Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.064903 Published Online: 04 July 2025

REVIEW

# Intrusion Detection in Internet of Medical Things Using Digital Twins—A Review

**Tony Thomas*, Ravi Prakash and Soumya Pal**

School of Computer Science and Engineering, Kerala University of Digital Sciences, Innovation and Technology (Digital University Kerala), Thiruvananthapuram, 695317, India

*Corresponding Author: Tony Thomas. Email: tony.thomas@duk.ac.in

Received: 27 February 2025; Accepted: 18 June 2025

**ABSTRACT:** The Internet of Medical Things (IoMT) is transforming healthcare by enabling real-time data collection, analysis, and personalized treatment through interconnected devices such as sensors and wearables. The integration of Digital Twins (DTs), the virtual replicas of physical components and processes, has also been found to be a game changer for the ever-evolving IoMT. However, these advancements in the healthcare domain come with significant cybersecurity challenges, exposing it to malicious attacks and several security threats. Intrusion Detection Systems (IDSs) serve as a critical defense mechanism, yet traditional IDS approaches often struggle with the complexity and scale of IoMT networks. With this context, this paper follows a systematic approach to analyze the existing literature and highlight the current trends and challenges related to IDS in the IoMT domain. We leveraged techniques like bibliographic and keyword analysis to collect 832 research works published from 2007 to 2025, aligned with the theme "Digital Twins and IDS in IoMT." It was found that by simulating device behaviours and network interactions in IoMT, DTs not only provide a proactive platform for early threat detection, but also offer a scalable and adaptive approach to mitigating evolving security threats in IoMT. Overall, this review provides a closer look into the role of IDS and DT in securing IoMT systems and sheds light on the possible research directions for developers and the research community.

**KEYWORDS:** Cybersecurity; digital twin; healthcare security; internet of medical things; IoMT; intrusion detection system; IDS

## 1 Introduction

The fourth industrial revolution, known as Industry 4.0, has rapidly transformed industries worldwide through its innovations. This digital revolution has significantly increased productivity through its adoption in different areas of industries like Cyber-Physical Systems (CPS) [1] and smart manufacturing. The main driving components behind today's Industry 4.0 paradigm include various advanced technologies like Machine Learning (ML), Deep Learning (DL), Artificial Intelligence (AI), the Internet of Things (IoT), and Digital Twins (DTs) [2,3]. These technologies have enabled businesses to automate processes, optimize operations, and create innovative products and services with higher efficiency [4,5].

In the evolving digital ecosystem, advanced technologies are being harnessed to transform physical assets from the real world into interconnected smart objects or things. This interconnectedness, among other things, lays the foundation of the IoT [6,7], enabling Machine-to-Machine, or M2M, communication for things in the network. These devices, including computers, smart sensors, and various mobile devices, are accessible via Internet Protocol, or IP, over cloud environments. Therefore, the core functional components

of any IoT system comprise devices, network infrastructure, communication protocols, and an application layer for device access and management within the IoT network. However, depending on the specific use case, specialized architectural models have been proposed for IoT solutions. Industrial IoT (IIoT) [8–10] is one such solution that entirely focuses on leveraging the IoT technology in different industrial contexts like Industrial Control Systems (ICS) [11,12], CPS [13–15], design and smart manufacturing [13,16], and many more.

The utilization of IIoT or IoT in healthcare is typically referred to as the Internet of Medical Things (IoMT) [17–19]. Although, the medical sector has always been adaptive towards technical changes, the COVID-19 pandemic particularly accelerated the adoption of novel technologies including IoT for a wide scope of applications such as social distance monitoring [20,21] and patient data collection [21,22]. The IoMT has successfully been applied in many other medical solutions like personalized assistance [23], disease diagnosis [24,25], and patient monitoring [18,19]. It has significantly advanced the healthcare domain, enhancing the capabilities of medical processes in multiple dimensions.

DT, a relatively nascent technology and a crucial element of the industrial metaverse, is another component that is making substantial contributions to the success of Industry 4.0. The functional components of DTs can be presented as a combination of data acquisition, management, modeling, and visualization [4]. These components enable DT to serve as a virtual representation of physical devices, networks, and simultaneously synchronized processes with the corresponding physical twin [1,3]. It enables professionals to remotely monitor, manage, and test physical assets in real-time [26,27]. Additionally, the AI and ML-integrated DTs are also used for smart decision-making and industrial automation. DTs have been used across industries for numerous applications related to supply chain management [28,29], autonomous vehicles [30], agriculture [31], and security [12,32,33].

Beyond these multidisciplinary applications of DT, it has also been frequently used in the healthcare domain [34,35]. As pointed out in [3], DTs are dominating prognostics and health management domains through various applications. It includes drug development [36–38], disease modeling [39], and medical training through simulations [40], to name a few. As these DT-based healthcare solutions are closely integrated with the IoT, this new dimension of technological evolution is further enhancing modern IoMT solutions.

The interconnected model of devices in an IoT network makes it challenging to maintain the privacy and security of the system to a large extent. IoT devices can continuously generate data that must be sent to the edge servers due to their limited storage, processing, and battery capacity [41]. In addition to that, these devices often suffer from hardware and firmware vulnerabilities, which can be exploited through various means [42–44]. The IoMT is transforming healthcare by connecting medical devices for real-time data exchange, advancing the current healthcare sector. However, in IoMT, this connectivity and inherent limitations introduce substantial cybersecurity risks [35]. These risks potentially compromise patient privacy, medication effectiveness, and security in healthcare through attacks on hardware, data flow, and the IoMT network itself [20,45,46]. Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) play a suitable role in ensuring the security of the network through unwanted traffic [47–50]. Therefore, noticing the criticality of the healthcare sector and the increasing security threats in this domain, it has become crucial to review the current security of IoMT networks.

Through a comprehensive synthesis of current research, this paper examines various IoMT architectures proposed in the literature, which emphasize service and communication efficiency, security, scalability, and responsiveness. It also highlights the role of DT-based IDS to safeguard IoMT networks against emerging cyber threats, optimizing operational efficiency and overall cybersecurity. Additionally, we present the impact of IDS development and its functional components across different scenarios. We also explore

approaches that incorporate Blockchain Technology (BCT), anomaly detection, AI/ML, and Federated Learning (FL) as part of distributed data strategies. These approaches offer innovative pathways for threat detection and improve detection accuracy while preserving data privacy. Through this systematic survey, we aim to answer the following four Research Questions (RQs):

**RQ1:** How does the Internet of Medical Things (IoMT) contribute towards the development of the smart healthcare industry?
**RQ2:** What are the security challenges in IoMT? How do the various Intrusion Detection System (IDS) solutions address them?
**RQ3:** How does Digital Twin (DT) technology play a vital role in IoMT security?
**RQ4:** What are the issues associated with integrating DTs in IoMT?

The rest of this paper is organized as follows: Section 2 outlines the methodology employed in this Systematic Literature Review (SLR), including the criteria for literature selection, and analysis. Section 3 provides an overview of the evolution and applications of the IoMT within the healthcare domain, emphasizing the integration of emerging technologies. Subsequently, Section 4 elaborates on the concept of DTs, exploring their architectures and their pivotal role within the IoMT infrastructure, as well. Section 5 investigates the security challenges prevalent in smart healthcare systems, with a detailed examination of IDS and their significance. Building upon the insights gained from these sections, Section 6 addresses the RQs formulated in Section 1. Finally, Section 7 presents potential directions for future research and applications, followed by the conclusion of the study in Section 8. The abbreviations table is also provided in Appendix A as Table A1.

## 2 Methodology

This study focuses on the theme "Digital Twins and IDS in IoMT" and aims to answer the four RQs raised in Section 1. We followed a systematic literature review approach inspired by [44,51]. To ensure a comprehensive review, we carried out a bibliographic analysis of the data collected from the Web of Science (WoS) database using two sets of queries, *"IDS for IoMT or Healthcare"* and *"Digital Twin for IoMT or Healthcare"*. To understand the inherent research trends with more depth, a keyword network was generated using the Visualization of Similarities viewer or VOSviewer software [52], which is shown in Fig. 1. Here, inter-keyword link strength is only indicated if it is 8 or higher. Moreover, all the keywords shown in Fig. 1 appeared at least 15 times. Four major keyword clusters emerged, with prominent terms including *digital twin(s), healthcare, artificial intelligence, security, internet of things, blockchain*, and *challenges*.

These clusters motivated us to categorize the retrieved articles into three groups, as described later in this section. We now detail the complete literature selection process followed in this review, which was conducted in three stages: *identification*, *screening*, and *final inclusion*.

### *2.1 Identification*

This is the first process for selecting the most suitable works for this review. Based on insights from our initial analysis (Fig. 1), we created the keywords and retrieved 832 research works from various databases, including Web of Science, and Scopus, using APIs through manually drafted Python scripts. We then removed 27 duplicate works to have a final set of 805 unique papers. These works were published in major digital venues including IEEE Xplore, Elsevier, Springer, MDPI, and Wiley. Fig. 2 indicates that most of these records were published in 2024 and belonged to the *"Open Access"* category. We also retrieved 16 relevant research articles through a manual search.

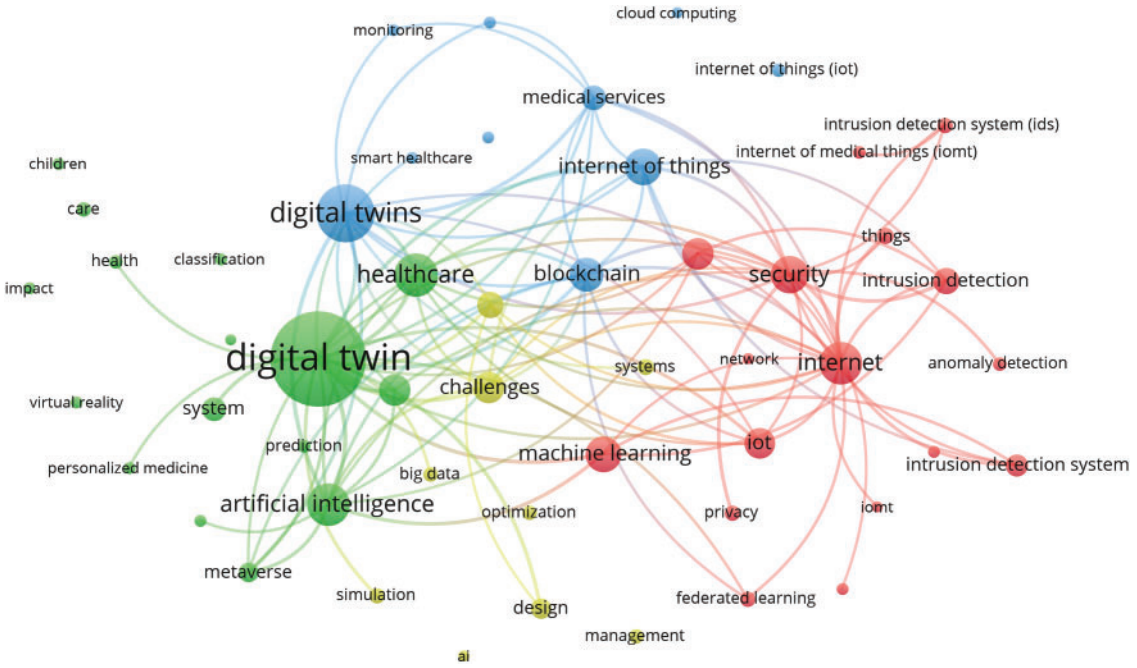


**Figure 1:** Network of top keywords from articles published on the theme "Digital Twins and IDS in IoMT"

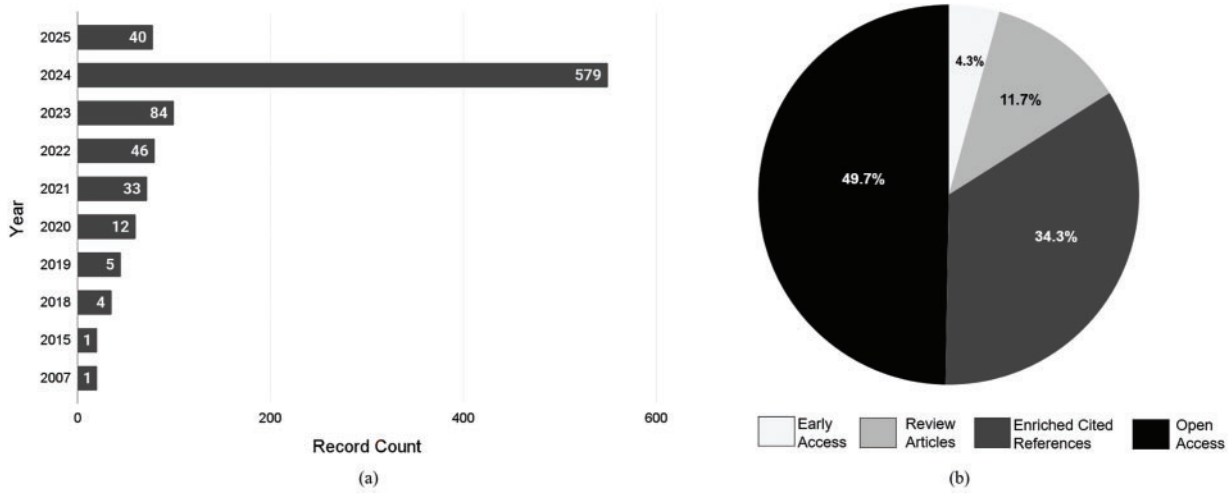


**Figure 2:** Year-wise publication count *(left)*, and publication type distribution *(right)* of 805 records

### *2.2 Screening*

After retrieving the research papers, we applied a systematic screening of all retrieved works to rationally include or exclude articles. The criteria for including the articles were as follows:

- **Publication venue:** Articles published in peer-reviewed conference proceedings or journals.
- **Citation count:** Articles cited at least four times.
- **Type of work:** Full-length research articles, review papers, or survey papers.
- **Peer-review status:** Only articles that underwent peer review.

Articles that did not meet these criteria were excluded from the study.

### 2.3 Final Inclusion

After the screening process, a total of $N = 116$ research papers were selected for final evaluation. Abstracts, results, and conclusions of these papers were manually reviewed, leading to the identification of $N = 53$ articles that closely aligned with the core theme of our research. Additionally, $N = 13$ articles were manually searched and analyzed by the authors to supplement the study. The final screening process of abstracts and results substantially minimized the risk of excluding quality papers from the study. Hence, we finally included $N = 66$ (53 + 13) articles in this review. Table 1 presents a summary of selected recent survey and review articles in the domains of IoMT, DTs, and IDS advancements. The complete article selection process for this review is illustrated in the PRISMA chart shown in Fig. 3.

**Table 1:** Some existing surveys and reviews on IoT/IoMT, DTs, and IDS

| Ref. | Focus | Relevance | Findings |
|---|---|---|---|
| [34] | Applications & challenges | IoMT, DT | PRISMA-based review of DT in healthcare, emphasizing current trends and its potential for patient care and other operations. Lack of implementation research is pointed as an opportunity. |
| [35] | Healthcare security | IoMT, IDS | A systematic review highlighting weakness of the IoMT and role of IDS to strengthen security. |
| [19] | Healthcare IoT | IoT/IoMT | Reviews IoT device capabilities & architectures in healthcare. Highlights security, interoperability, and scalability challenges; exploring future trends with TinyML & BCT. |
| [3] | Applications & challenges | IoMT, DT | Reviews role of DT in Industry 4.0, emphasizing prognostics and health management. Deals with modeling challenges, cyber-physical integration, and the need for advanced tools. |
| [1] | Cybersecurity & DT | IoT, DT | Explores DTs as a cybersecurity solution for Industry 4.0 CPS, addressing APT threats. It highlights key vulnerabilities, and proposes secure DT design for enhanced threat detection and mitigation. |
| [45] | ML/DL-based IDS for IoMT | IoMT, IDS | Surveys ML and DL-based IDS for IoMT, highlighting security challenges, and detection methods. Also suggests the need for lightweight, adaptive IDS for secure and efficient healthcare. |
| [51] | AI-based IDS for IoMT | IoMT, IDS | Reviews AI-based IDS in IoMT, with a novel taxonomy of IDS schemes. The work emphasizes architecting lightweight, real-time, and resource-aware security solutions for smart IDS. |
| [20] | Security & FL | IoMT, IDS | Surveys FL for privacy-preserving AI in smart healthcare. It covers real-world IoMT applications, highlights key benefits, and suggests future directions to enable secure and collaborative data analysis. |

(Continued)

**Table 1 (continued)**

| Ref. | Focus | Relevance | Findings |
|---|---|---|---|
| [18] | Security & FL | IoT/IoMT | Explores IoMT evolution and benefits with three case studies and highlights the role of BCT & AI to overcome staff shortages and long wait times. |
| [41] | FL-based IDS | IoT, IDS | Reviews FL for anomaly-based IDS in IoT by analyzing challenges like single-model convergence, and offers practical insights for privacy-preserving. |

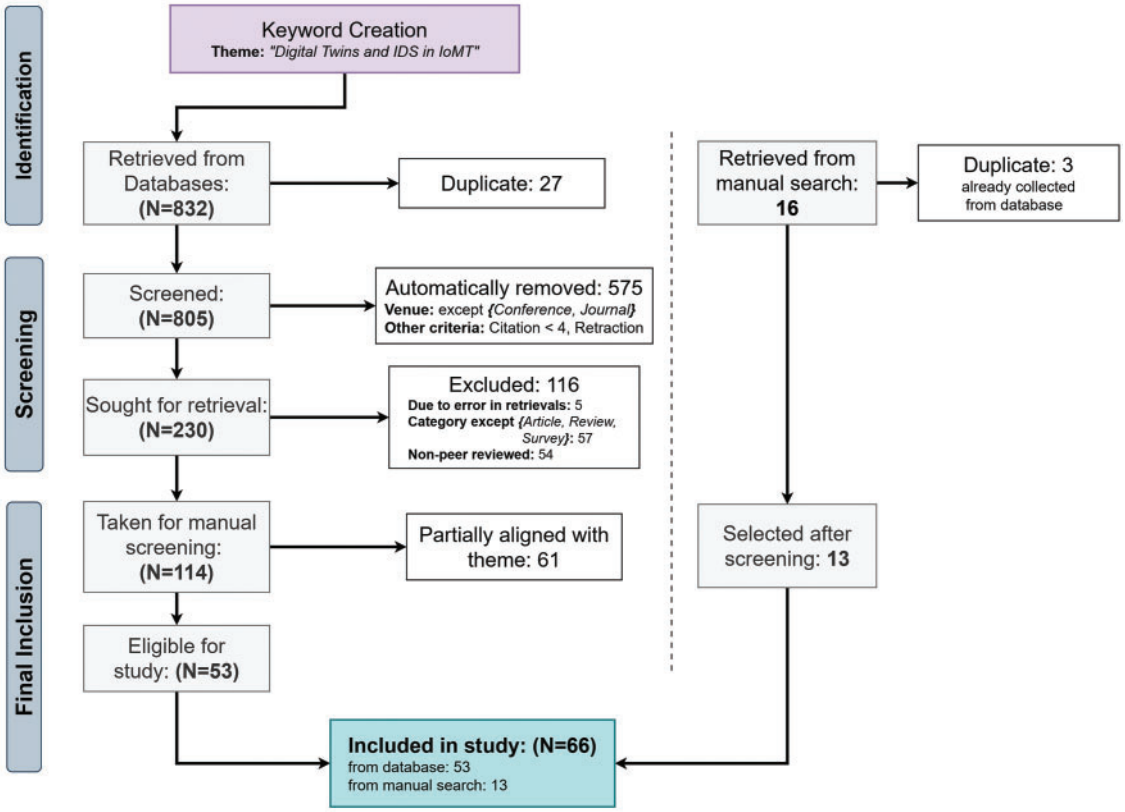


**Figure 3:** PRISMA chart of the selection of final articles

The selected set of 66 articles contributed to the three main categories—IoMT [18,19], DT [1,53], and Security. These papers are listed in Table 2, along with their relevance mapped to the four RQs. Here, **C** stands for I∩S∩D. Most of the papers selected in our research belong to more than one category, while three works [4,50,54] were categorized in all groups. Furthermore, papers contributed only to the *'security'* category were found to be largely aligned with the IDS technologies. We have represented the relevance of these papers to the categories using a Venn diagram, as shown in Fig. 4. It indicates that all the papers contributing to the IoMT were found to be relevant to the RQs.

**Table 2:** Mapping RQs with selected literature

| | I-(D∪S) | S-(I∪D) | D-(I∪S) | (I∩S)-C | (I∩D)-C | (S∩D)-C | C=I∩S∩D |
|---|---|---|---|---|---|---|---|
| **Paper** | [18–20,22,59] | [41,47,49,51, 98,100–102,104,105] | [1,3,8,53, 63–65,72, 77,121,122, 124,126] | [10,35,45,46, 55,90,74, 106–116] | [21,34,36,37, 40,62,67,68, 75,73] | [11,12,32,70, 117,118,123] | [4,50,54] |
| # | 5 | 10 | 13 | 18 | 10 | 7 | 3 |
| **RQ1** | ● | | | ● | ● | | ● |
| **RQ2** | ◐ | ◐ | | ● | | | |
| **RQ3** | | ◐ | ◐ | | ● | | ◐ |
| **RQ4** | | | ◐ | | ● | ◐ | ● |

Note: Legend: ●–completely addressed; ◐–partially addressed; **I**, **S**, **D** = Set of papers on IoMT, Security, DT, respectively.

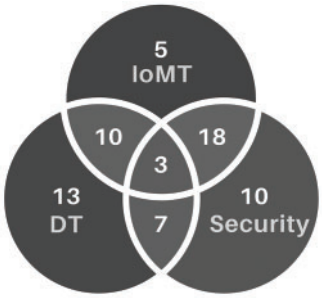


**Figure 4:** Categorization of selected papers based on three core research themes

Our preliminary analysis suggests a strong interrelationship between DTs and smart healthcare solutions leveraging the IoMT. However, existing research mainly focuses on limited aspects of the IoMT and its associated technologies, particularly concerning applications and healthcare security. This observation motivated us to conduct an in-depth investigation into the applications, challenges, and security considerations within the IoMT domain, and to explore the potential of DTs as a viable solution. In this survey, we initially discuss the existing IoMT and DT architectures and their applications across various domains. We then present the security challenges faced by IoMT networks and the different types of IDS used to ensure network security.

## 3 IoMT for Smart Healthcare

The IoMT is a specialized subset of IoT for the healthcare domain. It is recognized as a transformative technology with the potential to revolutionize the healthcare system for disease modeling, automated medication delivery, and many more. IoMT systems consist of numerous interconnected devices that assist healthcare professionals in collecting real-time data, enabling timely interventions and personalized treatments. Additionally, IoMT facilitates remote monitoring, allowing patient to receive medical care from their homes. Remote access to healthcare services enhances patient experience and frees up hospital resources.

As healthcare is a vast sector, the complexity of the IoMT system varies depending on the use case scenario. The complexity of an IoT/IoMT system typically depends on its various components. Based on the existing literature, three essential components can be identified, as illustrated in Fig. 5.

- **Hardware Components:** Hardware provides the foundation for the physical setup of IoMT that can be used for various purposes like patient data collection or monitoring.
- **Software Components:** Software is an integral component of any IoT system, serving as the interface between humans and machines. These components of IoMT are useful in processing and analyzing data, enabling valuable insights, facilitating seamless interaction, and ensuring the security of the system.
- **Communication Management:** Just like any IoT system, IoMT rely on some dedicated communication protocols to ensure the reliable and secure flow of information within the network. Some commonly used protocols include Message Queuing Telemetry Transport (MQTT), Bluetooth Low Energy (BLE), Constrained Application Protocol (CoAP), and ZigBee.

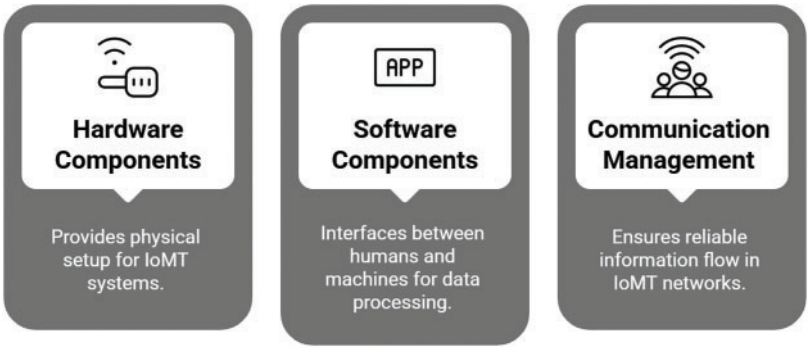


**Figure 5:** Three components of IoMT

Despite their systematic evolution and numerous benefits, the growing use of IoMT devices introduces significant security concerns. These devices are connected to the internet and rely on various communication protocols, making them susceptible to cyberattacks. Given that IoMT devices often handle sensitive patient data, any compromise in their security could lead to disastrous consequences, such as data breaches and disruption of medical treatments, which could put patients' lives at risk. To resolve various challenges and standardize medical IoT development, researchers have come up with several architectures for IoT/IoMT systems.

### *3.1 Architectures of IoMT*

Based on various IoT system architectures, researchers have emphasized the inclusion of multiple essential components. Being a subset of IoT systems, these architectures are also applicable for IoMT solutions. Here we discuss six common architectures of IoT/IoMT systems that are shown in Fig. 6.

#### *3.1.1 Traditional Three-Layer Architecture*

IoMT solutions rely on a range of functional components that work collectively to complete the tasks. These components can be hierarchically layered in three groups. In a traditional IoMT system, these three layers include *perception, network*, and *application layer* [19], as shown in Fig. 7. These layers can be considered the fundamental building blocks of any IoT system, as they are common across such networks. The functionality of each layer is as follows.

1. **Perception Layer:** This layer deals with recording the perception of the physical environment through different devices, actuators, and sensors for data collection. Hence, typically, the analogue data from the physical world is converted to a digital signal at the perception layer.

2. **Network Layer:** As the name suggests, this layer establishes communication between the device and the system over standard protocols. Popular IoT protocols such as MQTT, CoAP, ZigBee, BLE, and LPWAN are commonly used for communication across various network devices, including gateways, hubs, and switches. The network layer ensures the data transfer from the perception layer for further processing.
3. **Application Layer:** The processing of collected data and the presentation of insights occur at this final layer of the IoMT system. At this stage, the user can monitor, analyze, and process data received from the network layers while also interacting with the IoT system to make informed decisions.

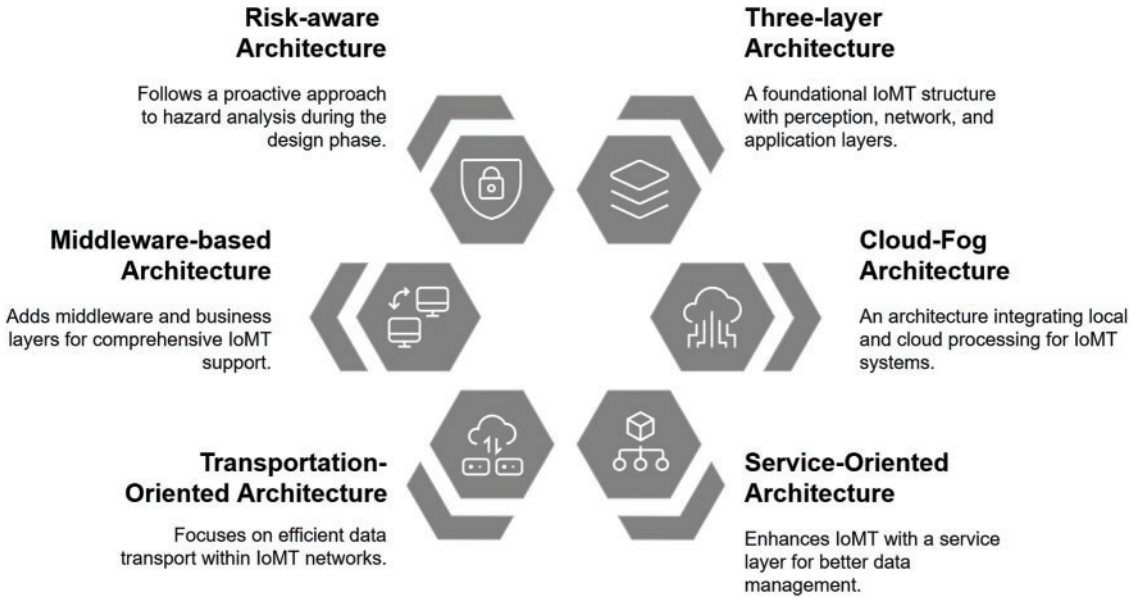


**Figure 6:** Six types of common IoT/IoMT architectures [18,19,51,55–58]

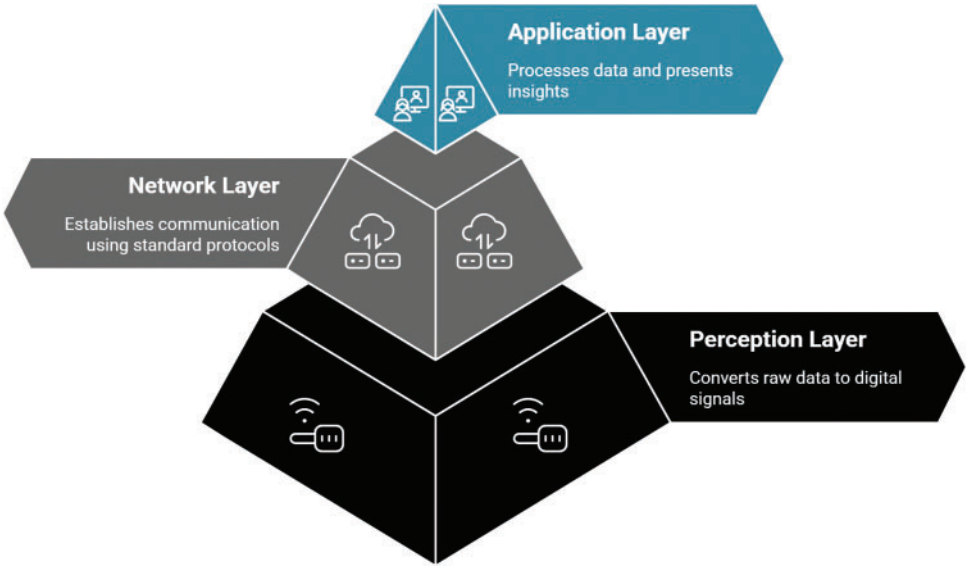


**Figure 7:** Traditional 3-layer architecture [19] of IoT/IoMT

*3.1.2 Cloud-Fog Architecture*

Cloud-Fog architecture [18,55] is also a three-layered IoMT architecture, where the layers are identified based on the hardware/software components, and data handling. The three layers in the cloud-fog architecture are—*things layer, fog layers*, and *cloud layers*.

1. **Things Layer:** The things layer comprises various devices, sensors, and actuators for patient monitoring. It also includes pharmacy controls, medical records, nutrition regimen generators, and more. This layer interacts closely with the users within the environment. The data for patient monitoring and remote care is collected at this layer.
2. **Fog Layer:** The fog layer operates above the things layer. This layer comprises local servers and gateway devices, which are essential components of a sparsely distributed fog networking framework. Here, lower-layer devices harness local processing power to provide real-time responses to users. Following this step, the gateway devices at this layer are responsible for forwarding data from these devices to the cloud layer for further processing.
3. **Cloud Layer:** This layer deals with data storage, computation, and analysis, which supports the decision-making process. The cloud layer also includes resources for storing data from the medical infrastructure, which can be accessed for analysis when needed.

*3.1.3 Service-Oriented Architecture*

In IoMT systems, tasks such as data storage over the cloud, data processing, and retrieval are also referred to as services. Hence, considering the services as a separate component from the application layer, the Service-Oriented Architecture or SOA-based architecture of IoT is an advancement over the traditional three-layer model [56]. Here, an additional layer is placed as the *service layer* between *network* and *application layers*. The service layer ensures the availability of sufficient services that are essential for the application layer in this framework. The main components of the service layer are associated with service management, discovery, composition, and interfacing.

*3.1.4 Transportation-Oriented Architecture*

As described in [51], three of the four layers in this architecture of the IoMT are identical to the SOA-based IoT model and have the same placement, as well. However, here the service layer is replaced with a *transport layer*. The transport layers aim to lighten the work at the network layer, as it primarily handles end-to-end data communication, ensuring that information collected from medical devices reaches the appropriate servers for analysis and storage. It securely transfers physiological data to medical servers for processing.

*3.1.5 Middleware-Based Architecture*

It is a five-layer IoT architecture where two extra layers are added along with the three essential layers of IoT systems. The newly added layers include the *middleware* and *business layers* [57].

1. **Middleware Layer:** This layer is placed between the network and application layers providing services for data management and communication.
2. **Business Layer:** The business layer is the final layer in this architecture, positioned above the application layer. Its primary function is to manage the data received from the application layer and apply processing steps efficiently.

*3.1.6 Risk-Aaware Architecture*

In IoMT networks, the interconnected system of body-area sensor networks, gateways, and cloud platforms facilitates real-time health data collection and personalized care. However, safety challenges, including component-level errors, emergent behaviours, and timing mismatches, can propagate through the system. It potentially leads to hazardous situations, as evidenced by real-world incidents such as pacemaker malfunctions.

To address these problems, a risk-aware IoMT model was proposed in [58] that introduces a proactive approach to hazard analysis during the design phase. This model leverages standardized languages like *architecture analysis* and *design language* and tools such as the Open Source Architectural Tool Environment to model errors, track their propagation, and identify safety constraints.

The methodology comprises four key steps for systematically identifying and analyzing hazards, as illustrated in Fig. 8. In the given context of [58], these steps are followed as follows:

1. Collecting historical fault data to identify and understand potential failure patterns.
2. Constructing feedback control loop architectures to diagnose abnormal interactions and system behaviours.
3. Designing safety architectures using modeling tools, such as *architecture analysis* and *design language* and EMV2, while defining safety requirements to mitigate hazards.
4. Applying the methodology to a pacemaker case study, where hazards and safety constraints are identified early in the Software Development Life Cycle (SDLC).

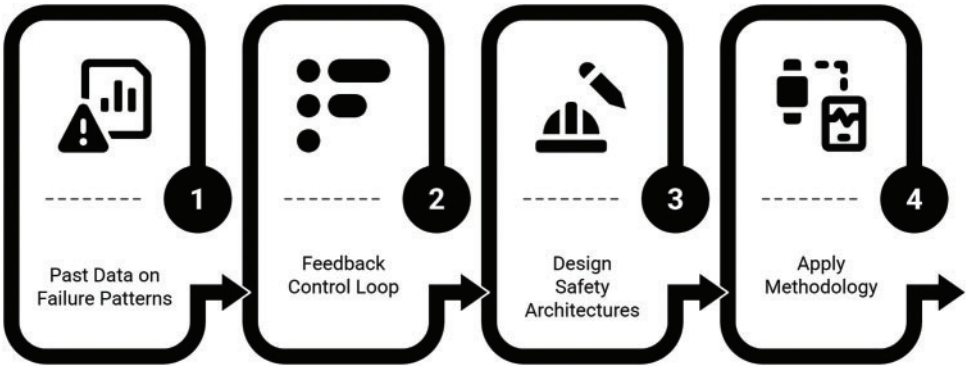


**Figure 8:** Four-step hazard identification and analysis

Timely identification of hazards ensures traceability, enhances the reliability of safety-critical IoT systems, and eliminates the need for specialized domain expertise.

### *3.2 Overall Contribution of IoMT*

So far, we have examined various IoMT architectures that have guided experts in developing suitable solutions across diverse medical applications and contexts. These architectures facilitate the integration of advanced technologies, enabling remote monitoring in smart healthcare systems and supporting the development of secure and robust medical solutions. As a result, they not only enhance personalized patient care but also offer more effective learning and training opportunities for healthcare practitioners. A summary of the overall contributions of IoMT is presented in Table 3.

**Table 3:** Contribution of IoMT in healthcare domain

| Advancements | Technology | Examples |
|---|---|---|
| Remote monitoring for patients | AI/ML | Solutions, based on the dedicated protocols, have been developed for healthcare monitoring through various medical sensors, actuators, and wearable devices for prompt support [18,19,22]. |
| Smart healthcare systems | AI/ML, BCT | BCT and AI-driven distributive data processing make the decision making robust while maintaining the privacy within smart healthcare solutions [20,22,59]. |
| Enhanced security in healthcare | Edge Computing, BCT | E-healthcare services maintain patient data privacy while reducing overall latency when these technologies are used [22,59]. |
| Personalized and context-aware healthcare | Cloud Computing | Personalized treatments and context-aware monitoring are enabled by the processing of large volumes of data on cloud servers [18,20]. |
| Surgical applications | Adaptive Learning, AR/VR/MR | Immersive simulations of critical medical conditions, like lung cancer, are valuable for medical training and adaptive diagnostics [40]. |
| Disease control and management | FL, BCT | Distributed learning techniques and BCT have proven their importance in overcoming the several challenges during the COVID-19 [18,20], including social distancing [21]. |
| Data-driven diagnostics/Treatment | AI/ML, FL | Smart healthcare leverage the AI and FL-based technologies for precise medication for diagnostics and treatments based on the historical data [18,19]. |

In summary, these architectures represent some of the most common IoT/IoMT system designs, each suited to different application scenarios. While they provide a foundation for connectivity and functionality, significant enhancements can be made to improve security and robustness. Furthermore, as discussed in Section 1, the integration of DTs in IoMT solutions is driving advancements in both application and security within the medical sector. In the following section, we will explore the evolution and adoption of DTs in the medical domain in greater detail.

## 4 Digital Twins

DT [53,60] serves as a virtual representation of a physical device or service. By facilitating the creation of an interactive virtual replica of the physical assets, DTs enable businesses to manage, test, and update the major industrial components like CPSs and ICSs. In the healthcare domain, DTs are used for numerous purposes like patient data modeling, drug design, and remote patient monitoring. As DTs can be created for devices in the physical world, IoT solutions have also started to utilize them in many scenarios [1,61,62]. We identified five distinct architectures for developing DTs, each adoptable across various domains. These are described in detail ahead in this section.

### *4.1 DT Architectures*

The DT technology has evolved into a fundamental component of modern cyber-physical systems, facilitating real-time monitoring, simulation, and decision-making across various domains. The architecture of a DT system determines its capabilities, efficiency, and adaptability to different applications. Several architectural models [33] have been proposed to address challenges related to data integration, security, scalability, and computational efficiency. This section explores such architectures, each designed to meet specific functional and operational needs, as shown in Fig. 9.

- **5-Dimensional Model:** A modular architecture that organizes the DT systems into five core components: physical entities, virtual models, DT data, connections, and services enhancing interoperability and system integration.
- **Digital Twin as a Proxy (DTaaP):** A four-layered approach that leverages DTs as logical hubs within Industrial CPS, ensuring efficient monitoring, diagnostics, and security through a structured communication framework.
- **CanTwin: 6-Layer Architecture:** A multi-layered DT model designed for real-time monitoring and management, particularly applied in environments requiring operational efficiency, such as canteen management during the COVID-19 pandemic.
- **Open-Source Architectures:** Leveraging open-source tools such as Eclipse Ditto, Apache Kafka, and InfluxDB, these architectures enable flexible and cost-effective DT implementations in Industry 4.0 and smart manufacturing.
- **Security-Oriented Architectures:** DT frameworks designed to enhance IoT and IoMT security by providing virtual replicas of physical devices, facilitating intrusion detection, anomaly analysis, and proactive cybersecurity measures.

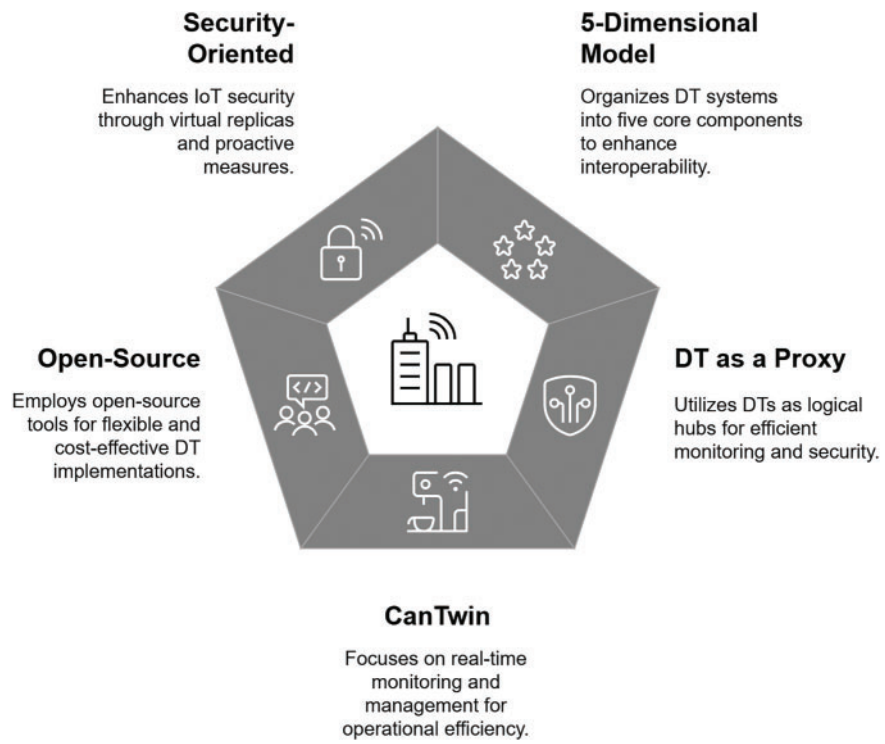


**Figure 9:** Architectures for the development of DTs [8,21,33,50,63–65]

Each of these architectures offers distinct advantages tailored to specific industry needs. The following sections provide an in-depth discussion of their structure, functionality, and real-world applications.

#### *4.1.1 5-Dimensional Model*

In [63], authors describe *makeTwin*, an architecture for digital twin systems, as fundamental to their functionality. It is characterized by a five-dimensional (5D) model consisting of the following components:

1. Physical entities
2. Virtual models
3. Digital twin data
4. Connections
5. Services

These components collectively facilitate robust interactions within the virtual environment. Along with the interactive components (DTs and physical devices) in this architecture, the perfect segregation of data handling and communication emphasizes modularity, which incorporates ten core functional modules to support the creation and deployment of digital twin applications. It allows the integration of various services like data processing, simulation, and visualization with the system, as exemplified by the *makeTwin* platform. The *makeTwin* platform also provides a comprehensive, flexible, and user-friendly architecture to meet diverse requirements by addressing challenges related to security and privacy concerns, and ultimately driving digital transformation and innovation across various industries.

#### *4.1.2 DTaaP: Digital Twin as a Proxy*

A DT emphasizes the Industry 4.0 characteristics of a device, product, and system. Therefore, it can be considered a logical hub in this context. It can be implemented for monitoring, diagnostics, prediction, and control in ICPS. In [64], the authors describe some challenges that affect the lifespan of the ICPS, and the concept of a DTaaP is proposed to overcome these challenges. The authors came up with a four-layer architectural model for the DTaaP that successfully meets the identified properties. All four layers of DTaaP are described below.

1. **Device Layer:** This layer of the proposed DTaaP model sets up the main industrial environment for the desired ICPS. The layer encloses all observable devices that should be monitored. It also includes the devices that can be remotely controlled and actuated.
2. **Communication Layer:** Each physical device also has a corresponding virtual replica. A communication layer is created to establish the communication between these synchronous physical-virtual device pairs. This layer can utilize a suitable communication architecture such as an Event-Driven Architecture (EDA) [66] or a SOA [56] according to the requirements.
3. **Proxy Layer:** The proxy layer acts as an abstraction between digital and real-world devices. The Digital Twin Framework (DTF) is deployed in this layer, which stores DTs according to device models. DTF is also responsible for providing connectivity and message translation to communicate with DTs. It ensures that DTs are only accessed by authorized parties. Authorized access is achieved by policies that can manage access rights for every single feature of a DT.
4. **Application Layer:** Interaction between users and DTs is realized at this layer. For interaction with a DT through the application layer, a user must be authorized and have sufficient access rights to the desired features of the DT.

The DTaaP architectural model implementation is based on the open-source Eclipse Ditto DTF in the proxy layer, which offers four main improvements to DT-based solutions: energy efficiency, availability and

state persistence, remote control, and security. These properties of the DTaaP model address issues associated with resource-constrained devices in an ICPS environment, such as a long lifespan, continuous service availability, and secure access and control. The experimental evaluation shows that this model is energy efficient, and the DT serves as an effective and efficient anchor point for security.

#### *4.1.3 CanTwin: 6-Layer Architecture*

The CanTwin model was applied in a real-world case study to manage a canteen during the COVID-19 pandemic [21]. The CanTwin architecture is designed to facilitate real-time monitoring and management of a canteen environment, particularly regarding social distancing measures. However, this architecture could be adopted for any of the similar use cases. The detailed overview of the 6 layers of this DT architecture is provided below:

1. **Physical Layer:** It represents the real-world environment where IoT devices are deployed. Sensors and actuators are used to monitor activities, environmental conditions, or device states. In this layer, privacy is maintained by tracking objects or individuals as abstract points.
2. **Data Layer:** This layer manages data collection, storage, and secure transmission. Sensor data is stored in scalable databases (e.g., MongoDB) and processed for insights. Security is ensured through encrypted communication and access controls for authorized users.
3. **Cognitive Unit Layer:** This layer transforms raw data into actionable insights. It helps to calculate metrics such as proximity, occupancy, or system efficiency and identifies patterns to improve system operations. This layer helps to optimize performance and ensure compliance with rules.
4. **Event Source Unit Layer:** This layer monitors the system anomalies and generates alerts.
5. **Service Layer:** It provides high-level services such as real-time monitoring, visualization, and predictive analytics. It offers ease in managing resource utilization, tracking compliance, and optimizing systems.
6. **User Interface Layer:** This layer offers an interactive dashboard for users to visualize system status and alerts. It allows monitoring and control of real-time IoT system. The interface simplifies interaction, making complex data accessible to end-users.

This comprehensive architecture not only addresses immediate health concerns but also enhances operational efficiency, making it a valuable model for similar applications in various environments.

#### *4.1.4 Open Source Architectures*

The open-source architectures are developed using free and open-source tools. Combined with the IoT for smart factories within Industry 4.0, DTs emphasize data acquisition, virtual representation, analytics, and visualization in real-time [8,65].

In [8], the authors proposed a universal architecture for DT-based systems by integrating five key open-source tools in the context of IIoT: Eclipse Hono, Eclipse Ditto, Apache Kafka, InfluxDB, and Grafana, as shown in Fig. 10. This architecture encompasses the main components of DT systems, including device connectivity, data streaming, storage, and interactive analytics. The significance of these tools in the proposed system is outlined below.

- **Eclipse Hono** provides a standardized interface for connecting, monitoring, and controlling IoT devices remotely across different protocols.
- **Eclipse Ditto** enables digital twin creation and secure interaction between physical and virtual assets.
- **Apache Kafka** facilitates real-time data streaming with scalability and fault tolerance.
- **InfluxDB** supports efficient time-series data storage.
- **Grafana** delivers a flexible analytics and visualization solution.

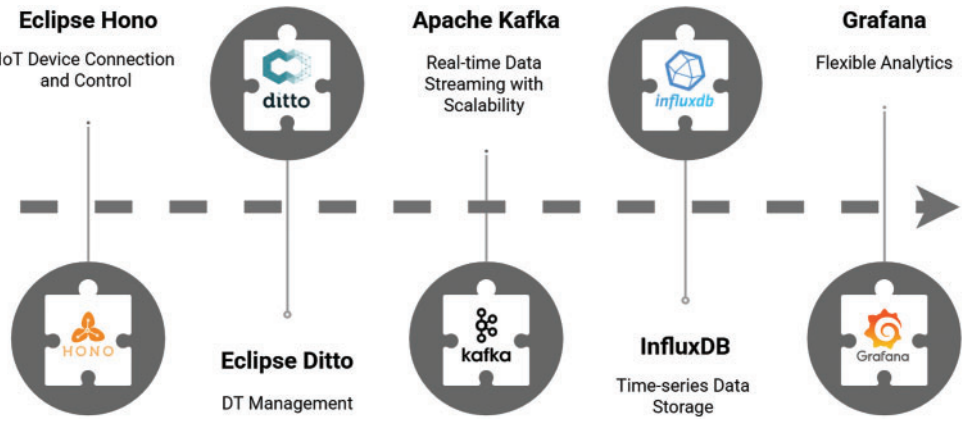


**Figure 10:** Open source DT architecture in [8]

Another novel DT framework was developed as per the concept of an open-source architectural model to manage a temperature-controlled physical system in real time [65]. Along with the *Eclipse Ditto*, this framework also includes *Raspberry Pi* and *OpenPLC* for remote monitoring and control. The role of *Eclipse Ditto* remains the same as in [8]. Fig. 11 shows a sequential coordination between three new open-source components in this DT architecture.

- **OpenPLC** is a program that automates the physical system by processing analog temperature data coming from the sensor.
- **Raspberry Pi** is used to integrate the physical devices.
- **Arduino** manages different tools to capture sensor data.

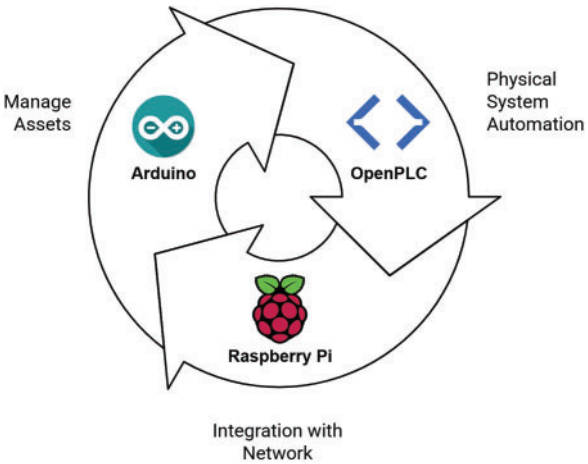


**Figure 11:** Open source DT architecture in [65]

Overall, we have noticed that open-source architecture significantly advances digital twin technology in smart manufacturing. It provides access to advanced tools and technologies, fostering collaboration between academia and industry. This collaborative approach accelerates innovation, enabling the development of new use cases and features. Additionally, open-source solutions make digital twins more affordable and accessible, empowering organizations of all sizes to leverage their benefits [8,65]. By facilitating rapid prototyping, experimentation, and knowledge sharing, open-source architectures drive the adoption of

digital twins, ultimately leading to improved operational efficiency, predictive maintenance, and enhanced system reliability.

#### *4.1.5 Security-Oriented Architectures*

Along with improving efficiency, maintenance, and system reliability, DTs play a vital role in security as well. In [50], authors emphasize the critical role of DTs in enhancing IoT/IoMT network security and management. Similar to [8], this security-oriented DTs model also leveraged Eclipse Ditto, InfluxDB, and Grafana, enabling real-time monitoring, interaction, and secure communication by setting up a testbed to create virtual representations of physical IoT/IoMT. Key properties of this framework are:

- DTs mirror physical counterparts and provide a unified and secure interface for managing device operations.
- Facilitating the cross-device and DT data exchange through standard protocols like MQTT and HTTP.
- Real-time data management and analysis to understand the device performance and system behaviour.
- Physical device abstraction through dynamic replication, centralized management, and enhanced security of the digital entities.

A security-oriented DTF strengthens the capability of systems to simulate real-world scenarios, allowing researchers to evaluate lightweight AIDS under various conditions.

We have noticed that DTs can significantly enhance the security of IoT/IoMT networks by creating a virtual replica of things and systems in the network. Such a kind of replication in the medical sector allows real-time monitoring and analysis of potential threats without disrupting actual medical operations. It also enables security professionals to detect anomalies, simulate cyberattacks, and evaluate vulnerabilities in a controlled environment, helping to proactively address weaknesses before they are exploited. Additionally, the DT can integrate with advanced technologies like BCT and ML for data security and automated threat detection. These advances provide a safe platform for testing incident response strategies through attack simulation, which ultimately strengthens the overall security of IoMT networks and keeps sensitive patient data protected.

### *4.2 Applications and Evolution*

In this section, we will present the various roles that DT plays in different scenarios. As DTs are used in various domains as a virtual proxy, these can be grouped based on their roles or types of usage. Fig. 12 shows some common roles of the DT across different domains. These applications of the DTs in IoT/IoMT and their security are described in this section.

- **A Proxy:** DTs are used in industrial and human-centric CPSs to represent the entities or individuals in real-time [64,67]. It is also used to replicate the devices in ICSs and healthcare sectors to monitor and interact with the systems. DTs are also built for the corresponding body parts for medical diagnosis and drug development [36].
- **Testing and Validation:** Being capable of strongly replicating the behaviour of physical twins, DTs act as a sandbox for testing new solutions. It allows the developer to validate solutions before deploying them on the physical twins [36]. In the medical sector, drug designing and development leverages this property of DTs [37].
- **Training and Assistance:** DTs provide remote access to the replica of physical assets. Considering its safety and cost efficiency, these models are used in educational and training environments. As they can improve work efficiency, DTs are helpful in critical medical scenarios like surgical training [40].

- **Synthetic Data Generation:** DTs operate in synchronization with their corresponding physical entities, making them uniquely specialized for their respective counterparts. Consequently, DTs are frequently utilized to generate synthetic data tailored to specific devices. This capability is particularly valuable for data anonymization to enhance privacy preservation and for addressing data imbalance challenges [1,68,69].
- **Security:** Since DTs can seamlessly integrate with advanced technologies such as BCT and AI/ML, they not only reduce the computational burden on physical devices but also enhance their security by incorporating robust protection mechanisms [1,70]. Research has demonstrated that each DT can deploy its own IDS to ensure a secure IoT/IoMT network [32].

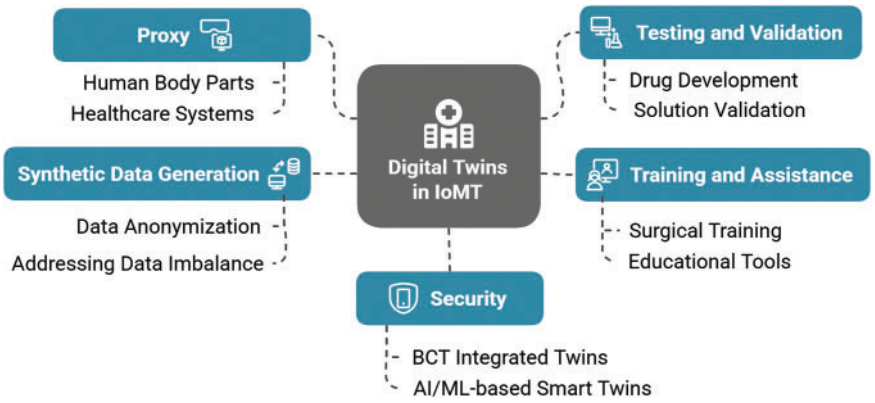


**Figure 12:** Common roles of DTs in medical domain

DTs enable parallel processing and automation by providing access to complex industrial and non-industrial systems while simultaneously interacting with their physical counterparts [71]. Additionally, they enhance security by serving as an abstraction layer [50], particularly for devices in critical environments such as ICS. Communication within DT systems follows three key paradigms: *a) Physical-to-Virtual (P2V)*, *b) Physical-to-Physical (P2P)*, and *c) Virtual-to-Virtual (V2V)* interactions, each requiring low latency, high reliability, and fault tolerance [53]. DTs primarily support P2V and V2V communication, with V2V interactions in complex networks extending across a vast number of participants, forming the foundation for DT Networks (DTNs).

DTNs mark a significant advancement in digital twin technology [72]. Unlike conventional DTs, DTNs facilitate seamless communication between physical and virtual entities, enabling real-time monitoring, control, and optimization across diverse domains. By leveraging IoT, cloud computing, 6G, and big data technologies, DTNs support advanced applications [53], including aviation and intelligent transportation, manufacturing and predictive maintenance, virtual commissioning, and remote operations. However, to fully harness their potential, challenges related to data security, privacy, and scalability must be effectively addressed.

### *4.3 Digital Twins in the Internet of Medical Things*

DTs are widely utilized across various application domains. Their prominence is also evident in the medical sector, especially in prognostics and health management solutions [3]. Some common applications of DT in IoMT are illustrated in Fig. 13 and Table 4.

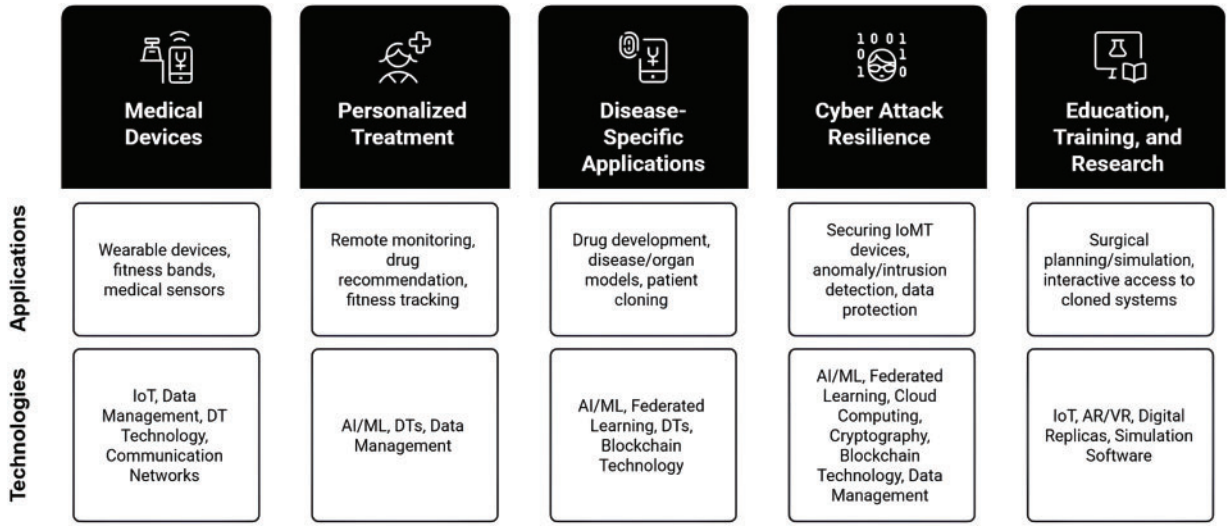


**Figure 13:** Applications of DT in IoMT development

**Table 4:** Examples of using DT in smart IoMT systems

| Categories | Examples |
|---|---|
| Medical devices | Wearable devices or sensors are mapped with the corresponding DT for real-time interaction and management [50]. |
| Personalized treatment | Using DT for actively monitoring the patient and personalized drug recommendation is found to be effective [21,34,68]. |
| Disease-specific applications | Disease-specific management like in case of COVID-19 and dengue [21,73], and drug development [37] are some novel applications of DT. |
| Cyber attack resilience | Centralized and decentralized anomaly detection [74] offer robust intrusion defense for secure smart healthcare IoMT systems [4] that can be addressed by DTs [69]. |
| Education, training, and research | Surgical simulations (e.g., lung cancer) [40], and ogran cloning (e.g, virtual liver) [36] leverage DT and immersive technologies for better medical training. |

The examples highlighted in Fig. 13 are categorized into five distinct groups. These examples are further elaborated in Table 4, which highlights the examples we analyzed in this work. More detailed discussions on each category of IoMT applications are provided in the following subsections.

*4.3.1 Medical Devices*

Separate DTs could be developed for the medical devices that are useful for patients. Such devices are either *implantable* or *wearable* [50,75], which are often found to be weak in terms of security, design, and authentication [35]. Implantable Medical Devices (IMDs) are placed in the human body, either permanently or temporarily, to support specific organs or tissues for direct treatment and monitoring. DTs of such devices can make it easier for continuous patient monitoring from remote locations. Internet of Wearable Medical

Devices (IoWDs) are hands-free gadgets with practical uses, powered by multiple sensors and enhanced with the ability to transfer and receive data over the network for supplementary health and fitness tracking. A fitness band or smartwatch can be considered an IoWD, whose DT can be used to monitor patient health in real time.

#### *4.3.2 Personalized and Remote Treatment*

The DT plays a pivotal role in providing personalized healthcare solutions and treatment, mainly in critical situations. To support such conditions, DTs can be used to replicate a human body part or to represent a patient's persona. Several DT-based solutions have been developed for patient monitoring through real-time data collection using various sensors [21,62,75]. Due to the real-time synchronization, these DTs can perform simultaneous analysis and make suitable proactive treatment adjustments, as well. One study also presented a DT-based solution for lung cancer care [68]. Such solutions indicate that DTs can significantly enhance the quality and effectiveness of modern healthcare systems.

#### *4.3.3 Disease Specific Applications*

COVID-19 has accelerated adoption of technology in healthcare. It led to the solutions developed using DT for monitoring social distancing [20] and diagnosis [20]. CanTwin [21] was one such solution that could consistently detect social distancing violations with 4-s latency. Moreover, the work showcased the applications of DTs for many other healthcare services.

Many diseases require special attention due to their novelty or uncommon transmission patterns, which may also evolve over time. DTs can be developed for such disease-specific scenarios to analyze the current progression and predict associated risks. A DT-based solution was proposed in [73] for managing dengue infections, where continuous patient health monitoring enabled early prediction of dengue likelihood. Such disease-specific DT implementations are also valuable for remote diagnosis and patient-centric disease modeling, enhancing personalized healthcare solutions [39].

#### *4.3.4 Cyber Attack Resilience*

The medical sector is not only embracing new technologies [3], but it is also increasingly becoming a target for cyber attacks [4,76]. DTs can be leveraged to address such challenges in IoT and IoMT solutions. In [1], the potential of DTs as a cybersecurity solution for CPS is explored. The study highlights that DTs can enhance the detection, response, and mitigation of cyber threats in IoT environments. Since IoMT is a subset of IoT, similar DT-based security solutions can be applied to safeguard IoMT systems from potential attacks. Additionally, DTs have been employed for privacy-preserving solutions through data anonymization techniques [1,68,69].

#### *4.3.5 Education, Training, and Research*

Education, training, and research represent critical applications of DTs, with the potential to significantly enhance the current state and future advancements in the smart healthcare sector. DT-driven surgical training and medical education can substantially improve the quality of healthcare services [21]. Furthermore, integrating DTs with AI has been demonstrated to be effective in various applications [36–38].

By combining DT-based solutions with advanced technologies such as ML, DL, Generative Adversarial Networks (GANs), Explainable AI (XAI), and BCT, robust, secure, and scalable healthcare solutions can be developed. These technologies not only automate repetitive tasks but also enable the creation of

intelligent systems capable of making informed decisions, thereby enhancing efficiency and accuracy in healthcare operations.

### *4.4 Issues Associated with DT*

#### *4.4.1 Security Issues*

DTs can be vulnerable not only in terms of the CIA triad—confidentiality, integrity, and availability—but also to threats targeting their physical counterparts and associated locations [4]. In the context of IoMT, the creation and maintenance of digital-physical links within a Digital Twin Network (DTN) require the exchange of sensitive patient data between the IoMT layer and the DT environment. Consequently, these factors raise significant concerns regarding data privacy and the integrity of medical information across various application scenarios [36,37,40,54]. Cyberattacks on DTs may exploit vulnerabilities in virtualization or cloning capabilities [4,33], potentially resulting in device spoofing or identity theft of the physical twin through a compromised digital counterpart.

Beyond these common security threats against numerous digital assets, the smart DTs could be vulnerable to adversarial attacks, as well. Such smart systems operate on advanced communication protocols like 6G and collaboratively tend to leverage the ML and FL methods for smart decision making. Hence, the malicious client-DT could lead to a data poisoning attack [77] against ML models.

#### *4.4.2 Other Challenges*

As the number of DTs in smart networks increases to support scalability, significant computational complexity is introduced within the DTN. Researchers also found that there have been limited work towards the implementation and DT lifecycle management [34]. In the case of ML-based DTNs, this challenge can be addressed through techniques such as ensemble modeling and optimized node arrangement [78,79]. Additionally, federated learning (FL)-based approaches [54], along with distributed and parallel simulation methods, can significantly accelerate the analysis of large-scale networks [80]. Furthermore, the use of sampling and modular techniques enables scalable DTN generation by focusing computational resources on critical network segments, thereby effectively managing complexity as the network grows [81].

Beyond these computational and security concerns, designing a robust IoMT system suitable for integration within a DTN must also adhere to regulatory frameworks such as HIPAA [82], which govern data ownership and privacy in the healthcare sector. These compliance requirements can present barriers to the seamless and widespread adoption of this promising integration. Navigating these trade-offs effectively is essential for realizing the full potential of DTs in enhancing IoMT security and advancing smart healthcare systems.

## 5 Smart Healthcare and Security

With the rapid advancement of Industry 4.0 technologies, the integration of smart healthcare systems with the IoMT has revolutionized patient care and medical services. However, this increased interconnectivity has also led to a significant rise in cyber threats. The impact of these attacks largely depends on the criticality of the targeted sector, and healthcare, being a highly sensitive domain that deals with vast amounts of confidential patient data, is particularly vulnerable.

IoMT, a key enabler of smart healthcare, connects medical devices, wearables, and healthcare infrastructure to facilitate real-time monitoring and data-driven decision-making. However, this interconnected ecosystem also creates opportunities for cybercriminals to exploit vulnerabilities, allowing attacks to spread rapidly across networks [1,46]. As a result, ensuring robust security measures in IoMT-based smart healthcare

systems is crucial to safeguarding patient privacy, data integrity, and overall system reliability. Some of the most common security threats in IoMT solutions are outlined below:

- **Device Vulnerabilities:** The hardware and firmware vulnerabilities associated with the lightweight IoMT devices [35] as well as high-end solutions like Computed Tomography (CT) scan and Magnetic Resonance Imaging (MRI) can be exploited to launch various attacks. These can include device failure, data manipulation, and privilege escalation [20,42,44].
- **Battery Drainage Attack:** IoMT solutions often consist of lightweight devices. These devices are designed to perform specific tasks only due to their limited battery capacity. Attackers generally exploit the resource constraint of these devices to drain the battery, which eventually puts the device to sleep or energy saving mode [83,84].
- **Eavesdropping Attack:** Due to the lack of privacy preserving in the communication channel of IoMT solutions, the attacker can eavesdrop on the information flow [85,86].
- **Advanced Persistent Threats (APTs):** The interconnected IoMT devices are also vulnerable to APT attacks, which can stay unidentified in the system for a longer duration and can also infect other devices in the network [1].
- **Other Attacks on IoMT:** Many of the previously mentioned attacks can be launched over the network through malicious requests. Such attacks on IoMT directly target the confidentiality, integrity, and availability constraints of the system [20,45]. Some of the most common threats against IoMT networks include Distributed Denial of Service (DDoS), Spoofing, and Man-in-the-Middle (MitM) attacks.

It is essential to identify and mitigate any cyber threats in IoMT for its seamless operation. The vulnerabilities within the network and its components are primarily responsible for these cyber attacks, which can mostly be classified into five distinct types, as explained in Table 5. Additionally, Fig. 14 provides a hierarchical summary of these vulnerabilities and their impacts.

**Table 5:** Potential cyber attacks in IoT/IoMT

| Category | Attack types | Description |
|---|---|---|
| Availability attacks | DoS/DDoS, Smurf | Disrupt access to resources, rendering systems unusable for legitimate users by overwhelming them with traffic or exploiting network protocols. |
| Integrity attacks | Injection, Backdoor, Worms, Data exfiltration | Compromise the trustworthiness and accuracy of data or system functionality through malicious code insertion, unauthorized access points, self-replicating malware, or unauthorized data theft. |
| Confidentiality attacks | MitM, Reconnaissance, Spoofing, Scanning, Heartbleed, Password Attack, Bruteforce, Patator (SSH/FTP), Ransomware, Botnet (like Mirai) | Aim to expose sensitive information to unauthorized parties by intercepting communications, gathering intelligence, disguising identities, probing for weaknesses, exploiting vulnerabilities, or gaining unauthorized credentials. |
| Access control attacks | Bruteforce, Patator (SSH/FTP), Password Attack, Backdoor | Focus on gaining unauthorized entry to systems or resources by attempting numerous login combinations, exploiting automated tools, or utilizing hidden entry points that bypass normal security mechanisms. |

(Continued)

**Table 5 (continued)**

| Category | Attack types | Description |
|---|---|---|
| Malware | Worms, Ransomware, Botnet or Mirai | Involve malicious software designed to harm or exploit systems, including self-propagating programs, data-encrypting extortionware, and networks of compromised devices controlled for malicious activities. |

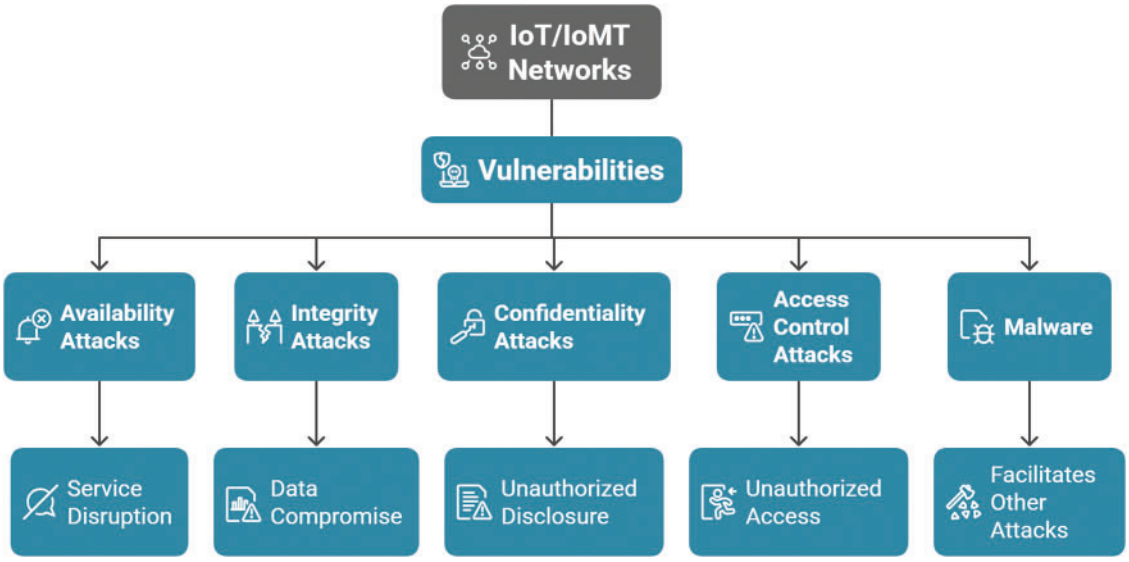


**Figure 14:** Security threats in IoT/IoMT

As a solution, the IDSs/IPSs are responsible for identifying malicious traffic in the network and preventing the system from various attacks, discussed so far. Most of the smart IDSs leverage advanced technologies like ML and DL for improved efficiency and responsiveness [45]. However, in order to develop such solutions, the data is a crucial requirement. Many of the benchmark datasets have been prepared to train these smart IDSs for security of IoT/IoMT networks. Table 6 covers the summary of attacks considered in four IoMT datasets.

**Table 6:** Attacks considered in different IoMT datasets

| Attack type | IoMT-TrafficData | ECU-IoHT | CICIoMTDataset | WUSTL-EHMS-2020 |
|---|---|---|---|---|
| DoS/DDoS | ✓ | ✓ | ✓ | ✗ |
| Injection | ✓ | ✓ | ✗ | ✗ |
| MitM | ✗ | ✗ | ✗ | ✓ |
| Reconnaissance | ✓ | ✗ | ✓ | ✗ |
| Spoofing | ✓ | ✓ | ✓ | ✗ |
| Scanning | ✓ | ✗ | ✗ | ✗ |
| Smurf | ✗ | ✓ | ✗ | ✗ |

In addition to the network datasets from IoMT, we also examined commonly used IoT and IIoT datasets related to the covered attacks, as summarized in Table 7. In total, we reviewed 11 datasets that have contributed to the development of various robust security solutions for IoT, with a particular focus on IoMT systems.

**Table 7:** Attacks considered in different IoT/IIoT datasets

| Attack type | TON_IoT | CICIDS 2017 | IoTID-20 | UNSW-NB15 | Edge-IIoTset | N-BaIoT |
|---|---|---|---|---|---|---|
| DoS/DDoS | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Injection | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| MitM | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ |
| Reconnaissance | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ |
| Backdoor | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ |
| Ransomware | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Mirai | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ |
| Bruteforce | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| **Others** | ✗ | FTP-Patator, SSH-Patator, Heartbleed | Scan | Fuzzers, Exploits, Shellcode, Worms | Password attack | Bashlite |

### *5.1 Benchmark IoT/IoMT Datasets*

Benchmark datasets are indispensable for developing and evaluating IDS in the ever-evolving IoT/IoMT landscape. These datasets provide standardized, real-world data, enabling researchers and developers to train, evaluate, and compare IDS models effectively. A robust benchmark dataset should accurately represent real-world traffic patterns, encompass a diverse range of attack scenarios, be correctly labeled, scalable, and publicly accessible. Creating such datasets poses significant challenges. Ensuring data privacy and security is paramount, especially when dealing with sensitive IoT/IoMT data. Simulating dynamic and adaptive attacks, which mimic real-world threat actors, is crucial for evaluating the robustness of IDS solutions. Developing datasets that capture the evolving tactics of attackers is essential to ensure the effectiveness of IDS.

To address the challenges outlined above and foster innovation in IoT/IoMT security, researchers and practitioners have developed a variety of benchmark datasets. These datasets provide a valuable resource for training, evaluating, and refining IDS models. In the following section, we will delve into some of the prominent benchmark datasets used in IoT/IoMT security research.

#### *5.1.1 CICIoMT2024*

The CICIOMT2024 dataset [87] addresses the growing security challenges in the healthcare IoMT landscape by providing a benchmark dataset designed to enhance cyber threat detection. A key contribution of this research is its IoMT testbed and innovative approach to simulating cyberattacks across different protocols. IoMT testbed comprises 40 IoMT devices, of which 25 are real devices and 15 are simulated devices. They divided these devices based on 3 protocols (eg, WiFi, MQTT, Bluetooth). In this IoMT testbed, they performed 18 different cyber attacks and stored the network traffic to develop the dataset. Additionally, the dataset facilitates the development of ML models for detecting and classifying cyberattacks, providing a robust resource for real-time threat detection and prevention. By integrating automated ML techniques, it enhances IoMT security, enabling more effective cyber defense in healthcare settings.

#### *5.1.2 IoMT-TrafficData*

The rapid growth of IoMT devices has introduced new security challenges. To address this, researchers have developed IoMT-TrafficData [88], a comprehensive dataset containing both benign and malicious network traffic [46]. This dataset enables the evaluation of IDSs specifically designed for IoMT environments. The study [46] highlights the effectiveness of flow-based features over packet-based features in detecting malicious traffic. By leveraging ML algorithms, researchers can develop robust IDSs capable of identifying and preventing attacks. The paper presents a detailed methodology for dataset creation, including scenario composition, attack generation, and data collection.

#### *5.1.3 ECU-IoHT*

The ECU-IoHT dataset [89] offers a significant contribution to the field of IoT/IoMT security. It addresses the critical need for publicly available datasets that reflect real-world cyberattacks targeting Internet of Healthcare Things (IoHT) systems. By capturing a diverse range of attack scenarios, including ARP spoofing, DDoS, SMURF, and injection attacks, this dataset enables researchers and security professionals to gain invaluable insights into the tactics, techniques, and procedures employed by malicious actors.

#### *5.1.4 WUSTL-EHMS-2020*

This dataset, collected from a real-time Enhanced Healthcare Monitoring System (EHMS) testbed, offers a unique blend of network flow metrics and patient biometric data. By combining these two data streams, the WUSTL-EHMS-2020 dataset [90] provides a comprehensive view of potential cyberattacks in IoMT environments. It is particularly useful for developing and evaluating IDS capable of detecting a wide range of cyber threats, including man-in-the-middle attacks and data breaches. The WUSTL-EHMS-2020 dataset contributes to advancing the security of IoT/IoMT systems and protecting sensitive patient data.

#### *5.1.5 Other IoT Datasets*

Some other notable IoT datasets, such as WUSTL-IIOT-2021 [91] (similar to WUSTL-EHMS-2020), Edge-IIoTset [92], TON_IoT [9], CICIDS2017 [93], IoTID20 [94], N-BaIoT [95], and UNSW-NB15 [96], have significantly contributed to the field of IoT security research. KDDCUP99 [97] and NSL-KDD are two network traffic datasets. These datasets encompass a broad spectrum of normal and anomalous behaviours, including network traffic patterns, device interactions, and system logs. Analyzing these datasets provides researchers with valuable insights into potential vulnerabilities, attack strategies, and emerging threats. They have played a crucial role in the development and evaluation of intrusion detection systems, anomaly detection techniques, and other security solutions for IoT systems.

### *5.2 Role of IDS in Network Security*

IDSs aim to identify any unwanted traffic flowing through the network. Hence, an IDS mainly relies on the network data and its properties. This data may contain information related to network traffic like packet size, protocol, ports, IP-address and many more. A robust IDS efficiently processes this information to distinguish between genuine and malicious data. Moreover, smart IDSs not only recognize the malicious traffic among the genuine flow but are also capable of analyzing further and detecting the type of attack among the malicious traffic.

Most of the modern IDSs are developed using ML/DL and ensemble methods [47,49,98–100]. However, researchers have come up with various models for securing IoT networks from intrusions and presented meaningful insight from the same. Some of the takeaways about the IDS in IoT are discussed in this

section. Table 8 provides a comprehensive summary of aforementioned benchmark IoT and IoMT datasets utilized for IDS development. It categorizes datasets based on their domain (IoT, IoMT, or IIoT) and highlights the types of cyberattacks they cover. Additionally, it presents key features such as network traffic patterns, device-specific behaviours, and attack diversity, which are essential for evaluating and improving IDS models. These datasets span various application areas, IoHT, IIoT, and general IoT security, making them valuable resources for cybersecurity research.

**Table 8:** Summary of benchmark IoT/IoMT datasets for IDS development

| Dataset | Domain | Attacks covered | Key features |
|---|---|---|---|
| CICIoMT2024 | IoMT | 18 cyberattacks (WiFi, MQTT, Bluetooth) | IoMT testbed with 40 devices (25 real, 15 simulated); ML-based intrusion detection |
| IoMT-TrafficData | IoMT | Various attack types | Flow-based vs. packet-based feature comparison; IDS development |
| ECU-IoHT | IoHT | ARP spoofing, DDoS, SMURF, Injection | Real-world healthcare cyberattacks; IoHT-specific security analysis |
| WUSTL-EHMS-2020 | IoMT | Man-in-the-middle, data breaches | Network flow + patient biometric data; EHMS testbed |
| WUSTL-IIOT-2021 | IIoT | Various industrial cyber threats | Industrial IoT dataset; ICS security applications |
| Edge-IIoTset | IIoT | Botnets, DDoS, MitM, Scanning | Edge-based IIoT security; attack diversity |
| TON_IoT | IoT | DDoS, Data exfiltration, Backdoor | Telemetry and log-based IoT dataset |
| CICIDS2017 | IoT/Network | DoS, DDoS, Web attacks, Botnet | Network traffic with labeled attacks; IDS benchmark |
| IoTID20 | IoT | Various IoT cyber threats | IoT-specific malicious behaviour analysis |
| N-BaIoT | IoT/Botnet | Botnet attacks on IoT devices | IoT botnet behaviour profiling; anomaly detection |
| UNSW-NB15 | IoT/Network | Generic network-based threats | Hybrid feature-based IDS evaluation |

### *5.2.1 Feature Selection vs. Feature Extraction*

The characteristics of network traffic utilized by IDS as input are known as features. Given the potentially large number of features in network data, selecting the most relevant ones for analysis is crucial for effective anomaly detection: a process referred to as Feature Selection (FS). However, in many cases, new features need to be generated either by transforming existing features or through direct data analysis. This process, known as Feature Creation (FC), has been shown to enhance the performance of IDS.

The study by [101] addresses a key challenge in Network IDS (NIDS) for the IoT by comparing two feature reduction techniques: FS and Feature Extraction (FE). The results demonstrate that while FS improves classification accuracy, FE offers greater robustness to variations in feature count and enables the detection of a broader range of attacks. These findings can significantly improve the efficiency and accuracy of NIDS, particularly in resource-constrained IoT environments, including IoMT.

#### *5.2.2 Process Awareness*

Processes in IoT/IoMT systems are crucial operational technologies that are important for their functioning. Hence, the liveness of these processes is essential for these systems. However, identifying processes is a difficult task. It was found that IoT messaging protocols like MQTT and corresponding communication patterns also carry contextual information. The contextual information is helpful in identifying specific processes that could further assist in detecting the intrusion in IoT networks [102]. This novel framework, named MISSION, leveraged distributed tracing and process mining for process-aware intrusion detection in MQTT networks. It improved the explainability of anomaly-based NIDS. A process-aware IDS can effectively identify process-aware attacks like unauthorized data publishing and malicious topic subscriptions.

#### *5.2.3 Centralized Approach*

A centralized IDS is a single and only entity that offers intrusion detection to the complete network. This enables the IDS to have access to the entire network's traffic. Being a centralized system makes such a lightweight IDS most suitable for a small group of IoT devices [48]. It is found that the centralized IDSs are not only efficient to address security risks, but also more cost-effective [103]. However, such an IDS is not suitable for large or complex IoT networks and does not offer scalability.

#### *5.2.4 Decentralized Approach*

Decentralized approaches for IDS development utilize the concept of FL to offer a promising solution for enhancing the security of IoMT systems [41,98–100,104]. Through a collaborative learning process across multiple devices without sharing raw data, FL addresses privacy concerns and improves the robustness of IDS. In this approach, local ML/DL-based IDS models are trained on individual devices using their respective datasets. These models are then aggregated to create a global model, which is shared with all devices. This decentralized learning process ensures that sensitive medical data remains localized, mitigating the risk of data breaches. Additionally, FL allows for more efficient and scalable IDS deployment in large-scale IoMT networks, as it can accommodate diverse and heterogeneous data sources. By leveraging the collective intelligence of multiple devices, FL-based IDS can be scalable [105] and better detect and respond to emerging threats, safeguarding the integrity and security of IoMT systems.

#### *5.2.5 Combining Network and Medical Data*

IDSs typically analyze network traffic; however, their approach can be significantly adopted based on specific use cases. Researchers have observed that incorporating ML-based intrusion detection can enhance the security of healthcare systems by integrating biometric data or contextual environmental information [74,90] alongside network flow metrics. Studies indicate that such a hybrid data approach can lead to the development of more robust IDS solutions. Furthermore, research in [90] demonstrates that combining advanced ML/DL techniques with real-time monitoring systems effectively addresses critical gaps in healthcare security, improving both intrusion detection accuracy and the overall performance of IDSs in these environments.

### *5.3 IDS for Secure IoMT*

IDSs leverage different techniques to detect attacks in a network. These techniques can be of three types—*a) signature-based, b) anomaly-based*, and *c) specification-based attack detection* [45]. In this section, we will elaborate on the technical aspects including the benefits and limitations of these IDSs.

#### *5.3.1 Signature-Based IDS*

Signature-based intrusion detection techniques operate by matching known intrusion signatures, making them effective for identifying previously recognized attack patterns. A similar approach was proposed by Ghubaish et al. [22] to enhance security in IoMT systems. IoMT devices enable smart healthcare applications, allowing users to monitor essential health metrics such as blood pressure and heart rate. However, as discussed earlier in this section, these solutions remain vulnerable to cyberattacks targeting data collection, transmission, and storage. To secure these three phases, Ghubaish et al. [22] introduced state-of-the-art techniques for detecting and mitigating various known attacks on IoMT devices. Their framework defines 11 security requirements to ensure data confidentiality, integrity, availability, nonrepudiation, and authentication. The proposed approach incorporates multiple cryptographic methods, including a) symmetric, b) asymmetric, and c) keyless cryptographic techniques, to enhance IoMT security. Furthermore, ensuring efficient communication between sensors and gateways is critical in resource-constrained IoMT environments, which can be addressed using the CoAP [22].

#### *5.3.2 Anomaly-Based IDS*

Signature-based IDS effectively detect known attacks but rely on an up-to-date signature database. Research has demonstrated that the uniqueness of human biometrics can be leveraged for various applications, such as IoMT-based EHMS [90]. Studies have found that integrating physiological metrics like heart rate and blood pressure with network data enhances intrusion detection efficiency, even when attack signatures are unknown. This approach addresses the limitations of signature-based IDS, which struggles with detecting zero-day attacks due to the absence of predefined signatures. The solution also strengthens customized healthcare services by incorporating additional security layers.

ML, including Random Forest (RF), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Artificial Neural Networks (ANN), have been tested against potential threats like MitM attacks within EHMS, improving intrusion detection accuracy by 25%. To further enhance zero-day attack detection [10], AIDS [50,74,102,106] have emerged as a viable solution. Unlike signature-based IDS, AIDS detects intrusions by analyzing behavioural patterns in network traffic, allowing for more dynamic threat identification. These systems integrate AI, ML, and Deep DL-based approaches to efficiently detect anomalies [90] and are evaluated using the metrics outlined in Table 9. Here, TP, FP, TN, and FN represent true positive, false positive, true negative, and false negative counts, respectively.

Various approaches have been explored to develop optimal AIDS. These approaches incorporate diverse data preparation methods, effective model development techniques, and advanced learning paradigms such as ensemble learning [107–109] and federated learning [110,111]. An ensemble classifier designed for IDS proved effective in mitigating attacks on IoMT devices, including DoS/DDoS and Sybil attacks [107]. This research utilized the KDD Cup 1999 dataset, where data preparation involved Principal Component Analysis (PCA) for feature reduction, followed by the development of six different ensemble classifiers for comparative analysis. Among these models, bagged decision trees demonstrated the best performance, achieving an accuracy of 93.2%.

**Table 9:** Metrics used for performance evaluation of AIDS

| Evaluation matrix | Formula | Description |
|---|---|---|
| Confusion Matrix | – | A combination of TP, FP, TN, and FN. |
| Accuracy | $\frac{TP+TN}{TP+TN+FP+FN}$ | Proportion of correctly classified (true) instances out of the total number of instances. |
| Precision | $\frac{TP}{TP+FP}$ | Proportion of true predictions among all positive predictions. |
| Recall | $\frac{TP}{TP+FN}$ | Recall/sensitivity is the proportion of true predictions among all true instances. |
| F1-Score | $2 \times \frac{Precision \times Recall}{Precision + Recall}$ | It is the harmonic mean of precision and recall. Useful with unbalanced datasets. |
| FAR | $\frac{FP}{FP+TN}$ | False Prediction/Acceptance Rate (FAR or FPR) is the proportion of FP among all false instances. |
| FRR | $\frac{FN}{FN+TP}$ | False Rejection Rate is the proportion of FN among all true instances. |

Further advancements were proposed in [108], where an explainable ensemble-based IDS method for IoMT applications was developed using boosting techniques such as XGBoost, AdaBoost, and CatBoost. These models were tested on the CICIoMT-2024 dataset, with XGBoost achieving the highest accuracy of 95.01% in distinguishing between various attacks and benign traffic. This study highlights the potential of explainable AI to enhance the interpretability of modern AIDS solutions.

To overcome the limitations of conventional ML classifiers, including low accuracy and difficulties in detecting novel attacks, a protocol-based IDS was introduced as an enhancement to AIDS [112]. This approach focuses on monitoring IoT application protocols such as MQTT, AMQP, and CoAP. The novel ML model, IDS-ADP3, was trained on the CICIoMT-2024 dataset and optimized through hyperparameter tuning. The evaluation of IDS-ADP3 using four different metrics, including accuracy and F1-score, demonstrated its effectiveness, achieving an accuracy of 97% for the AMQP protocol.

Despite the advantages of these IDS approaches, the resource constraints of IoMT devices must be considered [54,74]. Addressing this challenge, Yamuna et al. [109] developed an AIDS solution that integrates a Modified Whale Optimization Algorithm (MWOA) for feature selection and RF for classification. The MWOA-RF approach achieved an impressive accuracy of 99.82% on the WUSTL-EHMS-2020 dataset. Preprocessing techniques, such as data normalization and feature selection, significantly enhanced detection efficiency, with RF outperforming SVM across multiple evaluation metrics.

Apart from the centralized IDSs, distributed IDS architectures, as proposed in [113], also offer a promising approach to secure IoMT environments, particularly for resource-constrained devices. By leveraging mobile agents and ML techniques, these hierarchical and distributed systems can effectively detect and mitigate attacks at both local and global levels in the network. It was also found that profiling of normal device behaviour can be done using polynomial regression for anomaly detection. Here the best case accuracy ranged between 99.80% and 97.93% and that for the worst case was 95.21% and 93.17%. However, energy efficiency remains a critical concern for such distributed systems. In continuation, [114] presents an intelligent and explainable IDS by combining edge computing, AI, and advanced techniques like PSO and ensemble learning. This IDS achieved high accuracy (96.56%) on the WUSTL-EHMS-2020 dataset while minimizing resource consumption. The framework combines efficient feature engineering through Particle Swarm Optimization (PSO) and ensemble learning techniques, achieving robust intrusion detection. The

integration of shapley additive explanations enables explainability, fostering trust and understanding among healthcare professionals, and also provides a scalable and efficient approach to securing IoMT devices. It ensures the integrity and confidentiality of sensitive healthcare data.

While traditional ML-based IDSs offer effective anomaly detection, they often rely on centralized data collection, raising privacy concerns. FL offers a privacy-preserving alternative by enabling collaborative model training across decentralized devices (Section 5.2). In the context of IoMT, such a decentralized approach can enhance data security and privacy [20,54,59,115]. In this series, BEdgeHealth [59] leverages Mobile Edge Computing (MEC) and BCT to secure data sharing and offloading (storing data from edge devices to the server). BCT provides high security for health data sharing as well. By combining smart contracts with the Interplanetary File System (IPFS), this architecture ensures data integrity, traceability, and efficient retrieval. Here, the smart contract ensures data integrity and traceability, while IPFS accelerates data retrieval. This decentralized approach reduces latency, energy consumption, and memory usage, making it a promising solution for secure and efficient data sharing in IoMT environments. Furthermore, the IDS-Chain framework [116] offers a decentralized collaborative approach to intrusion detection in IoMT networks. By leveraging blockchain technology, IDS-Chain provides a secure and trusted platform for sharing information and detecting attacks. The three-layer architecture, including DaaS and CaaS, enables efficient and distributed attack detection. However, scalability, latency, and computational resource limitations in fog computing remain significant challenges for the practical implementation of this framework. Later in 2022, Ali and others [20] explored various FL architectures, including horizontal, vertical, and transferred FL, each for the different data distribution scenarios (Fig. 15).

- **Horizontal FL:** Here, the features of the dataset remain identical across all of the participating nodes, where the IDS model is trained. Therefore, features overlap for multiple nodes in this model of FL.
- **Vertical FL:** In this approach of FL, data is vertically distributed among the modes making all features not available for every node. Therefore, data overlaps for multiple nodes in this model of FL.
- **Transferred FL:** It is a specialized type of FL designed for scenarios where datasets across participant nodes have neither overlapping features nor overlapping data samples.

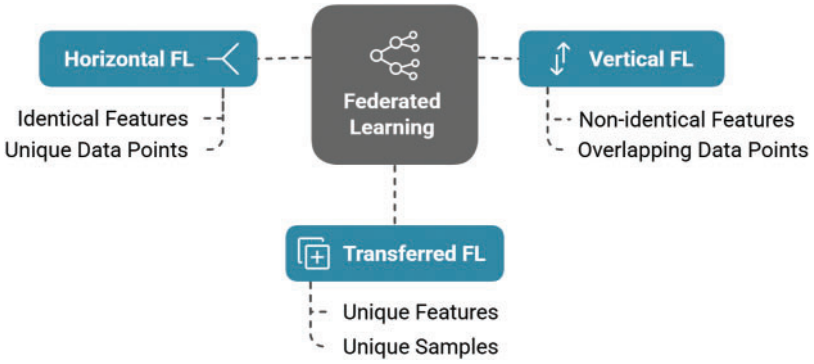


**Figure 15:** Three types of FL

Additionally, authors introduced privacy-enabled and incentive-enabled designs, to address potential attacks and incentivize participation. Overall, the paper emphasizes the potential of FL in revolutionizing healthcare by enabling collaborative research, improving diagnostic accuracy, and safeguarding patient privacy, while addressing the challenges of data heterogeneity, computational efficiency, and secure communication in 5G and 6G networks.

So far, we have explored several works on addressing the privacy issues using FL. Gupta et al. [54] also addressed the significant privacy concerns associated with centralized data collection and analysis by leveraging Hierarchical FL (HFL) and DTs that will be discussed in Section 5.4. However, HFL has also been used for attack detection in IoMT. In one of the recent works [110], a novel Dew-Cloud-based framework utilizing HFL and Hierarchical Long Short-Term Memory (HLSTM) was introduced for IDS in IoMT. The proposed framework combined decentralized and centralized architectures to enhance data privacy and scalability to address data breaches and attacks on medical devices. The inclusion of components such as networks of wearable devices, edge devices, dew servers, and cloud servers creates a robust system for IoMT applications. The solution was evaluated on the TON-IoT and NSL-KDD datasets, and demonstrated that the HFL-HLSTM model achieves superior performance compared to existing methods in both binary and multi-class classification for intrusion. Some other advancements in FL-based IDS for IoMT include transfer learning [115] and BCT [111]. A novel federated transfer learning-based IDS approach was proposed by developing a privacy-preserving IDS capable of high accuracy and adoptability [115]. The method aimed to secure IoMT networks by effectively combining FL and Transfer Learning (TL), and utilized a Deep Neural Network (DNN) for knowledge transfer. The FL and TL-based IDS was trained and evaluated with CICIDS2017 dataset and was found to offer a scalable and privacy-centric intrusion detection. IDS demonstrated its capability to detect various attack types while maintaining low prediction times and high detection rates.

Considering the benefits of using FL and BCT to improve the performance of AIDS, authors of [111] proposed the concept of a novel architecture that integrates both BCT and FL for an IDS in IoMT environments comprising wearable health devices for data collection. Overcoming the limitations of conventional ML-based AIDS, this work presented that the IDS framework consisting of FL with BCT-based learning channels, ensures secure and decentralized model training. Demonstrated on Hyperledger Fabric, this IDS solution enhanced security through permissioned access, immutable ledgers, and smart contracts for policy enforcement. While the conceptual framework is robust, its implementation and performance are yet to be validated.

### *5.3.3 Specification-Based IDS*

The integration of ML/DL techniques has significantly advanced the field of AIDS for IoMT networks. While ML-based IDSs offer lightweight and interpretable solutions, DL approaches provide superior accuracy and scalability. However, these AIDS approaches face challenges such as false positives, false negatives, and susceptibility to adversarial attacks.

To address these limitations, researchers have proposed various innovative solutions. A Specification-Based Intrusion Detection System is a security mechanism that detects malicious behaviour by defining strict rules or specifications of expected system behaviour and flagging any deviations as potential attacks. It operates based on predefined policies and does not rely solely on anomaly detection or signature-based techniques. The specification-based IDS could be advantageous over AIDS as these systems also integrate the abilities of signature-based IDS [90]. Meta-IDS [10] is one such IDS that combines signature-based and anomaly-based detection techniques. Meta-IDS leverages a two-stage meta-learning approach to improve the performance of weak learners like Decision Trees, Random Forest, and AdaBoost, and a meta-learner, XGBoost. The IDS was trained on WUSTL-EHMS-2020, IoTID20, and WUSTL-IIOT-2021 datasets and achieved 99.57%, 99.91%, 99.99% of accuracy, respectively. By integrating advanced feature engineering and anomaly detection techniques like RFE and LDA, Meta-IDS offers a robust and adaptable solution for securing IoMT networks against both known and zero-day attacks.

### *5.4 Digital Twins for Advanced IDS Development*

An IDS significantly strengthens the security of an IoMT network by providing advanced threat detection and response capabilities, when combined with a DT. The IDS monitors network traffic and device behaviour to identify suspicious activities or potential security breaches, such as unauthorized access, malware, or abnormal data flow. By using a DT, the IDS operates in a virtual replica of the IoMT network, allowing for more accurate and risk-free detection of intrusions and improved maintenance.

#### *5.4.1 System-Oriented*

CPS are the new generation of digital systems that can seamlessly integrate computational and physical components. IoT has significantly supported the implementation of CPS. As the DTs can be created for the corresponding physical devices in IoT networks, DT solutions for CPS have recently become an area of interest for the businesses [12,117,118]. Authors of [117] proposed an *Anomaly deTection with digiTAl twIN* (ATTAIN) for addressing the complexities of CPS anomaly detection using DTs. The DTs are integrated with a robust GAN to automate the system behaviour representation and anomaly detection. A key innovation is the use of the Online-Timed Automaton Learning Algorithm (OTALA) [119] to construct probabilistic real-time automata for modeling CPS behaviour. ATTAIN's superior performance over state-of-the-art methods has been demonstrated on three different datasets, including SWaT [120], which gave the best precision, recall, and F1-score (97.59%).

ICS are a subset of CPS. Unlike the CPS, which may include a wider range of systems like autonomous vehicles and healthcare devices, ICS are developed for distinct industrial processes like water treatment. A hybrid digital twin-based IDS was introduced in [118] for the SWaT dataset. A physics-based modeling and data-driven techniques were used to simulate the SWaT behaviour with DT. The DT solution demonstrated effective detection of eight out of nine attack types. Hence, the proposed IDS was found to be adaptive to the different cyber attacks and demonstrated strong performance.

Another study [12] focused on attack detection in ICS, which are increasingly exposed to the internet and often lack built-in security mechanisms. The authors developed an ML-powered DT to replicate the ICS environment in real-time while integrating intrusion detection capabilities. The proposed model included three Programmable Logic Controllers (PLCs) and sensors to monitor flow levels and other industrial processes. To evaluate its effectiveness, multiple attack scenarios, such as command injection and network-based Denial-of-Service (DoS) attacks, were simulated without impacting the physical system. The paper introduced a stacked model combining traditional ML techniques with a Multilayer Perceptron (MLP) algorithm, achieving an accuracy of 92.70% and surpassing the performance of individual models. Additionally, an earlier work on ICS security [11] explored a cloud-based IDS leveraging DTs to detect and mitigate MitM attacks.

#### *5.4.2 Attack/Threat-Oriented*

DDoS is a very common attack on IoT networks. A DT-enabled intelligent DDoS detection system was proposed for autonomous core networks, which utilized the online learning methods for real-time adaptation [121]. The solution reduces data complexity by employing a YANG model and an AutoFS module for feature selection. Here, synchronized real-time communication was set up between physical and digital twins. The DDoS detection model was developed using a semi-supervised approach as unlabeled data were handled by combining clustering and ensemble learning methods. The proposed MLP-based DDoS classifier was tested on CICDDoS2019 and ToN_IoT datasets, and it was found that it outperformed existing methods like RF, DNN, and Long Short-Term Memory (LSTM), achieving an accuracy of 97%. The work

highlighted the significance of integrating router health monitoring and IGP protocols for comprehensive network management.

CNN and Bi-directional LSTM are also used along with DTs for IoT attack detection [122]. This approach effectively fuses spatial and temporal features for better collection. A DNN-based classifier trained on the UNSW-NB15 and CICIDS2017 datasets in a simulated IoT environment performed well for attack detection. However, the solution needs to address attack detection, especially for minority classes, in case of imbalanced datasets. The solution achieved F1-scores of 99.08% and 99.91% on UNSW-NB15 and CICIDS2017 datasets, respectively.

In the same series, another work introduced an AI-based IDS for DT-enabled critical infrastructure [123]. This framework uses DTs to monitor real-time system behaviours for anomaly detection. This work specifically targeted the vulnerabilities in PLC-based data transmission and utilized ML classifiers, including logistic regression, SVM, Quadratic Discriminant Analysis (QDA), and random forest, to effectively detect IoT attacks.

#### *5.4.3 Behaviour-Oriented*

Each instance of the network traffic data is spatial information in itself and hence can be processed using algorithms like CNN. However, contextual information can further improve the performance of intrusion detection and may require the consideration of temporal information as well. Researchers have introduced a concept of intelligent digital twins for identifying the behaviour of IoT attacks through spatio-temporal feature fusion [32]. Here, DTs utilize deep learning techniques to smartly simulate realistic IoT environments.

The authors used multivariate correlation analysis and feature selection for data pre-processing, ensuring high-quality input for the model and developed a hybrid model for spatial and temporal feature extraction using CNN and Bi-directional LSTM, respectively. Softmax activation function and Adam optimizer were used for the model convergence. Evaluated on UNSW-NB15 and CICIDS2017 datasets, results indicated that such a behaviour-based hybrid DL IDS performs significantly well. It not only addresses class imbalance issues but also underscores the importance of spatio-temporal feature fusion in improving detection rates for diverse cyberattacks.

#### *5.4.4 Recent Approaches*

Apart from securing the DT-based systems through IDS, researchers have also tried integrating DTs to develop IDS systems. As discussed in Section 5.2, the performance of IDSs can be improved if trained with medical data along with the network traffic. However, due to the sensitivity of medical information and its privacy concerns, IDS should not directly use it for analysis. This problem can be addressed in the following ways.

1. Integrating ML-based IDS within each DT
2. Adopting FL approach for smart IDSs

A DT-based IDS addresses this challenge by integrating the intrusion detection system within the DT of the device, ensuring security while simultaneously enabling the use of medical data for predictive analysis. In a related study [70], the increasing security challenges in smart infrastructure networks were tackled by integrating DTs of physical assets with AI in real-time. The proposed AI-driven IDS leveraged a hybrid approach combining Autoencoders and Recurrent Neural Networks (RNN) for continuous network monitoring. This method enhanced complex threat identification by enabling timely anomaly detection and proactive security measures, supported by advanced data preprocessing techniques.

FL-based local IDS models [54] further ensure data privacy by sharing only model parameters for aggregation and optimal model creation. He et al. [124] extended this concept by integrating FL with DTNs, developing a Federated Continuous Learning (FCL) framework, FCL-SBLS, for intrusion detection in Unmanned Aerial Vehicle (UAV) networks. This hybrid IDS addressed the limitations of traditional centralized ML-based intrusion detection methods. Additionally, the term SBLS in the framework stands for Scalable Broad Learning System (SBLS) [125] that combines incremental learning, enabling adaptation to emerging intrusion patterns while preserving prior knowledge, thereby mitigating catastrophic forgetting. Furthermore, DTN-assisted unmanned aerial vehicle selection can be optimized using a Deep Reinforcement Learning (DRL) algorithm, enhancing both data utility and training efficiency.

### *5.5 DT-IDS and IoMT*

Considering the various benefits of using DT in IDS development, it can significantly contribute to the security of IoMT systems. Table 10 highlights the scope of using DT for security in IoMT. It also lists some requirements that should be considered while working towards these scopes. The IoMT systems consist of various types of medical devices and entities. Hence, ensuring medical data privacy and network security can be challenging to enable every corresponding physical twin to be equally productive in real-time due to various limitations.

**Table 10:** Examples of DT in IoMT security

| Scope of DT for security | Example |
|---|---|
| Layer of Abstraction | Device as a Service [50,53] to avoid direct interaction with the physical device. |
| Security Monitoring | Virtual resources security [4], and decentralized training using FL [54] to maintain the privacy. |
| Threat Intelligence | Inter-DT communication [53] for fast and robust threat intelligence. |
| Predictive Security | Real-time prediction [70] of unusual health conditions or anomalous data patterns. |
| Anomaly/Intrusion Detection | AI/ML and FL-based IDS [35,54,74,106] for detecting zero-day attacks. |
| Security Testing and Validation | DT/DTN Cloning [33], IDS/IPS integration, testbed [50] setup is done for experimentation and educational purposes. |
| Risk Mitigation and Incident Response | Integration with security toolkit and other technologies for implementation [34,50], and event management within DTN [4]. |

As with conventional IoT systems, devices used in IoMT solutions are typically lightweight and possess limited processing capabilities. While it is feasible to design individual DT-based security mechanisms for each device, accessible through the DTN, such mechanisms necessitate real-time, synchronous communication with their physical counterparts. This continuous interaction can result in rapid battery depletion, posing a significant cost in terms of DT utilization.

Moreover, in a DTN consisting of multiple identical digital twins linked to various physical devices, training traditional data-driven anomaly detection models becomes challenging due to data heterogeneity.

As discussed earlier, federated learning (FL)-based models offer a promising approach for building distributed classification models that can effectively address this heterogeneity. However, as illustrated in Fig. 16, FL-based intrusion detection systems (IDS) involve trade-offs between adaptability and performance, which are further elaborated in Table 11.

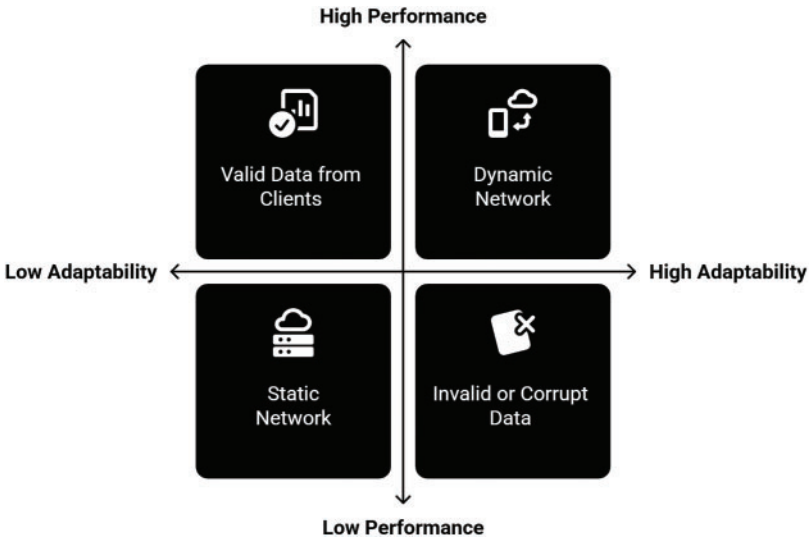


**Figure 16:** Performance and adaptability trade-off in FL-based IDS

**Table 11:** Trade-offs between the properties of FL-based IDS and their impacts

| System Property | Possibility | Impact |
|---|---|---|
| Rapid Data Flow | Real-time Processing<br>Delayed Processing | High resource consumption<br>High latency |
| IDS Model Performance | Valid Data from Clients<br>Invalid or Corrupt Data (Adversarial Attacks, e.g., Data Poisoning) | High performance<br>Low performance |
| FL Architecture | Dynamic Network with Variable Clients<br>Static Network with Fixed Clients | Dynamically Adaptive Architecture<br>Static and Less Flexible Architecture |

Therefore, as highlighted by the inherent trade-offs in designing and deploying an FL-based IDS, issues like rapid data flow optimization can reduce the resource usage without compromising the robustness of the IDS. The performance of the IDS model is directly dependent on the integrity of data from potentially vulnerable IoMT devices within the FL framework, and architectural choices in the FL setup significantly impact the adaptability of the security solution in a dynamic IoMT environment. Hence, while offering significant potential to enhance smart medical infrastructure, these interconnected challenges require an in-depth exploration for the holistic and secure development of DT-integrated IoMT systems.

## 6 Insights and Answers to the Research Questions

So far, we have conducted a comprehensive review of existing research on advancements in the IoMT domain, highlighting their benefits and limitations. Based on our analysis, this section presents insights and answers to the research questions raised in Section 1.

### *6.1 IoMT's Role in Smart Healthcare Development*

The evolution of Industry 4.0 through rapid advancements in technologies, like IoT, has led to an increased demand for scalable and adaptable healthcare systems. The COVID-19 pandemic further accelerated this need by amplifying the demand for remote healthcare services. It highlights the critical role of IoMT in addressing global health challenges. We discussed in Section 3 that as an integral part of this technological revolution, IoMT has significantly contributed to the development of the smart healthcare industry. IoMT facilitates real-time data collection, analysis, and sharing by interconnecting medical devices, software applications, and systems, which leads to enhanced patient care and improved operational efficiency.

The rise of telehealth practices [18] during COVID-19 underscores the potential of IoMT in providing remote healthcare services, especially in underserved areas. It has been used for numerous applications like monitoring social distancing, disease diagnosis, etc. Another notable example is the use of CanTwin [21], a DT-integrated IoMT technology, to facilitate social distancing during the pandemic. By creating virtual representations of individuals and their interactions, CanTwin helped in monitoring and controlling the spread of the virus.

Apart from the aforementioned specific use cases, various IoMT devices, like smart pacemakers, fitness bands, and other wearable devices, assist both healthcare professionals and patients in quick and real-time health monitoring. Additionally, IoMT-enabled personalized services offer a significant advantage in the smart healthcare industry.

### *6.2 Security Challenges in IoMT and Current Solutions*

IoMT systems rely on diverse technologies and specialized devices, each comprising hardware and software components that face various security challenges [35], as discussed in Section 5. Fig. 17 illustrates the four most common types of attacks targeting IoMT networks and devices. The likelihood of cyberattacks in these systems is heavily influenced by the specific components within the IoMT infrastructure.

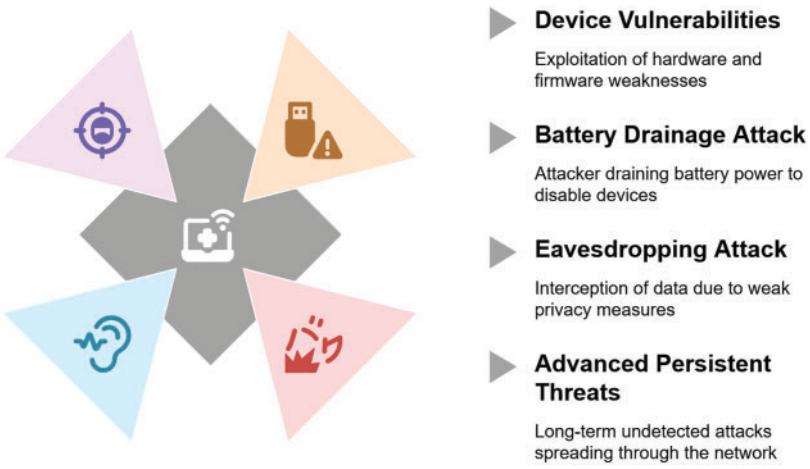


**Figure 17:** Common security threats in IoMT

Furthermore, while offering numerous benefits, the interconnected nature of IoMT devices also increases the risk of cyberattacks. Adversaries exploit this connectivity to launch network-based attacks and propagate malicious code across the system. Table 6 lists common IoMT attacks, which are typically mitigated using an IDS.

Most of the cyberattacks target the network and involve malicious traffic, making IDSs essential for securing IoMT infrastructure [35]. Anomaly-based and specification-based IDSs enhance traditional signature-based models by leveraging ML, DL, FL, and AI techniques to detect zero-day attacks (Section 5.3). In addition to IDSs, data and communication security challenges are mitigated using advanced encryption methods and secure protocols [22].

### *6.3 Role of Digital Twins in IoMT Security*

DT technology enhances IoMT security by creating virtual replicas of physical entities, such as the human body and connected medical devices, enabling real-time monitoring and anomaly detection [36]. Integration of IMDs and IoWDs within the IoMT framework supports continuous monitoring, predictive analytics, and adaptive IDS without disrupting medical operations.

As an abstraction layer [50], DT ensures external entities interact only with the digital replica, securely processing data while safeguarding patient information and device functionality. This isolation shields physical systems from direct interaction and mitigates potential cyber threats. Additionally, DTs generate synthetic data [69], crucial for training ML/DL models to enhance IDS efficiency. Their integration with advanced technologies like BCT and AI/ML further strengthens security [1,70], facilitating automated anomaly detection and proactive threat mitigation. DTs also enable comprehensive modeling and simulation of IoMT systems, helping identify vulnerabilities, simulate attacks, and predict security risks before they occur. Built-in security features, such as integrated IDS [32] and enhance system resilience by providing a testing platform for incident response strategies.

Beyond security, DTs also improve accessibility and cost efficiency in healthcare by enabling remote medical services. The integration of cloud storage and edge computing ensures scalability and decentralized data processing, reducing the risks associated with data transmission and storage. These capabilities make DTs essential for building secure, efficient, and resilient IoMT ecosystems, ensuring patient safety, data integrity, and uninterrupted medical operations.

### *6.4 Challenges in Integrating DTs in IoMT*

The integration of DT has the potential to significantly enhance the security and overall functionality of IoMT systems by enabling virtual replicas that support advanced intrusion detection systems (IDS). DTs allow for sophisticated threat analysis, simulation of attack scenarios, and implementation of active security measures, without impacting the physical devices. However, given the nascent stage of DT technology, integrating DTs into advanced IoMT environments remains a complex challenge [4,34,77,126].

Table 12 outlines several key requirements for DT integration and their associated dependencies, many of which present significant practical challenges. The main challenges in ensuring these dependencies can be broadly categorized into: *a) Resource Constraints*, *b) Implementation Complexity*, and *c) Security Risks*. These three categories are discussed in detail in the following subsections.

1. **Resource Constraints:** While DT offers a powerful solution for advanced IDS development in IoMT through real-time monitoring and complex security analytics, its substantial computational and storage demands create a significant trade-off. The capabilities that make DTs ideal for sophisticated threat analysis often exceed the limited resources available on many IoMT devices and within edge network

infrastructures. For instance, due to the limited computational capabilities of medical IoT devices, rapid exchange of real-time data and instructions could lead to battery drainage. However, integrating higher computation capabilities of DT could reduce both data dependency and decision-making latency. Therefore, achieving near real-time synchronization between DTs and their physical counterparts can be more challenging in dynamically scalable IoMT environments, due to the growing number of DTs and interactions within the DTN.

2. **Implementation Complexity:** While DTs offer significant potential in accurately replicating IoMT environments for improved security and IDS testing, their implementation is inherently complex [50]. Capturing the intricate behaviour and interactions of IoMT devices and networks demands specialized domain knowledge and substantial computational resources. Achieving a synchronized system between physical devices and their digital counterparts, while managing heterogeneous data streams with low latency and high security, poses a considerable challenge.
3. **Security Risks:** Although DTs enhance IoMT security through real-time monitoring and proactive threat detection, their reliance on continuous data exchange introduces new vulnerabilities [4]. The transmission of sensitive patient data between physical IoMT devices and their virtual twin creates potential attack points. Additionally, DT-integrated IDS systems that employ ML and DL techniques are susceptible to adversarial threats, such as data poisoning attacks [77].

**Table 12:** Challenges associated with integrating DT in IoMT

| Requirements | Dependencies |
|---|---|
| Real-time Synchronization [36,62,67] | Ensure frequent, high-speed communication to optimize interaction with physical devices DTs, while minimizing latency. |
| System Scalability and Standardization [19,34,36,40,67,75] | Systematic method to architect DTN synchronized with IoMT that can dynamically vary based on the applications. |
| Heterogeneous Data Management [4,21,68] | Robust data handling across the DTN that originates from nonidentical DTs and medical devices. |
| AI/ML and FL-based IDS [54,70,77,110,111,115] | Dataset validation and automation in IDS training and deployment. |

Fig. 18 illustrates the key challenges associated with integrating DTs into IoMT systems. These challenges must be addressed to ensure effective adoption of DT in IoMT. Addressing resource constraints involves careful allocation and optimization to avoid performance degradation or excessive energy consumption in resource-limited IoMT devices. As discussed in Section 4.4, scalability further impacts resource usage and associated costs [78]. Tackling implementation complexity [34] requires streamlining the modeling process, designing robust and scalable DT-IoMT architectures, and addressing regulatory considerations related to patient data ownership and privacy. These steps are critical to facilitate the broader adoption of DT in healthcare. Finally, mitigating the security risks that arise from continuous data exchange between physical and virtual entities necessitates strong security frameworks and privacy-preserving mechanisms. These are essential for realizing the full security benefits of DT integration without introducing new vulnerabilities to the IoMT environment.

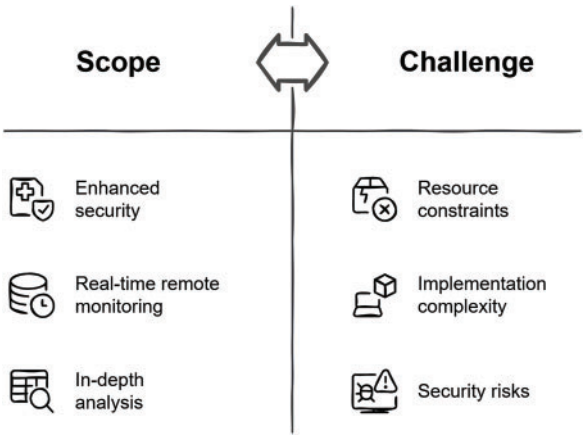


**Figure 18:** Scope of integrating DT in IoMT and associated challenges

## 7 Future Directions

In this paper, we explored the transformative evolution of smart IoMT solutions and examined the role of DTs in enhancing medical applications. These technologies improve outcomes for end-users and significantly assist healthcare professionals by streamlining the management and operation of digital healthcare infrastructures. The inherent capabilities of DTs—such as dynamic synchronization, real-time monitoring, and seamless integration with physical medical devices—present promising opportunities for advancing remote healthcare delivery and improving access to personalized services.

However, in addition to these developments, we also discussed the existing vulnerabilities and security challenges within IoMT systems and the broader healthcare context [85,86]. Existing DT-based solutions still require substantial enhancements, particularly in intelligent integration for achieving adaptive and robust system responses. Table 13 outlines the scope of our findings for the four research questions (RQs) presented earlier in Section 6, offering a clear view of existing gaps and future research opportunities.

**Table 13:** Scope of findings of this review

| RQ | Focus | Findings | Scope |
|---|---|---|---|
| RQ1 | IoMT Contribution to Smart Healthcare | The evolution in architectures, components, and applications of IoMT leads to its wide adoption in the medical domain. | Emphasizes standardization of context-aware IoMT for robust and seamless smart healthcare solutions and development. |
| RQ2 | Security Challenges in IoMT and IDS | Ensuring data privacy and real-time intrusion detection is crucial in interconnected IoMT devices operating across diverse technologies. | Leverage the advanced technologies like FL and BCT to address the existing limitations of traditional IDS in resource-constrained IoMT. |
| RQ3 | Role of DT in IoMT and its Security | DT enables comprehensive modeling for remote healthcare solutions. It also provides security through real-time threat detection and mitigation. | Develop a privacy-aware DTN to enhance security and address the limitations of traditional ML-based IDS to improve the incident response time. |

(Continued)

**Table 13 (continued)**

| RQ | Focus | Findings | Scope |
|---|---|---|---|
| RQ4 | Issues Integrating DTs in IoMT | Scalable DTN lag adaptive management and security due to the various resource constraints and complex network traffic. | Propose a standard development and operational framework for DTs in the healthcare domain that complies with regulations like HIPAA and GDPR. |

Based on the findings in Table 13, we suggest three future directions for the continued advancement towards robust DT-based smart IoMT solutions. These potential future directions are described in the following subsections.

### *7.1 Context-Aware and Privacy Preserving IDS Systems for IoMT*

Inspired by the findings of RQ2, we suggest that efforts could be made to create a more intelligent security model for the IoMT by leveraging real-world medical and environmental context alongside advanced ML within IDS solutions [35]. This unique integration of technology with real-world medical context will introduce a dynamic security mechanism for IoMT. The approach involves designing privacy-preserving techniques like homomorphic encryption (HE) [127] and FL [98,100,105] to train and operate these systems without compromising sensitive patient data. The HE can ensure building insights from sensitive patients' data without disclosing the original information. Additionally, using the FL model to develop IDS will speed up the model training process, preserving the data belonging to the individual clients or nodes in the IoMT.

Developing such a systematic framework for the medical domain can be realized in four phases, as shown in Fig. 19. Starting with identifying the application use-case, complexity of the IoMT should be defined. It should be followed by selecting the most suitable IoMT architectures for setting up the network. This phase will also address the appropriate data encryption and processing. However, certain challenges related to the HE-based data encryption and FL should be addressed. Phase 3 may involve the development of an initial proof of concept, which can serve as a foundation for the final standardized framework in Phase 4, including detailed specifications to support broader adoption.

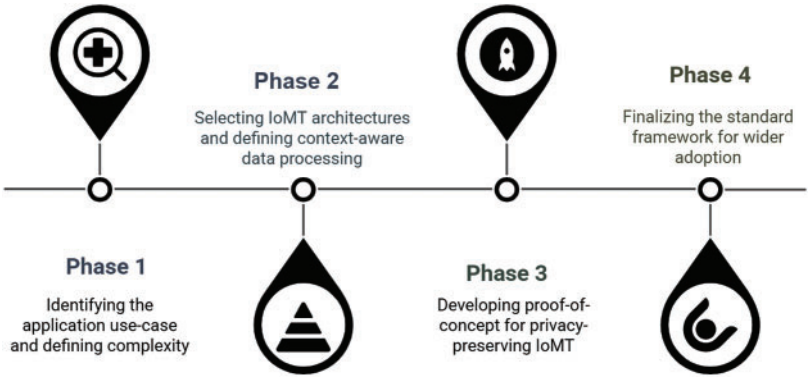


**Figure 19:** Four phases for context-aware and privacy-preserving IDS for IoMT

### *7.2 DT-Based IDS for Fast Incident Response IoMT*

The abstraction offered by DT technology can be leveraged to enhance security operations in IoMT. Based on the findings related to the RQ3 and RQ4, embedding the IDS capabilities within the DT can be very helpful. Training robust IDS collectively through individual DTs and deploying it for the entire DTN can enable an optimal threat detection and mitigate issues like unauthorized access, data manipulation, and zero-day attacks. Furthermore, empowering every DT for localized security checks will reduce latency and improve overall responsiveness of the system against cyberattacks. To create such a resilient IDS solution, the work can be structured into three major milestones.

1. Defining the DT for devices within the IoMT solution.
2. Secure data handling and IDS development for DTN.
3. Adaptive threat detection and incident response.

This initial stage focuses on establishing clear criteria to determine which devices and components within an IoMT solution are suitable for DT development. It will emphasize the most essential properties of DTs for enhanced security and management. Once the traditional DTs are successfully created, the next phase should start with developing secure mechanisms for handling data within the DTN, while adhering to regulations like HIPAA [82]. The development and deployment of IDS, specifically designed to monitor and protect the DTN infrastructure, should be followed simultaneously. Finally, adaptive threat detection and response need to be introduced in the last stage that leverages individual DTs for localized monitoring and the DTN-level IDS for comprehensive analysis for quick response. It can enable the system to adapt to a dual-level security through a weighted decision-making process based on the specific security situation.

### *7.3 Standard Framework for Secure DT Development in the Medical Domain*

The findings of RQ1, RQ3, and RQ4 collectively indicate that a standard framework is necessary for the secure DT-based healthcare infrastructure. However, the standards like ISO 23247 [128] have been introduced for DT in manufacturing, while security-oriented DT development standards can uniquely integrate real-world medical context. Utilizing the existing development standards and explicitly incorporating regulations, like HIPAA, as a part of the framework, will make a unique and necessary step towards responsible DT adoption in medicine. Such a framework will advance the DT development beyond tools to ensure the placement of domain-specific security considerations.

It was pointed out in [34] that there is a crucial requirement for research in implementation side of the DT technologies, especially in the medical sector. Therefore, as shown in Fig. 20, secure medical DT development is possible in four phases. Starting with analyzing healthcare regulations and security requirements a framework that incorporates the necessary specifications and guidelines for secure data management. In the later stage, developing methods for regulatory compliance and governance specific to medical DTs should be followed. Finally, the solution must be validated via experiments and case studies to promote its adoption within the healthcare industry.

Beyond the suggested future scope, the ongoing evolution and early adoption of DT technology in dynamic real-world scenarios create ample research opportunities. This is particularly relevant for the highly sensitive and cyberattack-prone medical sector [76] that requires application-focused security solutions. Therefore, the effective use of advanced technologies like AI and BCT can enable the development of adaptive security measures to counter evolving threats.


**Figure 20:** Framework for secure DT development in IoMT

## 8 Conclusions

This paper carried out a systematic literature review guided by four research questions aligned with the theme "Digital Twins and IDS in IoM." We collected 805 unique papers from diverse publishing venues and categories for our initial analysis. These papers were collected from 2007 to 2025. Following the initial insights, we finalized 66 most suitable works for answering the RQs. It was found that among the screened articles on *IoMT*, *DT*, and *Security*, only three showed close relevance to all three domains. The work comprehensively explored the evolving field of the IoMT and its critical role in revolutionizing healthcare delivery. In the first part of the paper, we began with RQ1 by examining the fundamental architecture, components, and diverse applications of IoMT, emphasizing its potential to enhance patient care, improve healthcare efficiency, and facilitate remote monitoring. Subsequently, we elaborated on the transformative power of DTs across various industries, including their significant contributions to the Industry 4.0 revolution. We then highlighted the pivotal role of DTs in advancing healthcare by enabling predictive maintenance, personalized treatment plans, and improved patient outcomes.

Furthermore, the study acknowledged the inherent security vulnerabilities within the IoMT ecosystem, arising due to the factors like device limitations and vulnerabilities, issues with communication protocols, and interoperability challenges. Recognizing the critical need for robust security measures, we investigated the role and types of IDS employed to mitigate these threats. We also explored emerging trends in IDS technology, including ML, DL, and AI integration for enhanced threat detection and response capabilities. Such application and security-oriented analysis of DTs and IoMT addressed the issues raised in RQ2 and RQ3. Finally, this paper not only underscored the profound potential of leveraging DTs to develop more secure, efficient, and adaptive IDS solutions for IoMT environments, but also provided insights into the significant challenges associated with DTs as an answer to RQ4.

By creating virtual replicas of IoMT systems, DTs can facilitate real-time threat simulations, rapid prototyping the security measures, and optimizing IDS performance through continuous learning and adaptation. This synergistic approach, combining the power of DTs with advanced AI/ML techniques, holds immense promise for building a more secure and resilient future for healthcare in the age of the IoMT. This

paper not only provides clear insight into the future of IoMT with DTs but also paves the way for research toward securing modern and future healthcare infrastructure.

**Acknowledgement:** Thanks to the anonymous reviewers and editors.

**Funding Statement:** This research is conducted as part of the project titled "Digital Twin-based Intrusion Detection System Using Federated Learning for IoMT" (2024–2027), supported by C3iHub, IIT Kanpur, India, under Sanction Order No.: IHUB-NTIHAC/2024/01/3.

**Author Contributions:** The authors confirm contribution to the paper as follows: Conceptualization, Tony Thomas, Ravi Prakash; methodology, Tony Thomas, Ravi Prakash; software, Tony Thomas, Ravi Prakash; validation, Tony Thomas, Ravi Prakash; formal analysis, Tony Thomas, Ravi Prakash, Soumya Pal; investigation, Tony Thomas, Ravi Prakash, Soumya Pal; resources, Tony Thomas, Ravi Prakash; data curation, Tony Thomas, Ravi Prakash, Soumya Pal; writing—original draft preparation, Tony Thomas, Ravi Prakash, Soumya Pal; writing—review and editing, Tony Thomas, Ravi Prakash; visualization, Tony Thomas, Ravi Prakash; supervision, Tony Thomas; project administration, Tony Thomas; funding acquisition, Tony Thomas. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** No datasets were used or generated during the current study.

**Ethics Approval:** This study did not involve any human or animal subjects, and therefore, ethical approval was not required.

**Conflicts of Interest:** The authors declare no conflicts of interest to report regarding the present study.

## Appendix A

**Table A1:** Abbreviations used in this paper

| Abbreviation | Definition | Abbreviation | Definition |
|---|---|---|---|
| AI | Artificial Intelligence | ICS | Industrial Control Systems |
| AIDS | Anomaly-based IDS | IDS | Intrusion Detection System |
| ANN | Artificial Neural Network | IIoT | Industrial IoT |
| BCT | Blockchain Technology | IoHT | Internet of Healthcare Things |
| BLE | Bluetooth Low Energy | IoMT | Internet of Medical Things |
| CoAP | Constrained Application Protocol | IoT | Internet of Things |
| CPS | Cyber-Physical Systems | IoWD | Internet of Wearable Medical Devices |
| DDoS | Distributed DoS | | |
| DL | Deep Learning | LSTM | Long Short-Term Memory |
| DNN | Deep Neural Network | ML | Machine Learning |
| DoS | Denial of Service | MitM | Man in the Middle |
| DT | Digital Twin | MLP | Multi-layer Perceptron |
| DTaaP | Digital Twin as a Proxy | MQTT | Message Queuing Telemetry Transport |
| DTF | Digital Twin Framework | | |
| DTN | Digital Twin Network | NIDS | Network IDS |
| EHMS | Enhanced Healthcare Monitoring System | P2P | Physical-to-Physical |
| | | P2V | Physical-to-Virtual |

(Continued)

**Table A1 (continued)**

| Abbreviation | Definition | Abbreviation | Definition |
|---|---|---|---|
| FC | Feature Creation | PLC | Programmable Logic Controllers |
| FE | Feature Extraction | RF | Random Forest |
| FL | Federated Learning | RQ | Research Question |
| FS | Feature Selection | SOA | Service-Oriented Architecture |
| FTP | File Transfer Protocol | SSH | Secure Shell |
| GAN | Generative Adversarial Network | SVM | Support Vector Machine |
| HFL | Hierarchical FL | TL | Transfer Learning |
| HLSTM | Hierarchical LSTM | V2V | Virtual-to-Virtual |

## References


1. Lo C, Win TY, Rezaeifar Z, Khan Z, Legg P. Digital twins in Industry 4.0 cyber security. In: 2023 IEEE Smart World Congress (SWC); 2023 Aug 28–31; Portsmouth, UK. p. 1–4. doi:10.1109/swc57546.2023.10449147.
2. Manavalan E, Jayakrishna K. A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. Comput Ind Eng. 2019;127:925–53.
3. Tao F, Zhang H, Liu A, Nee AYC. Digital twin in industry: state-of-the-Art. IEEE Trans Ind Inform. 2019;15(4):2405–15. doi:10.1109/tii.2018.2873186.
4. Alcaraz C, Lopez J. Digital twin: a comprehensive survey of security threats. IEEE Commun Surv Tutorials. 2022;24(3):1475–503.
5. Huda S, Nogami Y, Rahayu M, Akada T, Hossain MB. IoT-Enabled plant monitoring system with power optimization and secure authentication. Comput Mater Contin. 2024;81(2):1546–2226. doi:10.32604/cmc.2024.058144.
6. Khanna A, Kaur S. Internet of things (IoT), applications and challenges: a comprehensive review. Wireless Personal Commun. 2020;114(2):1687–762. doi:10.1007/s11277-020-07446-4.
7. Wang M, Xu C, Chen X, Hao H, Zhong L, Wu DO. Design of multipath transmission control for information-centric Internet of Things: a distributed stochastic optimization framework. IEEE Internet Things J. 2019;6(6):9475–88. doi:10.1109/jiot.2019.2929263.
8. Kamath V, Morgan J, Ali MI. Industrial IoT and digital twins for a smart factory: an open source toolkit for application design and benchmarking. In: 2020 Global Internet of Things Summit (GIoTS); 2020 Jun 3–5; Dublin, Ireland. p. 1–6. doi:10.1109/giots49054.2020.9119497.
9. Alsaedi A, Moustafa N, Tari Z, Mahmood A, Anwar A. TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access. 2020;8:165130–50. doi:10.1109/access.2020.3022862.
10. Zukaib U, Cui X, Zheng C, Hassan M, Shen Z. Meta-IDS: meta-learning based smart intrusion detection system for internet of medical things (IoMT) network. IEEE Internet Things J. 2024;11(13):23080–95. doi:10.1109/jiot.2024.3387294.
11. Akbarian F, Tärneberg W, Fitzgerald E, Kihl M. A security framework in digital twins for cloud-based industrial control systems: intrusion detection and mitigation. In: 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA); 2021 Sep 7–10; Vasteras, Sweden. p. 1–8.
12. Varghese SA, Ghadim AD, Balador A, Alimadadi Z, Papadimitratos P. 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); 2022 Mar 21–25; Pisa, Italy. p. 611–7.
13. Tan Y, Yang W, Yoshida K, Takakuwa S. Application of IoT-aided simulation to manufacturing systems in cyber-physical system. Machines. 2019;7(1):2. doi:10.3390/machines7010002.

14. Khujamatov H, Reypnazarov E, Khasanov D, Akhmedov N. IoT, IIoT, and cyber-physical systems integration. In: Emergence of cyber physical system and IoT in smart automation and robotics: computer engineering in automation. Cham, Switzerland: Springer; 2021. p. 31–50.
15. Pivoto DG, De Almeida LF, da Rosa Righi R, Rodrigues JJ, Lugli AB, Alberti AM. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: a literature review. J Manufac Syst. 2021;58(4):176–92. doi:10.1016/j.jmsy.2020.11.017.
16. Ryalat M, ElMoaqet H, AlFaouri M. Design of a smart factory based on cyber-physical systems and Internet of Things towards Industry 4.0. Appl Sci. 2023;13(4):2156. doi:10.3390/app13042156.
17. Mitra A, Roy U, Tripathy B. IoMT in healthcare industry—concepts and applications. In: Next generation healthcare informatics. Singapore: Springer; 2022. p. 121–46. doi:10.1007/978-981-19-2416-3_8.
18. Razdan S, Sharma S. Internet of medical things (IoMT): overview, emerging technologies, and case studies. IETE Techn Rev. 2022;39(4):775–88. doi:10.1080/02564602.2021.1927863.
19. Islam MM, Nooruddin S, Karray F, Muhammad G. Internet of Things: device capabilities, architectures, protocols, and smart applications in healthcare domain. IEEE Internet Things J. 2023;10(4):3611–41. doi:10.1109/jiot.2022.3228795.
20. Ali M, Naeem F, Tariq M, Kaddoum G. Federated learning for privacy preservation in smart healthcare systems: a comprehensive survey. IEEE J Biomed Health Inform. 2022;27(2):778–89. doi:10.1109/jbhi.2022.3181823.
21. De Benedictis A, Mazzocca N, Somma A, Strigaro C. Digital twins in healthcare: an architectural proposal and its application in a social distancing case study. IEEE J Biomed Health Inform. 2022;27(10):5143–54. doi:10.1109/jbhi.2022.3205506.
22. Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (IoMT) systems security. IEEE Internet Things J. 2020;8(11):8707–18. doi:10.1109/jiot.2020.3045653.
23. Jarrah M, Al Hamadi H, Abu-Khadrah A, Ghazal TM. IoMT-based smart healthcare of elderly people using deep extreme learning machine. Comput Mater Contin. 2023;76(1):19–33. doi:10.32604/cmc.2023.032775.
24. Singh J, Sandhu JK, Kumar Y. Metaheuristic-based hyperparameter optimization for multi-disease detection and diagnosis in machine learning. Serv Oriented Comput Appl. 2024;18(2):163–82. doi:10.1007/s11761-023-00382-8.
25. Khan MA, Algarni F. A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS. IEEE Access. 2020;8:122259–69. doi:10.1109/access.2020.3006424.
26. Singh M, Srivastava R, Fuenmayor E, Kuts V, Qiao Y, Murray N, et al. Applications of digital twin across industries: a review. Appl Sci. 2022;12(11):5727. doi:10.3390/app12115727.
27. Kong LCW, Harper S, Mitchell D, Blanche J, Lim T, Flynn D. Interactive digital twins framework for asset management through internet. In: 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT); 2020 Dec 12–16; Dubai, United Arab Emirates. p. 1–7.
28. Barykin SY, Bochkarev AA, Dobronravin E, Sergeev SM. The place and role of digital twin in supply chain management. Acad Strategic Manag J. 2021;20:1–19.
29. Wang L, Deng T, Shen ZJM, Hu H, Qi Y. Digital twin-driven smart supply chain. Front Eng Manag. 2022;9(1):56–70. doi:10.1007/s42524-021-0186-9.
30. Ibrahim M, Rassõlkin A, Vaimann T, Kallaste A. Overview on digital twin for autonomous electrical vehicles propulsion drive system. Sustainability. 2022;14(2):601. doi:10.3390/su14020601.
31. Pylianidis C, Osinga S, Athanasiadis IN. Introducing digital twins to agriculture. Comput Electron Agric. 2021;184(4):105942. doi:10.1016/j.compag.2020.105942.
32. Akbarian F, Fitzgerald E, Kihl M. Intrusion detection in digital twins for industrial control systems. In: 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM); 2020 Sep 17–19; Online. p. 1–6.
33. Prakash R, Thomas T. Towards secure AI-driven industrial metaverse with NFT digital twins. In: 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS); 2025 Jan 6–10; Bengaluru, India. p. 721–9.
34. Xames MD, Topcu TG. A systematic literature review of digital twin research for healthcare systems: research trends, gaps, and realization challenges. IEEE Access. 2024;12(1):4099–126. doi:10.1109/access.2023.3349379.

35. Naghib A, Gharehchopogh FS, Zamanifar A. A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities. Artif Intell Rev. 2025;58(4):1–88. doi:10.1007/s10462-024-11101-w.
36. Subramanian K. Digital twin for drug discovery and development-the virtual liver. J Indian Inst Sci. 2020;100(4):653–62. doi:10.1007/s41745-020-00185-2.
37. An G, Cockrell C. Drug development digital twins for drug discovery, testing and repurposing: a schema for requirements and development. Front Syst Biol. 2022;2:928387. doi:10.3389/fsysb.2022.928387.
38. Mariam Z, Niazi SK, Magoola M. Unlocking the future of drug development: generative AI, Digital Twins, and Beyond. BioMedInformatics. 2024;4(2):1441–56. doi:10.3390/biomedinformatics4020079.
39. Moingeon P, Chenel M, Rousseau C, Voisin E, Guedj M. Virtual patients, digital twins and causal disease models: paving the ground for in silico clinical trials. Drug Discov Today. 2023;28(7):103605. doi:10.1016/j.drudis.2023.103605.
40. Tai Y, Zhang L, Li Q, Zhu C, Chang V, Rodrigues JJ, et al. Digital-Twin-Enabled IoMT system for surgical simulation using rAC-GAN. IEEE Internet Things J. 2022;9(21):20918–31. doi:10.1109/jiot.2022.3176300.
41. Isma'ila UA, Danyaro KU, Muazu AA, Maiwada UD. Review on approaches of federated modeling in anomaly-based intrusion detection for IoT devices. IEEE Access. 2024;12(1):30941–61. doi:10.1109/access.2024.3369915.
42. Rasool RU, Ahmad HF, Rafique W, Qayyum A, Qadir J. Security and privacy of internet of medical things: a contemporary review in the age of surveillance, botnets, and adversarial ML. J Netw Comput Appl. 2022;201(1):103332. doi:10.1016/j.jnca.2022.103332.
43. Hromada D, RLdC Costa, Santos L, Rabadão C. Security aspects of the internet of things. In: Research anthology on convergence of blockchain, internet of things, and security. New York, NY, USA: IGI Global; 2023. p. 67–87. doi:10.4018/978-1-6684-7132-6.ch005.
44. Ahmed SF, Alam MSB, Afrin S, Rafa SJ, Rafa N, Gandomi AH. Insights into Internet of Medical Things (IoMT): data fusion, security issues and potential solutions. Inf Fusion. 2024;102(4):102060. doi:10.1016/j.inffus.2023.102060.
45. Rbah Y, Mahfoudi M, Balboul Y, Fattah M, Mazer S, Elbekkali M, et al. Machine learning and deep learning methods for intrusion detection systems in IoMT: a survey. In: 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET); 2022 Mar 3–4; Meknes, Morocco. p. 1–9.
46. Areia J, Bispo I, Santos L, Costa RLDC. IoMT-TrafficData: dataset and tools for benchmarking intrusion detection in internet of medical things. IEEE Access. 2024;12(3):115370–85. doi:10.1109/access.2024.3437214.
47. Verma A, Ranga V. ELNIDS: ensemble learning based network intrusion detection system for RPL based Internet of Things. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). 2019 Apr 18–19; Ghaziabad, India. p. 1–6.
48. Priya DD, Kiran A, Purushotham P. Lightweight Intrusion Detection System (L-IDS) for the Internet of Things. In: 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC); 2022 Nov 19–20; Bhubaneswar, India. p. 1–4.
49. Alruwaili FF. Intrusion detection and prevention in Industrial IoT: a technological survey. In: 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME); 2021 Oct 7–8; Mauritius. p. 1–5.
50. Zachos G, Mantas G, Essop I, Porfyrakis K, Bastos JMC, Rodriguez J. An IoT/IoMT security testbed for anomaly-based intrusion detection systems. In: 2023 IFIP Networking Conference (IFIP Networking); 2023 Jun 12–15; Barcelona, Spain. p. 1–6.
51. Hernandez-Jaimes ML, Martinez-Cruz A, Ramírez-Gutiérrez KA, Feregrino-Uribe C. Artificial intelligence for IoMT security: a review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. Internet Things. 2023;23(3):100887. doi:10.1016/j.iot.2023.100887.
52. VOSviewer version 1.6.20 [Internet]. [cited 2024 Nov 28]. Available from: https://app.vosviewer.com/.
53. Wu Y, Zhang K, Zhang Y. Digital twin networks: a survey. IEEE Internet Things J. 2021;8(18):13789–804. doi:10.1109/jiot.2021.3079510.

54. Gupta D, Kayode O, Bhatt S, Gupta M, Tosun AS. Hierarchical federated learning based anomaly detection using digital twins for smart healthcare. In: 2021 IEEE 7th International Conference on Collaboration and Internet Computing (CIC); 2021 Dec 13–15; Atlanta, GA, USA. p. 16–25.
55. Nandy S, Adhikari M, Khan MA, Menon VG, Verma S. An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. IEEE J Biomed Health Informs. 2021;26(5):1969–76. doi:10.1109/jbhi.2021.3101686.
56. Lombardi M, Pascale F, Santaniello D. Internet of things: a general overview between architectures, protocols and applications. Information. 2021;12(2):87. doi:10.3390/info12020087.
57. Zhang J, Ma M, Wang P, Sun XD. Middleware for the Internet of Things: a survey on requirements, enabling technologies, and solutions. J Syst Archit. 2021;117(10):102098. doi:10.1016/j.sysarc.2021.102098.
58. Rashid FKM, Osman OS, Mcgee ET, Raad H. Discovering hazards in IoT architectures: a safety analysis approach for medical use cases. IEEE Access. 2023;11(24):53671–86. doi:10.1109/access.2023.3280414.
59. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. BEdgeHealth: a decentralized architecture for edge-based IoMT networks using blockchain. IEEE Internet Things J. 2021;8(14):11743–57. doi:10.1109/jiot.2021.3058953.
60. Attaran M, Celik BG. Digital Twin: benefits, use cases, challenges, and opportunities. Decision Anal J. 2023;6(80):100165. doi:10.1016/j.dajour.2023.100165.
61. Minerva R, Lee GM, Crespi N. Digital twin in the IoT context: a survey on technical features, scenarios, and architectural models. Proc IEEE. 2020;108(10):1785–824. doi:10.1109/jproc.2020.2998530.
62. Elayan H, Aloqaily M, Guizani M. Digital twin for intelligent context-aware IoT healthcare systems. IEEE Internet Things J. 2021;8(23):16749–57. doi:10.1109/jiot.2021.3051158.
63. Fei T, Xuemin S, Cheng J, Yonghuai Z, Weiran L, Yong W, et al. makeTwin: a reference architecture for digital twin software platform. Chin J Aeronautics. 2024;37(1):1–18. doi:10.1016/j.cja.2023.05.002.
64. Aziz A, Schelén O, Bodin U. Digital twin as a proxy for industrial cyber-physical systems. In: Proceedings of the 2023 10th International Conference on Wireless Communication and Sensor Networks; 2023 Jan 6–8; Chengdu, China. p. 85–92.
65. Shah K, Prabhakar T, Sarweshkumar C, Abhishek S, Kumar TV. Construction of a digital twin framework using free and open-source software programs. IEEE Internet Comput. 2021;26(5):50–9. doi:10.1109/mic.2021.3051798.
66. Lazzari L, Farias K. Uncovering the hidden potential of event-driven architecture: a research agenda. arXiv:2308.05270. 2023.
67. Löcklin A, Jung T, Jazdi N, Ruppert T, Weyrich M. Architecture of a human-digital twin as common interface for operator 4.0 applications. Procedia CIRP. 2021;104:458–63. doi:10.1016/j.procir.2021.11.077.
68. Angulo C, Gonzalez-Abril L, Raya C, Ortega JA. A proposal to evolving towards digital twins in healthcare. In: The 8th International Work-Conference on Bioinformatics and Biomedical Engineering; 2020 Sep 30–Oct 2; Granada, Spain. p. 418–26.
69. Castellani A, Schmitt S, Squartini S. Real-world anomaly detection by using digital twin systems and weakly supervised learning. IEEE Trans Ind Inform. 2020;17(7):4733–42. doi:10.1109/tii.2020.3019788.
70. Sasikala M, John YM, Jothi B, Nandhini S, Kumar S. Integrating digital twins with AI for real-time intrusion detection in smart infrastructure networks. In: 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS); 2024 Aug 23–24; Hassan, India. p. 1–6.
71. Qamsane Y, Phillips JR, Savaglio C, Warner D, James SC, Barton K. Open process automation-and digital twin-based performance monitoring of a process manufacturing system. IEEE Access. 2022;10(1):60823–35. doi:10.1109/access.2022.3179982.
72. Aheleroff S, Xu X, Zhong RY, Lu Y. Digital twin as a service (DTaaS) in Industry 4.0: an architecture reference model. Adv Eng Inform. 2021;47(2):101225. doi:10.1016/j.aei.2020.101225.
73. Manocha A, Bhatia M, Kumar G. Smart monitoring solution for dengue infection control: a digital twin-inspired approach. Comput Methods Programs Biomed. 2024;257(10):108459. doi:10.1016/j.cmpb.2024.108459.
74. Zachos G, Essop I, Mantas G, Porfyrakis K, Ribeiro JC, Rodriguez J. An anomaly-based intrusion detection system for internet of medical things networks. Electronics. 2021;10(21):2562. doi:10.3390/electronics10212562.

75. Kabir MR, Ray S. DT-IoMT: a digital twin reference model for secure internet of medical things. In: 2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI); 2024 Jul 1–3; Knoxville, TN, USA. p. 433–8.
76. Prakash R, Nayar GR, Thomas T. Security risk assessment of metaverse based healthcare systems based on common vulnerabilities and exposures (CVE). In: 2023 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE); 2023 Nov 8–11; Kerala, India. p. 1–10.
77. Ferrag MA, Kantarci B, Cordeiro LC, Debbah M, Choo KKR. Poisoning attacks in federated edge learning for digital twin 6G-enabled IoTs: an anticipatory study. In: 2023 IEEE International Conference on Communications Workshops (ICC Workshops); 2023 May 28–Jun 1; Rome, Italy. p. 1253–8.
78. Lai X, He X, Pang Y, Zhang F, Zhou D, Sun W, et al. A scalable digital twin framework based on a novel adaptive ensemble surrogate model. J Mech Des. 2023;145(2):021701. doi:10.1115/1.4056077.
79. Xu X, Wang G, Yan H, Zhang L, Yao X. Deep-learning-enhanced digital twinning of complex composite structures and real-time mechanical interaction. Compos Sci Technol. 2023;241:110139. doi:10.1016/j.compscitech.2023.110139.
80. Huang Z, Zhang N, Shen J, Diamantopoulos G, Hua Z, Tziritas N, et al. Distributed simulation for digital twins of large-scale real-world DiffServ-based networks. arXiv:2405.20815. 2024.
81. Kellil M, Said SBH, Thi MT, Janneteau C, Olivereau A. Addressing the scalability of network digital twins: a network sampling approach. In: 2024 20th International Conference on Network and Service Management (CNSM); 2024 Oct 28–31; Prague, Czech Republic. p. 1–7.
82. Ne Khan, Rudman RJ. IoT medical device risks: data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019. South African J Bus Manag. 2025;56(1):4796. doi:10.4102/sajbm.v56i1.4796.
83. Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the internet of things. IEEE Commun Surv Tutorials. 2018;21(2):1636–75.
84. Franklin JM, Howell G, Ledgerwood S, Griffith JL. Security analysis of first responder mobile and wearable devices. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology; 2020.
85. Koutras D, Stergiopoulos G, Dasaklis T, Kotzanikolaou P, Glynos D, Douligeris C. Security in IoMT communications: a survey. Sensors. 2020;20(17):4828. doi:10.3390/s20174828.
86. Bouriche A, Bouriche S. A systematic review on security vulnerabilities to preveny types of attacks in iomt. Int J Computat, Inf Manuf (IJCIM). 2022;2(2):73–83. doi:10.54489/ijcim.v2i2.107.
87. Dadkhah S, Neto ECP, Ferreira R, Molokwu RC, Sadeghi S, Ghorbani AA. CICIoMT2024: a benchmark dataset for multi-protocol security assessment in IoMT. Internet Things. 2024;28(5):101351. doi:10.1016/j.iot.2024.101351.
88. Areia J, Bispo IA, Santos L, Costa RL. IoMT-TrafficData: a dataset for benchmarking intrusion detection in IoMT. Zenodo. 2023 [Dataset]. doi:10.5281/zenodo.8116338.
89. Ahmed M, Byreddy S, Nutakki A, Sikos LF, Haskell-Dowland P. ECU-IoHT: a dataset for analyzing cyberattacks in Internet of Health Things. Ad Hoc Netw. 2021;122(8):102621. doi:10.1016/j.adhoc.2021.102621.
90. Hady AA, Ghubaish A, Salman T, Unal D, Jain R. Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access. 2020;8:106576–84. doi:10.1109/access.2020.3000421.
91. Zolanvari M, Teixeira MA, Gupta L, Khan KM, Jain R. WUSTL-IIOT-2021 dataset for IIoT cybersecurity research. 2021 [Internet]. [cited 2024 Nov 28]. Available from: http://www.cse.wustl.edu/$\sim$jain/iiot2/index.html.
92. Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H. Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications: centralized and federated learning. IEEE Dataport. 2022 [Dataset]. doi:10.21227/mbc1-1h68.
93. Sharafaldin I, Lashkari AH, Ghorbani AA. Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp. 2018;1(2018):108–16.
94. Ullah I, Mahmoud QH. A scheme for generating a dataset for anomalous activity detection in IoT networks. In: Canadian Conference on Artificial Intelligence; 2020 May 13–15; Ottawa, ON, Canada. p. 508–20.
95. Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Breitenbacher D, Shabtai A. UCI Machine Learning Repository. 2018 [Dataset]. doi:10.24432/C5RC8J.
96. Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: Military Communications and Information Systems Conference (MilCIS); 2015 Nov 10–12; Canberra, ACT, Australia. p. 1–6.

97. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications; 2009 Jul 8–10; Ottawa, ON, Canada. p. 1–6.
98. Sun S, Sharma P, Nwodo K, Stavrou A, Wang H. FedMADE: robust federated learning for intrusion detection in iot networks using a dynamic aggregation method. In: International Conference on Information Security; 2024 Oct 24–26; Arlington, VA, USA. p. 286–306.
99. Pope J, Spyridopoulos T, Kumar V, Raimondo F, Gunner S, Oikonomou G, et al. Intrusion detection at the IoT Edge using federated learning. In: Security and privacy in smart environments. Cham, Switzerland: Springer; 2024. p. 98–119. doi:10.1007/978-3-031-66708-4_5.
100. Olanrewaju-George B, Pranggono B. Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models. Cyber Secur Appl. 2025;3(46):100068. doi:10.1016/j.csa.2024.100068.
101. Li J, Othman MS, Chen H, Yusuf LM. Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning. J Big Data. 2024;11(1):36. doi:10.1186/s40537-024-00892-y.
102. Empl P, Böhm F, Pernul G. Process-aware intrusion detection in MQTT networks. In: Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy; 2024 Jun 19–21; Porto, Portugal. p. 91–102.
103. Shanthi D, Swapna N, Kiran A, Anoosha S. Ensemble approach of GP, ACOT, PSO, and SNN for predicting software reliability. Int J Eng Syst Modelling Simulation. 2024;15(2):68–75. doi:10.1504/ijesms.2024.136976.
104. Ennaji EM, El Hajla S, Maleh Y, Mounir S. Federated deep learning models for intrusion detection in IoT. In: Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security; 2024 Apr 18–19; Meknes, Morocco. p. 1–5.
105. Raza M, Saeed MJ, Riaz MB, Sattar MA. Federated learning for privacy preserving intrusion detection in software defined networks. IEEE Access. 2024;12:69551–67. doi:10.1109/access.2024.3395997.
106. Zachos G, Mantas G, Essop I, Porfyrakis K, Ribeiro JC, Rodriguez J. Prototyping an anomaly-based intrusion detection system for internet of medical things networks. In: 2022 IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD); 2022 Nov 2–3; Paris, France. p. 179–83. doi:10.1109/camad55695.2022.9966912.
107. Saba T. Intrusion detection in smart city hospitals using ensemble classifiers. In: 2020 13th International Conference on Developments in eSystems Engineering (DeSE); 2020 Dec 14–17; Liverpool, UK. p. 418–22.
108. Sohail F, Bhatti MAM, Awais M, Iqtidar A. Explainable boosting ensemble methods for intrusion detection in internet of medical things (IoMT) applications. In: 2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2); 2024 Oct 22–23; Islamabad, Pakistan. p. 1–8.
109. Yamuna K, Sugumaran M, Arthi A, Premkumar R. Design and analysis of intrusion detection system using machine learning in smart healthcare system. J Mech Continua Math Sci. 2024;19(7):17–27.
110. Singh P, Gaba GS, Kaur A, Hedabou M, Gurtov A. Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT. IEEE J Biomed Health Inform. 2022;27(2):722–31. doi:10.1109/jbhi.2022.3186250.
111. Zaabar B, Cheikhrouhou O, Abid M. Intrusion detection system for IoMT through blockchain-based federated learning. In: 2022 15th International Conference on Security of Information and Networks (SIN); 2022 Nov 11–13; Sousse, Tunisia. p. 1–8.
112. Udayakumar P, Anandan R. Evaluation of protocol-centric IDS for the IoMT leveraging ML techniques. In: 2024 IEEE World AI IoT Congress (AIIoT); 2024 May 29–31; Seattle, WA, USA. p. 546–51. doi:10.1109/aiiot61789.2024.10578945.
113. Thamilarasu G, Odesile A, Hoang A. An intrusion detection system for internet of medical things. IEEE Access. 2020;8:181560–76. doi:10.1109/access.2020.3026260.
114. Aljuhani A, Alamri A, Kumar P, Jolfaei A. An intelligent and explainable SAAS-based Intrusion Detection System for resource-constrained IoMT. IEEE Internet Things J. 2024;11(15):25454–63. doi:10.1109/jiot.2023.3327024.

115. Otoum Y, Wan Y, Nayak A. Federated transfer learning-based IDS for the internet of medical things (IoMT). In: 2021 IEEE Globecom Workshops (GC Wkshps); 2021 Dec 7–11; Madrid, Spain. p. 1–6. doi:10.1109/gcwkshps52748.2021.9682118.
116. Aljuhani A. IDS-Chain: a collaborative intrusion detection framework empowered blockchain for internet of medical things. In: 2022 IEEE Cloud Summit; 2022 Oct 20–21; Fairfax, VA, USA. p. 57–62. doi:10.1109/cloudsummit54781.2022.00015.
117. Xu Q, Ali S, Yue T. Digital twin-based anomaly detection in cyber-physical systems. In: 14th IEEE Conference on Software Testing, Verification and Validation (ICST); 2021 Apr 12–16; Porto de Galinhas, Brazil. p. 205–16.
118. Bozdal M. Security through digital twin-based intrusion detection: a SWaT dataset analysis. In: 2023 16th International Conference on Information Security and Cryptology (ISCTürkiye); 2023 Oct 18–19; Ankara, Turkey. p. 1–6.
119. Maier A. Online passive learning of timed automata for cyber-physical production systems. In: 2014 12th IEEE International Conference on Industrial Informatics (INDIN); 2014 Jul 27–30; Porto Alegre, Brazil. p. 60–6.
120. Mathur AP, Tippenhauer NO. SWaT: A water treatment testbed for research and training on ICS security. In: 2016 International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater). 2016 Apr 11; Vienna, Austria. p. 31–6. doi:10.1109/cyswater.2016.7469060.
121. Yigit Y, Bal B, Karameseoglu A, Duong TQ, Canberk B. Digital twin-enabled intelligent DDOS detection mechanism for autonomous core networks. IEEE Commun Standards Magaz. 2022;6(3):38–44. doi:10.1109/mcomstd.0001.2100022.
122. Wang H, Di X, Wang Y, Ren B, Gao G, Deng J. An intelligent digital twin method based on spatio-temporal feature fusion for IoT attack behavior identification. IEEE J Sel Areas Commun. 2023;41(11):3561–72. doi:10.1109/jsac.2023.3310091.
123. Patel T, Jadav NK, Rathod T, Tanwar S, Garg D, Shahinzadeh H. AI-based Secure Intrusion Detection Framework for Digital Twin-enabled Critical Infrastructure. In: 2023 14th International Conference on Information and Knowledge Technology (IKT); 2023 Dec 26–28; Isfahan, Iran. p. 24–9.
124. He X, Chen Q, Tang L, Wang W, Liu T, Li L, et al. Federated continuous learning based on stacked broad learning system assisted by digital twin networks: an incremental learning approach for intrusion detection in UAV networks. IEEE Internet Things J. 2023;10(22):19825–38. doi:10.1109/jiot.2023.3282648.
125. Liu Z, Chen CP, Feng S, Feng Q, Zhang T. Stacked broad learning system: from incremental flatted structure to deep model. IEEE Trans Syst Man Cybern Syst. 2020;51(1):209–22. doi:10.1109/tsmc.2020.3043147.
126. Karaarslan E, Babiker M. Digital twin security threats and countermeasures: an introduction. In: 2021 International Conference on Information Security and Cryptology (ISCTURKEY); 2021 Dec 2–3; Ankara, Turkey. p. 7–11.
127. Li J, Kuang X, Lin S, Ma X, Tang Y. Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. Inf Sci. 2020;526(2):166–79. doi:10.1016/j.ins.2020.03.041.
128. Shao G, Frechette S, Srinivasan V. An analysis of the new ISO 23247 series of standards on digital twin framework for manufacturing. In: 2023 MSEC International Manufacturing Science and Engineering Conference; 2023 Jun 12–16; New Brunswick, NJ, USA. p. 1–10.