performance bottlenecks. Solutions include optimizing algorithms for scalability, utilizing cloud computing resources, and employing distributed computing techniques to handle the computational demands of large-scale DT applications. These strategic measures collectively contribute to the robust and effective implementation of DTs in industrial contexts.

5.6 | Novel applications or theoretical contributions

As a result of the SLR and comprehensive analysis of pertinent papers, discernible trends and advancements have come to light in the realm of DT. Notably, a primary driver for the emergence of novel applications and theoretical contributions is the overarching aim to enhance security within industrial contexts. These innovative approaches represent a significant evolution in DT technology, with a core focus on fortifying security measures. Key among these applications is the development of adaptive security models within DTs, allowing for dynamic adjustments to security parameters in response to real-time threat assessments and changes in the industrial environment. In conjunction, the utilization of DT for predictive security analytics takes center stage, harnessing historical data and system behavior analysis to proactively predict potential security threats. Furthermore, the implementation of behavioral analysis for anomaly detection within DT serves as a crucial application, offering an early warning system for potential security breaches or vulnerabilities. As a cutting-edge theoretical contribution, the exploration of blockchain integration with DTs emerges, aiming to enhance security through decentralized and tamper-proof record-keeping for critical industrial data. The overarching goal of these advancements is to elevate the security standards within the industrial landscape, reflecting a pivotal shift in the application and theoretical foundations of DTs technology.

5.7 | Feasibility and potential limitations of integrating DT technology in real industrial environments

Based on the results of the SLR, a range of feasibility considerations and potential limitations have been identified in the implementation of DT within industrial settings. Scalability, a crucial aspect, is deemed feasible through meticulous resource allocation, load balancing, and streamlined data processing. However, challenges may arise due to limited computational resources and high implementation costs, posing obstacles to achieving seamless scalability. Interoperability, another key factor, is attainable by developing and adopting industry-wide standards for communication and data exchange. Nonetheless, existing legacy systems may present limitations, requiring additional efforts for integration. Adapting DT to diverse industrial settings is feasible by designing flexible architectures and frameworks tailored to the unique characteristics of different environments. However, industries with highly specialized or proprietary systems may encounter challenges in integration without significant customization. Addressing data privacy and ethical concerns is considered feasible through the implementation of stringent privacy policies and ethical guidelines. Nevertheless, the need to balance data access with privacy considerations may pose challenges, particularly in industries subject to strict regulatory requirements. In light of these limitations, the SLR emphasizes the importance of strategic approaches, such as optimizing resource allocation, promoting standardized communication, and designing flexible architectures, to enhance the overall feasibility of implementing DT in diverse industrial contexts.

6 | CONCLUSION

Overall, this SLR based on 67 papers highlighted that DT technology is evolving to become vital technology, particularly in Industry 4.0. Industries such as the power grid, automotive industry, water treatment plants, transportation systems, smart cities, and satellite internet are a few of the sectors that benefited from DT. This technology offers real-time cybersecurity insights through an emulation environment for threat detection, vulnerability assessment, security awareness training, and threat intelligence. Luckily, these security measures can be implemented without disrupting the ongoing operations of these industries.

Based on the analyzed papers, machine learning, and data analytics are the two primary technologies that are widely used to enable DT security features. Due to the capability to analyze large amounts of data generated by DTs, machine learning algorithms can be used to detect anomalies and identify potential security threats.

DT technology offers numerous benefits for Industry 4.0 use cases. But it also poses security challenges related to safeguarding the data collected and transmitted, especially with systems including storage, power, and computationally constrained devices. Moreover, the SLR revealed that there is a limited amount of research on how to secure communication between DTs and resource-constrained devices. In other words, in most studies, security concerns related to the data used by DTs during transmission were either neglected or traditional encryption methods were suggested. The most commonly suggested traditional encryption methods were AES, SHA-256, and RSA which are not feasible for deployment in devices with limited processing power and memory.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ENDNOTES

[*] https://www.vosviewer.com/ A tool for visualizing bibliometric network including the occurrence of keywords, coauthorship relationship.

[†] Frameworks provide a foundation with pre-defined components for application development, platforms offer a comprehensive environment supporting the development lifecycle, and architectures define the high-level structure and interactions of a system.

[‡] Theoretical proposals typically involve the development of conceptual frameworks or methodologies aimed at addressing specific challenges or objectives within a given field. In contrast, case-based solutions focus on providing practical remedies or interventions tailored to specific real-world scenarios or use cases. Experimental evaluations, on the other hand, involve rigorous testing and validation of proposed solutions through controlled experiments or simulations to assess their effectiveness, performance, and feasibility in real-world settings. These experiments often serve to validate the practical applicability and potential impact of the proposed approaches or technologies.
[§] digitaL twin-based Anomaly deTecTion wIth Curriculum lEarning (LATTICE).
[¶] Anomaly deTection with digiTAl twIN (ATTAIN).
[#] A proposed solution of securing communication channels between DT and its physical assets using a lightweight algorithm is under review.

ORCID

Mohammed El-Hajj https://orcid.org/0000-0002-4022-9999
Taru Itäpelto https://orcid.org/0000-0001-7862-265X

REFERENCES

1. Abikoye OC, Bajeh AO, Awotunde JB, et al. Application of Internet of Thing and cyber physical system in Industry 4.0 smart manufacturing. *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation*. Springer; 2021:203-217.
2. Sousa B, Arieiro M, Pereira V, Correia J, Lourenço N, Cruz T. ELEGANT: security of critical infrastructures with digital twins. *IEEE Access*. 2021;9:107574-107588.
3. Eckhart M, Ekelhart A, Weippl E. *Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins*. Institute of Electrical and Electronics Engineers Inc.; 2019:1222-1225.
4. Pirbhulal S, Abie H, Shukla A. Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications. *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*. IEEE; 2022:1-5.
5. Saad A, Faddel S, Youssef T, Mohammed OA. On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks. *IEEE Trans Smart Grid*. 2020;11(6):5138-5150.
6. Tao F, Zhang H, Liu A, Nee AYC. Digital twin in industry: state-of-the-art. *IEEE Trans Industr Inform*. 2019;15(4):2405-2415.
7. Atalay M, Murat U, Oksuz B, Parlaktuna AM, Pisirir E, Testik MC. Digital twins in manufacturing: systematic literature review for physical-digital layer categorization and future research directions. *Int J Comput Integr Manuf*. 2022;35(7):679-705. doi:10.1080/0951192X.2021.2022762
8. Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering. Vol. 2. 2007.
9. Faleiro R, Pan L, Pokhrel SR, Doss R. Digital twin for cybersecurity: towards enhancing cyber resilience. *Broadband Communications, Networks, and Systems*. Springer; 2022:57-76 http://link.springer.com/chapter/10.1007/978-3-030-93479-84
10. Dietz M, Schlette D, Pernul G. *Harnessing Digital Twin Security Simulations for Systematic Cyber Threat Intelligence*. IEEE; 2022:789-797.
11. Salim MM, Comivi AK, Nurbek T, Park H, Park JH. A Blockchain-enabled secure digital twin framework for early botnet detection in IIoT environment. *Sensors*. 2022;22(16):6133. https://www.mdpi.com/1424-8220/22/16/6133
12. Xiao Y, Jia Y, Hu Q, Cheng X, Gong B, Yu J. CommandFence: a novel digital-twin-based preventive framework for securing smart home systems. *IEEE Trans Dependable Secure Comput*. 2022;20:2450-2465.
13. Marksteiner S, Bronfman S, Wolf M, Lazebnik E. Using cyber digital twins for automated automotive cybersecurity testing. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE; 2021:123-128.
14. Dietz M, Vielberth M, Pernul G. Integrating digital twin security simulations in the security operations center. *Proceedings of the 15th International Conference on Availability, Reliability and Security*. ACM; 2020:1-9 https://doi-org.ezproxy2.utwente.nl/10.1145/3407023.3407039
15. Grasselli C, Melis A, Rinieri L, Berardi D, Gori G, Sadi AA. An industrial network digital twin for enhanced security of cyber-physical systems. *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE; 2022:1-7.
16. Guo Y, Yan A, Wang J. Cyber security risk analysis of physical protection systems of nuclear power plants and research on the cyber security test platform using digital twin technology. *2021 International Conference on Power System Technology (POWERCON)*. IEEE; 2021:1889-1892.
17. Li J, Zhang L, Hong Q, Yu Y, Zhai L. Space spider: a hyper large scientific infrastructure based on digital twin for the space internet. *Proceedings of the 1st Workshop on Digital Twin & Edge AI for Industrial IoT*. ACM; 2022:31-36 https://doi-org.ezproxy2.utwente.nl/10.1145/3566099.3569007
18. Danilczyk W, Sun YL, He H. Smart grid anomaly detection using a deep learning digital twin. *2020 52nd North American Power Symposium (NAPS)*. IEEE; 2021:1-6.
19. Shitole AB, Kandasamy NK, Liew LS, Sim L, Bui AK. Real-time digital twin of residential energy storage system for cyber-security study. *2021 IEEE 2nd International Conference on Smart Technologies for Power, Energy and Control (STPEC)*. IEEE; 2021:1-6.
20. Akbarian F, Fitzgerald E, Kihl M. Intrusion detection in digital twins for industrial control systems. *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE; 2020:1-6.
21. Maillet-Contoz L, Michel E, Nava MD, Brun PE, Leprêtre K, Massot G. End-to-end security validation of IoT systems based on digital twins of end-devices. *2020 Global Internet of Things Summit (GIoTS)*. IEEE; 2020:1-6.

22. Sellitto GP, Aranha H, Masi M, Pavleska T. Enabling a zero trust architecture in smart grids through a digital twin. *Dependable Computing—EDCC 2021 Workshops*. Springer International Publishing; 2021:73-81.
23. Dietz M, Hageman L, von Hornung C, Pernul G. Employing digital twins for security-by-design system testing. *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*. Association for Computing Machinery; 2022:97-106. doi:10.1145/3510547.3517929
24. Xu J, He C, Luan TH. Efficient authentication for vehicular digital twin communications. *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE; 2021:1-5.
25. Bitton T, Stan O, Inokuchi M, et al. Deriving a cost-effective digital twin of an ICS to facilitate security evaluation. *Computer Security. ESORICS 2018*. Vol 11098. Springer; 2018:533-554.
26. Cathey G, Benson J, Gupta M, Sandhu R. Edge centric secure data sharing with digital twins in smart ecosystems. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE; 2021:70-79.
27. Wang X, Gao Y, Deng L, Chen M. DTCPN: A digital twin cyber platform based on NFV. *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE; 2022:579-583.
28. Francia G, Hall G. Digital twins for industrial control systems security. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE; 2021:801-805.
29. Lopez J, Rubio JE, Alcaraz C. Digital twins for intelligent authorization in the B5G-enabled smart grid. *IEEE Wirel Commun*. 2021;28(2):48-55.
30. Bécue A, Praddaude M, Maia E, Hogrel N, Praça I, Yaich R. Digital twins for enhanced resilience: aerospace manufacturing. *Scenario*. 2022;451:107-118.
31. Veledar O, Damjanovic-Behrendt V, Macher G. Digital twins for dependability improvement of autonomous driving. *Systems, Software and Services Process Improvement. EuroSPI 2019*. Vol 1060. Springer; 2019:415-426.
32. Holmes D, Papathanasaki M, Maglaras L, Ferrag MA, Nepal S, Janicke H. Digital twins and cyber security—solution or challenge? *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE; 2021:1-8.
33. Varghese SA, Dehlaghi Ghadim A, Balador A, Alimadadi Z, Papadimitratos P. Digital twin-based intrusion detection for industrial control systems. *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE; 2022:611-617.
34. Hossen T, Gursoy M, Mirafzal B. Digital twin for self-security of smart inverters. *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*. IEEE; 2021:713-718.
35. Nguyen L, Segovia M, Mallouli W, EMd O, Cavalli AR. Digital twin for IoT environments: a testing and simulation tool. *Quality of Information and Communications Technology. QUATIC 2022*. Springer; 2022:205-219 http://link.springer.com/chapter/10.1007/978-3-031-14179-914
36. Almeaibed S, Al-Rubaye S, Tsourdos A, Avdelidis NP. Digital twin analysis to promote safety and security in autonomous vehicles. *IEEE Commun Stand Mag*. 2021;5:40-46.
37. Bécue A, Fourastier Y, Praça I, et al. CyberFactory#1—securing the Industry 4.0 with cyber-ranges and digital twins. *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. Institute of Electrical and Electronics Engineers Inc; 2018:1-4.
38. Wu J, Guo J, Lv Z. Deep learning driven security in digital twins of drone network. *IEEE International Conference on Communications*. IEEE; 2022:1-6.
39. Salvi A, Spagnoletti P, Noori NS. Cyber-resilience of critical cyber infrastructures: integrating digital twins in the electric power ecosystem. *Comput Secur*. 2022;112:102507 https://www.sciencedirect.com/science/article/pii/S016740482100331X
40. Chukkapalli SSL, Pillai N, Mittal S, Joshi A. Cyber-physical system security surveillance using knowledge graph based digital twins - a smart farming usecase. *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE; 2021:1-6.
41. Hadar E, Kravchenko D, Basovskiy A. Cyber digital twin simulator for automatic gathering and prioritization of security controls' requirements. *2020 IEEE 28th International Requirements Engineering Conference (RE)*. IEEE; 2020:250-259.
42. Kumar P, Kumar R, Kumar A, Franklin AA, Garg S, Singh S. Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network. *IEEE Trans Netw Sci Eng*. 2022;10:2802-2813.
43. Danilczyk W, Sun Y, He H. ANGEL: an intelligent digital twin framework for microgrid security. *2019 North American Power Symposium (NAPS)*. IEEE; 2019:1-6.
44. Masi M, Sellitto GP, Aranha H, Pavleska T. Securing critical infrastructures with a cybersecurity digital twin. *Softw Syst Model*. 2023;22:689-707.
45. Kandasamy NK, Venugopalan S, Wong TK, Leu NJ. An electric power digital twin for cyber security testing, research and education. *Comput Electr Eng*. 2022;101:108061. doi:10.1016/j.compeleceng.2022.108061
46. Akbarian F, Tärneberg W, Fitzgerald E, Kihl M. A security framework in digital twins for cloud-based industrial control systems: intrusion detection and mitigation. *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE; 2021:01-08.
47. Atalay M, Angin P. A digital twins approach to smart grid security testing and standardization. *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*. IEEE; 2020:435-440.
48. Hóu Z, Li Q, Foo E, Dong JS, de Souza P. A digital twin runtime verification framework for protecting satellites systems from cyber attacks. *2022 26th International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE; 2022:117-122.

49. Rebecchi F, Pastor A, Mozo A, et al. A digital twin for the 5G era: the SPIDER cyber range. *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE; 2022:567-572.
50. Gehrmann C, Gunnarsson M. A digital twin based industrial automation and control system security architecture. *IEEE Trans Industr Inform*. 2020;16(1):669-680.
51. Lai C, Wang M, Zheng D. SPDT: secure and privacy-preserving scheme for digital twin-based traffic control. *2022 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE; 2022:144-149.
52. Vielberth M, Glas M, Dietz M, Karagiannis S, Magkos E, Pernul G. A digital twin-based cyber range for SOC analysts. *Data and Applications Security and Privacy XXXV*. Springer; 2021:293-311.
53. Suhail S, Malik SUR, Jurdak R, Hussain R, Matulevičius R, Svetinovic D. Towards situational aware cyber-physical systems: a security-enhancing use case of blockchain-based digital twins. *Comput Ind*. 2022;141:103699 https://www.sciencedirect.com/science/article/pii/S0166361522000963
54. Harrison L. Cybersecurity threat modeling and mitigation using the digital twin. *ATZelectronics Worldw*. 2022;17:40-43.
55. Arya V, Gaurav A, Gupta BB, Hsu CH, Baghban H. Detection of malicious node in VANETs using digital twin. In: Hsu CH, Xu M, Cao H, Baghban H, Shawkat Ali ABM, eds. *Big Data Intelligence and Computing*. Springer Nature; 2023:204-212.
56. Wang K, Du H, Su L. Digital twin network based network slice security provision. *2022 IEEE 2nd International Conference on Digital Twins and Parallel Intelligence (DTPI)*. IEEE; 2022:1-6.
57. Xu Q, Ali S, Yue T. Digital twin-based anomaly detection with curriculum learning in cyber-physical systems. *ACM Trans Softw Eng Methodol*. 2023;2:113.
58. Dietz M, Pernul G. Unleashing the digital Twin's potential for ICS security. *IEEE Secur Priv*. 2020;18(4):20-27.
59. Epiphaniou G, Hammoudeh M, Yuan H, Maple C, Ani U. Digital twins in cyber effects modelling of IoT/CPS points of low resilience. *Simul Model Pract Theory*. 2023;125:102744 https://www.sciencedirect.com/science/article/pii/S1569190X23000229
60. Ayyalusamy V, Sivaneasan B, Kandasamy N, Xiao JF, Abidi K, Chandra A. Hybrid digital twin architecture for power system cyber security analysis. *2022 IEEE PES Innovative Smart Grid Technologies*. IEEE; 2022:270-274.
61. Sun Y, Xu X, Qiang R, Yuan Q. Research on security management and control of power grid digital twin based on edge computing. *2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*. IEEE; 2021:606-610.
62. van der Wal EW, El-Hajj M. Securing networks of IoT devices with digital twins and automated adversary emulation. *2022 26th International Computer Science and Engineering Conference (ICSEC)*. IEEE; 2022:241-246.
63. Liu J, Zhang S, Liu H, Zhang Y. Distributed collaborative anomaly detection for trusted digital twin vehicular edge networks. *Wireless Algorithms, Systems, and Applications. WASA 2021*. Springer; 2021:378-389.
64. Suhail S, Iqbal M, Hussain R, Jurdak R. ENIGMA: an explainable digital twin security solution for cyber–physical systems. *Comput Ind*. 2023;151:103961.
65. Somers RJ, Douthwaite JA, Wagg DJ, Walkinshaw N, Hierons RM. Digital-twin-based testing for cyber–physical systems: a systematic literature review. *Inf Softw Technol*. 2023;156:107145.
66. Murillo A, Taormina R, Tippenhauer N, Galelli S. Co-simulating physical processes and network data for high-fidelity cyber-security experiments. *Sixth Annual Industrial Control System Security (ICSS) Workshop*. ACM; 2020:13-20.
67. Patel A, Schenk T, Knorn S, Patzlaff H, Obradovic D, Halblaub AB. Real-time, simulation-based identification of cyber-security attacks of industrial plants. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE; 2021:267-272.
68. Shi L, Krishnan S, Wen S. Study cybersecurity of cyber physical system in the virtual environment: a survey and new direction. *Proceedings of the 2022 Australasian Computer Science Week*. ACM; 2022:46-55.
69. Böhm F, Dietz M, Preindl T, Pernul G. Augmented reality and the digital twin: state-of-the-art and perspectives for cybersecurity. *J Cybersecur Priv*. 2021;1(3):519-538.
70. Jia YJ, Chen QA, Wang S, et al. ContexloT: towards providing contextual integrity to appified IoT platforms. *NDSS Symposium 2017, San Diego*. Vol 2. Internet Society; 2017:1-15.
71. Celik ZB, McDaniel P, Tan G. Soteria: automated IoT safety and security analysis. *2018 USENIX Annual Technical Conference (USENIX ATC 18)*. USENIX; 2018:147-158.
72. Costantino G, De Vincenzi M, Matteucci I. A comparative analysis of UNECE WP. 29 R155 and ISO/SAE 21434. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE; 2022:340-347.
73. Litman T. *Autonomous Vehicle Implementation Predictions*. Victoria Transport Policy Institute; 2017.
74. Lv Z, Cheng C, Song H. Digital twins based on quantum networking. *IEEE Netw*. 2022;36(5):88-93.
75. De Benedictis A, Esposito C, Somma A. Toward the adoption of secure cyber digital twins to enhance cyber-physical systems security. *Quality of Information and Communications Technology. QUATIC 2022*. Springer; 2022:307-321.
76. Chen H, Jeremiah SR, Lee C, Park JH. A digital twin-based heuristic multi-cooperation scheduling framework for smart manufacturing in IIoT environment. *Appl Sci*. 2023;13(3):1440. https://www.mdpi.com/2076-3417/13/3/1440
77. Zheng Q, Wang J, Shen Y, Ding P, Cheriet M. Blockchain based trustworthy digital twin in the Internet of Things. *2022 International Conference on Information Processing and Network Provisioning (ICIPNP)*. IEEE; 2022:152-155.
78. Danilczyk W, Sun YL, He H. Blockchain checksum for establishing secure communications for digital twin technology. *2021 North American Power Symposium (NAPS)*. IEEE; 2021:1-6.
79. Liu J, Zhang L, Li C, Bai J, Lv H, Lv Z. Blockchain-based secure communication of intelligent transportation digital twins system. *IEEE Trans Intell Transp Syst*. 2022;23(11):22630-22640.
80. Pervez Z, Khan Z, Ghafoor A, Soomro K. SIGNED: smart cIty diGital twiN vErifiable data framework. *IEEE Access*. 2023;11:29430-29446.

81. Feng H, Chen D, Lv H. Sensible and secure IoT communication for digital twins, cyber twins, web twins. *Internet Things Cyber-Phys Syst*. 2021;1:34-44. https://www.sciencedirect.com/science/article/pii/S2667345221000067

82. Fuller A, Fan Z, Day C, Barlow C. Digital twin: enabling technologies, challenges and open research. *IEEE Access*. 2020;8:108952-108971.

How to cite this article: El-Hajj M, Itäpelto T, Gebremariam T. Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications. *Security and Privacy*. 2024;e396. doi: 10.1002/spy2.396