International Journal of Electronics and Communications System
Volume 4, Issue 1, 1-17.
ISSN: 2798-2610
http://ejournal.radenintan.ac.id/index.php/IJECS/index
DOI: 10.24042/ijecs.v4i1.22279

Mitigating Security Threats for Digital Twin Platform: A Systematic Review with Future Scope and Research Challenges

Swati Lipsa *
Odisha University of Technology and Research, Bhubaneswar, INDIA

Ranjan Kumar Dash
Odisha University of Technology and Research, Bhubaneswar, INDIA

Korhan Cengiz
Department of Electrical-Electronics Engineering, Istinye University, Istanbul, TURKEY

Article Info

Article history:

Received: March 16, 2024
Revised: May 05, 2024
Accepted: June 10, 2024

Keywords:

Blockchain;
Digital twin;
Edge computing;
Fog computing;
Internet of Things;
Intrusion Detection System.

Abstract

In Industry 4.0, the digital twin (DT) enables users to simulate future states and configurations for prediction, optimization, and estimation. Although the potential of digital twin technology has been demonstrated by its proliferation in traditional industrial sectors, including construction, manufacturing, transportation, supply chain, healthcare, and agriculture, the risks involved with their integration have frequently been overlooked. Moreover, as a digital approach, it is intuitive to believe it is susceptible to adversarial attacks. This issue necessitates research into the multitude of attacks that the digital twin may face. This study enumerates various probable operation-specific attacks against digital twin platforms. Also, a comprehensive review of different existing techniques has been carried out to combat these attacks. A comparison of these strategies is provided to shed light on their efficacy against various attacks. Finally, future directions and research issues are highlighted that will help researchers expand the digital twin platform.

To cite this article: S. Lipsa, R. K. Dash and K. Cengiz, "Mitigating security threats for digital twin platform: A systematic review with future scope and research challenges," *Int. J. Electron. Commun. Syst.* Vol. 4, No. 1, pp. 1-17, 2024.

INTRODUCTION

A virtual replica of a real-world product, procedure, or service can be called a digital twin [1], [2]. These virtual models are now a crucial part of modern engineering to spur innovation and boost performance due to the rapid growth of machine learning and factors like big data. Digital twins (DTs) revolutionize processes across several sectors and lines of business [3]. Learning about the usages will aid in successfully incorporating digital twins into existing corporate operations. The idea of digital twins has garnered attention in numerous fields, such as supply chain logistics [4], construction, healthcare [5], [6], remote equipment diagnostics, manufacturing [7], [8], retail [9], and predictive maintenance [10]. They are helpful throughout the product life cycle, from conceptualization to post-production analysis and maintenance.

The digital twins and the Internet of Things are redefining the interaction between the digital and the real world. The Internet of Things (IoT) resembles a digital network that connects and communicates with numerous devices over the Internet. It is gradually making its way into every facet of human existence. The proliferation of IoT sensors is partly responsible for developing digital twins. IoT enables connectivity and access to intellectual prowess in the real world and is interconnected with digital twins. Digital twins of physical items, operational procedures, or people and tasks cannot reach their full potential without the Internet of Things as a fundamental strategic factor. A crucial prerequisite for a digital twin is capturing the real-world aspects of the three P (Products, Procedures, and persons) through sensors and IoT.

Although digital twins have significantly improved the efficiency of many industries [11], they also present substantial risks in the event of a malfunction, like cyberattacks, forgotten maintenance, supply chain fraud,

• **Corresponding author:**
Swati Lipsa, Odisha University of Technology and Research, INDIA. ✉ slipsait@outr.ac.in

human error, and other problems that pose serious threats to the reliability of the system and undermine confidence in the data it generates and utilizes. After all, a twin who acts on inaccurate information is not a twin at all. As cyber-attackers' sophistication is rising, it is no longer sufficient for businesses to monitor networks and react to real attacks. Instead, they must implement more preventive and proactive measures. These facts make it clear that there is a need for a new approach to security and trustworthiness that recognizes the interconnectedness of all objects and that each person's actions have consequences for others. In a nutshell, both the technological and business spheres need to work together to ensure the safety of a digital twin.

Digital twins should be viewed as mission-critical systems that raise privacy concerns regarding the entities involved the physical location of assets, and the availability, integrity, and confidentiality of data and other resources. Thus, it is important to analyze how potential privacy and security concerns can influence the digital twin's normal operations immediately or in the long run.

The different challenges digital twins can face during their implementation in real-life scenarios have been discussed [3]. The prime focus of this study is the industry-specific applications of digital twins as an industrial Metaverse [12]. The various cyber-security risks that may hinder the workings of the digital twin have been discussed [13]. The work also evaluates how the digital twin can mitigate risks. A study identified the ten most highly ranked threats for digital twins by considering five different operating scenarios [14].

The study [15] discusses the generic layered architecture of the IoT. Furthermore, the different protocols associated with different layers are well explained. This paper also presents layer-specific attacks and their countermeasures. The digital twin that works on the architecture of IoT has different layers and operations compared to IoT. Hence, layer-specific attacks on digital twins, along with their impacts on different operations, must be discussed carefully with the existing mitigation techniques for their countermeasures.

The paper [16] mainly concentrates on the risk factors when deploying digital twins as cyber-physical systems. The cyber security challenges associated with the digital twin, as put forth by this study, include integrity, confidentiality, availability, data ownership, and IP leakage and safety. They have also mentioned some challenges that the digital twin itself can manage. However, the depicted challenges are more concerned with the underlying software or the level of its implementation, including the advanced training required for the personnel associated with this. While the paper brings a clear picture of the risks associated with digital twins, it is far from reviewing works related to the network threats that are intrinsically unavoidable in a digital environment.

A comprehensive survey of security threats in digital twins can be found in [17]. This work described a four-layer digital twin, clearly identifying different operations associated with each layer. In addition, a layer-wise classification of security threats has been performed well-fashioned. Another topic of interest in the paper is the impact of these attacks on various DT operations. The security approaches were explored and discussed.

This topic is of utmost importance and relevant to individuals interested in cybersecurity and digital twins. The growing prevalence of digital twin technology in diverse sectors serves as clear evidence of the importance of this area of study. For example, digital twins are employed in healthcare to track patient health and optimize treatment regimens. In the manufacturing industry, digital twins are utilized to enhance manufacturing operations and save downtime. In the transportation business, digital twins are used to oversee and improve vehicle performance. In general, mitigating security threats for digital twin platforms is an important field that helps to ensure the safety and security of digital twin applications across various industries.

This review is needed because digital twin platforms are vulnerable to cyber-attacks, leading to data breaches, system failures, and other security issues. If adequate cybersecurity controls are not implemented, digital twins can expand a company's attack surface, give threat actors access to previously inaccessible control systems, and expose preexisting vulnerabilities. It is imperative that readers in the fields of cybersecurity and digital twins be aware of the security risks inherent in digital twin platforms and the countermeasures that can be

implemented to reduce or eliminate these risks. Therefore, researchers and practitioners in this field develop and implement security measures that protect digital twin platforms from cyber-attacks. These measures include authentication and access control, encryption, intrusion detection, and threat intelligence.

The rest of the paper is arranged as follows. The enabling approaches of the digital twin are presented in Section 2. Section 3 delves into the layered architecture of the digital twin on the IoT platform. Section 4 discusses the various security threats to digital twins. Section 5 addresses the numerous cutting-edge approaches for mitigating the threats above, while Section 6 compares these methods. The future work and research challenges are outlined in Section 7, and Section 8 concludes the paper.

Table 1 summarizes the review papers discussed above by considering criteria like whether they have discussed layer-specific threats, operation-specific threats, number of threats, and their mitigation techniques. Further, their limitation is also figured out, which motivates us to perform more searches to address them. The most important issue to address is to what extent these threats have been mitigated or, in other words, to perform a review on different mitigation techniques for digital twins.

The papers mentioned above envisioned various security threats to digital twins differently. Additionally, many approaches like blockchain, anomaly detection, intrusion detection, and AI/ML based approaches have been suggested to combat the attacks. However, adversarial attacks are quite likely to occur as the digital twin's application domains extend from simple to critical ranges. This, in turn, motivated many researchers to propose numerous mitigation techniques to ensure the security of the digital twin as much as possible. As a result, it is necessary to analyze the extent to which these works can mitigate attacks. Furthermore, the following questions should also be answered:

- The capability of existing techniques to mitigate all or a subset of adversarial attacks in a digital twin.
- What are the methods adopted to mitigate such attacks?
- Which mitigating techniques are most appropriate for digital twins?
- Is it necessary to find any research gaps between these techniques?
- Should a single standalone method or a hybrid model be used to mitigate security threats?

Table 1. Summary of Related Works

Paper	Scope/Domain	Layer-Specific Threats Identification	Operation-Specific Threats Identification	Mention of Threats Mitigating Techniques	Number of Threats	Limitation
[3]	Challenges and application of digital twin	No	No	No	-	Threats and their mitigation techniques have not been discussed
[12]	The operational scope of digital twin in the industry	No	No	No	-	Threats and their mitigation techniques have not been discussed
[13]	Analyze the cyber-security threats associated with systems using digital twin technology	No	No	Yes	Only risk	Only risks associated with cybersecurity have been mentioned

[14]	Identifying the cybersecurity threats that would emerge by 2030 / Cybersecurity	No	No	No	21 Not mentioned explicitly	The main domain discussed in cybersecurity
[15]	Study of communication protocols and security threats in IoT. / IoT	Yes	No	Yes	14	The study is confined to only IoT
[16]	Identification of challenges of digital twin by Delphi approach	No	No	No	23 challenges	Threats and their mitigation technique have not been discussed
[17]	Explores the current state of the digital twin and categorizes the probable threats related to it. / Digital twin	Yes	Partial	No		Existing mitigation techniques have not been discussed.

To determine the answers to the abovementioned concerns, performing a comprehensive review of existing mitigation techniques is pertinent. This motivates us to conduct a systematic review to get a clear picture of how effective such approaches have been in mitigating these attacks. In addition to this, the contributions of this paper are as follows:

- List out the DT operations that are more vulnerable to different attacks.
- Bring similar operations under the same umbrella to reduce the number of operations.
- Perform a technique-wise review of existing works to clearly compare them.
- Suggest some research challenges about these mitigation techniques.

METHOD

Identification of Vulnerable Operations from the Layered Architecture of Digital Twin in IoT Platform

Of the many techniques, the Internet of Things (IoT) outshines as the most promising platform to bring the digital twin to reality. Figure 1 depicts a generic architecture of the digital twin in the IoT platform, followed by its detailed architecture in Figure 2 [18]. The generic architecture provides a basis for the layering purpose, while the different operations, integration, governance, and security are the main factors shown in Figure 2.

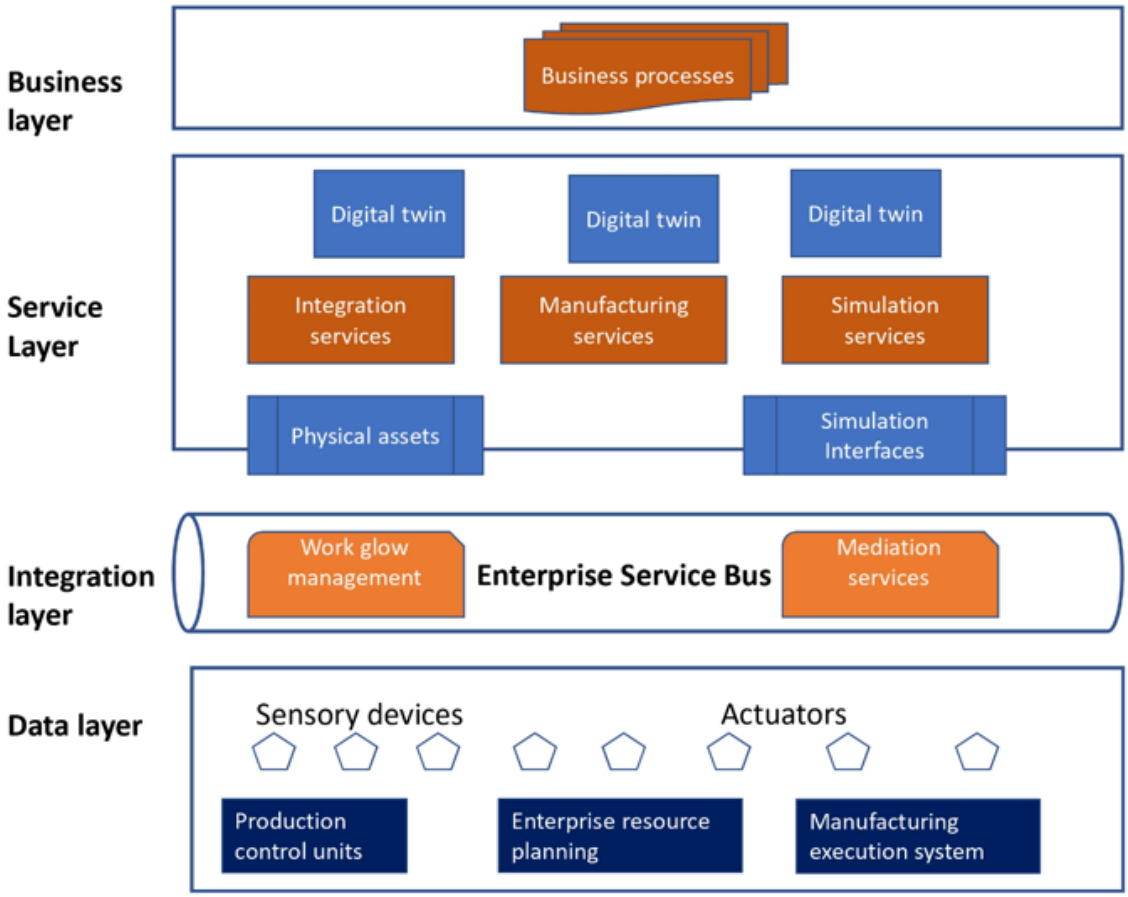
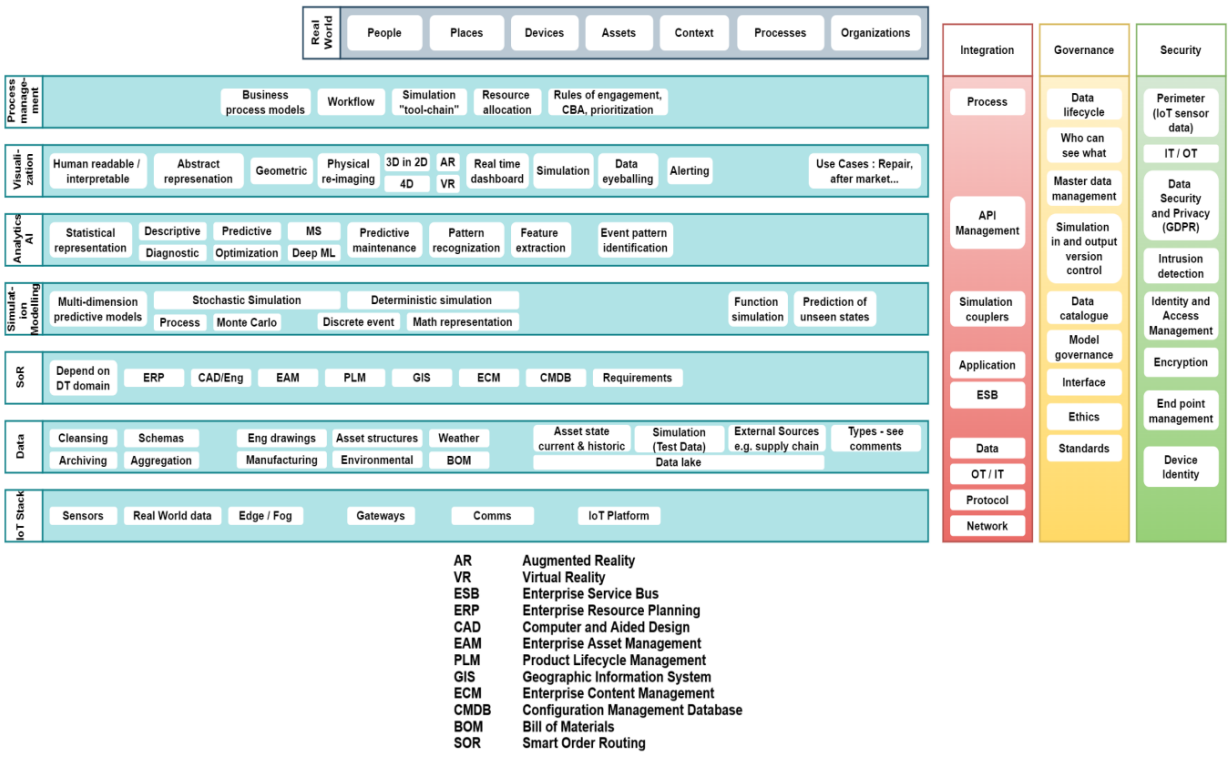


Figure 1. Generic Architecture of Digital Twin



AR	Augmented Reality
VR	Virtual Reality
ESB	Enterprise Service Bus
ERP	Enterprise Resource Planning
CAD	Computer and Aided Design
EAM	Enterprise Asset Management
PLM	Product Lifecycle Management
GIS	Geographic Information System
ECM	Enterprise Content Management
CMDB	Configuration Management Database
BOM	Bill of Materials
SOR	Smart Order Routing

Figure 2. Detailed Architecture of Digital Twin

The generic architecture of a digital twin has four different layers: the Data layer, the Integration layer, the Service layer, and the Business layer.

The detailed architectural model consists of functional and operational units such as IoT Stack, Data, SoR, Simulation and methodology, Analytics AI, Visualization and Process management, and Real-world. The level of integration, governance, and security are also presented in this figure.

The data layer is hardware-specific and contains different physical objects with sensors, actuator nodes, cameras, and drones. The different technologies associated with this layer are sensing, measuring, material, process, dynamics, etc. These techniques extract multiple levels of knowledge, including thermal, dynamics, electromagnetism, acoustics, structural mechanics, and hydro-mechatronics.

The integration layer collects, stores, processes, and transmits these data to the upper layer. The data fusion technique processes the data collected from heterogeneous sources. The technologies used to communicate data across the system are the Internet, interfaces, communication, interaction, and collaboration.

The service layer provides a simulation environment for physical objects by incorporating a chain of services. It replicates the physical objects and prepares a digital twin model of that object using the data extracted from the lower layers. At this layer, physical-to-virtual mapping is also established. To ensure accurate modeling of physical objects, the technologies used in this layer are modeling technology, simulation technology, visualization technology, verification, validation, and accreditation technology (VVA).

The business layer provides business intelligence tools and techniques to record the real-time activities of each physical object and the sensors. This layer's key functions are to monitor the manufacturing process to increase production, provide predictive maintenance, and provide digital diagnostics. Automated diagnostic solutions are integrated to handle different disruptive activities in the system.

The identified vulnerable operations that align with [17] are enumerated in Table 2.

Table 2. List of DT Operations Vulnerable to Security Threats

Operation	Mapped with	Abbreviation	Security
Physical space	Real-world, IoT stack	OP1	Device identity
Physical-to-Virtual connections	Network, protocol, OT/IT	OP2	End-point management
Virtual-to-Physical communication	Network, protocol, OT/IT	OP3	End-point management
Simulation of a physical object	Simulation and modeling	OP4	Intrusion detection system
Physical-to-Virtual mapping	Network, protocol, OT/IT, Simulation, and modeling	OP5	End-point management, encryption
Central data storage	Data	OP6	Encryption
Verification, validation, and accreditation	Simulation and modeling, Analytics AI	OP7	Data security and privacy
Decision-making	Analytics AI, Process management	OP8	Data security and privacy
Prediction and detection	Simulation and modeling, Analytics AI, Process management	OP9	Data security and privacy

Security Threats in Digital Twin Environment

Due to the massive virtualization of resources to facilitate different domain-specific activities, the digital twin is the best choice among industries for its adoption. Being a digital technology, it is also very susceptible to security threats. The security vulnerability of communicating channels is greater than that of any working space, physical or logical. As they are less secure, the attackers get a fair chance of entering the system through them. In addition to these vulnerabilities, each layer is vulnerable to different attacks (Figure 3).

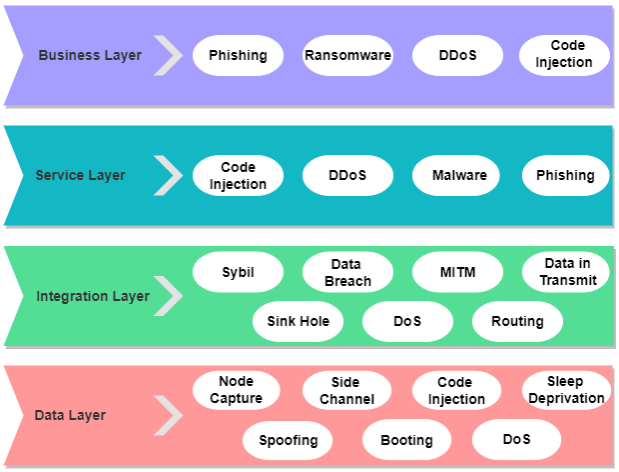


Figure 3. Layer-specific Attack in Digital Twin Environment

These layer-specific attacks mostly conform to the work carried out in [17]. Attacks on the physical layer are directly associated with tempering or replacing the sensor nodes. Attacks on the integration layer include routing attacks, man-in-the-middle attacks, denial-of-service attacks, etc. The application layer is vulnerable to phishing attacks, data breaches, etc. These attacks are enumerated below.

- Node capture attack (ST1): In this attack, the attackers replace the deployed sensor nodes with malicious sensor nodes. This results in injecting malicious data into the IoT system, which, in turn, forces the system to behave abnormally and, in its worst case, completely halts it.
- Malicious code injection attack (ST2): This attack involves injecting malicious code into the working sensor nodes. This malicious code compels the sensor nodes to work under the attacker's operational control, and the attacker can then access the whole IoT system to relinquish complete control of the network.
- Side-channel attack (ST3): This attack involves the attackers stealing sensitive data. Electromagnetic, laser-based, and timing attacks are examples of this type of attack.
- Sleep deprivation attack (ST4): This attack forces the sensor nodes to drain their batteries by running malicious codes.
- Booting attack (ST5): The sensor nodes are prone to attacks during their booting process due to the lack of any enabled security software.
- Data in transit attack (ST6): The attackers attack the data packets during their transit in the communication channel of the network.
- Spoofing attack (ST7): It is the act of someone impersonating another in an effort to obtain trust, gain unauthorized access to devices, and steal information.
- Routing attack (ST8): The different routing attacks are packet-dropping attacks, flooding attacks, traffic attacks, version number attacks, and local repair attacks.
- Man-in-the-Middle attack (MITM)(ST9): This attack occurs when an attacker stealthily listens to conversations between the sender and receiver, who think they are communicating directly with each other.
- A denial-of-service attack (DoS)(ST10): This threat halts a system or network, rendering it unavailable to its intended recipients.
- Distributed Denial-of-Service attack (DDoS)(ST11): It is a type of DoS attack in which a network of connected online devices, or "botnet", is utilized to flood a targeted system with spurious traffic.
- Sinkhole attack (ST12): It uses falsified information to divert traffic through a targeted node, turning it into a beneficial routing sink.
- Sybil attack (ST13): It employs a single system to manage numerous active false identities (also known as Sybil identities) concurrently in a peer-to-peer network.
- Phishing (ST14): It occurs when hackers send fraudulent emails intended to deceive recipients into tricking a scam.
- Data theft (ST15): It occurs when sensitive information is inadvertently disclosed publicly. It is the result of an internal trigger.
- Data breach (ST16): An event occurs due to a cyberattack. It necessitates an external trigger to commence the chain of events that results in data compromise.
- Spyware, Malware, and Ransomware (ST17): Malware is any program developed with the specific intent to harm or interfere with a computer's routine operations. Ransomware and spyware are two of the most harmful types of malwares.

Table 3 maps the various attacks and their effect on different operations in the digital twin environment.

The attacks ST1 to ST4 can affect all the operations listed in Table 3. Thus, their effects

on the digital twin can be considered very high (VH). The chances of an ST5 attack are very low, i.e., only during the booting of the device. Hence, it can be treated as low (L). ST6 to ST13 are network-specific attacks; thus, they cannot affect the devices directly but can tamper with data integrity. Therefore, their severity can also be considered very high (VH), while attacks such as ST14 to ST17 are application-specific and can affect only the operation related to the application. Hence, their severity can be treated as High (H).

Methodology Adopted to Collect the Relevant Research Papers

This step is critical, as it defines how to collect relevant papers. The papers are searched based on keywords. The keywords comprise different security threats (ST1-ST7), which have been discussed earlier. Furthermore, mitigation techniques, such as blockchain, intrusion detection systems, AI/ML-based techniques as standalone techniques or embedded with edge/fog computing, are the other input for this search. The abstract of the paper is read to find its suitability for inclusion in the reference list.

The steps to collect the relevant papers are depicted in Fig.

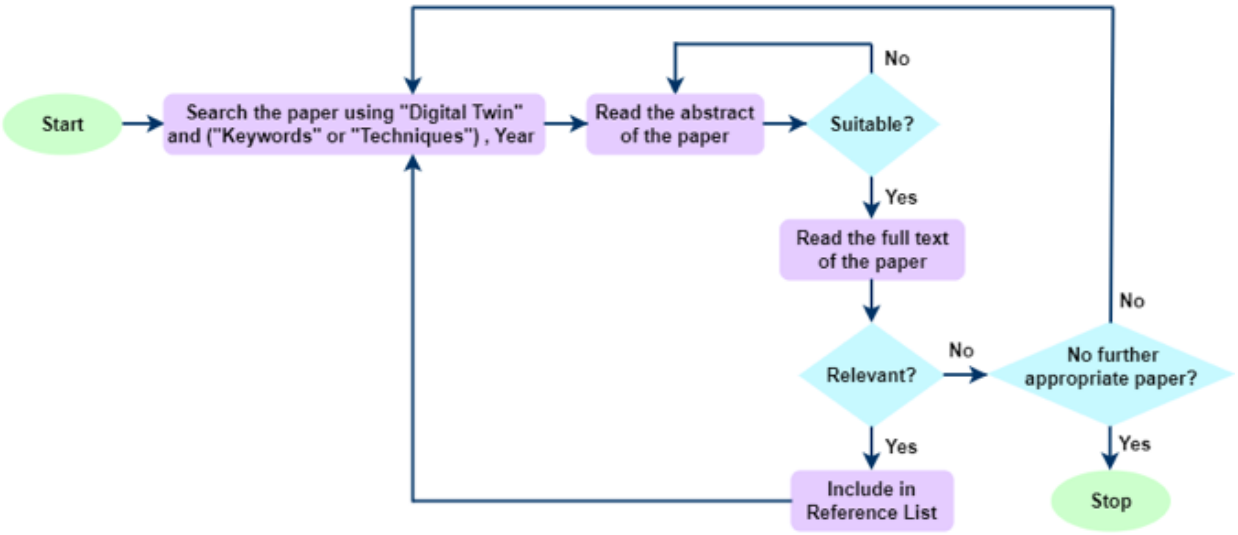


Figure 4. Flowchart for Relevant Paper Collection

RESULT AND DISCUSSION

State-of-the-Arts Methods to Mitigate Security Issues in Digital Twin

Blockchain

Blockchain is a decentralized ledger that stores transactions across a computer network. The individual entities in a blockchain are the blocks that are immutable and indistinguishable. Blockchains are created chronologically and time-stamped.

It is an ideal choice among researchers to mitigate the different attacks on digital twins.

A study [18] used blockchain for a secure end-to-end connection for additive manufacturing in the aircraft industry. A blockchain-based digital twin (DT-BC) approach has been introduced [19] for an industrial internet platform for enhancing manufacturing processes. The work presented by [20] consists of a DT model based on the blockchain framework for personalized production based on digital twins, blockchain, and additive manufacturing to meet the requirements of Industry 4.0 [21]. The blockchain of things (MBCoT) architecture is proposed for intelligent manufacturing systems. They replaced the Internet of Things with the Blockchain of Things in this work.

Ethertwin, an owner-specific decentralized model for digital twins, was developed in [22] to address the issue of decentralized data sharing for digital twins. The work [23] showed that integrating digital twins with blockchain provided security, and the transactions could be traceable. Blockchain has been used [24] to protect software copyrights and integrate heterogeneous resources in the social manufacturing community. The authors [25] proposed Big Digital Twin Data (BDTD), an integrated model of digital twins and big data.

They also embed blockchain in BDTD for security purposes. Digital Twin Wireless Networks (DTWN) [26] is a model in which the digital twin is implemented over wireless networks. The privacy of data in this network is preserved by using the blockchain. Proof-of-Federalism (PoF) has been proposed in [27], which is a consensus algorithm for autonomous digital twin networks (DTN). A sustainable and shareable blockchain-based digital twin model has been introduced in [28] to mitigate many security challenges in a digital twin environment.

Table 3. The Mapping of Various Attacks with Different DT Operations

	OP1	OP2	OP3	OP4	OP5	OP6	OP7	OP8	OP9	Severity
ST1	√	√	√	√	√	√	√	√	√	VH
ST2	√	√	√	√	√	√	√	√	√	VH
ST3	×	√	√	×	×	×	×	×	×	L
ST4	√	×	×	×	×	×	×	×	×	L
ST5	√	×	×	×	×	×	×	×	×	L
ST6	×	√	√	√	√	√	√	√	√	VH
ST7	√	√	√	√	√	√	√	√	√	VH
ST8	×	√	√	√	√	√	√	√	√	VH
ST9	√	√	√	√	√	√	√	√	√	VH
ST10	×	√	√	√	√	√	√	√	√	VH
ST11	×	√	√	√	√	√	√	√	√	VH
ST12	×	√	√	√	√	√	√	√	√	VH
ST13	×	√	√	√	√	√	√	√	√	VH
ST14	×	×	×	×	×	√	√	√	√	H
ST15	×	×	×	×	×	√	√	√	√	H
ST16	×	×	×	×	×	√	√	√	√	H
ST17	×	×	×	×	×	√	√	√	√	H

A blockchain-based digital twin framework was presented in [29] to detect Bot formation in a Smart Factory environment. In [30], a blockchain-enabled synchronized provable data possession scheme (BSPDP) was designed for digital twins. This work used tag verification to secure the virtual space of digital twins. A blockchain-based digital twin model has been adopted to secure the virtual space of the 6G nodes in [1]. The transfer learning was also used for data security purposes. A blockchain-based hierarchical digital twin IoT (HDTIoT) model has been designed [31] to provide a reliable and secure real-time computing environment.

The work rendered by the researchers discussed above strongly infers that the blockchain is a technique to establish a secure digital platform for many real-time applications. Additionally, blockchain can also be used for end-to-end authentication purposes.

Edge Computing

The huge amount of data generated on a real-time basis must be stored distantly in the cloud for better storage and processing [32], [33]. While storing the data in a cloud computing environment provides better management, attackers can alter the integrity of the data during its transmission to cloud servers. Therefore, edge computing can be effectively adopted to avoid these attacks [34].

By adopting edge computing, edge servers are placed between the sensors and the cloud server. The edge server stores the data and performs some processing before sending them to the cloud server. Data encryption techniques can protect data from intruders while transmitting it. Using edge computing empowered by artificial intelligence mitigates many security issues in the digital twin environment [35], [36]. Moreover, it can also mitigate latency and bandwidth issues. Thus, the overall cost of data transmission can also be drastically reduced, as it provides data processing at the data source and sends the data to the cloud server. The effective uses of

edge computing for security can be found in detail in [37], [38].

Fog Computing

Fog computing is a technique to store and process data generated from devices connected to the Internet of Things. Fog nodes are the intermediate servers between IoT devices and a cloud server. It works differently from edge computing by selectively sending the required data to the cloud server. Like edge computing, it mitigates many security issues, latency issues, and bandwidth issues. The work [39] used a fog network to detect light spam accounts on mobile social networks. The encryption scheme has been applied in [40] to facilitate a secured connection in fog computing.

The work [41] suggested secure attribute-based data sharing in fog computing. A ciphertext policy-based encryption technique is presented in [42]. A secured access control mechanism has been proposed in [43] to ensure fog computing security. The works discussed here attempt to secure the fog networks, thereby providing better security management for the operations of the digital twin if the fog nodes are used for sensing the data across the physical layer.

Intrusion Detection System (IDS)

The intrusion detection system monitors network traffic and sends alerts in response to malicious activities. The IDS may be signature-based or anomaly-based, depending upon the type of attack that it would detect. An intrusion detection algorithm in the digital twin was implemented to facilitate remote monitoring for security purposes [44]. The authors [45] comprehensively reviewed different network intrusion detection systems (IDS). They noted that machine learning-based IDSs are more secure and privacy-preserving. The work [46] used a feed-forward neural network to develop an IDS to detect security threats like DoS, DDoS, and information theft.

The paper [47] proposed SVELTE, an IDS that detects target routing attacks like spoofing, selective forwarding, and sinkholes.

An IDS based on a hybrid CNN model has been proposed in [48] for detecting eavesdropping, sinkhole attacks, and DoS attacks. The authors [49] used ANN to detect DoS and DDoS attacks in simulated IoT networks.

An IDS has been developed in [50] that uses a genetic algorithm and deep belief network (DBN) to detect intrusions like probes and DoS in conventional IoT platforms. [51] Embedded blockchain with a digital signature to prevent worm attacks, flooding attacks, and malicious code injection attacks. Recurrent ANN has been used in [52] to design IDS for fog nodes to prevent attacks like a probe or DoS.

[53] describes a supervised approach-based IDS for smart home applications that detect attacks such as reconnaissance, DoS, man-in-the-middle, and reply attacks.

A two-stage hierarchical Network Intrusion Detection (H2ID) with a MultiModal Deep AutoEncoder (M2-DAE) was presented in [54] to detect attacks such as DoS, DDoS, data theft, and scan attacks. A new IDS has been suggested in [55] for the IoT environment to detect DoS, probe, exploit, and generic. An adversarial attack is proposed in [56] for DL-based network IDS (NIDSs) in the IoT platform. A deep learning (DL)--based IDS by [57] was presented to detect attacks like DoS, probe, user-to-root (U2R), and remote-to-local (R2L) attacks. A DL-based IDS fine-tuned by neighborhood search-based particle swarm optimization (NSBPSO) is designed [58] to detect different network attacks.

Machine learning-based IDS can also be found in [59]. Similarly, Graph Neural Networks (GNN) based IDS and an ensemble-based voting classifier-based IDS are presented in [60], [61], [62], used federated learning in a digital twin environment to detect DDoS attacks. The work in [63] addressed timing attacks on the DT system, which makes the devices' timing asynchronous, thus drastically hampering data transmission. A new approach, namely Anomaly detection with digiTAl twIN (ATTAIN), has been developed in [64] using a GCN-LSTM-based Generative Adversarial Network (GAN) for the detection of an anomaly.

The work [65] discussed AI's role in overcoming security issues in digital twins. The authors [66] proposed a real-time stacked ensemble classifier to detect DoS, command injection, and calculated and naive measurement modifications. Similar works can also be found in [67], [68], [69], and [70]. Table 4 presents the existing works related to IDS to mitigate different security threats (ST1-ST17).

Table 4. Comparison of Existing Work Related to IDS to Mitigate Different Security Threats

Paper	ST1	ST2	ST3	ST4	ST5	ST6	ST7	ST8	ST9	ST10	ST11	ST12	ST13	ST14	ST15	ST16	ST17
[46]	×	×	×	×	×	×	×	×	×	√	√	×	×	×	√	×	×
[47]	×	×	×	×	×	×	√	√	×	×	×	√	×	×	×	×	×
[48]	×	×	×	×	×	×	×	×	×	√	×	√	×	×	×	×	×
[49]	×	×	×	×	×	×	×	×	×	√	√	×	×	×	×	×	×
[50]	×	×	×	×	×	×	×	×	×	√	×	×	×	×	×	×	×
[51]	×	√	×	×	×	×	×	√	×	×	×	×	×	×	×	√	√
[52]	×	×	√	×	×	×	×	×	×	√	×	×	×	×	×	×	×
[53]	×	×	×	×	×	√	×	×	√	√	×	×	×	×	√	×	×
[54]	×	×	×	×	×	×	×	×	×	√	√	×	×	×	√	×	×
[55]	×	×	×	×	×	×	×	√	×	√	×	×	×	×	√	×	×
[56]	×	×	×	×	×	√	×	√	×	√	×	×	×	×	×	×	×
[57]	×	×	×	×	×	×	×	√	×	√	×	×	×	×	√	×	×
[58]	×	×	×	×	×	×	×	√	×	×	×	×	×	×	√	×	×
[59]	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
[60]	×	×	×	×	×	×	×	√	×	√	×	×	×	×	√	×	×
[61]	×	×	×	×	×	×	×	×	×	√	×	×	×	×	√	×	×
[62]	×	×	×	×	×	×	×	√	×	√	×	×	×	×	×	×	×
[63]	×	×	×	×	×	×	×	×	×	√	×	×	×	×	√	×	×
[64]	×	×	×	×	×	×	×	√	×	×	×	×	×	×	√	×	×
[65]	×	×	×	×	×	×	×	√	×	√	×	×	×	×	√	×	×
[66]	×	×	×	×	×	×	×	×	×	√	×	×	×	×	√	×	×

Comparison of Different State-of-the-Art Methods to Mitigate Security Issues in Digital Twin

The various state-of-the-art techniques for addressing security concerns with a digital twin are highlighted in Table 5. The attacks (ST1, ST2, ST4, ST5) about the sensor nodes are physical attacks by the adversary. Therefore, mitigating these threats requires implementing physical mechanisms to prevent unauthorized access to these devices. Side-channel attacks can be avoided by using blockchain technology. Furthermore, by decentralizing data as blocks across the network, the blockchain mitigates data in-transit attacks (ST6) and spoofing attacks. Among the approaches outlined, IDS can only detect network-specific attacks such as routing attacks (ST8), man-in-the-middle attacks (ST9), DoS attacks (ST10), and DDoS attacks (ST11). IDS employs supervised machine learning models that have been pre-trained to detect such attacks. Even though blockchain technology embedded with other technology can handle DoS (ST9) and DDoS (ST10) attacks, it is far from mitigating these attacks. The Sybil attack is extremely severe, but none of the techniques can mitigate it. Phishing attacks (ST14) can only be mitigated by human intervention, along with smart techniques like auto-filtering unwanted emails or emails received from strangers. All techniques discussed so far are capable of mitigating attacks related to application layers, such as data theft (ST15), data breach (ST16), and spyware, malware, and ransomware (ST17).

Future Scope and Open Research Challenges

Improved and Real-time IDS

Although IDS can resist network-specific threats, more research is needed. This is because IDS relies on machine learning-based pre-trained models trained on a particular dataset. Although these models render very high accuracy over the validation dataset, their prediction accuracy is challenging when deployed over real-time scenarios. In this regard, the model must be trained and validated over real-time data extracted after deployment.

Integration of Blockchain and Digital Signature

The decentralized power of blockchain can be effectively utilized by embedding it with digital signatures to mitigate most attacks, including the Sybil attack [67]. However, the inclusion of a digital signature may ramp up memory requirements and CPU processing. Thus, memory-efficient and time-efficient digital signature-based blockchain technology should be proposed and simulated to mitigate such attacks.

Secured Channelization

Both fog computing and edge computing provide flexibility in processing the sensed data from the devices and sending the important data to the cloud server. Though they provide some security means, as discussed earlier, establishing secured channels with devices may mitigate side-channel attacks, routing attacks, and sinkhole attacks, to name a few. Thus, it provides an open research challenge to researchers to propose different models for secured channel establishment.

Integration of Blockchain with Edge/Fog Computing

The blockchain can be integrated with edge computing or fog computing to transmit sensitive data as blocks to the cloud server. Thereby mitigating some attacks (refer to Table 5).

Table 5. The Comparison of Different State-of-the-Art Methods to Mitigate Security Threats in Digital Twin

ST	Blockchain	Edge Computing	Fog Computing	IDS
ST1	×	×	×	×
ST2	×	×	×	×
ST3	√	×	×	×
ST4	×	×	×	×
ST5	×	×	×	×
ST6	√	√	√	×
ST7	√	×	×	×
ST8	×	×	×	√
ST9	×	×	×	√
ST10	×	×	×	√
ST11	×	×	×	√
ST12	×	×	×	×
ST13	×	×	×	×
ST14	√	√	√	√
ST15	√	√	√	√
ST16	√	√	√	√
ST17	√	√	√	√

CONCLUSION

As a digital representation of a physical object, system, or structure, digital twins focus on providing businesses with real-time insights into the entire lifespan of these assets; however, the same level of control and visibility can also be a doorway for malicious hackers. This paper discusses the obstacles and possible solutions associated with protecting the physical systems' data generated or enhanced by digital twin technology. We explore the potential security threats of digital twin technology and highlight some of the most pressing concerns that researchers and

practitioners will need to address in the future to harness the full benefits of the digital twin.

REFERENCES

[1] M. O. Ozdogan, L. Carkacioglu, and B. Canberk, "Digital twin driven blockchain based reliable and efficient 6G edge network," in *2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, IEEE, 2022, pp. 342–348, doi: https://doi.org/10.1109/DCOSS54816.2022.00062.

[2] R. Stark, C. Fresemann, and K. Lindow, "Development and operation of Digital Twins for technical systems and services," *CIRP Ann.*, vol. 68, no. 1, pp. 129–132, 2019, doi: https://doi.org/10.1016/j.cirp.2019.04.024.

[3] D. M. Botín-Sanabria, A.-S. Mihaita, R. E. Peimbert-García, M. A. Ramírez-Moreno, R. A. Ramírez-Mendoza, and J. de J. Lozoya-Santos, "Digital twin technology challenges and applications: A comprehensive review," *Remote Sens.*, vol. 14, no. 6, p. 1335, 2022, doi: https://doi.org/10.3390/rs14061335.

[4] M. Liebenberg and M. Jarke, "Information systems engineering with Digital Shadows: Concept and use cases in the Internet of Production," *Inf. Syst.*, vol. 114, p. 102182, Mar. 2023, doi: https://doi.org/10.1016/j.is.2023.102182.

[5] H. Hassani, X. Huang, and S. MacFeely, "Impactful Digital Twin in the Healthcare Revolution," *Big Data Cogn. Comput.*, vol. 6, no. 3, p. 83, Aug. 2022, doi: https://doi.org/10.3390/bdcc6030083.

[6] S. Sarp, M. Kuzlu, Y. Zhao, and O. Gueler, "Digital Twin in Healthcare: A Study for Chronic Wound Management," *IEEE J. Biomed. Heal. Informatics*, vol. 27, no. 11, pp. 5634–5643, Nov. 2023, doi: https://doi.org/10.1109/JBHI.2023.3299028.

[7] Z. Zhu, X. Xi, X. Xu, and Y. Cai, "Digital Twin-driven machining process for thin-walled part manufacturing," *J. Manuf. Syst.*, vol. 59, pp. 453–466, Apr. 2021, doi: https://doi.org/10.1016/j.jmsy.2021.03.015.

[8] Y. Fan *et al.*, "A digital-twin visualized architecture for Flexible Manufacturing System," *J. Manuf. Syst.*, vol. 60, pp. 176–201, Jul. 2021, doi: https://doi.org/10.1016/j.jmsy.2021.05.010.

[9] Y. Maïzi and Y. Bendavid, "Building a digital twin for IoT smart stores: a case in retail and apparel industry," *Int. J. Simul. Process Model.*, vol. 16, no. 2, p. 147, 2021, doi: https://doi.org/10.1504/IJSPM.2021.115868.

[10] R. R. Singh, G. Bhatti, D. Kalel, I. Vairavasundaram, and F. Alsaif, "Building a Digital Twin Powered Intelligent Predictive Maintenance System for Industrial AC Machines," *Machines*, vol. 11, no. 8, p. 796, Aug. 2023, doi: https://doi.org/10.3390/machines11080796.

[11] R. Rayhana, L. Bai, G. Xiao, M. Liao, and Z. Liu, "Digital Twin Models: Functions, Challenges, and Industry Applications," *IEEE J. Radio Freq. Identif.*, pp. 1–1, 2024, doi: https://doi.org/10.1109/JRFID.2024.3387996.

[12] D. Mourtzis, "Digital twin inception in the Era of industrial metaverse," *Front. Manuf. Technol.*, vol. 3, p. 1155735, 2023, doi: https://doi.org/10.3389/fmtec.2023.1155735.

[13] D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal, and H. Janicke, "Digital Twins and Cyber Security–solution or challenge?," in *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, IEEE, 2021, pp. 1–8, doi: https://doi.org/10.3390/bdcc6030083.

[14] R. Mattioli *et al.*, *Identifying Emerging Cybersecurity Threats and Challenges for 2030*. ENISA_2, 2023. [Online]. Available: https://books.google.co.id/books?id=zlXbzwEACAAJ

[15] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security

threats," *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 1–13, 2023, https://doi.org/10.1016/j.iotcps.2022.12.003.

[16] B. Lei, P. Janssen, J. Stoter, and F. Biljecki, "Challenges of urban digital twins: A systematic review and a Delphi expert survey," *Autom. Constr.*, vol. 147, p. 104716, 2023, https://doi.org/10.1016/j.autcon.2022.104716.

[17] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 3, pp. 1475–1503, 2022, doi: https://doi.org/10.1109/COMST.2022.3171465.

[18] C. Mandolla, A. M. Petruzzelli, G. Percoco, and A. Urbinati, "Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry," *Comput. Ind.*, vol. 109, pp. 134–152, 2019, https://doi.org/10.1016/j.compind.2019.04.011.

[19] F. Tao *et al.*, "Digital twin and blockchain enhanced smart manufacturing service collaboration and management," *J. Manuf. Syst.*, vol. 62, pp. 903–914, 2022, doi: https://doi.org/10.1016/j.jmsy.2020.11.008.

[20] D. Guo *et al.*, "A framework for personalized production based on digital twin, blockchain and additive manufacturing in the context of Industry 4.0," in *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)*, IEEE, 2020, pp. 1181–1186, doi: https://doi.org/10.1109/CASE48305.2020.9216732

[21] C. Zhang, G. Zhou, H. Li, and Y. Cao, "Manufacturing blockchain of things for the configuration of a data-and knowledge-driven digital twin manufacturing cell," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11884–11894, 2020, doi: https://doi.org/10.1109/JIOT.2020.3005729.

[22] B. Putz, M. Dietz, P. Empl, and G. Pernul, "Ethertwin: Blockchain-based secure digital twin information management," *Inf. Process. Manag.*, vol. 58, no. 1, p. 102425, 2021, doi: https://doi.org/10.1016/j.ipm.2020.102425.

[23] D. Lee, S. H. Lee, N. Masoud, M. S. Krishnan, and V. C. Li, "Integrated digital twin and blockchain framework to support accountable information sharing in construction projects," *Autom. Constr.*, vol. 127, p. 103688, 2021, doi: https://doi.org/10.1016/j.autcon.2021.103688

[24] M. Li, Z. Li, X. Huang, and T. Qu, "Blockchain-based digital twin sharing platform for reconfigurable socialized manufacturing resource integration," *Int. J. Prod. Econ.*, vol. 240, p. 108223, 2021, doi: https://doi.org/10.1016/j.ijpe.2021.108223.

[25] W. Shen, T. Hu, C. Zhang, and S. Ma, "Secure sharing of big digital twin data for smart manufacturing based on blockchain," *J. Manuf. Syst.*, vol. 61, pp. 338–350, 2021, doi: https://doi.org/10.1016/j.jmsy.2021.09.014.

[26] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks," *IEEE Trans. Ind. Informatics*, vol. 17, no. 7, pp. 5098–5107, 2020, doi: https://doi.org/10.1109/TII.2020.3017668.

[27] Y. Qu, L. Gao, Y. Xiang, S. Shen, and S. Yu, "Fedtwin: Blockchain-enabled adaptive asynchronous federated learning for digital twin networks," *IEEE Netw.*, vol. 36, no. 6, pp. 183–190, 2022, doi: https://doi.org/10.1109/MNET.105.2100620.

[28] C. Wang, Z. Cai, and Y. Li, "Sustainable blockchain-based digital twin management architecture for IoT devices," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6535–6548, 2022, doi: https://doi.org/10.1109/JIOT.2022.3153653.

[29] M. M. Salim, A. K. Comivi, T. Nurbek, H. Park, and J. H. Park, "A blockchain-enabled secure digital twin framework

for early botnet detection in IIoT environment," *Sensors*, vol. 22, no. 16, p. 6133, 2022, doi: https://doi.org/10.3390/s22166133.

[30] T. Li, H. Wang, D. He, and J. Yu, "Synchronized provable data possession based on blockchain for digital twin," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 472–485, 2022, doi: https://doi.org/10.1109/TIFS.2022.3144869.

[31] D. Wang, B. Li, B. Song, Y. Liu, K. Muhammad, and X. Zhou, "Dual-driven resource management for sustainable computing in the blockchain-supported digital twin IoT," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6549–6560, 2022, doi: https://doi.org/10.1109/JIOT.2022.3162714.

[32] Y. Liu *et al.*, "A novel cloud-based framework for the elderly healthcare services using digital twin," *IEEE access*, vol. 7, pp. 49088–49101, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2909828.

[33] S. Lipsa, R. K. Dash, and K. Cengiz, "An adaptive software-defined networking (SDN) for load balancing in cloud computing," *Intell. Netw. Des. Driven by Big Data Anal. IoT, AI Cloud Comput.*, p. 135, 2022, doi: https://doi.org/10.1049/PBPC054E_ch7.

[34] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2924045.

[35] G. Premsankar, M. Di Francesco, and T. Taleb, "Edge computing for the Internet of Things: A case study," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1275–1284, 2018, doi: https://doi.org/10.1109/JIOT.2018.2805263.

[36] L. Rosencrance, "6 significant issues that edge computing in IoT solves," TechTarget. [Online]. Available: https://www.techtarget.com/iotagenda/feature/6-significant-issues-that-edge-computing-in-IoT-solves

[37] M. Alrowaily and Z. Lu, "Secure edge computing in IoT systems: Review and case studies," in *2018 IEEE/ACM symposium on edge computing (SEC)*, IEEE, 2018, pp. 440–444, doi: https://doi.org/10.1109/SEC.2018.00060.

[38] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE access*, vol. 6, pp. 18209–18237, 2018, doi: https://doi.org/10.1109/ACCESS.2018.2820162.

[39] J. Zhang, Q. Li, X. Wang, B. Feng, and D. Guo, "Towards fast and lightweight spam account detection in mobile social networks through fog computing," *Peer-to-Peer Netw. Appl.*, vol. 11, pp. 778–792, 2018, doi: https://doi.org/10.1007/s12083-017-0559-3.

[40] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE access*, vol. 5, pp. 9131–9138, 2017, doi: https://doi.org/10.1109/ACCESS.2017.2705076.

[41] A. Alotaibi, A. Barnawi, and M. Buhari, "Attribute-based secure data sharing with efficient revocation in fog computing," *J. Inf. Secur.*, vol. 8, no. 3, pp. 203–222, 2017, doi: https://doi.org/10.4236/jis.2017.83014.

[42] Y. Jiang, W. Susilo, Y. Mu, and F. Guo, "Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 720–729, 2018, doi: https://doi.org/10.1016/j.future.2017.01.026.

[43] Z. Yu, M. H. Au, Q. Xu, R. Yang, and J. Han, "Towards leakage-resilient fine-grained access control in fog computing," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 763–777, 2018, doi: https://doi.org/10.1016/j.future.2017.01.025.

[44] F. Akbarian, E. Fitzgerald, and M. Kihl, "Intrusion detection in digital twins for industrial control systems," in *2020 International Conference on Software,*

Telecommunications and Computer Networks (SoftCOM), IEEE, 2020, pp. 1–6, doi: https://doi.org/10.23919/SoftCOM50211.2020.9238162.

[45] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, doi: https://doi.org/10.1109/COMST.2019.2896380.

[46] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC)*, IEEE, 2019, pp. 256–25609, doi: https://doi.org/10.1109/PRDC47002.2019.00056.

[47] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013, doi: https://doi.org/10.1016/j.adhoc.2013.04.014.

[48] S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for internet of things (IoT)," *J. ISMAC*, vol. 2, no. 04, pp. 190–199, 2020, doi: https://doi.org/10.36548/jismac.2020.4.002.

[49] E. Hodo *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, 2016, pp. 1–6, doi: https://doi.org/10.1109/ISNCC.2016.7746067.

[50] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2903723.

[51] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Futur. Gener. Comput. Syst.*, vol. 96, pp. 481–489, 2019, doi: https://doi.org/10.1016/j.future.2019.02.064.

[52] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simul. Model. Pract. Theory*, vol. 101, p. 102031, 2020, doi: https://doi.org/10.1016/j.simpat.2019.102031.

[53] F. Alsakran, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion detection systems for smart home iot devices: experimental comparison study," in *International Symposium on Security in Computing and Communication*, Springer, 2019, pp. 87–98, doi: https://doi.org/10.1007/978-981-15-4825-3_7.

[54] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescapé, "A hierarchical hybrid intrusion detection approach in IoT scenarios," in *GLOBECOM 2020-2020 IEEE global communications conference*, IEEE, 2020, pp. 1–7, doi: https://doi.org/10.1109/GLOBECOM42002.2020.9348167.

[55] V. Kumar, A. K. Das, and D. Sinha, "UIDS: a unified intrusion detection system for IoT environment," *Evol. Intell.*, vol. 14, no. 1, pp. 47–59, 2021, doi: https://doi.org/10.1007/s12065-019-00291-w.

[56] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, and M. Qiu, "Adversarial attacks against network intrusion detection in IoT systems," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10327–10335, 2020, doi: https://doi.org/10.1109/JIOT.2020.3048038.

[57] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3803, 2022, doi: https://doi.org/10.1002/ett.3803.

[58] S. Baniasadi, O. Rostami, D. Martín, and M. Kaveh, "A novel deep supervised learning-based approach for intrusion detection in IoT systems," *Sensors*, vol. 22, no. 12, p. 4459, 2022, doi: https://doi.org/10.3390/s22124459.

[59] M. Sarhan, S. Layeghy, N. Moustafa, M.

Gallagher, and M. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT networks," *Digit. Commun. Networks*, 2022, doi: https://doi.org/10.1016/j.dcan.2022.08.012.

[60] W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann, "E-graphsage: A graph neural network based intrusion detection system for iot," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2022, pp. 1–9, doi: https://doi.org/10.1109/NOMS54207.2022.9789878.

[61] M. A. Khan *et al.*, "Voting classifier-based intrusion detection for iot networks," in *Advances on Smart and Soft Computing: Proceedings of ICACIn 2021*, Springer, 2022, pp. 313–328, doi: https://doi.org/10.48550/arXiv.2104.10015.

[62] D. Su and Z. Qu, "Detection ddos of attacks based on federated learning with digital twin network," in *International Conference on Knowledge Science, Engineering and Management*, Springer, 2022, pp. 153–164, doi: https://doi.org/10.1007/978-3-031-10989-8_13.

[63] T. Mohamed, M. Kezunovic, J. Lusher, J. C. Liu, and J. Ren, "The use of digital twin for timing intrusion detection in synchrophasor systems," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, IEEE, 2022, pp. 1–5, doi: https://doi.org/10.1109/PESGM48719.2022.9916964.

[64] Q. Xu, S. Ali, and T. Yue, "Digital twin-based anomaly detection in cyber-physical systems," in *2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST)*, IEEE, 2021, pp. 205–216, doi: https://doi.org/10.1109/ICST49551.2021.00031.

[65] M. Groshev, C. Guimarães, J. Martín-Pérez, and A. de la Oliva, "Toward intelligent cyber-physical systems: Digital twin meets artificial intelligence," *IEEE Commun. Mag.*, vol. 59, no. 8, pp. 14–20, 2021, doi: https://doi.org/10.1109/MCOM.001.2001237.

[66] S. A. Varghese, A. D. Ghadim, A. Balador, Z. Alimadadi, and P. Papadimitratos, "Digital twin-based intrusion detection for industrial control systems," in *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, IEEE, 2022, pp. 611–617, doi: https://doi.org/10.1109/PerComWorkshops53856.2022.9767492.

[67] S. Lipsa, T. N. Nguyen, and R. K. Dash, "A New Signature-Based Blockchain Paradigm: Foreseeable Impact on Healthcare Applications," *IEEE Internet Things Mag.*, vol. 5, no. 3, pp. 146–151, 2022, doi: https://doi.org/10.1109/IOTM.001.2200017.

[68] S. Lipsa and R. K. Dash, "A Novel Dimensionality Reduction Strategy Based on Linear Regression with a Fine-Pruned Decision Tree Classifier for Detecting DDoS Attacks in Cloud Computing Environments," in *International Symposium on Artificial Intelligence*, Springer, 2022, pp. 15–25, doi: https://doi.org/10.1007/978-3-031-22485-0_2.

[69] S. Lipsa and R. K. Dash, "A novel intrusion detection system based on deep learning and random forest for digital twin on IOT platform," *Int. J. Sch. Res. Eng. Technol*, vol. 2, pp. 51–64, 2023, doi: 10.56781/ijsret.2023.2.1.0020.

[70] K. Cengiz, S. Lipsa, R. K. Dash, N. Ivković, and M. Konecki, "A novel intrusion detection system based on artificial neural network and genetic algorithm with a new dimensionality reduction technique for UAV communication," *IEEE Access*, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3349469.