Systematic Literature Review: Digital Twins' Role in Enhancing Security for Industry 4.0 Applications

Teklit Gebremariam[1*] | **Taru Itapelo**[1*] | **Mohammed El-Hajj**[1*]

[1]SCS,EEMCS,University of Twente, Enschede, Netherlands

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

Present address
[*]SCS, EEMCS, University of Twente, Enschede, Netherlands

Funding information

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). 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 Digital Twins (DT) 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 systematic literature review, based on the analysis of 67 papers published between 2018 and 2023, underscores the evolving significance of Digital Twin technology, particularly within the ambit of Industry 4.0. The findings illuminate the pervasive influence of Digital Twin technology across multiple industrial sectors. The result SLR revealed that DT is growing and being widely adopted as a security tool particularly in Industry

[*]Equally contributing authors.

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, Systematic Literature Review, SLR, DT, Security, Industry 4.0, IIoT

1 | INTRODUCTION

Industry 4.0, characterized by cyber-physical systems, 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 [3, 2]. DTs contribute to security enhancement through IoT-based 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 Digital Twin (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 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 systematic literature review, 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 systematic literature review. 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 systematic literature review 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 systematic literature review 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. Firstly, *Parsifal*, an online tool explicitly designed to automate systematic literature reviews, facilitated the structured collection of relevant literature. Secondly, *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 systematic literature review aims to address two primary research questions within the domain of DT integration for enhancing security in Industry 4.0. Firstly, 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. Secondly, 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 systematic literature review, 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 Digital Twin 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 Digital Twin 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 Systematic Literature Review. 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 Digital Twin 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 5.5. 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 Systematic Literature Review (SLR) involves a meticulous examination of existing research within a precisely defined domain, utilizing systematic methodologies to identify, select, and critically appraise relevant articles while scrutinizing data obtained from these studies. Maintaining rigor in an SLR mandates employing methods that are both reproducible and transparent [9]. While various types of literature reviews, such as exploratory reviews, aim to unearth published theories, empirical data, and research methodologies in academic literature [10], our objective surpasses a surface-level examination. Our goal is to pinpoint specific gaps existing within the current state of research. Hence, in this study, we adopt an SLR approach. This section delineates the framework employed for executing the systematic literature review. Initially, a precise search string will be formulated, and subsequently utilized to query predetermined online databases. Following this, a meticulous screening process will be implemented to discard irrelevant articles, and the retained corpus will undergo comprehensive analysis. Finally, the study will articulate the identified knowledge gaps and propose potential directions for future research. The Systematic Literature Review (SLR) serves as a formal and structured process for synthesizing pertinent research studies aimed at addressing predetermined re-

search inquiries [8]. Its primary objective involves offering a comprehensive overview of the existing literature while discerning gaps in research domains [11]. Conducting an SLR enables researchers to acquire in-depth knowledge and insights within a specific field or topic, facilitating the identification of areas necessitating further investigation.

This paper strictly adheres to the well-established three-phase approach delineated by Kitchenham and Charter [8], encompassing protocol planning, review execution, and results reporting. Adherence to this approach ensures the systematic literature review is conducted in a methodical and transparent manner, aligning with the guidelines set forth by Kitchenham and Charter [8]. Utilizing these guidelines alongside supplementary resources, we depict the review process in a comprehensive flow diagram illustrated in Figure 1.

The literature review in this study aims to achieve two principal objectives:

1. To **Investigate** and **Identify** the utilization of Digital Twin technology in fortifying the security of Industry 4.0 applications.
2. To **Identify** the diverse security mechanisms detailed in literature for securing the data communication channel between the Digital Twin and (I)IoT devices.

2.1 | Review Protocol

According to Kitchenham and Charter [8], it is important to define a review protocol that outlines the procedures and methods prior to commencing the review process. The protocol serves as a road map for conducting the review and ensures that the study can be replicated by providing a clear and detailed plan of the procedures to be followed [11]. Hence, in the subsequent section, we provide details of the review protocol that includes defining PICOC, research question, search query used, academic digital library selected, inclusion and exclusion criteria, and extraction form.

2.1.1 | Defining PI(C)OC

The PICOC framework, denoting Population, Intervention, Comparison, Output, and Context, is widely utilized in medical and social science studies to delineate the research focus [11]. Extending beyond medical and social sciences, Kitchenham and Charter [8] and Carrera [11] demonstrated the adaptability of this technique in structuring research inquiries within computer science-related studies.

For this systematic literature review, the PICOC criteria are applied, excluding the Comparison component to identify keywords. The remaining criteria are defined as follows:

- **Population:** The research motivation stems from addressing security concerns in communication between DT and resource-constrained (I)IoT devices. Therefore, the "Population" under study pertains to (I)IoT devices utilized in conjunction with DT technology to bolster security within Industry 4.0.
- **Intervention:** Our intervention aims to resolve the aforementioned security issue, focusing on implementing robust security mechanisms tailored for power, storage, and computation-constrained (I)IoT devices. Terms such as "authentication," "cryptography," "security," and "encryption" represent the intervention strategies.
- **Comparison:** Not applicable in this context.

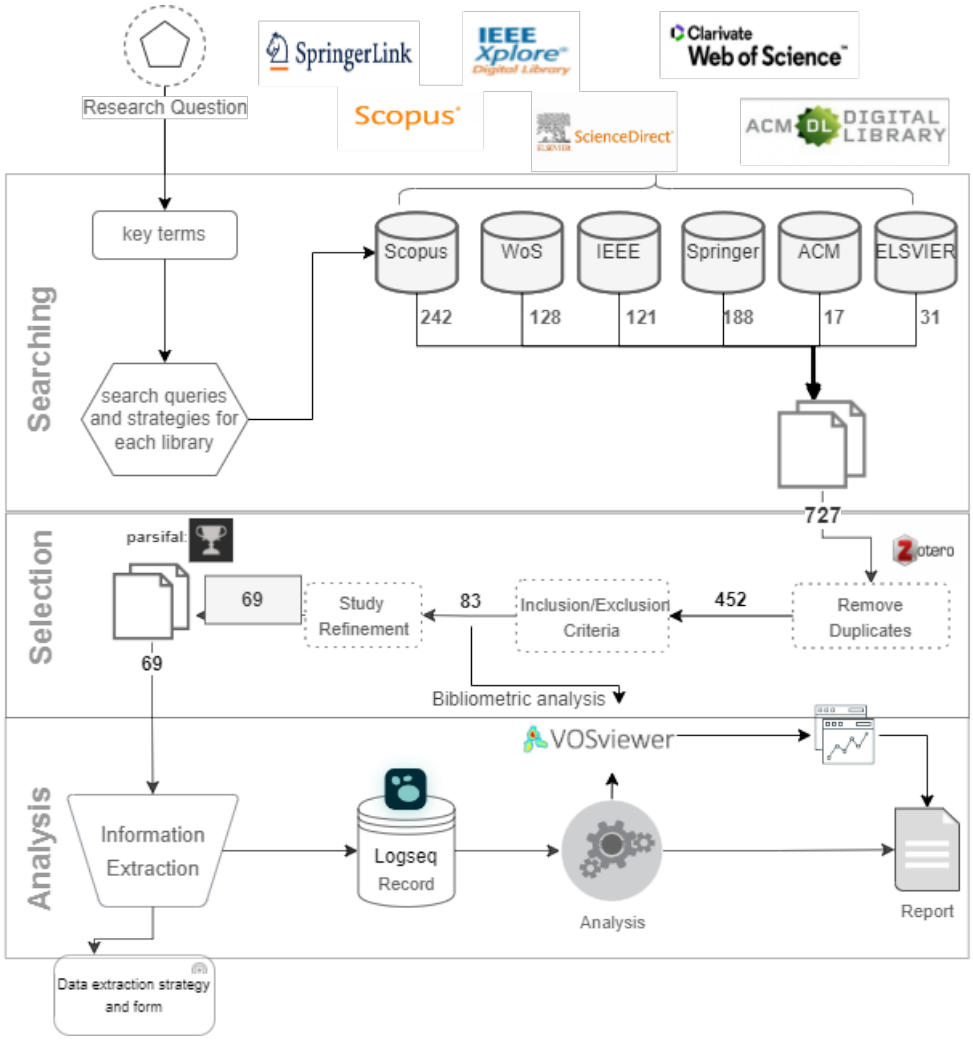


FIGURE 1 Systematic Literature Review Process Diagram

- **Outcome:** The envisioned outcome involves the enhancement of communication security between DT and (I)IoT devices, ensuring the integrity and confidentiality of exchanged data.
- **Context:** This systematic literature review concentrates on Industry 4.0 applications encompassing smart cities, smart homes, smart grids, smart health, and smart manufacturing, emphasizing their relevance within the study's scope.

This description of PICOC criteria serves to guide and structure the systematic exploration of relevant literature, focusing on the defined parameters within the context of enhancing security in the integration of DT and (I)IoT technologies.

2.2 | Search keys and Strategies

Guided by the PICOC criteria and research questions, we formulate four primary search strings to generate search queries for each chosen database. These strings consist of "Digital Twin," "IoT," "Authentication," and "Industry." Synonyms, alternate spellings, and semantically related terms are accounted for with each keyword, and they are combined using the term "OR."

During a pilot search on the majority of databases, we identified that adding synonyms of "Digital Twin" does not return new papers compared to searching using only the term "Digital Twin". Even though we included the synonym terms in the table below, we avoided using them during query construction to simplify our search string. The key terms and variants are summarized in Table 1

TABLE 1 Key Terms and Key Variants of Search Query

Key terms	**Variants / Synonyms / Similar Semantic Meaning**
Digital Twin	DT, digital-twin, digital-twins, digital twin, digital twins
(Industrial)Internet of Things	IoT, IIoT, internet-of-things, internet-of-thing, industrial internet of things, industrial-internet-of-thing, sensors, smart devices
Authentication	security, encryption, cryptography
Industry	industry 4.0, manufacturing, smart manufacturing, factory, smart factory, cyber-physical system, cyber-physical systems, cyber-physical systems, cyber-physical system, infrastructures.

2.3 | Digital Library Sources

To conduct a comprehensive literature review relevant to our research question, we utilized six electronic databases renowned for publishing computer science research papers. Of these six databases, we selected four, namely ScienceDirect, Scopus, IEEExplore, and ACM, adhering to the recommendation by Brereton et al. [12] and in Kitchenham and Charter [8].

2.4 | Inclusion and Exclusion Criteria

Inclusion: We only considered studies written in English, accessible in full text, and published in journals or conferences in the field of computer science between 2018 and 2023. Note that we run our search queries on the 14th of March and the 13th of May 2023.

Exclusion: Any studies that did not meet the inclusion criteria, including those written in a language other than English, not accessible in full text, papers classified as grey literature, published before 2018, or not related to computer science or our research questions, were excluded from the selection process. Our preliminary findings revealed that a significant number of papers–exceeding twenty–that incorporate the term "Digital Twin" in their abstracts, keywords, or titles had been published since 2018. Another reason is the fact that Digital Twin is a new research topic and growing; most of the relevant papers have been published in the last six years.

Table 2 provides the inclusion and exclusion criteria employed to filter research studies from the search results of databases.

TABLE 2 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

2.5 | Data Extraction Form

Kitchenham and Charter [8] stated that a well-designed data extraction form is helpful for gathering information from primary studies to address research questions. To ensure this in our study, we utilized the web-based tool, *parsif.al*, to structure and design the data extraction form used to collect data from the selected articles. The data extraction form used in this systematic literature review is presented in Table 3.

TABLE 3 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

The distinction between contribution categories and study types offers a robust framework for identifying prevalent patterns within the research literature. For instance, a dominance of papers exploring theoretical concepts over experimental studies might indicate that the research community is at an early stage of comprehending the issue, signaling a necessity for additional empirical investigations. Contribution categories represent various forms of contributions to research. For example, a framework contributes guidelines or principles, while an algorithm furnishes a systematic sequence for problem resolution. Meanwhile, Study types vary in terms of the methodologies employed. A case study involves an in-depth analysis of a specific sector, whereas a paper is classified as an "Experiment" if it presents findings from a conducted experimental test of a hypothesis. Similarly, a paper qualifies as a "Review Paper" when it succinctly

synthesizes and evaluates existing literature on the subject matter.

3 | PERFORMING THE SYSTEMATIC LITERATURE REVIEW

In section 2, we outlined the systematic literature review process. This section delves into the practical execution of the methodology detailed there, presenting the outcomes of each stage. For this study, a comprehensive search was conducted across prominent online digital databases, specifically ScienceDirect, SpringerLink, Scopus, IEEExplore, ACM, and Web of Science, renowned for their publication of computer science-related research studies. The search outcomes were refined based on specific inclusion and exclusion criteria detailed in Section 2.4. It's imperative to note that the inclusion criteria were limited to papers published between 2018 and 2023, focusing solely on articles from journals and conference proceedings, thereby forming the basis of the final search result. Each selected database employed distinct search queries and strategies due to their varied search mechanisms. Detailed specifics pertaining to the search strategies utilized for each database are elucidated in the subsequent sections. This approach aimed to encompass a comprehensive array of relevant articles within the defined scope of computer science, ensuring a systematic and exhaustive retrieval of pertinent literature from these 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 "Digital Twin" 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 digital twin 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*")) 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 Internet of Things 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") 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*") 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,i.e, all papers were accessible and published in English between 2018-2023

Query

[Title: "digital?twin*"] 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”
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*" 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*")

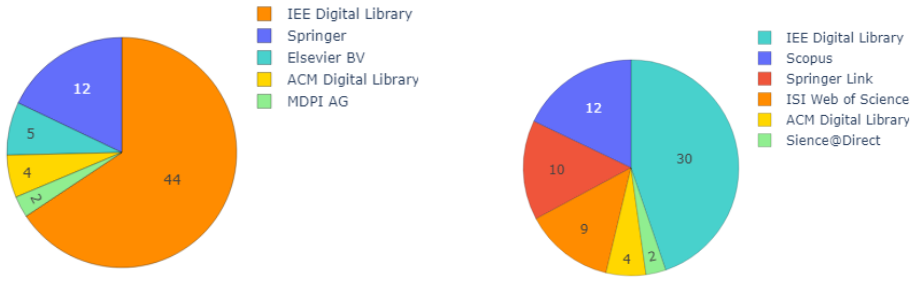
Filter: We used the following filters: Discipline: Computer Science and Engineering; Content-Type: Conference Paper and Article; Language: English
We filtered papers with "digital twin" in their title using a few lines of Python scripts. Finally, we were able to find 188 papers from the SpringerLink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

3.2 | Search Result and Bibliometric Analysis

After completing the selection process, which involved applying inclusion and exclusion criteria and eliminating duplicate studies, 67 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 44 of them. SpringerLink was the second largest contributor, with 12 publications, while Elsevier (5), ACM (4), and MDPI (2) 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, i.e. 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 Digital Twin and (I)IoT applications. This trend indicates a growing interest and concern among researchers in the Digital Twin and (I)IoT security field and highlights the relevance of this systematic literature review.

Note that the data in the figure of search results obtained on May 14th, 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,



(a) Number of Selected Papers Per publisher.

(b) Number of Selected Papers Per Pource.

FIGURE 2 An Analysis of Paper Distribution Based on Source and Publisher.

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 [1] 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", 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 Digital Twin 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

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

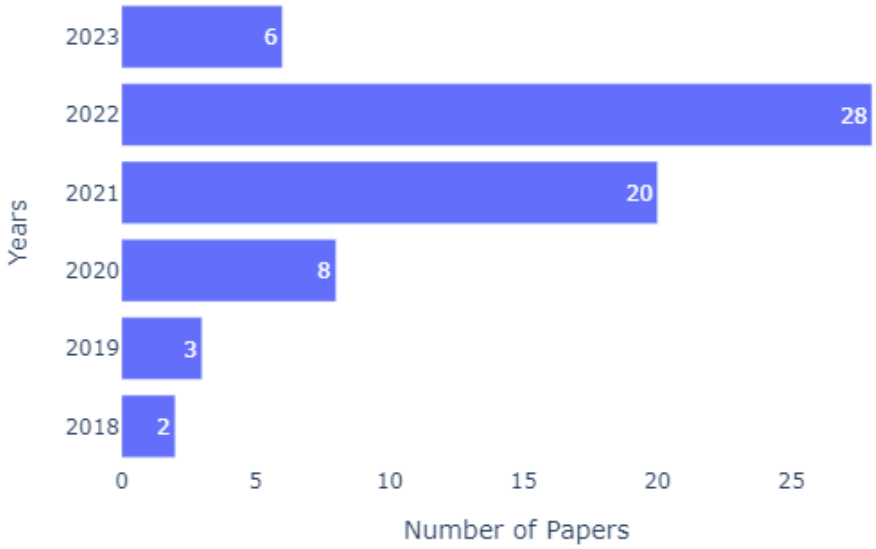


FIGURE 3 Distribution of Papers Published Per Year

most frequently mentioned word, indicating the selected papers focus on using Digital Twin 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 Digital Twin environment.

This analysis identified several key enabling technologies, namely 'blockchain(9),' 'machine learning(8)' 'cloud computing(4)' and 'analytics(3)'. These technologies are the main driving force of Digital Twin to be used as a security tool.

Our frequency analysis also revealed the prevalent adoption of Digital Twin within Industry 4.0, as evidenced by terms such as 'cyber-physical systems(8)', 'smart grid(7)', and 'industrial control systems(6)'. These industry sectors highlight the integration and utilization of Digital Twin in critical infrastructure, indicating its role in providing various services including security-related functions.

The main security and non-security functions of Digital Twin identified from the analysis were 'anomaly detection(7)', 'network security(6)', and 'simulation(6)'. This indicates the growing interest in leveraging Digital Twin 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.

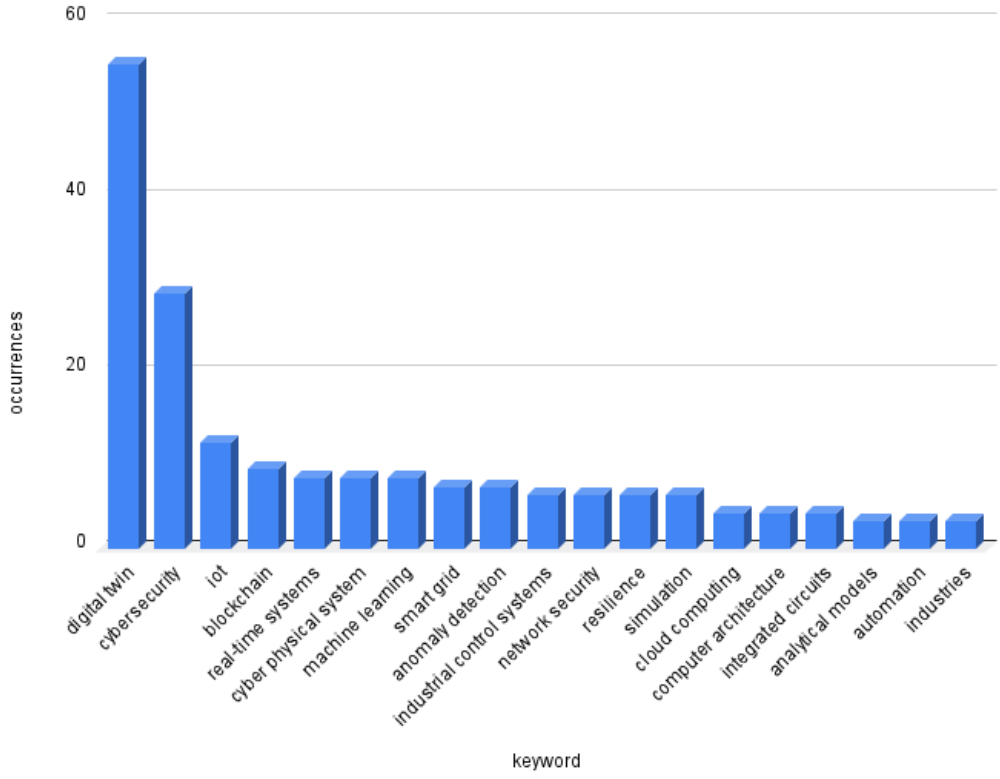


FIGURE 4 Frequency of Keywords from Keyword Section of 67 Papers

3.2.2 | Keyword Co-relationship Network

In order to gain further insights into the evolution of research in the field of Digital Twin 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 Digital Twin, 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 was on utilizing Digital Twin 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 Digital Twin has shifted towards utilizing these technologies and augmenting Digital Twin 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

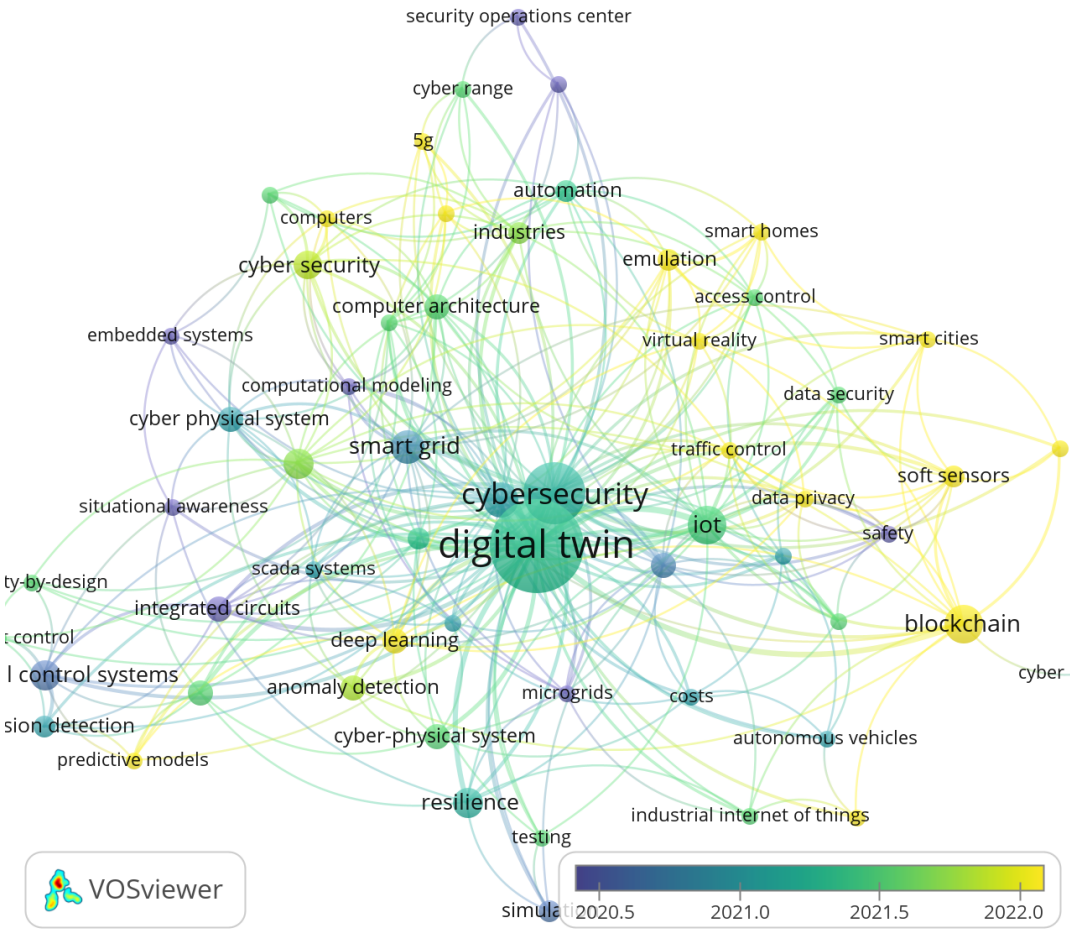


FIGURE 5 keyword co-relationship from VOSviewer

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, industrial Internet of things (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 cyber-physical systems, industry 4.0, network security, situational awareness, and smart grids. 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 encom-

passes topics such as blockchain, cyber Digital Twin, 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 Internet of Things (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 and security. It includes topics such as industrial control systems, integrated circuits, intelligent control, intrusion detection, machine learning, predictive models, and security-by-design. The focus here is on ensuring the security and reliability of industrial control systems, 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, cyber-physical systems, 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 cyber-physical systems, 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

We conducted a systematic literature review to identify relevant studies on the topic of Digital Twin security and Industry 4.0. The initial search of electronic databases yielded 727 papers. We then applied the inclusion and exclusion criteria listed in Table 2, which resulted in 452 papers. We screened the titles and abstracts of these papers to include papers that explicitly discussed the role of the digital twin in securing Industry 4.0. We then conducted a full-text review of the 83 papers and excluded 16 papers that were not relevant to our research question for the following reasons:

- **Irrelevant to (I)IoT and Industry 4.0**: Some papers were not relevant to securing applications related to **(I)IoT** in an **Industry 4.0** context. For instance, we came across a study that used a **Digital Twin** to secure a data center, which did not fit within our scope.
- **Duplicate Content**: We identified instances where the same study was submitted to different journals with different metadata, yet contained nearly identical content. Unfortunately, the tools we employed couldn't always catch these duplicates.
- **Non-Conference Source**: We excluded studies that were sourced from book chapters rather than conference proceedings, as they didn't align with our criteria.
- **Lack of Relevance to Research Questions**: Some studies simply weren't relevant to any of the research questions we were addressing.
- **Unrelated to Industry Use Case**: Studies that focused on securing **(I)IoT** devices without any connection to an

industry use case were also among the excluded papers.

As a result of this refinement and selection process, the final set of 67 papers was identified for in-depth data extraction and analysis. In the subsequent section, we present a review of these papers, with a focus on addressing two research questions presented 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 Digital Twin technology to augment security measures within Industry 4.0. The initial research question sought to identify extant solutions harnessing Digital Twin to fortify security within Industry 4.0 use cases, while the subsequent question aimed to discern the mechanisms employed in securing communication between Digital Twin 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.vThe 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 3, was developed. This systematic approach facilitated comprehensive scrutiny of each selected paper, enabling detailed insights into the deployment of Digital Twin 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 Digital Twin 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 subsection aims to answer the first research question of this paper which is how digital twin is used to enhance security in Industry 4.0 use cases.

Though the integration of operational technology and IT systems in Industry 4.0 increases the risk of cyber attacks [13] and technologies like Digital Twin offer possibilities to improve security [14]. In fact, the literature review also suggests that Digital Twin can be applied to enhance security in Industry 4.0 applications across multiple sectors. Table 4 summarises some of the research contributions that show the use of Digital Twin to improve the security of Industry 4.0 in various domains.

The research papers were classified and analyzed based on several criteria, including the target sector (use case), the purpose of DT, the enabling technology used (integrated with DT), the contribution (category of methodology), and the type of study (characteristics of the study). The table demonstrates the wide range of sectors in which Digital Twins can be applied to improve security in industries including satellite, energy, power grid, intelligent transport systems, water, agriculture, the automotive industry, and manufacturing.

The Enabling technologies used in the studies include big data, AI(machine learning), cloud computing and data ana-

lytics, edge computing, blockchain, and NFV, among others. These technologies enable researchers to build DT-based systems equipped with security features for various use cases.

The contributions of the studies were identified as frameworks, platforms, and architectures. We classify a contribution as a platform if the research presents a tool that can be deployed and used to provide security services like intrusion detection. If the authors provide only a high-level overview of the proposed solution, we classify it as an architecture. On the other hand, if details are presented for each component of the architecture, we classify it as a framework.

Regarding the study types, Table 4 shows that there are theoretical studies, case-based and experimental-based studies, and review-type studies. Theoretical studies tend to focus on proposing conceptual frameworks and architectures. And case-based studies try to provide solutions targeting specific industry sectors. Whereas experimental studies tend to evaluate the proposed frameworks and algorithms through an experiment and proof of concept. Note that a study can be both case-based and experimental if an experiment is performed on a target industry sector.

Table 4: Digital Twin: Use Cases, Purpose, Enabling Technology, Contribution Category, and Study Type in References

Ref	Use Case	Purpose	Enabling Technology	Contribution Category	Study type
[15]	Smart manufacturing	Botnet detection	ML and Blockchain	Framework	Experiment
[16]	Smart Home	Intrusion detection and prevention	Deep Learning (Deep Q-Network)	Platform	Experiment
[4]	Healthcare	Vulnerability Assessment/Testing	-	Framework	Theoretical
[17]	Automotive	Black-box Testing	-	Framework	Theoretical
[18]	ICS	Attack Testing	Analytics	Framework	Experiment
[19]	CPS	Risk Assessment/Testing	cloud Computing, Network Function Virtualization(NFV)	Architecture	Theoretical
[20]	Nuclear Plant	Testing	3D Modeling, Software Defined Network (SDN)	-	Theoretical
[21]	Satellite	Simulation	Big Data and AI	Platform	-
[22]	Smart grid	Anomaly detection	Machine Learning	Architecture	Experiment
[23]	Energy	Testing	-	Platform	Case-Study
[5]	Power grid	Anomaly detection	Cloud Computing and Data Analytics	Framework and Algorithms	Experiment based
[24]	ICS	Simulating and Testing	Machine Learning	Algorithm	Experiment

Continued on next page

Table 4: Digital Twin: Use Cases, Purpose, Enabling Technology, Contribution Category, and Study Type in References (Continued)

Ref	Use Case	Purpose	Enabling Technology	Contribution Category	Study type
[14]	ICS	Simulation	-	Framework and Algorithms	Experiment
[3]	CPS	Monitoring, Incident Handling, Testing	-	Framework	Theoretical
[25]	Water, Agriculture	Simulation and Testing	Data Analytics	Architecture	Case study and Experiment
[26]	Smart Grid	device policy enforcement	-	Architecture	Theoretical
[27]	ICS	Testing and Security Assessment	-	Framework	Experiment
[2]	ICS	Intrusion Detection	Machine Learning	Architecture	Experiment
[28]	Automotive Industry	-	-	Framework and Algorithm	Theoretical
[29]	ICS	Testing	-	Framework	Experiment
[30]	Intelligent Transportation	Access Control	Edge Computing	Architecture	Case-study
[31]	Enterprise Network	Simulation	NFV, Big data processing	Platform	Experiment
[32]	ICS	Testing, Vulnerability assessment	-	-	Experiment
[33]	Smart Grid	Detection	Blockchain	Architecture	Theoretical
[34]	Aerospace	Simulation(Attack)	-	-	Case-study
[35]	Automotive industry	Predictive analytics	-	Platform	-
[36]	-	-	-	-	Review paper
[37]	ICS	Intrusion Detection	Machine Learning	Framework	Experiment
[13]	-	-	-	-	Review paper
[38]	Power Grid	Model	-	Algorithm	Experiment
[39]	Intelligent Transport System	Testing and Simulating	-	Platform	Case-study and Experiment
[40]	Automotive Industry	-	Analytics	Framework	Case-study

Continued on next page

Table 4: Digital Twin: Use Cases, Purpose, Enabling Technology, Contribution Category, and Study Type in References (Continued)

Ref	Use Case	Purpose	Enabling Technology	Contribution Category	Study type
[41]	Manufacturing	Simulation Testing-Training	-	Theoretical	
[42]	CPS of Drones	Simulation	AI - Deep Learning	Model	Experiment
[43]	Power Grid	Situational Awareness	Data Analytics	Model	Theoretical
[44]	Agriculture sector	Anomaly detection	Machine Learning	Framework	Experiment
[45]	Enterprises	-	Analytics	-	Experiment
[46]	IIoT Network	Simulation, Intrusion Detection	Blockchain, Deep Learning	Framework	Experiment
[47]	Smart Grid	Data Visualization	-	Framework	Experiment
[48]	Intelligent Transport Systems	-	-	Architecture	-
[49]	Smart Grid	Training	-	Platform	Case-study
[50]	ICS	Intrusion Detection	Cloud Computing	Framework, Algorithm	Experiment
[51]	Smart Grid	Testing	-	Framework	Theoretical
[52]	Satellites and Space	Penetration Testing	-	Framework and Algorithm	Theoretical
[53]	5G Network	Simulation - Training and Testing	Machine learning	Architecture	Experiment
[54]	ICS	Data sharing	-	Model, Architecture	Case study
[55]	Transportation	-	Cloud	-	-
[56]	CPS	Training	-	Platform	Experiment
[57]	Automotive industry	Testing	Blockchain	Framework	Use-case
[58]	Automotive	Threat Modeling, Testing	Analytics	-	Experiment
[59]	Transportation	Detection	Machine learning	Framework	-
[60]	5G Network	Detection	-	Framework	-
[61]	CPS	Anomaly Detection	Machine Learning	Framework	Case Study
[62]	ICS	Simulation, Testing	-	-	-

Continued on next page

Table 4: Digital Twin: Use Cases, Purpose, Enabling Technology, Contribution Category, and Study Type in References (Continued)

Ref	Use Case	Purpose	Enabling Technology	Contribution Category	Study type
[63]	CPS/IoT	Security Assessment	AI and Modeling and Simulation Tools	-	Experiment through Proof of Concept
[64]	Smart Power Grid	Vulnerability Assessment	MATLAB-SIMULINK, Node-RED	Architecture	Experiment through test-bed
[65]	Power Grid	Security Management	Edge Computing	Architecture	Theoretical
[66]	IoT	Vulnerability Assessment	Automated Adversary Emulation *(Caldera)*	Architecture	Experiment
[67]	Vehicular Network/ Automotive	Anomaly Detection	Machine Learning, Edge Computing	Architecture	Experiment

Note that, the data extracted using extraction form from Table 3 and presented in Table 4 doesn't include data from papers that focus only on securing the data used by Digital Twin technology.

4.1.1 | Power Grid

The study by Danilczyk et al.[47] proposed a framework named "Automatic Network Guardian for Electrical Systems (ANGEL)," which used real-time data visualization to enhance the security and resiliency of microgrids. The framework modeled both the cyber and physical layers of the microgrid, allowing it to detect discrepancies between simulated and physical systems under various operating conditions. The framework's two-way coupling between the simulation and the physical system enabled it to update and improve its simulations, detect unnatural changes, and evaluate meter data accuracy, thereby improving security. According to the authors, ANGEL could also be equipped with machine learning to have self-healing capabilities that could mitigate component failures and cyber-attacks. While the ANGEL framework was promising, it had limitations, including potential false positives and difficulty detecting some types of malicious attacks. Additionally, the framework was still in development and had not yet been tested on a real-world microgrid system for further evaluation.

Another study by Saad et al.[5] presented an IoT-based Digital Twin for microgrids that aimed to improve their resilience against cyber attacks. The proposed framework was implemented as a cloud-based Digital Twin platform that acts as a central hub for the networked microgrid system. It is designed to model both the physical and cyber layers of the microgrid, allowing it to detect false data injection (FDIA) and denial of service (DoS) attacks. The framework utilized observer-based What-If scenarios to take corrective action when an attack is detected, ensuring the safe and seamless operation of the networked microgrids. The proposed Digital Twin framework was validated using a practical setup of the distributed control system and Amazon Web Services (AWS) and was able to quickly detect and mitigate a range of cyber attacks. The authors argue that combining deep learning and Luenberger Observer(LO) enhances the speed, accuracy, and predictability of attacks. In general, the proposed IoT-based Digital Twin framework presented

a practical solution to improve the resilience of microgrids against cyber attacks.

In[38] 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 Digital Twin. This Digital Twin 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 smart grids from man-in-the-middle attacks. By thoroughly examining incoming commands via the Digital Twin before involving the local controller, the method effectively prevents unsafe set points from being implemented.

The study undertaken by Atalay et al.[51] 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 smart grids 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 Digital Twins-based approach for the security testing lifecycle of smart grids, 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, Sellitto et al.[26] proposed a methodology to build a cybersecurity Digital Twin 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 Digital Twin 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 Digital Twin model that allows dynamic enforcement of security policies that reflect Smart Grid topology changes over time.

Salvi et al.[43] targeted the electrical energy sector to increase the cyber-resilience of Critical Control Infrastructures (CCIs) using a Digital Twin 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 by Danilczyk et al.[22] presented a deep-learning convolutional neural network (CNN) as a module within the Automatic Network Guardian for Electrical Systems (ANGEL) Digital Twin 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 Digital Twin 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 Smart Grids (SG) in physical test beds, Kandasmy et al.[49] build 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 Digital Twin 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 Digital Twin 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 [65] this study, the author's contribution lies in proposing a security management and control model for the power grid digital twin using edge computing technology. They highlighted the increasing demand for power grid security and the vulnerabilities posed by edge computing and digital twin technologies and constructed a power grid digital twin 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 digital twin's physical layer, supporting practical applications like equipment detection, fault alarm, and maintenance planning.

The authors of this [64] research paper proposed a Hybrid Digital Twin (HDT) system for cyber security analysis in smart grids and other cyber-physical systems. The HDT system comprises a MATLAB-SIMULINK digital model representing the physical system and multiple single-board computers representing the cyber components. The Digital Twin was used in this research to identify the cyber-security vulnerabilities in smart grids and other cyber-physical systems. 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 cyber-physical systems, addressing the challenges in securing power grids and other critical infrastructure.

4.1.2 | Smart Factory

Lopez et al.[33] aim in their research to analyze the evolution of digital twins in smart grid infrastructures and their role in implementing intelligent authorization policies. The authors study the application of AI technologies, including machine learning and blockchain, in the context of digital twins to manage dynamic information flows and detect cybersecurity issues in real time. They provide a mid-term and long-term analysis of the pending challenges of DTs and discuss the three-stage process of Digital Twin evolution, starting from monitoring systems with limited analysis capabilities to fully semantic, self-learning platforms. The contribution of this article lies in the analysis of the future smart grid through the evolution of digital twins, pointing out the most relevant challenges they face. The authors conclude that digital twins will play a fundamental role in driving the progress of the electricity grid toward a fully

decentralized and autonomous model, governed by intelligent authorization systems. However, standardization and information security efforts are necessary, along with deep research into machine learning specifically applied to critical infrastructures and smart cities.

In[23] paper presented by Shitole et al. aims to develop a low-cost Real-Time Digital Twin (RTDT) of an interconnected and distributed Residential Energy Storage System (RESS) controlled and monitored via Cloud-based Energy Management System (CEMS), to analyse the cyber-security of such systems and develop appropriate Intrusion Detection Systems against cyber attacks. The proposed RTDT allows for flexibility in modifying, scaling, and replicating the system without compromising its real-time fidelity. The development procedure can be easily replicated to develop RTDT of any Cyber-Physical System (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 is developed using a low-cost single-board computer with Simulink Desktop Real-Time, which reduces overall development costs. Overall, this paper presented a reliable and economical solution for cyber security studies on RESS through the development of an RTDT.

Salim et al.[15] proposed a secure blockchain-enabled digital framework for the early detection of botnet formation in a smart factory environment. The proposed framework integrates a Digital Twin (DT), a packet auditor (PA), deep learning models, blockchain, and smart contracts(SC) for securing the data flow of a smart factory environment. The Digital Twin 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 Digital Twin and the PA for detecting corrupt device data transmission. Smart contracts-based Digital Twin and PA authentication were used to ensure malicious nodes do not participate in data synchronization. Botnet spread was prevented using Digital Twin certificate revocation. A comparative analysis with existing research showed that the proposed framework provides data security, integrity, privacy, device availability, and non-repudiation. In [41] paper by Bécue et al. discussed ITEA initiative CyberFactory#1 project, which aims to develop a system of systems to optimize and ensure the resilience of digital factories and factories of the future (FoF) in the face of increasing digitization and connectivity. The project focused on optimizing the efficiency and security of the network of factories, proposing novel architectures and methodologies to address cyber and physical threats and safety concerns. It also integrated technical, economic, human, and societal dimensions. This study used Digital Twin to support cybersecurity testing and training, together with cyber ranges, to enable risk anticipation and accurate impact prediction. The project demonstrates key capabilities in realistic environments and reflects the variety of possible new factory types and business model shifts.

4.1.3 | Health

An automated framework for improving cybersecurity in IoT-based healthcare applications using Digital Twin that includes innovative healthcare security techniques such as system modeling, traffic, and attack generation, impact assessment, attack and response strategies, and cyber-attack prevention processes proposed by Pirbhulal et al.[4]. The authors investigated the applicability of Digital Twin for cyber-attack prevention and presented a strategic procedure for enhancing cybersecurity. The proposed framework can help update access control policies and enhance cybersecurity, and it provides an automated cybersecurity solution by incorporating system models and resolving known vulnerabilities and threats. However, the limitation of this research is that it is a theoretical study and needs to be validated through experiments and simulations. The authors concluded that Digital Twin is a valuable tool for enhancing cybersecurity in healthcare systems, as it provides analysis, design, and optimization of systems to improve accuracy, speed, and effectiveness, and it can simulate security breaches and develop decision-making and mitigative

responses to simulated cyber-attacks.

4.1.4 | Smart Home

In their[16] paper, Xiao et al. 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 created by Jia et al., and 17 benign SmartApps with logic errors developed by Celik et al. 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 benign 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

Cathey et al.[30] presented a novel edge-centric access control architecture for IoT environments using techniques called Tag Based Access Control(TBAC), which utilises digital twins to separate data based on tags assigned on the fly, limiting access to authorised users and applications. The proposed architecture is lightweight, supports low-latency and real-time security mechanisms, and improves system security and efficiency by minimising data sharing and granting individual access to data subsets. The paper demonstrated the usefulness of TBAC in smart environments such as manufacturing and internet-connected vehicles.

A Digital Twin-based tool named Testing and Simulation(TaS) was presented in[39] paper by Nguyen et al. for testing and simulating IoT environments to improve testing methodologies and evaluate the possible impact of IoT systems on the physical world. The tool supports functional and nonfunctional testing and can be used to detect and predict failures in evolving IoT environments. The tool had been tested and validated through experiments performed in the context of the H2020 ENACT project. The contribution of the paper lies in the design of a tool that allows the real-time connection of the physical system to a new software version deployed in the DT, enabling verification that changes made in the code do not impact existing software functionality. The tool has been applied in different domains, showing that it is generic and can be used to achieve different test objectives. Although TaS automates several steps in the test process, the author pointed out the limitations regarding testing scenario generation that could be improved.

The authors in this [59] work proposed a framework that utilizes Digital Twin (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 [40], Almeaibed et al. proposed a standard framework for the creation of vehicular digital twins that streamlines data collection, processing, and analytics. The authors also highlighted the importance of Digital Twin 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 digital twins in the autonomous vehicle industry and addressing privacy, safety, security, and cyber attack mitigation.

Another research that focused on autonomous vehicles to tackle safety and security issues in connected cars and Autonomous Driving was presented by Veledar et al.[35]. With the scope of IoT4CPS, a guideline for the secure integration of IoT into autonomous driving (AD), the authors suggested three main steps for designing Digital Twins to address security vulnerabilities in AD. The proposed three steps are: First, identifying assets, modeling them, and defining security and safety objectives. Second, designing security and safety evaluation metrics. Last, performing threat modeling and test case demonstrators based on security and safety risk assessment and forecasting.

A study by Marksteiner et al. [17] 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 for vehicular systems

Xu et al.[28] introduced a conceptual framework called the Vehicular Digital Twin (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 digital twins 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.

A framework called Trusted Twins for Securing Cyber-Physical Systems (TTS-CPS) that utilizes blockchain-based Digital Twins (DTs) to strengthen the security of Cyber-Physical Systems (CPSs) was presented by Suhail et al.[57]. The aim of the TTS-CPS framework is to ensure the trustworthiness of data generated based on Digital Twin specification through Integrity Checking Mechanisms (ICMs). The authors argued that the framework helps to establish more understanding and confidence in the decisions made by underlying systems through storing and retrieving Safety and Security (S&S) rules from the blockchain. In the paper, the authors demonstrated the feasibility of the TTS-CPS framework in an assembly line of the automotive industry through a prototypical implementation supporting simulated network topology, Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), and physical devices.

Liu et.al [67] proposed a new approach called Digital Twin Vehicular Edge Networks (DITVEN) to enhance security in vehicular networks. They suggested using Digital Twins, to capture their characteristics and detect anomalies. To ensure network safety, the approach includes a distributed trust evaluation system (to ensure the credibility of digital twins), mutual trust evaluation, and anomaly detection techniques, and it considers the cooperative context for interaction between physical and digital twin vehicles.

Lee Harrison [58] from Siemens addressed the challenges posed by the increasing connectivity and complexity of modern vehicles as they progress towards full autonomy level 5. 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 digital twin environment for comprehensive testing of vehicle systems under various conditions. The ultimate goal was to achieve full autonomy (level 5) and ensure both safety and security against present and future cyber attackers.

4.1.7 | Water Treatment

The authors in[25] introduced an approach for the integration, verification, and validation of security in IoT devices. The approach is based on the Digital Twin 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.

4.1.8 | Space Industry

In[34] this research, the authors highlighted the utilization of digital twins (DTs) in the aerospace manufacturing industry where the Industrial Internet of Things (IIoT) was being integrated with Airbus Defence and Space factories. They conducted a case study to show how Digital Twin-based simulation solutions can be used for simulating attacks and designing countermeasures without affecting the internal operation of manufacturing. The study's results demonstrate that DTs can effectively aid the industry in enhancing cybersecurity while adopting connected and collaborative manufacturing techniques.

Hóu et al.[52] proposed a method for improving the capability of detecting cybersecurity issues in satellite communication using run-time verification based on digital twins. The proposed monitoring and evaluating software or hardware system against user-defined properties. In addition, it uses state synchronization and encryption for secure communication between the physical and Digital Twin and incorporates a cryptographic algorithm into their state synchronization protocol to guarantee the correctness of the state. However, the framework has some weaknesses, such as the lack of discussion on the security protocols used for secure communication and the absence of security and performance analysis.

In [21], Li et al. claimed to add contribution by defining characteristic hyper-large scientific infrastructures and evaluation indicators of traditional large scientific infrastructures. Due to security risks facing the space Internet, the paper proposed constructing a hyper-large scientific infrastructure called Space Spider, which simulates the space Internet's entire life cycle and creates a system for space Internet attack and defense. Additionally, the paper introduced Spiderland, an open experimental platform for studying space Internet applications and security.

4.1.9 | Enterprise Network

Wang et al.[31] 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 Digital Twin 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 [45] 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 Digital Twin 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 [37] from Varghese et al. introduced a DT-based security framework for industrial control systems (ICS) that can simulate attacks and defense mechanisms. Four process-related attack scenarios were tested on an open-source Digital Twin 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 seconds). The proposed framework extends the capabilities of an existing ICS Digital Twin framework with an ML-based IDS module and provides a platform for developing intrusion detection and prevention systems.

In[48] Masi et al. discussed the use of Digital Twin (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.

Dietz et al.[27] discussed the security issues of industrial control systems (ICS) 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 Digital Twin 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 Digital Twin presented in this study is a tool for security-by-design system testing in industrial control systems.

In another study, Dietz et al.[62] 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 digital twins (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, Eckhart et al.[3] proposed a digital-twin cyber situational awareness framework for cyber-physical systems (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 digital twins and to complete the record-and-replay feature.

Dietz et al.[18] 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 paper by Grasselli et al.[19] presented the implementation of a Digital Twin for industrial networks to facilitate cyber-security testing and validation without interfering with the real cyber-physical system. 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 Digital Twin technology in addressing cyber-security concerns in Cyber-Physical Systems.

Sousa et al.[2] introduced an off-premises approach to designing and deploying digital twins (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 Digital Twin 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 digital twins as security enablers and data sharing for Industrial Automation and Control Systems (IACS) was discussed in detail by Gehrmann et al.[54]. The authors 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 Industrial Control Systems(ICS) which makes them more vulnerable to cyber attacks, Akbarian et al. [24] proposed a Digital Twin-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 (SVM) 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.

Akbarian et al.[50] proposed a similar security framework to prior work[24] for industrial control systems (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 by Francia et al.[32] proposed the use of digital twins in Industrial Control Systems (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 digital twins for various environments, expanding the Digital Twin testbed for more elaborate ICS integrations and security testing, and automating the process of creating security scenarios for the effective utilization of digital twins in security training and education.

A framework that utilizes Digital Twin 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[14]. By combining a general CTI process with Digital Twin 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 Digital Twin 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 by Bitton et.al [29] suggested a method for creating a cost-effective digital twin 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 non-linear programming to find an optimal solution (i.e., a digital twin specification), which satisfies all of the constraints. The proposed method maximises the impact of the digital twin 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 digital twin), as well as the test's execution costs (e.g., security expert's time/salary). The output of the proposed method specified the digital twin configuration, i.e., which components of the ICS should be implemented and at which implementation level.

Xu et.al [61] 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.

The work by Vielberth et al. [56] demonstrated the development and implementation of a digital twin-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 [63], the authors proposed and recommended the utilization of Digital Twin (DT) to enhance the cyber resilience of cyber-physical systems (CPS) in Critical National Infrastructure (CNI). They suggested that Digital Twin could be combined with a cyber range to analyze how the system behaved under attack. The Digital Twin 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 Digital Twin 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 digital twins and methodologies for characterizing threat sources could result in cost-effective security and resilience assessments.

4.1.11 | 5G and Communication Network

Wang et al. [60] introduced and proposed the application of digital twin 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 digital twin 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, Rebecchi et al. [53] 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 Netwrok

To improve communication security and data privacy for the Digital Twin powered Industrial Internet of Things (IIoT) network, Kumar et al. [46] introduced a framework that combined blockchain and deep learning. They presented a new Digital Twin model 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 Digital Twin empowered (I)IoT network.

A study by Ewout Willem and Mohammed El-Hajj [66] showed the potential use of Digital Twins 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 Digital Twins 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 Digital Twin 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. [42] studied the utilization of Digital Twin 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. Digital Twin 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 [44], 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 Digital Twin modules for anomaly detection. The researchers initially used the collected data to generate knowledge graphs with the smart farm ontology and then employed the Digital Twin 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 [20] proposed the utilization of Digital Twin technology to enhance the security of physical protection systems (PPS) in nuclear power plants. They developed a cyber security test platform based on digital twin technology, enabling the evaluation of security measures without affecting the actual physical system. The digital twin 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 digital twin 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.

4.2 | RQ2: (I)IoT-DT Security: Literature's Security Mechanisms

This subsection provides an answer to the second research question of this paper which is to identify the security mechanism presented in the literature to ensure secure data communication between (I)IoT and Digital Twin.

To ensure the reliability and security of DT-based systems, it is essential to have secure communication between the physical and digital components. The computational, power, and storage limitation of those physical components ((I)IoT) has to be taken into consideration. In this regard, we analyzed 14 papers that discuss data confidentiality, integrity, and privacy in the Digital Twin ecosystem. Table 5 provides a summary of the security mechanisms employed

in the literature.

The reviewed studies cover topics such as access control systems, cryptography, authentication protocols, privacy protection mechanisms, quantum networking, and blockchain-based data sharing. We aim to provide an overview of the current state of research concerning securing communication in cyber-physical systems based on Digital Twin and (I)IoT components.

Gehrmann et al. [54] 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 [28] 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.

Jingyi Wu et al. [42] presented a method that focused on the privacy and confidentiality of data used for training detection models in drones of cyber-physical systems. 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.

Kumar et al. [46] 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 [15] Salim's work involved securing the communication between IoT devices and Digital Twins 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.

A study conducted by Zhigan Lv et al. [68] aimed to enhance the communication security between industrial Internet of Things devices (IIoT) and Digital Twins (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.

Lai et al. [55] presented a scheme for secure and privacy-preserving traffic control data sharing using digital twins. 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 [69] De Benedictis addressed the security and trustworthiness of the communication between the digital twin 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.

The authors in [70] proposed a secure smart manufacturing framework through the integration of Digital Twin (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.

Zhen et al. [71] proposed a data security sharing architecture based on a dual Blockchain network to solve the security problems of the Internet of Things. 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 Internet of Things system based on Digital Twin to address the data security transmission between the physical system, digital twin 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 [72], 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 digital twin applications, particularly in high-value domains such as the power grid.

Lie et.al [73] 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 [74] the authors introduced a framework called SIGNED, which aimed to enable a secure and verifiable exchange of digital twin 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 Feng et al. [75] presented work to enhance IoT communication security in digital twin 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 (JSS) information with the untracked Kalman filter algorithm can effectively estimate the interference source location and other related state information.

TABLE 5 Security Mechanism for protecting the communication between DT and its mapped physical asset

Ref	Security mechanism(s)	Goal(s)
[54]	Central access control system based on OAuth and XACML	Secure access control
[28]	Anonymous communication based on secret-handshake scheme and group signature	Unforgeability and conditional traceability (privacy)
[42]	Differential privacy techniques	Privacy and confidentiality of data
[46]	Blockchain and Smart contract based Proof-of-Authentication(PoA)	Validate the legitimacy and integrity of data collected from (I)IoT nodes.
[15]	Blockchain, Smart contract and Deep learning	Integrity of data, detect botnet behaviour
[68]	Quantum communication technologies	Improve overall security of communication between DT and IIoT
[69]	Trusted Execution Environment and Unclonable Functions(PUFs)	Security and Trustworthiness of communication
[55]	Attribute-based Access Control	Secure data storage
[70]	Blockchain	To authenticate data generated from cluster before they are used in DT
[71]	Authorization Blockchain and Storage Blockchain	Secure data sharing through authorization
[72]	Blockchain and SHA-256 hash for chained checksum	To increase the security and trustworthiness of sensor reading for Digital Twin application.
[73]	Blockchain, access control secure transmission protocol	Improve the communication security of Interent of Vehicles(IoV).
[74]	framework based on verifiable data register(VDR) and credentials	Secure and protect the privacy of data exchange in Digital Twin ecosystem.
[75]	Attribute-Based Encryption (ABE) and Symmetric encryption scheme	To ensure the secure communication of Digital Twin and IoT.

4.3 | Insights into Digital Twin Technology in Industry 4.0

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

4.3.1 | Digital Twin Adoption by Sector

Fig 6 provides insights into the adoption of digital twins based on their use cases or targeted industry sectors. The data are the results of data collected from the reviewed papers using the data extraction form (**??**). The CPS/ICS (Cyber-Physical Systems/Industrial Control Systems) sector emerges as the main area for digital twin adoption. It is worth noting that, CPS/ICs is an umbrella term that includes other specific industries like smart cities, oil and gas, etc. When it comes to specific industries, the power grid sector stands out as the most extensively researched area for the deployment of digital twins. It was observed that Digital Twin 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 Digital Twin 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 Digital Twin technology.

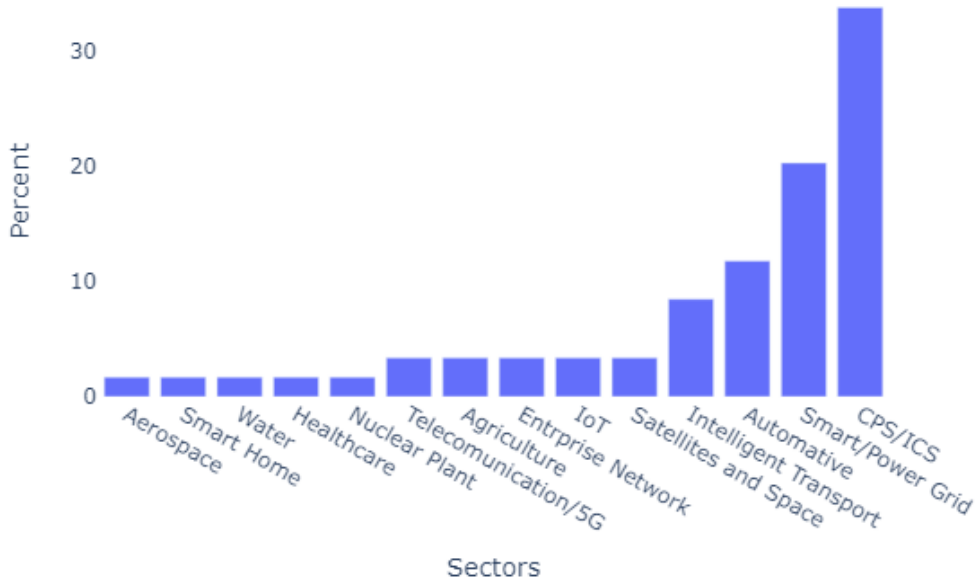


FIGURE 6 Use Case of Digital Twin

4.3.2 | Digital Twin as Security Tool

The first research question (**RQ1**)) of this paper seeks to explore the utilization of Digital Twin as a security tool. Indeed, Digital Twin 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, Digital Twin can be used to

provide security-related operations without causing any disruptions to the actual ongoing processes.

Hence, Digital Twin 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 Digital Twin and actual environment and an environment for access control.

In addition, a limited number of papers highlighted that Digital Twin can be used to provide functionality such as data visualization, threat modeling, situational awareness, and data sharing, all of which can be leveraged for security purposes.

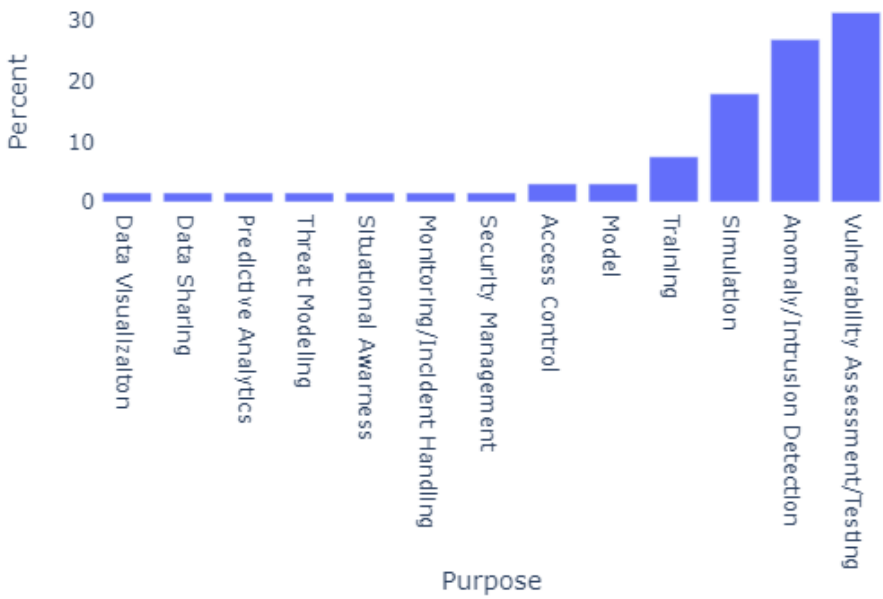


FIGURE 7 Distribution of Papers Based on Security Service Provided By Digital Twin.

The security services provided by DT technology within various industries are presented in Fig 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 Digital Twins 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 service provided. Specifically, it is the primary motivation behind deploying the Digital Twin 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 Digital Twins 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 [76]. 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 Digital Twin to augment its capabilities.

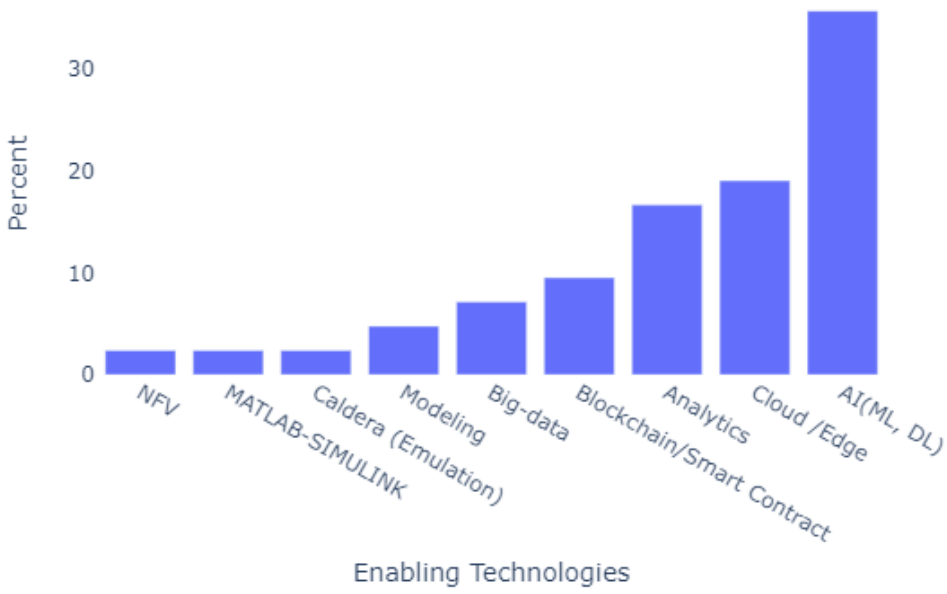


FIGURE 8 Distribution of Papers Based on Enabling Technology Integrated With Digital TWin

Fig 8 shows the distribution of enabling technologies used or implemented with digital twin technology to provide various functionalities and services. Among the enabling technologies, machine learning (ML) emerged as the most dominant Digital Twin functionality augmenter. Different ML algorithms and models were proposed in the literature to equip Digital Twin 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 Digital Twin mainly to enhance the security and privacy of shared data.

4.4 | Security Mechanisms Analysis From Literature

Securing the communication channel between Digital Twin 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 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 Digital Twin ecosystem in the existing literature is Blockchain (Smart Contract) technology. In [46, 15, 71, 73, 72, 70] 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 [28, 42, 55, 74] 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 [54, 55, 69]. 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 Digital Twin 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 Lv et al. [68] delved into the realm of quantum communication and quantum entanglement. It is a theoretical proposed solution that may not even be possible in the near future 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 Digital Twin technology in Industry 4.0 domain to enhance security requirements. The study was carried out using the three-phase approach of conducting a systematic literature review that included designing a review protocol, conducting the review, and analyzing. The aim was to investigate how Digital Twin 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 Digital Twin.

In this systematic literature review, 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 listed in Table 2.4, 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.

We observed that publishing research studies on using Digital Twin as a security solution began in 2018, and the adoption of Digital Twin 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 Digital Twin-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 Digital Twin. Then, we briefly look into how Digital Twin is used as a security tool. Finally, we reflect on security mechanisms discussed in the literature for protecting data flow between Digital Twin 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 Digital Twin 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, digital twins 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 Digital Twin as an integrated platform of a virtual model and enabling technologies to process collected data from the operating environment through (I)IoT sensors in order to gain insight for monitoring, optimization, and security purposes.

One crucial aspect emphasized by authors for deploying a properly functioning Digital Twin 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 Digital Twin 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.

5.1.2 | Digital Twin as security tools

Digital Twins 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, a number of solutions were proposed to detect anomalies [44] and intrusions in cyber-physical systems(CPS) and industrial control systems (ICS) [37, 24]. In this regard, the potential threats are DDoS, botnet activities, network breaches, and anomaly processes.

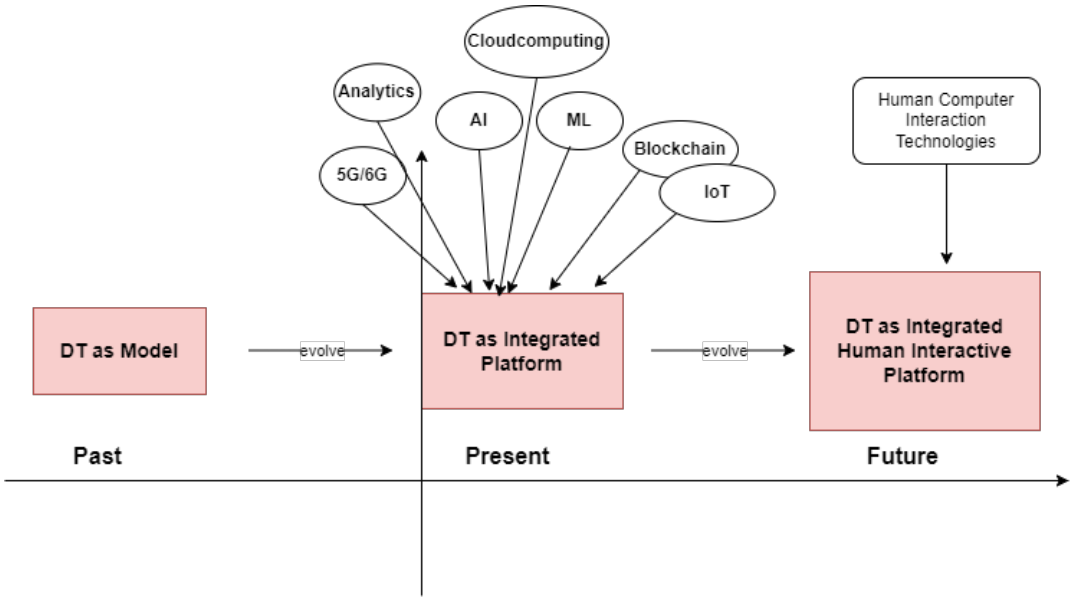


FIGURE 9 Evolution of Digital Twin Over Time

The majority of papers discussed setting up a digital twin in a standalone environment to enhance the security of a targeted industry [40, 35, 44, 34]. However, we found a few papers that presented the idea of sharing cyber threat intelligence(CTI) [14, 40] data generated using Digital Twin across industries to improve security collectively, which is a unique approach to using digital twin 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 Digital Twin 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 Digital Twin. 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 Digital Twin-based solutions.

5.3 | Future Directions

The application of Digital Twins 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 Digital Twin 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 digital twins 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 digital twins 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 Digital Twin. 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 Digital Twin as simulation software. Few papers, particularly within the healthcare sector, propose solutions utilizing simulation software under the consideration of Digital Twin. This view of Digital Twin as merely a simulation model or tool without bidirectional data flows between the Digital Twin and the mirrored real system may lead to confusion and potentially incorrect conclusions regarding the potential benefits and drawbacks of Digital Twin 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 Digital Twin 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 Digital Twins.

5.5 | Conclusion

Overall, this systematic literature review based on 67 papers highlighted that Digital Twin 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 Digital Twin. 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 digital twin security features. Due to the capability to analyze large amounts of data generated by Digital Twins, machine learning algorithms can be used to detect anomalies and identify potential security threats.

Digital Twin 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 Digital Twins 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.

references

[1] Abikoye OC, Bajeh AO, Awotunde JB, Ameen AO, Mojeed HA, Abdulraheem M, et al. Application of internet of thing and cyber physical system in Industry 4.0 smart manufacturing. In: Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation Springer; 2021.p. 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 2019;p. 1222–1225. Publisher: Institute of Electrical and Electronics Engineers Inc.

[4] Pirbhulal S, Abie H, Shukla A. Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications 2022;p. 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 Transactions on 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 Transactions on Industrial Informatics 2019 Apr;15(4):2405–2415. Conference Name: IEEE Transactions on Industrial Informatics.

[7] Atalay M, Murat U, Oksuz B, Parlaktuna AM, Pisirir E, Testik MC. Digital twins in manufacturing: systematic literature review for physical,Äìdigital layer categorization and future research directions. International Journal of Computer Integrated Manufacturing 2022 Jul;35(7):679–705. https://doi.org/10.1080/0951192X.2021.2022762, publisher: Taylor & Francis _eprint: https://doi.org/10.1080/0951192X.2021.2022762.

[8] Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering 2007 Jan;2.

[9] Paul J, Lim WM, O'Cass A, Hao AW, Bresciani S. Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). International Journal of Consumer Studies 2021;45(4):O1–O16.

[10] Adams J, Khan HT, Raeside R, White D. Research methods for graduate business and social science students. Response books; 2007.

[11] Carrera-Rivera A, Ochoa W, Larrinaga F, Lasa G. How-to conduct a systematic literature review: A quick guide for computer science research. MethodsX 2022 Jan;9:101895. https://www.sciencedirect.com/science/article/pii/S2215016122002746.

[12] Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M. Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software 2007;80(4):571–583. https://www.sciencedirect.com/science/article/pii/S016412120600197X.

[13] Faleiro R, Pan L, Pokhrel SR, Doss R; Springer. Digital twin for cybersecurity: Towards enhancing cyber resilience. Broadband Communications, Networks, and Systems 2022;p. 57–76. http://link.springer.com/chapter/10.1007/978-3-030-93479-8_4.

[14] Dietz M, Schlette D, Pernul G. Harnessing Digital Twin Security Simulations for systematic Cyber Threat Intelligence 2022;p. 789–797. Publisher:IEEE.

[15] 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). https://www.mdpi.com/1424-8220/22/16/6133.

[16] 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 Transactions on Dependable and Secure Computing 2022;p. 1–17.

[17] Marksteiner S, Bronfman S, Wolf M, Lazebnik E. Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing 2021;p. 123–128.

[18] Dietz M, Vielberth M, Pernul G. Integrating Digital Twin Security Simulations in the Security Operations Center 2020;https://doi-org.ezproxy2.utwente.nl/10.1145/3407023.3407039.

[19] 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;p. 1–7.

[20] 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. In: 2021 International Conference on Power System Technology (POWERCON); 2021. p. 1889–1892.

[21] 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 2022;p. 31–36. https://doi-org.ezproxy2.utwente.nl/10.1145/3566099.3569007.

[22] Danilczyk W, Sun YL, He H. Smart Grid Anomaly Detection using a Deep Learning Digital Twin 2021;p. 1–6.

[23] Shitole AB, Kandasamy NK, Liew LS, Sim L, Bui AK. Real-Time Digital Twin of Residential Energy Storage System for Cyber-Security Study 2021;p. 1–6. Publisher: IEEE.

[24] Akbarian F, Fitzgerald E, Kihl M. Intrusion detection in digital twins for industrial control systems 2020;p. 1–6. Publisher: IEEE.

[25] 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. In: 2020 Global Internet of Things Summit (GIoTS); 2020. p. 1–6.

[26] Sellitto GP, Aranha H, Masi M, Pavleska T; Springer. Enabling a zero trust architecture in smart grids through a digital twin 2021;p. 73–81. Publisher:Springer International Publishing.

[27] Dietz M, Hageman L, von Hornung C, Pernul G. Employing Digital Twins for Security-by-Design System Testing 2022;p. 97–106. https://doi.org/10.1145/3510547.3517929.

[28] Xu J, He C, Luan TH. Efficient Authentication for Vehicular Digital Twin Communications. Software and Systems Modeling 2021;p. 1–5. Publisher: Springer Science and Business Media Deutschland GmbH.

[29] Bitton T, Stan O, Inokuchi M, Ohta Y, Yamada Y, Yagyu T, et al. Deriving a Cost-Effective Digital Twin of an ICS to Facilitate Security Evaluation 2018;11098.

[30] Cathey G, Benson J, Gupta M, Sandhu R. Edge Centric Secure Data Sharing with Digital Twins in Smart Ecosystems 2021;p. 70–79.

[31] Wang X, Gao Y, Deng L, Chen M. DTCPN: A Digital Twin Cyber Platform Based on NFV 2022;p. 579–583.

[32] Francia G, Hall G. Digital Twins for Industrial Control Systems Security 2021;p. 801–805.

[33] Lopez J, Rubio JE, Alcaraz C. Digital Twins for Intelligent Authorization in the B5G-Enabled Smart Grid. IEEE Wireless Communications 2021;28(2):48–55.

[34] Bécue A, Praddaude M, Maia E, Hogrel N, Praça I, Yaich R. Digital Twins for Enhanced Resilience: Aerospace Manufacturing Scenario 2022;451:107–118.

[35] Veledar O, Damjanovic-Behrendt V, Macher G. Digital Twins for Dependability Improvement of Autonomous Driving 2019;1060:415–426.

[36] Holmes D, Papathanasaki M, Maglaras L, Ferrag MA, Nepal S, Janicke H. Digital Twins and Cyber Security – solution or challenge? 2021;p. 1–8.

[37] Varghese SA, Dehlaghi Ghadim A, Balador A, Alimadadi Z, Papadimitratos P. Digital Twin-based Intrusion Detection for Industrial Control Systems 2022;p. 611–617.

[38] Hossen T, Gursoy M, Mirafzal B. Digital Twin for Self-Security of Smart Inverters 2021;p. 713–718.

[39] Nguyen L, Segovia M, Mallouli W, Oca EMd, Cavalli AR; Springer. Digital Twin for IoT Environments: A Testing and Simulation Tool 2022;p. 205–219. http://link.springer.com/chapter/10.1007/978-3-031-14179-9_14.

[40] Almeaibed S, Al-Rubaye S, Tsourdos A, Avdelidis NP. Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles. IEEE Communications Standards Magazine;5. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104017621&doi=10.1109%2fMCOMSTD.011.2100004&partnerID=40&md5=9f515d124e1abd0c968041f7a89aff5f.

[41] Bécue A, Fourastier Y, Praça I, Savarit A, Baron C, Gradussofs B, et al. CyberFactory#1 — Securing the industry 4.0 with cyber-ranges and digital twins 2018;2018-June:1–4. Publisher: Institute of Electrical and Electronics Engineers Inc.

[42] Wu J, Guo J, Lv Z. Deep Learning Driven Security in Digital Twins of Drone Network 2022;p. 1–6.

[43] Salvi A, Spagnoletti P, Noori NS. Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. Computers & Security 2022;112:102507. https://www.sciencedirect.com/science/article/pii/S016740482100331X.

[44] Chukkapalli SSL, Pillai N, Mittal S, Joshi A. Cyber-Physical System Security Surveillance using Knowledge Graph based Digital Twins - A Smart Farming Usecase 2021;p. 1–6.

[45] Hadar E, Kravchenko D, Basovskiy A. Cyber Digital Twin Simulator for Automatic Gathering and Prioritization of Security Controls' Requirements 2020;p. 250–259.

[46] 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 Transactions on Network Science and Engineering 2022;p. 1–13. Publisher: IEEE.

[47] Danilczyk W, Sun Y, He H. ANGEL: An Intelligent Digital Twin Framework for Microgrid Security 2019;p. 1–6.

[48] Masi M, Sellitto GP, Aranha H, Pavleska T. Securing critical infrastructures with a cybersecurity digital twin. Software and Systems Modeling 2023;p. 1–19.

[49] Kandasamy NK, Venugopalan S, Wong TK, Leu NJ. An Electric Power Digital Twin for Cyber Security Testing, Research and Education;101. https://doi.org/10.1016/j.compeleceng.2022.108061, publisher: Pergamon Press, Inc.

[50] 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;p. 01–08.

[51] Atalay M, Angin P. A Digital Twins Approach to Smart Grid Security Testing and Standardization 2020;p. 435–440. Publisher: IEEE.

[52] 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;p. 117–122.

[53] Rebecchi F, Pastor A, Mozo A, Lombardo C, Bruschi R, Aliferis I, et al. A Digital Twin for the 5G Era: the SPIDER Cyber Range 2022;p. 567–572.

[54] Gehrmann C, Gunnarsson M. A Digital Twin Based Industrial Automation and Control System Security Architecture. IEEE Transactions on Industrial Informatics 2020;16(1):669–680.

[55] Lai C, Wang M, Zheng D. SPDT: Secure and Privacy-Preserving Scheme for Digital Twin-based Traffic Control 2022;p. 144–149.

[56] Vielberth M, Glas M, Dietz M, Karagiannis S, Magkos E, Pernul G. A digital twin-based cyber range for SOC analysts. In: Data and Applications Security and Privacy XXXV: 35th Annual IFIP WG 11.3 Conference, DBSec 2021, Calgary, Canada, July 19–20, 2021, Proceedings 35 Springer; 2021. p. 293–311.

[57] 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. Computers in Industry 2022;141:103699. https://www.sciencedirect.com/science/article/pii/S0166361522000963.

[58] Harrison L. Cybersecurity Threat Modeling and Mitigation Using the Digital Twin 2022;17.

[59] 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, editors. Big Data Intelligence and Computing Singapore: Springer Nature Singapore; 2023. p. 204–212.

[60] Wang K, Du H, Su L. Digital Twin Network based Network Slice Security Provision. In: 2022 IEEE 2nd International Conference on Digital Twins and Parallel Intelligence (DTPI); 2022. p. 1–6.

[61] 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;https://doi-org.ezproxy2.utwente.nl/10.1145/3582571, just Accepted.

[62] Dietz M, Pernul G. Unleashing the Digital Twin's Potential for ICS Security. IEEE Security & Privacy 2020;18(4):20–27.

[63] Epiphaniou G, Hammoudeh M, Yuan H, Maple C, Ani U. Digital twins in cyber effects modelling of IoT/CPS points of low resilience. Simulation Modelling Practice and Theory 2023;125:102744. https://www.sciencedirect.com/science/article/pii/S1569190X23000229.

[64] Ayyalusamy V, Sivaneasan B, Kandasamy N, Xiao JF, K A, Chandra A. Hybrid Digital Twin Architecture for Power System Cyber Security Analysis. In: 2022 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia); 2022. p. 270–274.

[65] Sun Y, Xu X, Qiang R, Yuan Q. Research on Security Management and Control of Power Grid Digital Twin Based on Edge Computing. In: 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT); 2021. p. 606–610.

[66] van der Wal EW, El-Hajj M. Securing Networks of IoT Devices With Digital Twins and Automated Adversary Emulation. In: 2022 26th International Computer Science and Engineering Conference (ICSEC); 2022. p. 241–246.

[67] Liu J, Zhang S, Liu H, Zhang Y. Distributed Collaborative Anomaly Detection for Trusted Digital Twin Vehicular Edge Networks 2021;p. 378–389.

[68] Lv Z, Cheng C, Song H. Digital Twins Based on Quantum Networking. IEEE Network 2022;36(5):88–93.

[69] De Benedictis A, Esposito C, Somma A; Springer. Toward the Adoption of Secure Cyber Digital Twins to Enhance Cyber-Physical Systems Security 2022;p. 307–321.

[70] Chen H, Jeremiah SR, Lee C, Park JH. A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment. Applied Sciences 2023;13(3). https://www.mdpi.com/2076-3417/13/3/1440.

[71] Zheng Q, Wang J, Shen Y, Ding P, Cheriet M. Blockchain Based Trustworthy Digital Twin in the Internet of Things. In: 2022 International Conference on Information Processing and Network Provisioning (ICIPNP); 2022. p. 152–155.

[72] Danilczyk W, Sun YL, He H. Blockchain Checksum for Establishing Secure Communications for Digital Twin Technology. In: 2021 North American Power Symposium (NAPS); 2021. p. 1–6.

[73] Liu J, Zhang L, Li C, Bai J, Lv H, Lv Z. Blockchain-Based Secure Communication of Intelligent Transportation Digital Twins System. IEEE Transactions on Intelligent Transportation Systems 2022;23(11):22630–22640.

[74] Pervez Z, Khan Z, Ghafoor A, Soomro K. SIGNED: Smart cIty diGital twiN vErifiable Data Framework. IEEE Access 2023;11:29430–29446.

[75] Feng H, Chen D, Lv H. Sensible and secure IoT communication for digital twins, cyber twins, web twins. Internet of Things and Cyber-Physical Systems 2021;1:34–44. https://www.sciencedirect.com/science/article/pii/S2667345221000067.

[76] Fuller A, Zhong Fan, Fan Z, Charles Day, Day CR, Barlow C. Digital Twin: Enabling Technologies, Challenges and Open Research. arXiv: Computers and Society 2020 May;8:108952–108971. ARXIV_ID: 1911.01276 MAG ID: 2982936646 S2ID: 4b665972dce502b1789314dc93d2230223b92647.