Internet of Things 38 (2026) 101991

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

AI-driven security solutions for IoMT devices: A survey

Islam Hentous [a,b], Valentino Merlino [c,*], Tayeb Kenaza [b], Saïd Mahmoudi [a], Dario Allegra [c]

[a] Faculty of Engineering, University of Mons, Belgium
[b] Computer Security Laboratory, École Militaire Polytechnique, Algiers, Algeria
[c] Department of Mathematics and Computer Science, University of Catania, Italy

ARTICLE INFO

Keywords:
Internet of medical things
Artificial intelligence powered security
Privacy
IoMT
Malware detection
Blockchain

ABSTRACT

The Internet of Medical Things (IoMT) marks a transformative leap in modern healthcare by enabling intelligent, connected medical devices to support real-time monitoring, diagnostics, and treatment. However, this rapid digitalization also expands the attack surface of healthcare systems, exposing them to a wide array of sophisticated cyber threats. The unique characteristics of IoMT, including device heterogeneity, resource limitations, and operation across diverse network environments, render traditional cybersecurity approaches insufficient. In response, the integration of Artificial Intelligence (AI) into security architectures is emerging as a powerful paradigm shift. This survey systematically explores the fusion of AI and cybersecurity in IoMT, covering threat landscapes, attack surfaces, and existing defense mechanisms across medical environments. By identifying IoMT-specific security requirements and challenges, investigating AI-driven security mechanisms, and analyzing how such techniques can be adapted to IoMT constraints, this work fills a critical gap in existing research on secure medical IoT systems.

1. Introduction

Advances in artificial intelligence (AI), sensors, and wireless communications have all contributed to the growth of Internet of Things (IoT) devices and applications [1–5]. The proliferation of IoT devices and applications in various domains introduces numerous security challenges. Traditional security mechanisms are often inadequate for IoT due to the constraints of processing power, memory, and battery life in many devices [6]. The use of diverse and often incompatible protocols and technologies contributes to a fragmented and heterogeneous system, making it more difficult to secure and increasing the number of potential attack vectors [7–10]. The security landscape is further complicated by the varying security requirements and challenges presented by different IoT applications, such as smart cities [11], smart factories [12], smart homes [13], and smart healthcare [14]. One key component of smart healthcare is the Internet of Medical Things (IoMT), which encompasses a wide array of medical devices and applications [15].

The convergence of cybersecurity and AI has emerged as a transformative paradigm, offering proactive, intelligent, and adaptive defense mechanisms against increasingly complex threats [16]. In the context of the IoMT, this fusion is particularly critical, as medical systems face not only general cybersecurity challenges but also stringent domain-specific requirements. This includes the protection of highly sensitive health data, the critical nature of healthcare services [17], and mandatory compliance with a variety of international data protection and medical device regulations. Key frameworks include the Health Insurance Portability and Accountability Act (HIPAA) [18] in the United States, the General Data Protection Regulation (GDPR) [19] and Medical Device Regulation (MDR) [20]

* Corresponding author.
E-mail address: valentino.merlino@phd.unict.it (V. Merlino).

https://doi.org/10.1016/j.iot.2026.101991
Received 13 October 2025; Received in revised form 28 May 2026; Accepted 30 May 2026
Available online 9 June 2026

in the European Union. Other jurisdictions impose similarly rigorous standards, such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) [21], Brazil's Lei Geral de Proteção de Dados (LGPD) [22], Japan's Act on the Protection of Personal Information (APPI) [23], and Singapore's Personal Data Protection Act (PDPA) [24].

IoMT has significantly contributed to the advancement of healthcare by making medical services more accessible, reducing costs, and enhancing overall efficiency [25]. By enabling remote patient monitoring, real-time diagnostics, and automated medical processes, IoMT helps bridge healthcare gaps, particularly in underserved areas [26]. However, as reliance on connected medical devices grows, the need for robust security becomes even more critical. The need for robust security in IoMT is particularly critical due to the significant risks involved; security breaches can lead to significant financial losses and, more importantly, threaten patient safety and privacy [27]. The number and cost of attacks on hospitals and medical devices highlight the urgency of enhancing security measures in this domain.

This survey systematically explores the unique security challenges faced by IoMT systems, with a particular emphasis on how AI-based techniques can enhance their resilience and protection. Adhering to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology [28], we provide a transparent and comprehensive synthesis of current research in the field. Beyond addressing conventional IoT security concerns, this review highlights innovative AI-powered approaches that are being tailored to safeguard IoMT environments against a wide array of evolving cyber threats. Specifically, this encompasses malware detection, anomaly detection in physiological data, intrusion detection systems, AI-enhanced authentication protocols and blockchain-based trust architectures.

1.1. Related work

The application of AI to strengthen the security of IoMT devices has gained increasing interest over the past few years. To conduct a comprehensive survey on AI-driven security solutions for IoMT, we reviewed the most recent and relevant literature (Table 1), with a focus on studies that tackled both traditional security challenges and emerging AI-based mechanisms tailored to the specific constraints of IoMT systems.

Earlier research on IoMT security primarily focused on identifying vulnerabilities and proposing conventional mitigation techniques without integrating AI. For example, Sun et al. [29] and Kharroub et al. [30] provided overviews of IoMT security risks, highlighting common threats such as data breaches, unauthorized access, and denial-of-service attacks. Ghubaish et al. [31] and Elhoseny et al. [32] contributed further by categorizing threats and proposing framework-based countermeasures, yet none of these works investigated the potential of AI to address these security issues. Rasool et al. [33] similarly concentrated on traditional approaches, underscoring the need for adaptive and intelligent security mechanisms in response to evolving threats in IoMT environments.

In parallel, some studies began exploring AI-based security for the broader IoT, though without a focus on the unique characteristics of IoMT. Wu et al. [34] explored machine learning approaches for anomaly detection in IoT systems, while Barnawi et al. [35] presented a systematic review of AI techniques for IoT security. Alwahedi et al. [36] further evaluated the effectiveness of AI-based security models in general IoT environments. While valuable, these works do not address how AI solutions can be adapted to IoMT-specific constraints, such as strict latency requirements, resource limitations, and the critical sensitivity of medical data.

A more recent study by Messinis et al. [37] takes a step forward by specifically examining AI-based security mechanisms within the IoMT domain. This work highlights the role of AI in enhancing threat detection and response capabilities for IoMT networks. However, it stops short of thoroughly analyzing how AI models can be adapted to the computational and architectural constraints of medical devices. Moreover, it does not address which specific layers of the IoMT ecosystem, such as perception, network, or application, are most effectively secured through AI-based techniques.

Taken together, this body of literature reveals a clear progression from general IoT security frameworks to the exploration of AI-enhanced solutions.

Overall, prior work shows a clear progression from characterizing IoMT threats and traditional mitigations to proposing AI-based defenses for IoT more broadly. Yet these lines of research rarely converge: IoMT surveys typically stop short of AI integration, while AI-for-IoT surveys seldom account for IoMT-specific requirements (e.g., safety-critical latency, limited device resources, and stringent medical-data privacy).

However, a significant research gap remains in developing and analyzing AI-based security models that are explicitly designed for the operational and technical limitations of IoMT systems. This underscores the need for focused studies that not only integrate AI for threat detection and mitigation but also consider device-level constraints, real-time processing requirements, and the layered architecture of IoMT environments.

1.2. Survey organization and main contributions

Our survey aims to fill the gaps highlighted in the related works by providing a comprehensive and systematic review of AI-driven security mechanisms specifically adapted for IoMT systems. Although previous research has explored AI-based security in IoMT, existing studies lack a thorough analysis of how these mechanisms address the unique operational constraints, risks, and layered architecture of IoMT. In particular, there is no detailed investigation into how AI-based solutions can be tailored to different layers of the IoMT stack [38], from perception to application.

The contributions of this survey can be summarized as follows:

- It highlights the security requirements and challenges of IoMT systems.
- It investigates the use of AI techniques to address these complex security requirements.

Table 1
Comparison of IoMT security studies. differently by previous works, our study covers all the modern aspects of IoMT technologies.

References	Year	Authors	Including MIoT	Including AI-Powered Solutions	Adapted to IoMT-Specific Requirements
[29]	2018	Sun et al.	✓	✗	✗
[30]	2020	Kharroub et al.	✓	✗	✗
[31]	2020	Ghubaish et al.	✓	✗	✗
[34]	2020	Wu et al.	✗	✓	✗
[32]	2021	Elhoseny et al.	✓	✗	✗
[33]	2022	Rasool et al.	✓	✗	✗
[35]	2023	Barnawi et al.	✗	✓	✗
[36]	2024	Alwahedi et al.	✗	✓	✗
[37]	2024	Messinis et al.	✓	✓	✗
—	2025	**Our Study**	✓	✓	✓

- It explores how AI can be tailored to IoMT constraints, focusing on lightweight models, privacy-preserving methods, and real-time processing to enhance security effectively.

The remainder of this paper is organized as follows: Section 2 explores the specific characteristics of the IoMT paradigm. Section 3 outlines the survey methodology, highlighting its distinctions from general-purpose IoT networks and detailing the unique security challenges posed by IoMT. Section 4 presents the conducted review and addresses the research questions defined in the study. Section 5 provides a critical discussion of the findings and suggests potential directions for future research. Section 6 concludes the paper.

2. Background on IoMT and its security challenges

The IoMT is notably affecting modern healthcare by enabling seamless connectivity between medical devices, patients, healthcare professionals, and healthcare applications. It uses advanced network and data analysis technologies to provide real-time patient monitoring, remote diagnostic, and personalized treatment recommendations, significantly improving quality of care [39–41]. However, the integration of IoT devices into critical healthcare infrastructure introduces a number of challenges regarding reliability, security and privacy [42–44].

A robust understanding of the architecture and components of IoMT is essential to evaluate its capabilities and limitations. The IoMT ecosystem is characterized by a heterogeneous network of devices with computational and energy constraints. These devices collect and transmit sensitive medical data, often in real time, to facilitate informed diagnosis and decision making by healthcare professionals.

The increasing adoption of IoMT systems requires a focus on several critical aspects, including their architecture, data flow mechanisms, and security requirements. The inherent vulnerabilities of IoMT systems, coupled with their reliance on cloud computing and sensitive data sharing, present serious security challenges. Consequently, integrating novel security mechanisms, such as AI-driven solutions, has emerged as a key research direction to safeguard IoMT systems and applications.

This section provides an overview of the IoMT architecture, its components, and its applications. In addition, it explores the unique security challenges and requirements posed by IoMT systems, laying the groundwork for understanding the potential of AI-based solutions to address these challenges.

2.1. Key components of IoMT

The IoMT consists of various key components that work together to deliver efficient, data-driven healthcare solutions. These components include:

- **Medical Sensors and Devices:** These include wearable devices, implantable sensors, and diagnostic equipment that monitor and collect physiological data such as heart rate, blood pressure, glucose levels, and oxygen saturation. These devices serve as the primary data sources in the IoMT ecosystem.
- **Connectivity Modules:** IoMT relies on wireless communication technologies such as Bluetooth, Zigbee, Wi-Fi, 4G/5G, and Low Power Wide Area Networks (LPWANs) to facilitate data transmission between devices, gateways, and cloud servers.
- **Edge and Gateway Devices:** These intermediate devices aggregate and pre-process data from medical sensors before transmitting it to the cloud. They reduce latency and offload computational tasks, enabling real-time analytics and decision-making.
- **Cloud Infrastructure:** Cloud platforms store, process, and analyze large volumes of medical data. They host advanced AI and machine learning models that enable predictive analytics, anomaly detection, and other healthcare applications.
- **Healthcare Applications:** These include mobile and web applications that present processed data to healthcare professionals and patients. These applications provide dashboards, alerts, and telemedicine capabilities for remote monitoring and diagnosis.

Fig. 1 depicts the overall architecture of the IoMT, highlighting its key components and their interactions.

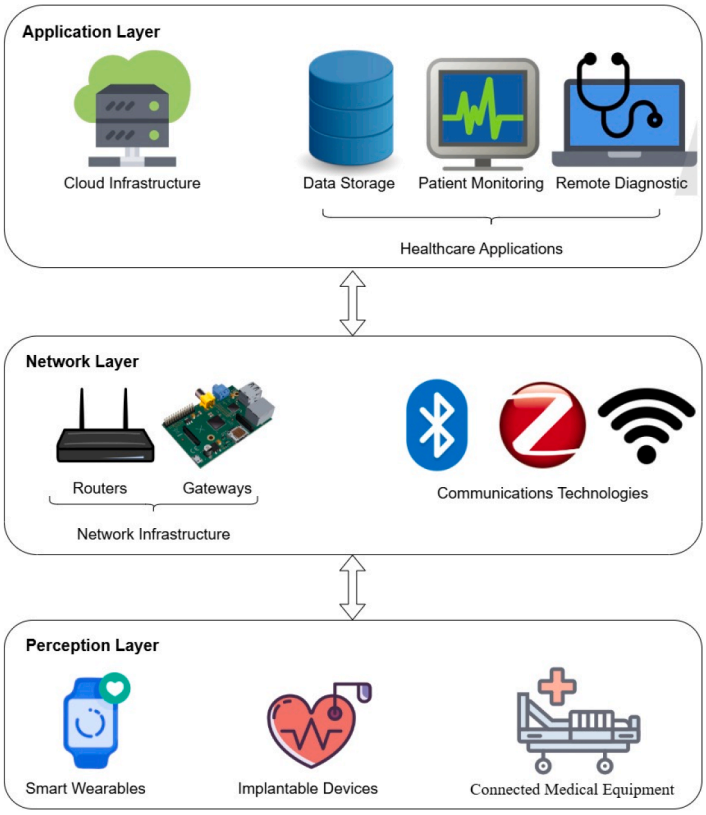

Fig. 1. IoMT three-layer architecture.

2.2. Applications of IoMT in healthcare

The IoMT encompasses specific, well-defined applications, and tailoring security measures to these use cases can significantly enhance overall security. One key application is Remote Health Monitoring, which enables healthcare professionals to track patients' vital signs and health parameters remotely using wearable and implantable medical devices. This allows for early detection of abnormal physiological patterns, ensuring timely intervention when needed [45]. It supports biomarker analysis for illness detection, and can even facilitate the remote identification of adverse drug reactions. Another vital use case is telemedicine and tele-dentistry [46], facilitating remote consultations and medical diagnoses to improve access to healthcare services, particularly in underserved areas. Predictive Analytics and clinical decision support systems are also integral to IoMT, leveraging data analysis to anticipate health-related events and support medical decision-making [45]. IoMT further supports applications in accident and emergency informatics [45], as well as testing and tracing for infectious disease outbreaks, offering rapid response tools in public health contexts. In hospital and clinical environments, IoMT provide solutions for medical equipment tracking and maintenance [47]. The connected nature of IoMT-based medical devices allows the monitoring of device availability, usage, and detect technical faults early, reducing downtime and enhancing patient safety. Ambient assisted living (AAL) represents another application area [46], where IoMT systems have the potential to be help elderly or disabled individuals maintain independence by providing safety, comfort, and health monitoring within their living environments. These applications highlight the critical role of IoMT in advancing healthcare, emphasizing the importance of robust security tailored to their unique demands.

2.3. Security challenges

The IoMT exhibits important differences compared to general IoT systems, particularly in terms of security and operational requirements. Before reviewing the security mechanisms proposed in the literature for IoMT devices, it is crucial to first define these specific characteristics. Although IoT and IoMT share many common challenges, such as resource constraints, secure key distribution, and scalability, the medical context imposes stricter demands. In particular, IoMT systems must handle highly sensitive medical data, requiring strong guarantees of privacy and regulatory compliance. Moreover, data integrity and availability are critical, as tampering or system unavailability can directly endanger patients' lives. Many IoMT applications are extremely time-sensitive, where even slight delays can have life-threatening consequences. Devices are often highly constrained in terms of battery life, especially when implanted in patients for extended periods, and the mobility of wearable and implantable devices further complicates the design

Table 2
Attacks on IoMT perception layer and their impact.

Type of Attack	Description	Potential Impact	Perception layer Relevance
Firmware Tampering [49]	Unauthorized modification of an IoMT device's embedded firmware, altering its intended behavior.	Tampered firmware can cause device malfunction (e.g. false readings or disabled alarms), directly endangering patient safety.	Targets the device firmware, which resides in the perception layer of IoMT.
Unauthorized Access [27]	Exploitation of weak authentication or default credentials on devices.	Unauthorized control of devices, compromised data integrity.	It involves the device software/firmware
Sensor Spoofing [50]	Crafting false sensor inputs (e.g. faked physiological signals) to deceive an IoMT device.	Leads to erroneous device outputs (false alarms or missed alerts), causing misdiagnosis or inappropriate treatment.	Directly involves the device's physical sensors
Physical Attack on Devices [51]	Direct physical tampering, theft, or damage to IoMT devices.	Device unavailability, data loss, or exposure of sensitive information.	It involves the device physically
Malware Infection [52]	Infection Installation of malicious software (viruses, trojans) on an IoMT device.	Can steal patient data or disrupt device functions (e.g. disabling alarms or altering drug delivery), posing serious safety risks.	Involves the device's software/firmware, which is part of the perception layer.
Side-Channel Attacks [53]	Exploiting indirect device emissions (power, timing, EM) to extract secret information.	Can reveal sensitive patient data or device secrets (e.g. cryptographic keys) without direct access, compromising confidentiality.	Exploiting indirect device emissions (power, timing, EM) to extract secret information.
Battery Depletion Attacks [54]	Forcing an IoMT device to exhaust its battery (e.g. through repeated tasks), causing a denial of service.	A drained device stops functioning (e.g. monitoring or therapy halts), which can critically endanger patients.	Targets the device's power resources, a key aspect of the perception-layer hardware.
Data Injection [55]	Injecting false or fabricated data into an IoMT system's inputs or data streams.	Corrupts patient data and triggers false alerts (e.g. simulating nonexistent medical conditions), undermining clinical decisions.	Involves tampering with sensor-generated data at the perception layer.

of secure solutions. Although physical access attacks are less common within secured healthcare facilities, IoMT devices frequently operate across diverse network environments, ranging from trusted hospital networks to unprotected home or public networks. Additionally, IoMT applications often serve specific and well-defined use cases, such as remote health monitoring, which further shapes their security needs.

Therefore, while generic IoT security solutions can sometimes be adapted to IoMT scenarios, they must be rigorously evaluated and reinforced against AI-specific threats, considering the unique operational and regulatory constraints of the healthcare sector. The IoMT architecture itself is typically organized into three layers: the perception layer, the network layer, and the application layer [48], each presenting distinct security requirements and challenges.

2.3.1. Perception layer

The perception layer, also known as the physical layer, consists of medical end devices, sensors, and actuators responsible for collecting medical data from patients and their environments. These devices face numerous security challenges due to their inherent hardware constraints, including limited processing power, memory, and battery life, which restrict the implementation of traditional security mechanisms. This is particularly critical for implantable devices, which must operate efficiently for months or even years without battery replacement. Additionally, device heterogeneity, stemming from various manufacturers with differing specifications, introduces interoperability and security standardization challenges. Many IoMT devices are highly mobile, as they are frequently worn or carried by patients, making them susceptible to unauthorized access, data interception, and potential tracking threats. Beyond mobility concerns, physical security risks also vary based on the deployment environment. While devices used in smart healthcare facilities benefit from controlled access and secure infrastructure, those used in home and public networks are exposed to higher risks of physical tampering and attacks such as cloning, spoofing, or unauthorized modifications.

Moreover, because these devices handle highly sensitive medical data, they require strict confidentiality measures. Ensuring data integrity, and availability at the perception layer is also critical–any compromise can lead to inaccurate diagnoses or severe patient harm. Table 2 provides an overview about specific attacks in the perception layer.

2.3.2. Network layer

The network layer facilitates communication between the perception layer and the application layer, enabling data transmission over various network infrastructures. This layer relies on wireless communications that are susceptible to vulnerabilities such as

Table 3
Attacks on the IoMT network layer and their impact.

Type of Attack	Description	Potential Impact	Network Layer Relevance
Man-in-the-Middle (MitM) [56]	Interception of communication between IoMT devices and servers.	Data alteration, eavesdropping, or injection of malicious commands.	Exploits intermediary network nodes or links to tamper with IoMT traffic.
Denial of Service (DoS) [52]	Overloading IoMT devices or their communication channels with spurious traffic.	Unavailability of critical monitoring services, potential risk to patient safety.	Targets bandwidth and processing resources of network gateways and links.
Routing Attacks [57]	Manipulation or misdirection of routing protocols (e.g., blackhole, wormhole).	Loss, delay, or misdirection of health data packets, risking misdiagnosis.	Undermines path selection and packet forwarding in IoMT networks.
Eavesdropping [38]	Unauthorized passive listening to unencrypted IoMT communications.	Compromise of sensitive patient data, regulatory non-compliance.	Involves capture and analysis of packets on network links or wireless channels.
Replay Attacks [58]	Reuse of previously captured IoMT messages or credentials to masquerade as a legitimate device.	Unauthorized device actions or data injections, undermining system integrity.	Relies on packet capture and retransmission within the network layer.

Table 4
Application-layer attacks in IoMT and their impact.

Type of Attack	Description	Potential Impact	Application Layer Relevance
Phishing Attacks [59]	Deceptive emails or spoofed web pages targeting healthcare staff or patients to steal credentials or deliver malware.	Compromised user accounts, unauthorized access to medical dashboards, leakage of sensitive patient data.	Exploits user-facing interfaces (web portals, mobile apps) used to manage IoMT devices.
Data Tampering [60]	Unauthorized alteration of medical records or telemetry data stored or processed by IoMT applications.	Misleading clinical decisions, incorrect diagnoses, and direct risk to patient safety.	Targets backend databases, application logic, and APIs that process IoMT data.
Ransomware [61]	Malware that encrypts application-layer data (EHRs, logs, configurations) and demands ransom for decryption.	Inaccessible patient records, disrupted care workflows, potential life-threatening delays.	Affects cloud storage, server file systems, and backup services used by IoMT management platforms.
SQL Injection [60]	Insertion of malicious SQL code into application inputs to manipulate IoMT databases.	Exposure or corruption of sensitive medical data, unauthorized data access or deletion.	Exploits poorly sanitized input fields in web/mobile applications interfacing with IoMT databases.
Cross-Site Scripting (XSS)	Injection of malicious scripts into IoMT web interfaces, executed in users' browsers.	Session hijacking, credential theft, or injection of further malware into the application.	Targets dashboards and control panels through which clinicians interact with IoMT systems.
API Exploitation	Abuse of insecure or misconfigured REST/GraphQL APIs to perform unauthorized operations.	Data exfiltration, unauthorized command execution on devices, or denial of service.	Leverages the application-layer endpoints that connect IoMT devices, analytics engines, and user clients.

eavesdropping, interference, and unauthorized access. Additionally, it handles a substantial amount of network traffic, characterized by large volume, variety, and velocity of data, which necessitates robust data management and transmission protocols. The network layer must also accommodate the heterogeneity of communication protocols, ensuring compatibility and seamless data flow across different devices and networks. Ensuring secure transmission is crucial to protect sensitive medical data and maintain patient privacy. Table 3 presents a list of attacks that target the network layer of the IoMT.

2.3.3. Application layer

The application layer processes, analyzes, and stores the data collected by IoMT devices, supporting various applications such as remote health monitoring, telemedicine, and predictive analytics for medical decision-making. This layer is responsible for managing highly sensitive personal medical information, necessitating strict adherence to regulations such as GDPR and HIPAA. It underpins critical healthcare services that have a direct impact on patient care and outcomes. The application layer must also ensure secure integration with other healthcare systems, which may have vulnerabilities, and manage interactions with clients who could potentially be malicious. Table 4 details attacks that target the application layer, along with their potential impacts.

3. Systematic map review of IoMT security research areas

This section outlines advanced security solutions tailored for IoMT systems, emphasizing the integration of AI-driven techniques, lightweight cryptographic methods, and distributed architectures. These approaches aim to provide scalable, efficient, and adaptive protection across the IoMT architecture, addressing the challenges identified in previous sections.

3.1. Adopted methodology

We first define a strict methodology for the literature survey, with a transparent search strategy and clearly defined inclusion and exclusion criteria for selected studies. This is essential to ensure the reproducibility of the study and the reliability of the conclusions. For this survey, we followed the PRISMA guidelines for systematic reviews. These guidelines ensure that our review will be transparent, complete, and accurate, facilitating its use by various stakeholders such as researchers, healthcare providers, and policymakers. By adhering to the PRISMA checklist and flow diagrams, our objective is to present our findings in a structured and reproducible manner, contributing valuable insights to the field.

3.1.1. Research questions

The first step is to clearly define the research questions. These questions are used to define the appropriate search queries and the inclusion criteria to be used to select the most relevant studies. Research questions must be carefully designed to align and directly support the objective of the study, ensuring that they effectively address key areas of investigation and contribute to achieving the intended goals and outcomes.

The first aim of the study is to estimate the intensity of publication as a first indicator of the potential of AI-assisted security in IoMT. This study also aims to identify the most promising security mechanisms and the areas where AI is best suited to mitigate security vulnerabilities, while investigating the ways in which AI-based security can be adapted to solve the security challenges that characterize IoMT systems and networks. The study aims to assess the effectiveness of the AI-based security mechanisms by identifying the common metrics used to measure their performance. Understanding these metrics helps to evaluate the practicality and trade-offs involved in implementing AI-based solutions in IoMT environments. The study aims to explore the real-world applications of AI-based security mechanisms in IoMT. This helps in understanding how these mechanisms are deployed in various healthcare scenarios and their impact on improving the security of patient data, medical devices, and communication networks in different use cases. Based on these goals, we have defined the following research questions:
RQ1: How many studies have investigated AI-based security mechanisms for IoMT?
RQ2: What AI-based security mechanisms are investigated in the literature?
RQ3: Which layers of the IoMT architecture can be secured using AI-based security mechanisms?
RQ4: Which metrics are used to evaluate AI-based security mechanisms?
RQ5: How are these mechanisms adapted for the specific characteristics of IoMT systems?
RQ6: In which IoMT use cases are these mechanisms applied?

Answering the research questions can help define IoMT security requirements and possible solutions.

3.2. Search strategy

We define the search strings and keywords based on the research questions the study aims to answer. We search for a combination of the keywords:

- “Internet of medical things”, “IoMT”
- “Security”, “Confidentiality”, “Integrity”, “Availability”
- “Artificial intelligence”, “Deep learning”, “Machine learning”, “ML”, “DL”, “AI”

We also have to select the academic libraries where we will search for relevant papers that fit our inclusion criteria.Three major academic databases were selected: Scopus, IEEE Xplore, and the ACM Digital Library. These databases were chosen for their broad and authoritative coverage of high-impact journals and conference proceedings in the fields of computer science, engineering, and information technology.

After the initial search, we expand the list of relevant papers using backward and forward snowballling techniques [62], as well as recommendations from Mendeley Reference Manager [63] and Connected Papers [64] to ensure the inclusion of all pertinent sources.

3.3. Inclusion and exclusion criteria

To ensure the inclusion of only relevant studies, we define a list of inclusion criteria. These criteria are selected on the basis of the research questions of the review. This includes:

- Studies that propose security mechanisms to ensure the security of IoMT systems.
- Studies that propose security mechanisms based on AI.
- Studies that propose mechanisms adapted to the characteristics of IoMT systems.

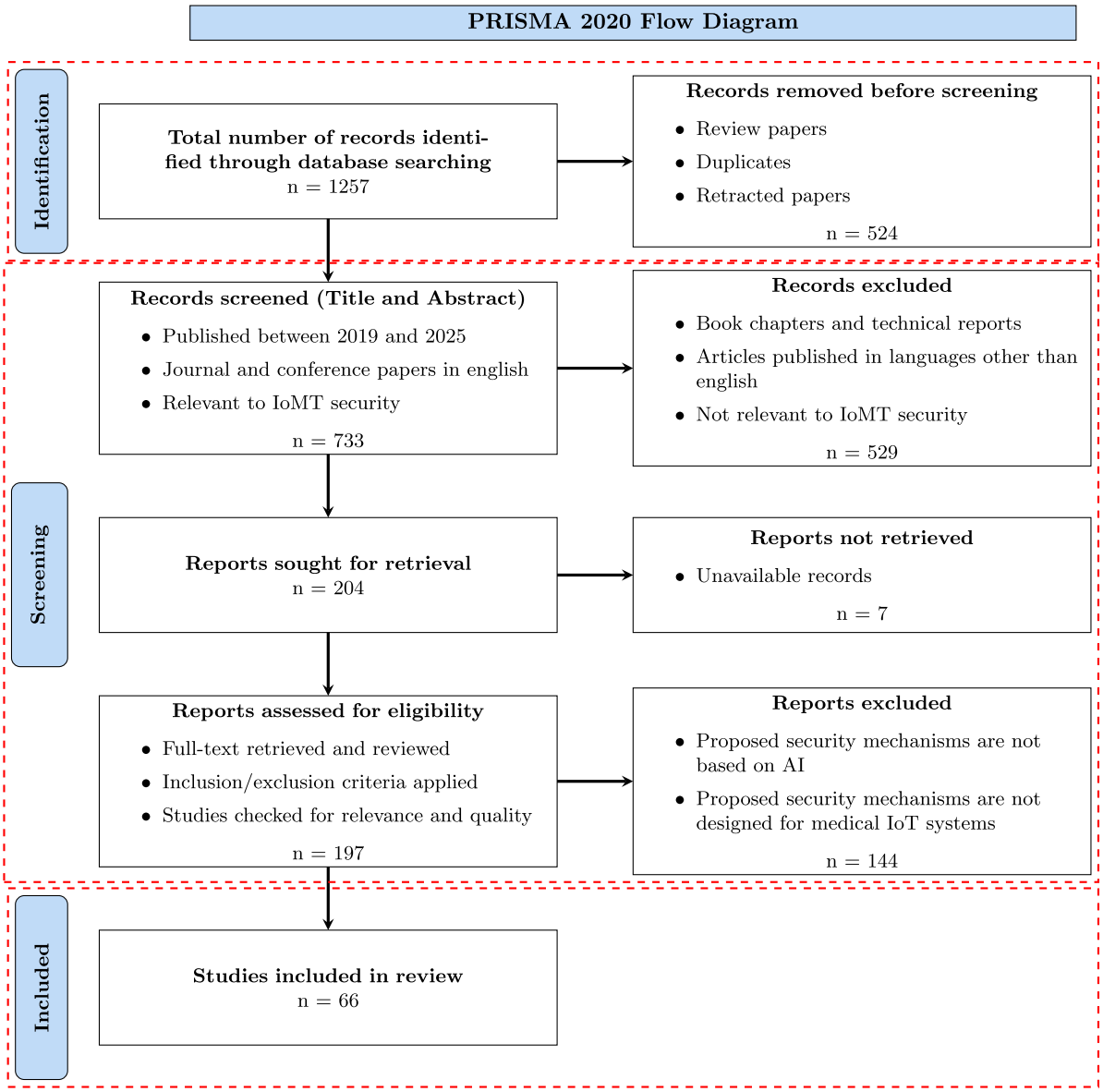

Fig. 2. PRISMA flow diagram.

- Peer-reviewed scientific papers published in English in scientific international journals or international conferences.

Studies that do not satisfy these criteria are excluded from the review, as shown in Fig. 2.

3.4. Data extraction and compilation

To effectively address the research questions, it is essential to systematically extract relevant information from the selected studies. This process involves identifying key variables and ensuring a structured, consistent approach to minimize bias and enhance comparability. The extracted data includes the objective of each study, the AI tools used to achieve them, the performance of each approach as well as the type of attacks mitigated and the layer secured. These informations provide critical insights into the methodologies, findings, and limitations of each study. By compiling this information, we can conduct a comprehensive comparative analysis, assessing the effectiveness of various techniques across different contexts. Furthermore, this approach enables us to identify emerging trends, recurring patterns, and research gaps, ultimately guiding future investigations and highlighting promising directions for advancement in the field (Fig. 2).

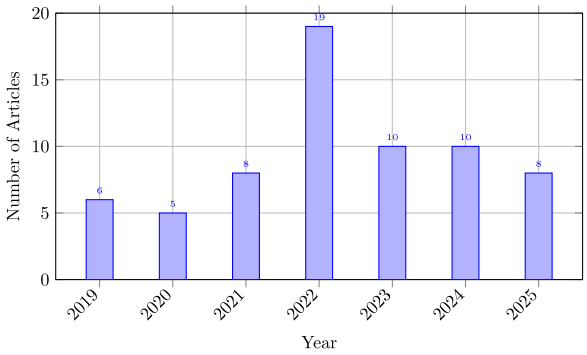

Fig. 3. Distribution of AI-based IoMT security articles from 2019 to 2024.

3.5. Selected papers

Fig. 2 summarizes the PRISMA paper selection methodology using a flow chart detailing every step. During the identification phase, we retrieved a total of 1257 papers using the selected keywords from all three databases. Duplicates, retracted articles, and review papers were removed before screening. Out of the 733 remaining articles, we applied the inclusion and exclusion criteria. By considering the titles, abstracts, and keywords of the articles, we excluded 529 that were not in English or were not relevant to IoMT security. While retrieving the full text for the remaining articles, 7 were excluded due to unavailability. After reviewing the full texts of the remaining 197 articles and applying the inclusion and exclusion criteria, we selected 60 studies based on relevance and quality.

A total of 66 relevant articles were identified that specifically explore AI-based security mechanisms in the context of IoMT. These studies were published over the last five years (2019–2024). The distribution of articles by year is presented in Fig. 3.

The distribution highlights an increasing interest in this field, with a noticeable rise in publications from 2021 onward, reflecting the growing relevance of AI-driven solutions in securing IoMT systems.

4. Review of AI-based security mechanisms for the IoMT

An IoMT architecture typically consists of three primary layers: the perception layer, which involves medical sensors and actuators; the network layer, comprising gateways and communication channels; and the application layer, encompassing cloud services and user interfaces [60]. IoMT devices, continuously generating sensitive patient data, impose stringent security and privacy requirements, given the critical nature of the information they handle. Recent studies have consistently demonstrated that integrating machine learning (ML) and deep learning (DL) techniques into security frameworks significantly enhances detection speed, accuracy, and robustness in IoMT environments [37]. As a result, AI-based security mechanisms are increasingly being tailored to each IoMT layer, addressing the specific threats and challenges inherent to each tier.

Building upon the security challenges identified in Section 2.3, this section reviews state-of-the-art AI-powered defenses, organized by layer: perception, network, and application. Each subsection highlights how ML and DL techniques are being leveraged to mitigate the unique security threats and constraints at each layer of the IoMT architecture. The reviewed studies are presented in chronological order, reflecting the ongoing progress and evolution of AI-based security solutions in this domain. By tracing the advancements over time, we demonstrate the increasing sophistication and adaptability of these solutions in addressing the complex and dynamic threats facing medical IoT systems.

4.1. Solutions for perception layer security

The perception layer of IoMT systems, comprising embedded, resource-constrained medical sensors and actuators, is particularly vulnerable to a diverse range of cyber threats. As outlined in Table 2, these threats include malware infections, firmware tampering, data injection, and physical attacks, all of which can compromise device integrity, disrupt clinical operations, or endanger patient safety. Given the limited computational and energy resources at this layer, implementing robust, real-time security mechanisms is both critical and challenging.

To address these constraints, recent research emphasizes lightweight *on-device* and *edge-based* AI techniques capable of operating efficiently within the limitations of IoMT hardware. In this section, we examine state-of-the-art approaches focused on *malware detection* and *anomaly detection*, which serve as key enablers of perception-layer resilience. These AI-driven methods aim to secure data at its point of origin, ensuring the trustworthiness of sensed information and device behavior, even in scenarios of intermittent network connectivity or device isolation.

4.1.1. Malware detection

Although various attacks threaten the perception layer of IoMT systems, as illustrated in Table 2, this section focuses specifically on malware detection due to its critical role in protecting the integrity and availability of embedded medical devices. Malware

can compromise device functionality, alter clinical readings, or disable safety-critical features, thereby posing significant risks to patient care. Given that malware typically targets the firmware and software components at the perception layer, developing effective detection strategies for this layer is paramount.

Malware detection is a key security mechanism for protecting IoMT devices from malicious software. However, the unique constraints of these devices, including limited computational resources, battery capacity, and the heterogeneity of hardware platforms, make traditional host-based security solutions difficult to apply. Moreover, the proprietary and closed nature of device firmware further complicates efforts to audit or secure code running on these devices. Although over-the-air firmware updates can patch known vulnerabilities, they do not prevent the deployment of previously unknown or zero-day malware.

Detection approaches generally fall into two categories, depending on where analysis occurs: on-device (real-time) detection and remote detection using cloud or server-side resources [65]. While remote detection offers greater computational capacity, it introduces latency and dependency on constant connectivity, which is not always guaranteed in medical environments. On-device detection, though more challenging due to limited hardware resources, offers the advantage of local, immediate response.

Recent research explores lightweight, non-intrusive techniques for on-device malware detection by leveraging side-channel analysis. These methods utilize signals such as power consumption [6], electromagnetic emissions [66], or thermal profiles [67] to infer anomalous behavior without requiring direct code inspection. Among these, energy consumption analysis has emerged as a particularly promising approach due to its resilience to environmental noise and strong correlation with software execution patterns.

A wide range of AI-driven side-channel-based malware detection strategies have been proposed in the literature for IoMT systems. These include techniques based on signal reconstruction, clustering, deep learning, and bio-inspired algorithms, applied across both electromagnetic and power-based channels. Table 5 summarizes these representative approaches, detailing their detection methods, performance, and types of attacks mitigated.

Energy-based malware detection can be deployed in multiple configurations:

- *Independent Monitoring Systems* [65], placed between the IoT device and its power source, offering third-party observability.
- *Smart Plug Integration*, where commercial smart plugs with energy monitoring capabilities are used to host detection logic.
- *Built-in Power Sensors*, where IoMT manufacturers integrate power monitoring into the device architecture, enabling native anomaly detection similar to smartphone-based solutions.
- *Remote Server Analysis*, which processes collected energy traces off-device–though at the cost of latency and dependence on network availability.

However, the first two configurations are not suitable for battery-powered, wireless medical wearables, which are prevalent in the IoMT ecosystem. Consequently, on-device or tightly integrated solutions are most viable for perception-layer protection in this domain.

Sehatbakhsh et al. [68] propose a side-channel analysis technique for malware detection in embedded medical devices using electromagnetic (EM) signals. To effectively compare noisy or weak EM traces, they introduce a novel distance metric called Correlation-based Amplitude and Phase Error (CAPE). This metric is used in conjunction with the Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) algorithm to cluster EM traces collected during runtime. A malware attack is flagged when the CAPE distance exceeds a predefined threshold of 50%. Their approach achieves a detection latency of 2 ms, with a True Positive Rate (TPR) of 99.9% and a False Positive Rate (FPR) of 0.1% in experiments on a syringe pump under a code reuse malware attack.

A series of works by Khan et al. further develop non-intrusive EM-based malware detection for medical devices. In [69], the authors present a lightweight method that monitors the EM emissions of a syringe pump without introducing any computational overhead or requiring changes to hardware or software. In the training phase, the system constructs a dictionary of EM signatures corresponding to normal device behavior. During detection, the real-time EM trace is matched against this dictionary using the 1-Nearest Neighbor (1-NN) algorithm, and significant deviations are used to flag malware. The system demonstrates excellent performance with an instruction-level latency of approximately 200–800 instructions, an AUC of 99.5%, a TPR of 100%, and an FPR of 1%.

In a subsequent work [70], Khan et al. enhance this approach by applying an artificial neural network to model normal EM behavior. EM signals are collected wirelessly, then digitized and used to train a multilayer perceptron (MLP). The MLP predicts the signal at a masked central point based on surrounding samples, and prediction errors serve as indicators of anomalous behavior such as control-flow hijack attacks. This neural approach also achieves high performance, with an AUC of 0.99, with a total system delay of 10.625 μs and an IoT-side detection latency of approximately 120 μs, while preserving the benefits of non-intrusive, real-time monitoring.

Beyond EM-based methods, Khan et al. [71] also explore malware detection in software-defined IoMT networks using a hybrid deep learning approach. They propose a system combining a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) network, trained on malware opcodes. This hybrid model captures both spatial and temporal patterns in malware behavior. Deployed at the SDN controller level, it imposes no computational burden on IoMT devices. Evaluated with 10-fold cross-validation on a publicly available IoT malware dataset, the system achieves a detection latency of 1.2 s, an accuracy of 99.83%, an F1-score of 99.77%, an AUC of 100%, a TPR of 99.91%, and an FPR of 1.3%.

Shifting focus to power-based detection, Albasir et al. [72] propose an approach that transforms power consumption traces into two-dimensional time-frequency representations using the Constant-Q Transform (CQT). Robust features are then extracted using Histograms of Oriented Gradients (HOG), framing malware detection as an image classification task. A Convolutional Neural Network is trained on these HOG images to detect anomalies. Tested across several malware types and device categories, this approach achieves an accuracy of 88% and an F-score of 85%, demonstrating the feasibility of power-based analysis in diverse IoT and IoMT systems.

Table 5
Summary of AI-based malware detection approaches for IoMT with mitigated attack types.

Reference	Year	Objective	Method	Performance	Kind of Attack Mitigated
Sehatbakhsh et al. [68]	2019	Malware detection using electromagnetic signatures of syringe pump	Clustering with HDBSCAN using a novel CAPE distance metric	Detection latency 2ms; True Positive Rate (TPR) 99.9%, False Positive Rate (FPR) 0.1%	Malware Infection
Khan et al. [69]	2019	Malware detection using electromagnetic signatures of syringe pump	1-NN signal reconstruction and error calculation	Instruction-Level Latency 200–800 instructions; Area Under the Curve(99.5%), TPR 100%, FPR 1%,	Malware Infection
Khan et al. [70]	2019	Malware detection using electromagnetic signatures of syringe pumps	MLP-based EM-signal reconstruction and thresholding for anomalies	Total System Delay 10.625 µs, Detection Latency (IoT) 120 µs; AUC 0.99	Malware Infection
Khan et al. [71]	2021	Malware detection on the SDN controller of the IoMT network	CNN-LSTM on malware opcodes	Detection latency 1.2 s; Accuracy (ACC) 99.83%, F1-Score 99.77%, AUC 100%, TPR 99.91%, FPR 1.3%	Malware Infection
Albasir et al. [72]	2023	Malware detection in IoT and medical CPS applications	CQT-based power signal, 2D CNN classifier	ACC 88%; F-score 85%	Malware Infection; Battery Depletion Attacks
Alrubayyi et al. [73]	2024	Malware detection directly on edge devices	Lightweight classification via NPS algorithm	ACC 96.80%, F1-Score 98.34	Malware Infection
Almotiri et al. [74]	2025	Malware detection on the SDN controller of the IoMT network	Bi-layered AI-based malware detection using both static features and image representation of malware samples	ACC 99%, F1-Score 99%	Malware Infection

Alrubayyi et al. [73] present a broader security framework for IoT, including a malware detection mechanism tailored to IoMT using Artificial Immune Systems (AIS). Their method employs a Negative and Positive Selection (NPS) algorithm to distinguish between benign and malicious activity. Two sets of detectors are generated during training: one matching self-data (positive selection) and another explicitly avoiding it (negative selection). This AIS-based system surpasses the Modified Negative Selection Algorithm (MNSA), achieving a 21% improvement in detection rate while reducing the number of required detectors by 65%, significantly lowering memory and computational requirements, and achieves an accuracy of 96.80% with an F1-score of 98.34%.

Almotiri et al. [74] propose a bi-layered AI-based malware detection framework for SDN-based IoMT systems. The layered design allows early detection of general malware, followed by specialized ransomware identification. Static features including API calls and entropy, as well as grayscale visual representations of malware executables, are extracted and classified using ML techniques. This architecture combines feature-based analysis using models like LightGBM, XGBoost, and DNN with an image-based analysis using a CNN model. The approach is evaluated on several malware datasets and achieves approximately 99% detection accuracy with an F1-score of about 99%.

We can divide the reviewed approaches into side channel analysis-based approaches (using electromagnetic signatures or power consumption) or detection-based on malware signatures. These approaches are mostly deployed outside the device itself but near the edge of the network. It should be noted that some works take advantage of the SDN network architecture to deploy the malware detection model on the controller node, which has a complete, centralized view of the network topology. The evaluation strategies adopted in most studies remain narrowly focused on detection accuracy despite IoMT-specific deployment constraints. Key factors such as energy consumption and computational overhead are crucial for edge-level deployment but are typically not considered.

4.1.2. Data anomaly detection

Medical data in IoMT systems is a prime target for cyberattacks, particularly false data injection and device tampering. These threats compromise the integrity of sensor-based networks, potentially leading to incorrect diagnoses, flawed treatment decisions, and severe risks to patient safety. Such attacks may stem from compromised sensors, man-in-the-middle interception of data streams, or malicious software-level modifications.

Given the centrality of the perception layer as the source of data, ensuring its security is critical. As noted earlier, this layer consists of embedded, resource-constrained sensors and actuators that are especially vulnerable to real-time manipulation and physical compromise. Within this context, anomaly detection has emerged as a vital AI-driven technique for safeguarding perception-layer integrity by identifying deviations from normal behavioral or physiological patterns.

Anomaly detection systems monitor the data streams generated by IoMT devices in real-time, flagging suspicious patterns that may indicate cyber threats or device faults. These techniques can detect internal anomalies, such as sensor degradation or outlier physiological readings, as well as external attacks, including data injection or firmware tampering. By leveraging machine learning, statistical modeling, and federated intelligence, such systems enhance resilience without imposing significant computational burdens on constrained devices.

Recent studies have explored various architectures for deploying anomaly detection in IoMT environments, ranging from edge-based federated learning to statistical correlation models and hybrid time-series classifiers. Table 6 provides a summary of representative anomaly detection approaches, detailing their objectives, techniques, performance, and the types of attacks they aim to mitigate. These works collectively highlight the feasibility of lightweight, intelligent detection systems as part of a robust perception-layer security framework.

Newaz et al. [75] propose HealthGuard, a security framework designed to detect malicious activities in IoMT environments by leveraging data from multiple medical devices assigned to the same patient. The framework exploits the correlation between anomalous physiological signals to differentiate genuine medical anomalies from false data injection attacks. Multiple machine learning algorithms, including Artificial Neural Networks (ANN), Decision Trees (DT), Random Forests (RF), and K-Nearest Neighbors (KNN), are evaluated for their effectiveness in anomaly detection. The models are trained on a dataset collected from eight distinct medical devices, representing twelve benign scenarios and three types of attack scenarios: tampered devices, denial-of-service (DoS) attacks, and false data injection. Among the tested models, the ANN-based approach achieved the highest performance, with an accuracy of 91% and an F1-score of 89%.

Ben et al. [76] propose an anomaly detection system that distinguishes medical anomalies from technical faults and malicious attacks. Dimensionality reduction with PCA is used to respect the resource constraints of mobile medical devices and reduce latency for real-time detection. It is a centralized approach deployed on the gateway level. A correlogram is extracted from the training data, the correlation between physiological attributes is used to distinguish medical anomalies from false data injections. The approach achieves an accuracy of 99.21%, a True Positive Rate (TPR) of 99.75%, and an F1-score of 99.35% while keeping a lower computational complexity than compared approaches.

Gupta et al. [77] propose a hierarchical federated learning-based approach for anomaly detection in a remote patient monitoring scenario. Local models are grouped by disease types and aggregated on edge cloudlets. Data anomaly detection is performed at the edge of the network, which reduces communication latency, and the use federated learning insures the privacy of patient data. The anomaly detection is performed using a new technique, the Federated Time Distributed LSTM model. The performance metrics are not specified in the corresponding study summary.

Haque et al. [78] focus on hyperparameter optimization of ML models used for data anomaly detection for zero-day cyberattack detection. The authors propose BIOCAD, an optimization framework that leverages bio-inspired metaheuristic algorithms such as Grey Wolf Optimization (GWO), Whale Optimization (WO), and Firefly Optimization (FO) to fine-tune model parameters, enhancing accuracy and robustness. The optimization improves the performance of the one-class SVM and DBSCAN anomaly detection models, achieving an accuracy of 99.5% with F-scores in the range 89%-100%.

Astillo et al. [79] propose a data anomaly detection method for diabetes management control system to detect anomalies in 3-tuple time series data. The system uses of two models, one model that uses current patient physiological data to estimate future data, and an other one that uses features such as message inter arrival time and estimation errors to distinguish between malicious and non malicious event. The model is CNN-based, compressed and implemented on the edge to reduce latency. The model is built with federated learning/independent learning to conserve patient data privacy, and reports an inference latency of 0.19–0.71 ms, storage consumption of 1749 Bytes, RAM usage of ~56.54 MiB, an accuracy of 99.17%, and an F1-score of 99.16%.

Sundas et al. [80] use medical data from sensors to detect exploitation by malicious actors performing data injection attacks, DoS attacks or in the case of compromised medical devices. Four different machine learning approaches (ANN, DT, RF, KNN) are used to distinguish benign activity, from either healthy or ill patients, and malicious activity, achieving an accuracy of 91% and an F-score of 90% and addressing data injection, DoS attacks, malware infection, battery depletion attacks, and compromised IoMT devices.

Raje et al. [81] use a combination of Hidden Markov Models and Support Vector Machine for data anomaly detection. HMM captures the temporal relationships in the time series while the SVM is used to classify normal and abnormal segments of IoMT data. The approach is tested on sensor data collected from several connected medical devices and achieves a detection accuracy of 98.66% (with an F1-score of 96.70%, a True Negative Rate (TNR) of 97.10%, and an FPR of 2.9%).

Rani et al. [82] propose a SmartHealth security framework that collects data from different medical devices, and uses it to detect cyber threats, including data injection attacks, device tampering, and DoS attacks. Machine learning models (ANN, DT, RF, KNN) analyze patient vitals to identify anomalies. The performance of SmartHealth is assessed in parallel attack scenarios to assess how simultaneous threats impact detection accuracy, reaching an accuracy of 91.77% and an F-score of 90%.

Song et al. [83] propose a ML-based approach to detect anomalous data resulting from security breaches and device malfunctions in the context of real-time health monitoring systems. The medical data is first divided into clusters, using the K-Means algorithm. The KNN algorithm is then used to detect anomalous data points based on neighbor distances and class labels. The method reports an authentication cost of 0.8 ms, an encryption time of 0.12 ms, and a decryption time of 0.1 ms, and achieves an accuracy of 85.51% with an F1-score of 85.41%.

Goumidi et al. [84] propose an approach for real-time anomaly detection that takes into account both network flow characteristics and sensor medical data to detect data injection and device tampering attacks. It is based on a stacking ensemble model using an XGBoost metalearner and RF and ANN as underlying base classifiers. The authors create a new dataset to evaluate their approach,

based on UNSW-NB15 and augmented with medical data. The proposed model achieves a testing time (latency) of 39 ms, an accuracy of 98.02%, an F1-score of 97.84%, and an AUC of 0.99.

Multiple machine learning, deep learning, and statistical time series analysis approaches have been proposed for data anomaly detection, with a majority of less CPU-intensive approaches being proposed. In these approaches, the detection is performed either at the edge of the network to reduce the latency or centralized in the cloud to decrease the computation load on edge nodes. These approaches try to detect data alteration attacks and device tampering only by using the correlation between several biometric features or traffic features, such as message interarrival time. Some approaches use federated learning to train the anomaly detection models without disclosing patient medical data. Regarding the evaluation, all the reviewed approaches focus on detection performance metrics (ACC & F1-score), while often overlooking IoMT-specific constraints, particularly for solutions intended to operate at the edge.

4.2. Solutions for network layer security

The network layer of IoMT systems serves as the communication backbone, linking perception-layer sensors to application-layer services such as cloud analytics, remote diagnostics, and clinical dashboards. This layer enables the continuous transmission of sensitive patient data across heterogeneous wireless and wired infrastructures, and therefore must ensure both reliable delivery and strong data confidentiality.

However, the network layer is highly susceptible to a range of cyber threats that exploit its openness, high traffic volumes, and protocol diversity. As summarized in Table 3, common attacks include man-in-the-middle interception, denial-of-service (DoS), routing manipulation, eavesdropping, and replay attacks. These intrusions can compromise patient privacy, disrupt real-time monitoring, or even allow adversaries to inject harmful commands into clinical workflows.

Given the mission-critical nature of IoMT traffic, defending this layer requires intrusion detection mechanisms that are both accurate and lightweight. Traditional IDS solutions, while effective in enterprise settings, often lack the scalability and responsiveness required in resource-constrained medical networks. Recent research has thus turned to AI-driven intrusion detection systems (IDS) that leverage machine learning to detect and classify anomalous traffic patterns with minimal human supervision.

These AI-based IDS approaches are typically deployed at edge gateways or intermediary servers, where they can monitor traffic in real time without burdening individual devices. By learning from traffic behavior over time, such systems can adapt to evolving threats, identify zero-day exploits, and flag abnormal routing or authentication anomalies. In addition, machine learning has also been integrated into authentication protocols at this layer, using signal-based or biometric device fingerprints to verify legitimate devices.

In this section, we examine the current state of AI-based defenses at the IoMT network layer, including lightweight IDS architectures, federated detection models, and signal-based authentication techniques. These strategies aim to provide secure, low-latency data transmission while preserving patient privacy and system resilience in the face of growing cyber threats.

4.2.1. Network intrusion detection

The protection of IoMT networks, where sensitive patient data is continuously transmitted to remote cloud platforms for analysis and visualization, critically depends on robust intrusion detection systems (IDS). In recent years, AI–based IDS have gained prominence for their ability to identify novel and zero-day threats. However, the design of an effective AI-driven IDS for IoMT remains an open research challenge, as it must satisfy stringent non-functional [85,86], namely scalability, fault tolerance, conservativeness (low false positive rate), ease of deployment, lightweightness, and extensibility, while operating under the severe resource and latency constraints of medical environments.

Key technical challenges include [87,88]:

1. **High Dimensionality of Input Features.** IoMT IDS may ingest hundreds of features derived from network flows, device logs, and physiological sensor signals. Without careful feature selection or dimensionality-reduction, ML models suffer from the “curse of dimensionality,” leading to overfitting, degraded detection accuracy, and excessive inference latency incompatible with real-time monitoring.
2. **Heterogeneous and Encrypted Data Sources.** Proposed IDS architectures variably exploit host-based logs, network-layer telemetry, and even end-to-end encrypted patient data. In many deployments, device logs may be unavailable or patient streams are encrypted for privacy, complicating consistent feature extraction across diverse IoMT devices.
3. **High-Volume, Low-Latency Data Streams.** Continuous monitoring of vital signs and device traffic generates large data volumes. IDS must process and classify these streams in near real time, demanding optimized ML pipelines and edge-oriented inference to avoid introducing harmful network or processing delays.
4. **Limited and Imbalanced Training Data.** Privacy considerations restrict access to real patient datasets, forcing many studies to rely on synthetic or small-scale collections. These datasets are often heavily class-imbalanced, exacerbating false-negative rates and impeding generalization to unseen attack patterns.
5. **Susceptibility to Adversarial Manipulation.** ML models are vulnerable to adversarial examples–carefully crafted inputs that evade detection–and to poisoning attacks that corrupt training data. Such threats have received insufficient attention in existing IoMT-IDS research.
6. **Scalability of Deep-Learning Approaches.** Deep architectures (e.g., CNNs, LSTMs) can achieve high accuracy in controlled experiments but impose significant computational and memory overhead. In resource-constrained IoMT gateways or edge nodes, these models may violate real-time constraints critical for patient safety

Table 6
Summary of AI-based data anomaly detection approaches for IoMT with mitigated attack types.

Reference	Year	Objective	Method	Performance	Kind of Attack Mitigated
Newaz et al. [75]	2019	Detect malicious activities across multiple medical devices by exploiting correlations in physiological signals.	ANN, DT, RF, KNN trained on eight-device dataset covering benign and three attack scenarios	ACC 91%; F-score 89%	Device Tampering, DoS attacks, and false data injection
Ben et al. [76]	2020	Distinguish medical anomalies from technical faults and malicious attacks using physiological correlations.	PCA for dimensionality reduction + statistical correlogram anomaly detection at gateway.	ACC 99.21%, True Positive Rate (TPR) 99.75%, F1-Score %99.35	Data Injection
Gupta et al. [77]	2021	Edge-based anomaly detection with privacy-preserving federated learning in remote patient monitoring.	Hierarchical federated time-distributed LSTM (FEDTIMEDIS) on edge cloudlets.	Not specified	Data Injection
Haque et al. [78]	2021	Prevent adversarial manipulation of sensor measurements in IoMT systems.	Unsupervised anomaly detection using OCSVM and DBSCAN with bio-inspired optimizers (GWO, WO, FO).	ACC 99.5%, F-Score 89% - 100%	Data Injection
Astillo et al. [79]	2022	Anomaly detection for diabetes management using 3-tuple time-series data on edge.	Compressed CNN with federated/independent learning; future-data estimation + interarrival-time features.	Inference latency 0.19-0.71ms; Storage Consumption 1749 Bytes; RAM Usage 56.54 MiB; ACC 99.17%, F1-Score 99.16%	Data Injection
Sundas et al. [80]	2022	Detect exploitation by malicious actors via data injection, DoS, or compromised devices.	ANN, DT, RF, KNN to classify benign/ill vs malicious activity on eight-device network.	ACC 91%; F-Score 90%	Data Injection; DoS attacks; Malware infection; Battery Depletion Attacks; Compromised IoMT device
Raje et al. [81]	2023	Real-time anomaly detection in IoMT time-series data using hybrid models.	Hidden Markov Models + SVM for temporal feature extraction and classification.	ACC 98.66%, F1-Score 96.70%, TNR 97.10%, FPR 2.9%	Data Injection; Unauthorized access; Device Tampering
Rani et al. [82]	2024	SmartHealth framework to detect cyber threats including data injection, tampering, and DoS.	ANN, DT, RF, KNN on parallel attack scenarios.	ACC 91.77%; F-Score 90%	Data Injection; Device Tampering
Song et al. [83]	2025	Data anomaly detection in real-time	K-means for data clustering, followed by KNN-based anomaly detection	Authentication Cost 0.8 ms, Encryption Time 0.12 ms, Decryption Time 0.1 ms; ACC 85.51%, F1-Score 85.41%	Data Injection; Device Tampering
Goumidi et al. [84]	2025	Real-time anomaly detection on the edge using both network and medical data	Stacking ensemble model with XGBoost as meta-learner, and Random Forest + ANN as base classifiers.	Testing Time (Latency) 39 ms; ACC 98.02%, F1-Score 97.84%, AUC 0.99	Data Injection; Device Tampering

There are different approaches for network intrusion detection, which can be classified based on their degree of centralization:

- **Centralized Intrusion Detection:** This approach performs intrusion detection at a single point in the network, typically at the gateway node where all traffic passes through. Since medical sensors are often too resource-constrained to perform intrusion detection themselves, this approach offloads the task to a more capable node. However, a centralized system creates a single point of failure; if compromised, the security of the entire network is at risk. Additionally, it can introduce latency, as all packets need to be analyzed by the gateway node, which may not be suitable for time-sensitive medical applications.
- **Distributed Intrusion Detection:** In this approach, intrusion detection is carried out in a distributed manner, often involving cooperation between the gateway node and individual sensors. This setup reduces the burden on the gateway node and minimizes network latency. Furthermore, distributed detection improves the accuracy of attack detection, as it is based on not only network traffic data but also information available to the individual nodes, such as energy consumption and resource utilization.

Thamilarasu et al. [85] develop a mobile agent based intrusion detection system where mobile agents migrate between the network nodes and perform intrusion detection in a distributed manner. Mobile agents are divided into sensor agents, which traverse the nodes on a set itinerary and use ML algorithms to detect intrusions based on the logs stored by each node over time, clusterhead agents that perform intrusion detection on cluster heads and detective agents created by cluster heads and which traverse the entire cluster in the case of suspicious activity detected by one of the sensor agents. The classfication used is a multi-class classification, with 3 classes: normal, malicious and suspicious to reduce false positives. This makes the architecture fault tolerant and scalable, and it reports an energy overhead of 5.2% - 7.03% and an accuracy range of 95.21%–99.8%.

Hady et al. [89] developed a system that utilizes a combination of network and patient data to classify network packets as either benign or malicious. Network data features include source-destination bytes, load, missing bytes, and inter-packet intervals, while patient data features include temperature, oxygen saturation, and pulse rate. To achieve this, the authors created a testbed that generates a dataset comprising both network and patient data metrics. This testbed is used to detect any spoofing or tampering in transmitted data during a Man-in-the-Middle (MITM) attack. A total of 16,000 samples were collected and labeled and oversampling techniques were used to balance the dataset between normal and attack traffic. The effectiveness of the approach was evaluated by comparing it to models that use only network data, using metrics such as accuracy and the area under the ROC curve (AUC), achieving a detection latency of 300 ms and an AUC of 0.92.

Despite these efforts, there are some drawbacks to this method. The system's performance is not optimal and could be improved by selecting optimal hyperparameters, reducing the feature space, and implementing more sophisticated attacks. Additionally, the data is transmitted in plain text due to the low processing power of the sensors, which poses a security risk.

Manimurugan et al. [90] use a deep belief neural network as an AI model for the classification of benign and malicious traffic. The study leverages the CICIDS 2017 dataset (network data) to assess performance, achieving 99.37% accuracy for normal traffic and 96.37% for various attack types. The approach is compared to other AI models using metrics such as accuracy/precision/recall/f1-score/detection-Rate.

Zachos et al. [91] present a ML based intrusion detection system to be implemented on the gateway of the IoMT edge network for the detection of network-based and host-based attacks. It uses network traffic data, as well as data from IoMT devices log files (including the gateway's log files) to detect anomalies. For this purpose, a set of monitoring and data acquisition (MDA) components are deployed on IoMT edge devices in order to collect host data and send it to a central detection (CD) component on the IoMT gateway. This approach is tested on the TON IoT telemetry dataset for the network traffic, as well as the "powertrace" dataset, and achieves an accuracy between 97% and 99.98% with an F1-score between 96.58% and 99.96%.

Essop et al. [92] propose a GAN-based method to generate synthetic data for intrusion detection in IoMT networks. The approach reports a testing latency (stacking ensemble) of 39 ms, an encryption time (AEAD) of 0.12 ms, and a decryption time (AEAD) of 0.1 ms, and achieves an accuracy in the range 95.25% - 99.86% for DoS, DDoS, and scan scenarios.

Lee et al. [93] propose a multi-class classification based intrusion detection model that utilizes network data generated by 6 real medical devices in the South Korean National Cancer Center to train a convolutional neural network. Ten relevant features are extracted from the dataset which removes the need for feature selection. Four classes were defined: normal, critical, major and minor depending on the severity of attack. Performance is compared with other ML algorithms including, NB, SVM, LR with different number of training instances. M-IDM exhibits the best performance, achieving an accuracy of 98.6% - 99.3%, an F-score of 93.7%, and an AUC of 0.96.

Awotunde et al. [94] propose an intrusion detection architecture for IoMT networks that combines a Multilayer Perceptron (MLP) classifier with a Deep Autoencoder (DAE) used for feature selection. The model is evaluated using the ToN-IoT dataset, which includes diverse IoT-related attack scenarios. The proposed system achieves a detection accuracy of 89%, performing better than the baseline approaches it was compared against.

Siniosoglou et al. [95] propose a FL-based intrusion detection system for IoMT networks using two lightweight Generative Adversarial Networks (GANs), one for detecting anomalies in patient biometric data and another for identifying threats in network traffic. The system is evaluated on two public datasets, i.e. CHARIS for clinical data and UNSW-NB15 for network traffic, achieving 92.98% and 78.37% detection accuracy respectively, with F1-scores ranging from 78.83% to 92.80% and AUC values ranging from 0.78 to 0.92. In both cases, the FL approach outperforms equivalent non-FL implementations, demonstrating its effectiveness in distributed, privacy-sensitive healthcare environments.

Idrissi et al. [96] present a novel approach to securing IoMT devices through the implementation of an IDS utilizing advanced machine learning techniques. The proposed IDS leverages gradient boosting machine algorithms, specifically XGBoost, LightGBM, and CatBoost, to detect anomalies and potential threats in IoMT networks. The research utilizes the WUSTL EHMS 2020 dataset, which is

specifically designed for the cybersecurity of IoMT systems. The evaluation results demonstrate that the proposed LightGBM-based IDS achieves 99.98% accuracy with an F1-score of 99.97%, with a testing inference latency of 233 ms (and reports a memory consumption figure of 929.72 MB in the study summary).

Li et al. [97] propose the butterfly optimization algorithm (BOA) as a new approach for feature selection for ML-based network intrusion detection systems. The method is tested and compared to other approaches for feature selection (decision tree, SVM and ant colony optimization). The comparison is performed using the NSL KDD dataset and two cost functions: the Rastrigin function and the sphere function. The BOA algorithm achieves the lowest value for both cost functions and outperforms other meta-heuristic algorithms. The classification is then performed using an ANN on the feature selected by BOA. The performed tests report an accuracy of 93.27% and an RMSE in the range 0.05 - 0.12.

Gupta et al. [98] propose a network intrusion detection system based on the random forest algorithm combined with Grid Search Cross-Validation as a hyperparameter optimization technique. This approach is tested using the wustl-ehms-2020 dataset [89], which contains a mix of network-related features and patient biometric features used for anomaly detection. The unbalanced dataset is preprocessed then augmented using the SMOTE algorithm, with the use of a feature selection algorithm. The approach is implemented and compared to other ML algorithms (LR, DT, RF, ETC with and without data augmentation) combined with Grid Search Cross-Validation, using the accuracy, recall, false positive rate, precision, f1-score, AUC, and prediction time. This approach shows superior performance in terms of accuracy and achieves low classification times, reporting a detection latency of 3.5 μs, an accuracy of 94.23%, an F-score of 93.8%, and an AUC of 0.9.

Ramana et al. [99] propose an approach based on a Gate Recurrent Unit (GRU) neural network combined with the whale optimisation algorithm to optimize the model's hyperparameters. It uses network characteristics for classification and reports a detection latency of 3.5 μs, an accuracy of 94.23%, and an F1-score of 93.8%.

Chaganti et al. [100] use Particle Swarm Optimization (PSO) and deep neural network architecture. A combination of network and patient biometric data are used for the classification. The proposed system is implemented on the gateway level and achieves 96% accuracy with an F1-score of 95%.

Saif et al. [101] propose a hybrid IDS using metaheuristic algorithms and machine learning classifiers. The best configuration, that combines genetic algorithms for feature selection from the NSL-KDD dataset and decision trees for classification attained an accuracy range of 88.83% - 99.88%, with testing time (latency) between 10.48 s and 130.22 s, CPU utilisation between 21% and 58%, and memory usage between 39% and 72%.

Akshay et al. [102] propose ImmuneNet, a lightweight ANN-based intrusion detection architecture for IoMT networks. It uses linear projections, MISH activation [103], and layer normalization, and incorporates SMOTE-based oversampling, correlation-based feature selection, and hyperparameter optimization to improve detection performance. The model, with under one million parameters, is evaluated on CIC IDS 2017/2018, and CIC Bell DNS 2021 datasets, reporting a model weight size of 3.253 MB - 3.265 MB and an accuracy in the range 99.2%–99.8%.

Binbusayyis et al. [104] investigates the performance of five ML algorithms (NB, KNN, DT, MLP and SVM) for intrusion detection in IoMT networks. The study evaluates the models on the Bot-IoT dataset, both before and after balancing the dataset, and compares the results of the five algorithms using the accuracy, detection rate, false alarm rate metrics and the ROC AUC metrics. Among the models tested, the Decision Tree outperforms the other models, achieving 100% accuracy, 100% detection rate, and 0% false alarm rate on the balanced dataset, with an AUC of 1.0.

Khan et al. [105] propose XSRU-IoMT, an intrusion detection architecture for IoMT networks that incorporates explainable AI to address the *black box* nature of deep learning models, with the goal of providing an interpretation of the model's output for security experts. The model utilizes bidirectional Simple Recurrent Units (SRUs) with skip connections to mitigate the vanishing gradient problem and accelerate training. The authors use Local Interpretable Model-Agnostic Explanations (LIME) to explain prediction outcomes. Evaluated on the TON IoT dataset, the model achieves a detection accuracy of 99.38% with an F1-score of 99.37%, and provides the explanation of the model's predictions.

Alalhareth et al. [106] propose LRGU-MIFS, a feature selection technique based on the LRGU redundancy coefficient. This approach evaluates the features individually using mutual information scores, and selects the most relevant features sequentially. This method adjusts the redundancy coefficient in a nonlinear way as opposed to previous methods. This approach is tested with several machine learning classifiers on the WUST-EHMS-2020 dataset that contains network and biometrics data, reporting a model weight size of 3.26 MB and an accuracy of approximately 93.4%.

Taouali et al. [107] propose a cyberattack detection approach for IoMT networks based on a Kernel Extreme Learning Machine (KELM). To address the high dimensionality of intrusion detection datasets, the method employs Kernel Principal Component Analysis (KPCA) and Kernel Partial Least Squares (KPLS) for feature extraction. The approach is evaluated on the WUSTL-EHMS-2020 dataset, which includes both network and biometric data, achieving a detection latency of 0.0408 s–0.0468 s, an accuracy of 99.9%, an F1-score of 99.9%, and an AUC of 0.99.

Faruqui et al. [108] propose an IDS architecture designed to address the research gap in IDS utilizing image data. The approach integrates an LSTM to analyze sequential network traffic and a CNN for detecting malicious image-based content. The packets are classified based on a predefined threshold value. The method is evaluated on the CIC-IDS2017 dataset, achieving a detection accuracy of 97.63% and an F1-score of 97.73%.

Norouzi et al. [109] propose an IDS for IoMT architectures using a hybrid Genetic Algorithm based Random Forest (GA-RF) model. The approach optimizes the traditional random forest by selecting an optimal subset of trees through genetic operations such as crossover, mutation, and elitist selection. This method enhances classification accuracy and efficiency compared to other benchmark

machine learning algorithms. Evaluated on the NSL-KDD and UNSW_2018_IoT_Botnet datasets, the proposed GA-RF model achieves a detection accuracy of 99.99% with an F1-score of approximately 100%.

Alalhareth et al. [110] propose a novel approach utilizing an LSTM with a self-tuning mechanism to adjust the number of epochs during training, combined with early stopping through fuzzy logic techniques. This method aims to mitigate overfitting and underfitting. The approach is evaluated on the WUSTL-EHMS-2020 dataset, achieving an accuracy of 96.7% with an F1-score of 96.6%, outperforming other benchmark methods.

Alalhareth et al. [111] propose a meta-learning-based intrusion detection approach for IoMT networks, focusing on dynamic and performance-driven ensemble optimization. The method introduces a weighted meta-learning technique that assigns voting weights to classifiers based on their accuracy, loss, and confidence levels. A meta-learner optimizes both the selection and weighting of classifiers within the ensemble, subject to a computational budget constraint reflecting the real-time and resource-limited nature of IoMT environments. The selection function uses meta-feature thresholds, while the weighting function prioritizes classifiers according to the meta-feature values of the models. The approach is evaluated using seven classifiers, using the bagging technique, on the WUSTL-EHMS-2020 dataset and reports 97% accuracy, CPU usage of 41 - 57%, memory usage of 45 - 49%, and inference time of 0.02–0.05 s.

Shambharkar at al. [112] investigate three deep learning models, i.e. Linear SVM, Convolutional SVM, and Categorical Embedding, for intrusion detection in IoMT systems. The objective is to detect man-in-the-middle attacks, including spoofing and IoT data injection. The models are evaluated using the WUSTL-EHMS-2020 dataset, which includes network traffic and biometric data, reporting a detection latency of 0.0396 s–0.3116 s, an accuracy of 99.96% - 100%, and an F1-score of 99.92%–100%.

Ioannou et al. [113] propose a power-efficient IDS designed to secure the transfer of sensitive medical data to remote cloud servers. The system focuses on three primary goals: classifying attacks, detecting anomalies (new attacks), and utilizing federated learning to ensure the classification model on the cloud server is continually updated whenever a new type of attack is identified. These goals are addressed by different AI models: an RF model is employed to detect and classify various attacks, a One-class Support Vector Machine (SVM) is used for anomaly detection (identifying new attacks), and a Federated Learning (FL) model updates the Enhanced RF parameters in real time with each new anomaly, reporting power consumption of 11.1–15.5 mW, detection latency of 1.06–1.37 s, CPU utilisation of 1%, RAM usage of 5% (1 GB), and an accuracy range of 99.7% - 99.98%.

Li et al. [114] aim to compare between 2 dimensionality reduction techniques: feature selection and feature extraction. A comprehensive performance evaluation is performed between the two, using metrics such as accuracy, precision, recall, F1-score, MCC, model training time, and inference time. The dataset used for this study is TON-IoT, and the study summary reports a detection latency range of 21.81 ms–227237.45 ms and an accuracy range of 77.62% - 89.10%.

Sun et al. [115] implement a machine learning-based intrusion detection system integrated to health app platforms and tailored for the IoMT environment. This approach uses Particle Swarm Optimization (PSO) for feature selection and Adaboost for network flows classification. Several classification algorithms (AdaBoost, KNN and naive Bayes) have been tested on the NSL KDD dataset of network traffic data for intrusion detection. Adaboost was found to achieve the highest performance in terms of accuracy, precision, and recal, reaching an accuracy of 98.5%. The proposed IDS uses PSO as a way to reduce the model's complexity and address the characteristics of IoMT, such as resource constraints, availability requirements and real-time transmissions.

Zukaib et al. [116] propose a meta-learning-based intrusion detection system for IoMT, combining five base learners with an XGBoost meta-learner optimized using the Bat Algorithm and a Parzen tree estimator. The system performs signature-based detection using the meta-learning model and handles zero-day attacks using mean-shift clustering and biased classifiers. It is designed for low-latency, resource-constrained environments and is trained on both network traffic and patient biometric data. On the WUSTL-EHMS 2020 dataset, the study summary reports an accuracy in the range 99.89%–99.92%.

Alalwany et al. [117] propose a ML-based IDS for IoMT networks using a stacking ensemble model integrated into a Kappa architecture for real-time data processing. The system combines several machine learning and deep learning models including DNN, CNN and LSTM to improve detection accuracy and decrease the number of false positives. The ECU-IoHT dataset, containing real network traffic with medical sensor data in the presence of attacks, is used for evaluation. The proposed approach achieves an accuracy of 99.13% - 99.30% in multi-class classification scenarios.

Nasayreh et al. [118] propose an intrusion detection framework for IoMT environments that combines a novel deep learning learning model as well as dimensionality reduction to improve cyberattack detection accuracy. The data is normalized using Power transform to make it more Gaussian. The method uses PCA for dimensionality reduction, an LSTM model for feature extraction and KNN for classification. It was evaluated on four IoMT datasets (ECU-IoHT, ICU, WUSTL-EHMS, and TON-IoT), achieving between 98.2% and 99.9% accuracy on WUSTL-EHMS and competitive results on the others, and reports a testing inference latency of 0.1376 s (Table 7).

Most of the reviewed approaches are deployed either in centralized servers or at the edge of the network. Their evaluation predominantly focuses on detection performance metrics, such as accuracy, precision, and recall, while often overlooking IoMT-specific constraints, particularly for solutions intended to operate at the edge, where computational resources and energy availability are limited.

Current research largely emphasizes the development of novel machine learning and deep learning models, feature selection strategies, and hyperparameter optimization techniques. Some studies additionally explore the architectural design of intrusion detection frameworks to improve scalability and detection effectiveness.

Intrusion detection is performed using network traffic; recent approaches propose leveraging additional data sources to enhance detection performance, including patient medical data and device-level logs. There is also a growing interest in explainable intrusion

Table 7
AI-based IoMT intrusion detection approaches (Network Layer) with mitigated attack types.

Reference	Year	Objective	Method	Performance	Kind of Attack Mitigated
Thamilarasu et al. [85]	2020	Distributed mobile-agent IDS for IoMT networks	Sensor, clusterhead, detective agents using multi-class ML classification	Energy Overhead 5.2% – 7.03%; ACC 95.21% – 99.8%	Network Intrusion
Hady et al. [89]	2020	MITM detection via combined network and patient data	ML on network + patient features (e.g., inter-packet time, vitals)	Detection Latency 300 ms; AUC 0.92	Man-in-the-Middle
Manimurugan et al. [90]	2020	DBN-based classification of benign vs. malicious IoT traffic	Deep belief network on CICIDS2017 dataset	ACC 99.37%-96.37%	Network Intrusion
Zachos et al. [91]	2021	Gateway-edge IDS using network + host logs	SVM, DT, RF, KNN, NB, LR on MDA components	ACC 97%-99.98%, F1-Score 96.58% – 99.96%	Network Intrusion
Essop et al. [92]	2021	Generating synthetic data for intrusion detection in IoMT networks	GAN for synthetic data generation	Testing latency (Staking Ensemble) 39 ms Encryption Time (AEAD) 0.12 ms, Decription Time (AEAD) 0.1 ms; ACC 95.25% – 99.86%	DoS, DDoS, Scan
Lee et al. [93]	2021	Multi-class IDS on real medical device traffic	CNN on six-device dataset; four severity classes	ACC 98.6%-99.3%: F-score 93.7%; AUC 0.96	Network Intrusion
Awotunde et al. [94]	2021	Deep learning for intrusion detection in healthcare IoT	DAE for feature selection and a MLP model for classification	ACC 89%	DoS, DDos, Injection, MitM, Password, Ransomware, Scanning, and XSS attacks
Siniosoglou et al. [95]	2021	Federated learning for distributed IoMT intrusion detection	Two GAN to detect anomalies in network and biometric data	ACC 78.37%-92.98%, F1-Score 78.83%-92.80%, AUC 0.78-0.92	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms attacks
Idrissi et al. [96]	2022	XGBoost, LightGBM, CatBoost IDS on WUSTL EHMS 2020	GBM algorithms on network + biometric features	Testing Inference Latency 233 ms; Memory Consumption (Naive-Bayesian Model) 929.72 MB; ACC 99.98% F1-Score 99.97%	Network Intrusion
Li et al. [97]	2022	BOA-based feature selection for IoMT network IDS	Butterfly optimization + ANN classification on NSL-KDD	ACC 93.27%, RMSE 0.05-0.12	Network Intrusion
Gupta et al. [98]	2022	Random Forest + GridSearchCV IDS on WUSTL EHMS-2020	RF w/ SMOTE + feature selection; hyperparam tuning	Detection latency 3.5 μs; ACC 94.23% F-Score 93.8%, AUC 0.9	Network Intrusion
Ramana et al. [99]	2022	GRU + whale optimization hyperparam tuning for IDS	GRU network optimized by WO on WSN-DS dataset	Detection latency 3.5 μs; ACC 94.23%, F1-Score 93.8%	Network Intrusion
Chaganti et al. [100]	2022	PSO + DNN IDS using network + biometric data	PSO for DNN hyperparams on gateway-level	ACC 96%, F1-Score 95%	Network Intrusion
Saif et al. [101]	2022	Hybrid metaheuristic + ML IDS for real-time healthcare	GA for FS + DT classification on NSL-KDD	Testing Time (Latency) 10.48–130.22 s; CPU Utilisation 21%-58%, Memory Usage 39%-72% ACC 99.88%-88.83%	Network Intrusion
Akshay et al. [102]	2022	Lightweight intrusion detection architecture for IoMT networks	ANN architecture with linear projections, MISH activation, and layer normalization	Model Weight Size 3.253 – 3.265 MB; ACC 99.2%-99.8%	Network Intrusion
Binbusayyis et al. [104]	2022	Investigation of the performance of ML algorithms for intrusion detection	Training 5 ML algorithms on the Bot-IoT dataset and comparing performance metrics	ACC 100%, AUC 1.0	DoS, DDoS, Scan and Theft network attacks

Table 7
Continued.

Reference	Year	Objective	Method	Performance	Kind of Attack Mitigated
Khan et al. [105]	2022	Provide interpretable intrusion detection in IoMT using explainable AI.	XSRU model with bidirectional SRUs, skip connections, and LIME for output explanation	ACC 99.38%, F1-score 99.37%	Password, Scanning, Ransomware, Backdoor, DoS, DDoS, MITM, Injection, and XSS attacks
Alalhareth et al. [106]	2023	LRGU-MIFS feature selection for IoMT IDS	Sequential MI-based FS; tested on WUST-EHMS-2020	Model Weight Size 3.26 MB; ACC 93.4%	Network Intrusion
Taouali et al. [107]	2023	Lightweight intelligent IDS for IoMT networks	KELM with KPCA and KPLS for feature extraction	Detection Latency 0.0408 s - 0.0468 s; ACC 99.9%, F1-Score 99.9, AUC 0.99	Network Intrusion
Faruqui et al. [108]	2023	Address the gap in IDSs using image data	LSTM and CNN based classifying via thresholding	ACC 97.63%, F1-score 97.73%	Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS
Norouzi et al. [109]	2023	Optimized IoMT IDS based on RF	Hybrid Genetic Algorithm–Random Forest (GA-RF) for optimized intrusion classification	ACC 99.99%, F1-score 100%	DoS, DDoS, Reconnaissance, Theft attacks
Alalhareth et al. [110]	2023	Hybrid metaheuristic + ML IDS for real-time healthcare	GA for FS + DT classification on NSL-KDD	ACC 96.7%, F1-Score 96.6%	Network Intrusion
Alalhareth et al. [111]	2024	Efficient meta-learning based intrusion detection in IoMT under resource constraints	Performance-driven meta-learning approach with classifier selection and weighting	ACC 97%; CPU usage 41–57%; Memory usage:45–49%; Inference time:0.02–0.05s	Network Intrusion
Shambharkar et al. [112]	2024	Detect man-in-the-middle attacks in IoMT systems using deep learning	Comparison of LinSVM, ConvSVM, and Categorical Embedding models	Detection Latency 0.0396 s - 0.3116 s; ACC 99.96%-100%, F1-Score 99.92%-100%	Man in the middle attacks
Ioannou et al. [113]	2024	Power-efficient IDS for IoMT data transfer, classification	Enhanced RF for known attacks; one-class SVM for anomalies; federated updates	Power Consumption 15.5 mW - 11.1 mW; Detection Latency 1.06 s - 1.37 s; CPU Utilisation 1%; Memory Usage (RAM) 5% (1 GB); ACC 99.98%-99.7%	Network Intrusion, Unauthorized Access
Li et al. [114]	2024	Compare feature selection vs. extraction for IoMT IDS	FS vs. FE on TON-IoT dataset; evaluate DT, MLP, RF	Detection latency 227237.45 ms - 21.81 ms; ACC 89.10%-77.62%	Network Intrusion
Sun et al. [115]	2024	PSO-AdaBoost IDS integrated in IoMT apps	PSO for feature selection; AdaBoost, KNN, NB	ACC 98.5%	Network Intrusion
Zukaib et al. [116]	2024	Meta-learning based IDS optimization for known and zero day attacks	XGBoost-based meta-learner for signature-based detection and mean shift clustering with biased classifiers for anomaly-based detection	ACC 99.89%-99.92%	Known and zero day network-based attacks
Alalwany et al. [117]	2025	Real-time intrusion detection system for IoMT networks with improved performance	A deep learning–based stacking ensemble integrated into a Kappa Architecture, using DNN, CNN and LSTM models	ACC 99.13% - 99.30%	ARP spoofing, DoS attacks, NMAP port scan, Smurf attacks
Nasayreh et al. [118]	2025	Efficient intrusion detection framework for IoMT systems	A hybrid approach combining LSTM for feature extraction and KNN for classification	Testing Inference Latency 0.1376 s; ACC 98.2%-99.9%	Network intrusions

detection techniques that aim to improve the transparency and trustworthiness of ML/DL-based detectors, facilitating their adoption in safety-critical medical systems.

4.2.2. Authentication protocols

Machine learning has been used in protocols to authenticate IoMT devices through fingerprinting. These approaches either use biometrics-based authentication or properties of transmitted radio signals as well as other physical layer features. These can serve as a digital fingerprint for users and IoMT devices respectively.

Mawgoud et al. [119] use SVM-based machine learning for the authentication of IoMT devices. The system provides fast and secure authentication without relying on cryptographic techniques. It classifies devices based on their physical attributes and communication patterns such as received signal strength indication and carrier frequency offset. The approach is demonstrated to require less computation time than a physical layer key generation approach such as PUF, while avoiding all false positives.

Pirbhulal et al. [120] et al. propose an authentication system that leverages unique QRS complex features extracted from ECG readings captured by medical sensors. The system utilizes a multilayer perceptron to classify authorized and unauthorized users. A secure communication channel (DSSS) is used to protect the signal from interference.

Rathore et al. [121] propose a biometric authentication system that uses ECG QRS complex data that is collected and filtered by implantable medical devices. Polynomial coefficients are extracted from the ECG using Legendre polynomial extraction and are used to train an MLP model for multi-class identification. The Direct Sequence Spread Spectrum spread-spectrum modulation technique is used to protect the system against eavesdropping attacks. The approach achieves a 100% accuracy when tested using the ECG-ID dataset with different polynomial degrees.

Kute et al. [122] propose a secure an approach scalable biometrics-based authentication for the IoMT. It makes use of the concept of cancellable biometrics, which can be regenerated if compromised, to enhance privacy and security. The system is cloud-based, making it suitable for constrained devices.

Almaiah et al. [123] propose a lightweight, decentralized authentication scheme based on a combination of deep learning and blockchain technologies. The system reduces latency by distributing the authentication process across multiple fog nodes, avoiding reliance on a central authority. A deep learning model, trained on encrypted data, is used to distinguish between honest and malicious participants in the blockchain network. This allows the system to identify trustworthy nodes for secure transaction validation. The overall architecture supports privacy-preserving authentication and integrity of data exchanges in IoMT environments.

Sadhu et al. [124] propose a group authentication protocol that leverages two ML models to authenticate to identify and authenticate a group of devices, one for generating partial authentication challenges and the other to identify the medical device, based on its response. This reduces storage and computational complexity compared to maintaining separate models for each device. The ML model is trained on unique challenge-response pairs generated from PUFs. During the authentication phase, the Edge Router (ER) generates partial challenges for devices using the MCmodel, combines them with random nonces, and sends them to the devices. Devices use their PUFs to generate responses, combine them with health data, and return the results to the ER. The ER processes the responses, hashes and masks the data, and sends it to the Cloud Server (CS), where the MLmodel verifies device identities and validates the data.

They also [125] present a PUF-based authentication protocol, where a ML model generates the challenge sent to PUF-equipped medical devices. The response to the challenge is then verified by a CRP mapping model that will authenticate the device. This approach reduces the space required by CRP storage in the database and it is designed to be resistant to impersonation, replay, man-in-the-middle, and modeling attacks. The framework is adapted to IoMT devices because it is lightweight, requiring 1.5ms of computation time and 68 bytes of communication overhead.

Adil et al. [126] introduces an AI-driven lightweight authentication scheme for intelligent IoMT-based cyber-physical systems, where a machine learning model dynamically predicts and selects the nearest and most reliable trusted authority for authentication. This approach reduces communication overhead, minimizes latency, and enhances the scalability and responsiveness of the system, particularly in delay-sensitive medical environments.

Alruwaili et al. [127] present ALBA, a lightweight location-based authentication system for IoMT gateways. The approach uses GPS data collected from smartphone gateways and the isolation forest unsupervised ML algorithm to authenticate users. The system is an additional layer of security that monitors the location of the gateway and can detect deviations from normal patterns to detect an attacker. The approach was evaluated on three datasets: a real-world GPS dataset, a public location history dataset from Kaggle, and a synthetically generated virtual dataset.

Hazratifard et al. [128] propose a biometric authentication system that provides continuous authentication based on ECG signals. The discrete Fourier transform is applied on raw ECG signals, which makes the model more robust to noise. It uses an ensemble siamese network to solve problems with previous ECG-based authentication systems such as sensitivity to imbalanced datasets and the difficulty to train the model on new users.

El-Moneim Kabel et al. [129] propose a biometrics-based authentication system based on ECG recognition with cancellable templates obtained by combining non-invertible transformation and low-weight encryption. This prevents the biometric data from being accessed by attackers while protecting against record multiplicity and brute force attacks (Table 8).

The reviewed approaches primarily aim to mitigate common IoMT authentication threats, including device spoofing, impersonation, replay attacks, man-in-the-middle attacks, and data injection, while simultaneously addressing IoMT-specific requirements such as the high sensitivity of medical data and the stringent energy constraints of medical devices. The proposed methods are designed to enable authentication with low computational and communication overhead at the device level, making them particularly suitable for resource-constrained medical devices such as wearables and implantable sensors.

Table 8
Summary of authentication techniques in IoMT using ML/AI.

Reference	Year	Objective	Method	Performance	Kind of Attack Mitigated
Mawgoud et al. [119]	2019	Fast authentication of IoMT devices without cryptography	SVM using device communication patterns (RSSI, CFO)	Latency 500 ms (90 devices); False Positives 0%	Device Spoofing; Data Injection
Pirbhulal et al. [120]	2019	Biometric authentication using ECG QRS features	MLP classifier, DSSS secure channel	Not specified	Device Spoofing; Data Injection
Rathore et al. [121]	2020	Multi-class identification using ECG signals	MLP with Legendre polynomial feature extraction	Average Computation Time 1.19 ms; Power Consumption (Active Core) 0.5 W; Memory Usage (RAM) 967 KB, Storage (Executable Size) 122 KB; ACC 99.99%	Device Spoofing; Data Injection; Eavesdropping; Replay attacks
Kute et al. [122]	2022	Scalable biometric-based authentication using cancellable biometrics	Cancellable biometric transformations in a cloud-based system	Not specified	Device Spoofing; Data Injection
Almaiah et al. [123]	2022	Secure and low-latency authentication for IoMT	Artificial Neural Network trained on encrypted data	ACC 93.3%	Device Spoofing; Data Injection
Sadhu et al. [124]	2022	Group authentication using PUF and ML	Dual ML models using CRPs from PUF; one for challenge generation, one for identification	ACC 99.54%; Latency 2.6ms	Device Spoofing; Data Injection; Side-Channel Attacks; Modeling Attacks; Physical attacks; DoS ; Replay ; Eavesdropping; MitM attacks
Sadhu et al. [125]	2022	Reduce storage overhead of PUF-based authentication	CRP mapping ML model to verify device responses	Latency 2.33ms; Memory 68 bytes	Device Spoofing; Impersonation; Replay; Man-in-the-middle; and Modeling attacks.
Adil et al. [126]	2022	Lightweight AI-driven authentication via trusted authority prediction	ML model to select nearest trusted authority dynamically	Latency 6.3ms	Device Spoofing, Eavesdropping, Replay, Inference attacks
Alruwaili et al. [127]	2023	Location-based anomaly detection for gateway authentication	GPS-based monitoring with Isolation Forest	Not specified	Device Spoofing; Data Injection
Hazratifard et al. [128]	2023	Robust and continuous ECG-based authentication	Ensemble Siamese Network on raw/DFT ECG	ACC 93.6–96.8%	Device Spoofing; Data Injection
El-Moneim et al. [129]	2024	Biometric authentication using ECG with template protection	ECG, non-invertible transformation, lightweight encryption	ACC 99.96%	Device Spoofing; Data Injection

The surveyed approaches can be broadly categorized into biometric-based authentication, signal- or location-based methods, and PUF-based approaches. Biometric-based authentication techniques leverage physiological or behavioral characteristics to authenticate not only the devices but also their users, which is difficult to achieve using traditional cryptographic mechanisms alone. These approaches show significant potential for the development of cancellable biometric features, enabling secure authentication while preventing the leakage of sensitive patient data and ensuring compliance with medical data protection regulations. However, a key limitation of biometric-based methods is their limited generalizability across heterogeneous IoMT networks, as certain biometrics (e.g., ECG-based features) are only applicable to devices equipped with specific sensors.

Signal-based authentication approaches exploit physical-layer characteristics to verify the legitimacy of IoMT nodes. While these methods are effective for stationary medical devices, they may suffer from reduced reliability and increased false positives in scenarios involving mobile, wearable, or implantable devices.

Regarding the evaluation, it predominantly focuses on detection performance metrics (ACC, AUC, F-score), while often overlooking IoMT-specific constraints, particularly for solutions intended to operate at the edge, where computational resources and energy availability are limited.

4.3. Solutions for application layer security

The application layer in IoMT systems is responsible for processing, analyzing, and storing sensitive medical data, enabling critical services such as telemedicine, remote diagnostics, and clinical decision support. Due to its central role in healthcare delivery and

its access to Electronic Health Records (EHRs), this layer is a prime target for cyberattacks. Threats such as phishing, ransomware, SQL injection, and data tampering exploit vulnerabilities in user interfaces, APIs, and backend infrastructures. As detailed in Table 4, these attacks can lead to unauthorized access, data breaches, and potentially life-threatening disruptions to care.

In this section, we examine the integration of blockchain with AI to further reinforce application-layer security. Blockchain technologies offer immutable logging, decentralized access control, and tamper-resistant data exchange–all of which are critical for maintaining auditability and user trust in healthcare systems. When combined with AI, blockchain-enhanced architectures enable adaptive access control, proactive anomaly detection, and secure message transmission across distributed IoMT environments.

4.3.1. AI powered blockchain

Blockchain technology has emerged as a foundational pillar for enhancing the security and trustworthiness of IoMT systems. Its decentralized and tamper-resistant architecture provides robust protection against common threats such as data repudiation, unauthorized access, and identity spoofing. By ensuring immutable logging of transactions, decentralized access control, and secure message exchanges, blockchain mitigates several vulnerabilities inherent in IoMT environments, particularly those related to data privacy and integrity.

In the context of healthcare, blockchain enables secure communication between IoMT devices and backend systems, while maintaining compliance with privacy regulations such as HIPAA and GDPR. Medical records, sensor telemetry, and access logs can be stored on distributed ledgers, preventing unauthorized modification and enabling traceable, auditable data flows across interconnected platforms. However, despite these advantages, existing blockchain-based IoMT architectures often address only isolated aspects of security, such as access control or traceability, without providing a holistic defense against evolving cyber threats.

To address this limitation, recent research has focused on integrating AI with blockchain to build intelligent and adaptive security frameworks. AI models, including ML and DL algorithms, can be employed for tasks such as anomaly detection, threat prediction, and dynamic access control, thus enhancing the responsiveness and resilience of IoMT networks. The synergy between blockchain and AI allows for real-time analysis of device behavior, detection of malicious activity, and the enforcement of context-aware security policies.

Several notable studies exemplify this integrated approach. Al-Otaibi et al. [130] proposed a KNN-based classifier that authenticates users based on device proximity, achieving 96% accuracy in protecting access to blockchain-stored medical records.

Further, Kumar et al. [131] integrated a zero-knowledge proof (ZKP) authentication protocol with a BiLSTM-based anomaly detection system, deployed within a permissioned blockchain to secure IoMT edge nodes against inference attacks.

Ashraf et al. [132] proposed a federated learning-enabled architecture that utilizes locally trained artificial neural networks (ANNs) individual devices to detect threats in IoT-driven healthcare environments, coordinating the aggregation of models via a blockchain ledger. Their system was evaluated using the BoT-IoT dataset and achieved 99.99% accuracy, highlighting the model's effectiveness in identifying threats in IoMT networks while maintaining strict privacy guarantees.

Alsemmeari et al. [133] combined a three-layer neural network (TNN) with a blockchain-secured fog layer to filter malicious sensor data, attaining 99.99% detection accuracy on an ICU dataset.

Dutta et al. [134] introduced *PoAh 2.0*, an novel blockchain consensus mechanism, that improves the original Proof of Authentication protocol by using AI for dynamic authentication. This approach ensures that access critical medical data requires stricter security checks. The sensitivity of each block is calculated before being added on the blockchain and three different levels of authentication are applied for access depending on the sensitivity of the data.

Khan et al. [135] propose a blockchain-based system for medical IoT that incorporates searchable encryption alongside a Hybrid DNN (HDNN) to enhance both security and performance. The AI component is central to the system, with two primary roles. First, it optimizes the encrypted search process by reducing query time and resource consumption, while maintaining high accuracy. The model can also predict future queries based on usage patterns, allowing the system to pre-process search results in advance, improving efficiency. Second, the AI is used for anomaly detection: it monitors search behavior to identify anomalies in search results, helping to protect against attacks and unauthorized access. The use of AI allows the system to provide efficient and secure access to sensitive medical data in a decentralized IoMT environment.

Anjum et al. [136] propose an approach in which a machine learning model performs automated access control for medical data on the blockchain. A RF classifier uses features that describe each request, including user role, data sensitivity, access location and the user's past access trends to distinguish between legitimate and malicious access patterns in real time. The approach is evaluated in a simulated OMNet++ environment and achieves lower latency, higher throughput and faster detection of attacks compared to baseline approaches.

Bezanjani et al. [137] propose a privacy-preserving framework for IoMT that combines blockchain, deep learning, and trust management to detect malicious behavior and protect sensitive medical data. The system consists of three main components: a reputation-based trust model to filter unreliable devices, a blockchain layer with lightweight proof-of-work, and an LSTM-based anomaly detection model optimized through singular value decomposition to identify attacks in real time. Evaluated on the NSL-KDD and UNSW-NB15 datasets, the approach achieves between 97% and 98% precision while reducing false positives compared to baseline models.

These efforts, summarized in Table 9, demonstrate the promise of combining blockchain's immutable infrastructure with AI's predictive capabilities to build scalable, secure, and intelligent IoMT ecosystems. Despite these advances, comprehensive frameworks that address the full spectrum of IoMT threats while maintaining efficiency and compliance remain an open research challenge.

Recent research highlights that the integration of AI into blockchain-based IoMT networks significantly extends the capabilities of blockchain beyond static security guarantees such as immutability and traceability. Specifically, AI is leveraged to perform anomaly

Table 9
Summary of blockchain-based and AI-driven authentication techniques in IoMT.

Reference	Year	Objective	Method	Performance	Kind of Attack Mitigated
Al-Garadi et al. [130]	2022	Authenticate users accessing blockchain medical data	KNN classifier based on device distance in a blockchain-based system	ACC 96%	Data Tampering, Spoofing, DoS
Kumar et al. [131]	2022	Secure authentication and attack detection in permissioned blockchain IoMT	ZKP for authentication, BiLSTM and variational autoencoder for anomaly detection	Accuracy, precision, F1-score (not quantified)	Data Tampering, Spoofing, DoS
Ashraf et al. [132]	2022	Secure IoT healthcare data with federated ML and blockchain	Federated ANN for anomaly detection, permissioned blockchain for model aggregation	ACC 99.99%	Data Tampering, Spoofing, DoS, Data poisoning
Alsemmeari et al. [133]	2023	Filter malicious sensor data before blockchain storage	TNN model for attack detection + blockchain for data integrity	ACC 99.99%	Data Tampering, Spoofing, DoS, MQTT DDoS, MQTT publishes flood attack, brute force attack, and SlowITE attack
Dutta et al. [134]	2024	Adaptive authentication based on transaction sensitivity in blockchain	AI-enhanced PoAh 2.0 for dynamic authentication based on data sensitivity	Not specified	Data Tampering, Spoofing, DoS, Sybil, 51%, and Replay attacks
Khan et al. [135]	2025	Improve search efficiency and security in a blockchain-based system	A hybrid deep neural network for query prediction and anomaly detection.	Improved search efficiency	Data Tampering, Spoofing, repudiation, information disclosure, and DoS
Anjum et al. [136]	2025	Automated access control to medical data using the blockchain	A RF classifier to classify legitimate and malicious requests	11.74% lower false rate and 12.36% faster access	Unauthorized access, Spoofing, Replay attacks
Bezanjani et al. [137]	2025	Detecting attacks and preserving medical data privacy	Combination of a trust-based model, blockchain, and an LSTM anomaly detector optimized using SVD	Precision 97%-98%	Unauthorized access, Spoofing, Replay attacks

detection, threat prediction, and intelligent access control by analyzing device behavior, network traffic, user access patterns, and data sensitivity in real time. Despite these advances, designing holistic AI–blockchain frameworks that balance security, privacy, regulatory compliance, and computational efficiency across heterogeneous IoMT deployments remains an open research challenge.

Although it is known that a blockchain-based solution can significantly impact computation load and latency, most of the reviewed approaches predominantly focus on detection performance metrics (ACC & F-score). Only one paper [136] has evaluated the latency.

5. Discussion and future directions

AI-based security mechanisms have been applied to secure all layers of the IoMT architecture. However, the majority of studies focus on the network layer, which appears to be the most targeted and vulnerable. Out of 66 reviewed studies, 41 address network-related threats such as authentication and intrusion detection. In contrast, 17 studies focus on the perception layer, and only 8 address the application layer. This distribution can be explained by the constraints inherent to each layer. The perception layer often operates under severe resource limitations (e.g., limited processing power or memory), which can hinder the deployment of AI-based solutions. On the other hand, the application layer typically faces fewer IoMT-specific constraints and is often secured using more general-purpose security mechanisms, reducing the need for dedicated AI-based approaches in that context.

AI-based security mechanisms are often adapted to IoMT environments by incorporating features and constraints specific to medical IoT. Several studies rely on datasets collected directly from IoMT networks, allowing models to better capture the unique traffic patterns and threat behaviors present in healthcare settings. Biometric data is also frequently used in authentication and anomaly detection solutions, reflecting the sensitive and user-specific nature of medical data. In addition, many approaches are tested on realistic and well-defined IoMT applications, improving their relevance and applicability. Privacy preservation is a key consideration as well, with techniques such as federated learning [138] being employed to ensure sensitive medical data remains local. However, some studies still rely on generic or poorly suited datasets, which limits their ability to fully address the unique challenges of IoMT systems.

The evaluation of AI-based security mechanisms in IoMT environments primarily relies on standard machine learning metrics for classification and anomaly detection, such as accuracy, precision, recall, F1-score, and area under the ROC curve (AUC). In some studies, accuracy is the sole metric reported, which is problematic given the imbalanced nature of security datasets, where high

accuracy can mask poor performance when detecting attack classes. Furthermore, most studies overlook constraints specific to IoMT, such as energy consumption, latency, and model interpretability, which are crucial when deploying AI models on edge devices with limited resources. This lack of system-level evaluation limits the practical applicability of many proposed solutions in real-world healthcare settings.

Most AI-based security mechanisms are applied and evaluated in the context of remote patient monitoring, as reflected in the datasets used and the scenarios simulated during testing. These systems typically involve continuous data collection from wearable or implanted devices and require real-time anomaly detection. However, there is a noticeable gap in research targeting other IoMT application domains, such as telemedicine, which introduces distinct challenges related to latency, bandwidth, and quality of service. Addressing these use cases would require adapting security mechanisms to operate effectively under different performance and connectivity constraints.

While the reviewed studies make significant contributions to the development of security solutions for IoMT systems, several key limitations and research gaps remain.

1. Neglect of system-level performance metrics: The majority of the selected studies prioritize classification metrics like detection accuracy as the primary evaluation criterion. However, accuracy alone fails to capture the challenges of deploying AI models in real-world IoMT environments, especially at the edge. Metrics such as energy consumption, latency, and model interpretability are rarely assessed, despite their critical importance for safe and responsive medical applications.We therefore suggest using a multidimensional evaluation framework that complements detection performance with metrics such as end-to-end latency, energy consumption per inference, memory footprint, computational complexity, network overhead and explainability, all of which directly impact the feasibility of AI-driven security solutions in IoMT networks.
2. Over-sensitive IDS behavior: Some intrusion detection models tend to generate excessive false alarms, even when the underlying machine learning model reports high accuracy. Blocking network traffic based on false positives can disrupt seamless IoMT communication and degrade service quality. Overemphasizing model accuracy while neglecting its practical usability represents a notable gap in current research.
3. Use of non-specialized datasets: A recurring limitation is the dependence on generic or outdated datasets,like the UNSW-NB15 network traffic dataset used by [95] and the NSL-KDD dataset used in [97] which were not designed for IoMT environments that do not reflect the unique characteristics of IoMT networks, such as topological diversity, device heterogeneity, or realistic physiological signal patterns. This restricts the scalability and applicability of proposed methods. Datasets with diverse realistic medical sensor behaviors such as the CICIoMT2024 network traffic dataset used by [139] and the attack detection dataset used by [89] are essential for reliable evaluation.
4. Limited threat coverage: Many existing security frameworks are designed to detect only a narrow range of attacks, such as DoS, DDoS, or MitM. These approaches often lack the flexibility to adapt to a wider or evolving threat landscape, limiting their usefulness in dynamic and heterogeneous IoMT systems. More generalizable, multi-attack detection capabilities are needed [113], especially for types of attacks that target constrained devices specifically and can have severe consequences in medical settings, such as battery depletion attacks, routing attacks or data tampering attacks.
5. AI introduces new vulnerabilities: While AI techniques improve threat detection, they also expand the system's attack surface. Vulnerabilities such as adversarial examples, model inversion, and membership inference attacks can compromise model integrity or expose sensitive information [140,141] . Robustness against such threats is rarely addressed.
6. Challenges in biometric authentication: Biometric authentication methods based on physiological signals (e.g., ECG, PPG) face issues of universality. Differences in sensor availability and variability in physiological signals across patients and use cases complicate generalization. This raises concerns about how to design reliable biometric authentication for diverse populations and sensor configurations.
7. Lack of explainability in AI-based security mechanisms: Many AI-driven solutions function as black boxes [142,143] , offering limited transparency. This lack of interpretability hinders user trust and complicates integration into critical healthcare workflows [144–146], where explainability is vital.

6. Conclusion

This paper reviews AI-driven security mechanisms for IoMT systems across all architectural layers and discusses how they are adapted to healthcare constraints (resource limitations, regulatory/privacy requirements, and medical-data sensitivity). Based on 66 studies, we observe that research is concentrated on network-layer threats (41 works), while the perception (17) and application (8) layers remain less explored. We further identify recurring limitations, particularly reliance on non-IoMT datasets and the limited consideration of deployment-critical metrics such as latency, energy overhead, and interpretability. Effectively, traditional cybersecurity techniques are ill-suited to the IoMT context due to the severe constraints of many medical devices. Wearables, implantables, and remote sensors typically lack the computational and power capacity to support standard cryptographic protocols or conventional IDS. Moreover, vulnerabilities exist at every layer of the IoMT architecture, underscoring the need for comprehensive, multi-layered defenses.

Current AI-based IoMT security mechanisms are often evaluated under unrealistic conditions: they rely on non-IoMT or synthetic datasets, report mainly accuracy-like metrics instead of deployment constraints (latency/energy/memory), and behave as black boxes with limited explainability. In addition, they frequently cover only a narrow set of attacks and rarely address AI-specific threats such as evasion, poisoning, or model inversion, making real-world adoption in clinical IoMT settings difficult. Additionally, solutions are

often evaluated in isolation without considering end-to-end integration into clinical workflows, existing hospital infrastructure, or legacy systems.

Furthermore, important gaps persist across the layered architecture. At the perception layer, physical tampering, sensor degradation, and side-channel vulnerabilities require stronger hardware-level protections. The network layer faces challenges related to protocol fragmentation, wireless interference, and the need for lightweight, low-latency security. At the application layer, the integration of AI security mechanisms with legacy systems and the inclusion of regulatory-compliant auditability, explainability, and policy enforcement must be addressed to enable clinical acceptance and certification.

Beyond technical shortcomings, socio-technical and deployment challenges remain significantly underexplored. These include interoperability with diverse healthcare information systems, usability and trust of AI-generated decisions by clinicians, and the long-term maintainability of distributed models across a heterogeneous and evolving device landscape. Human factors such as alert fatigue, training gaps, and resistance to change can undermine otherwise technically sound solutions. Regulatory compliance, lifecycle management, and real-time responsiveness under constrained network conditions are likewise essential yet often overlooked aspects of secure IoMT deployment.

To overcome these multi-dimensional challenges, future research must adopt a system-level perspective. Priority should be given to the creation of publicly available, domain-specific datasets and simulation testbeds that reflect the diversity, constraints, and adversarial settings of real IoMT deployments. AI models must be lightweight, explainable, privacy-preserving, and resilient to adversarial manipulations. Security solutions should adopt cross-layered designs that integrate sensing, networking, and application-level protections while supporting dynamic updates and regulatory audits. Moreover, interdisciplinary collaboration between computer scientists (such as data scientists, cybersecurity specialists, etc.), healthcare professionals, regulatory experts, and human factors specialists will be essential to align technological innovations with clinical workflows and governance structures.

In conclusion, while AI-driven security mechanisms offer substantial promise in addressing the evolving threat landscape of IoMT systems, their successful deployment depends on addressing a complex interplay of technical, human, and regulatory challenges. By grounding future solutions in clinical realities and system constraints, and by advancing both the scientific and practical foundations of secure, explainable, and sustainable AI, the community can move toward building robust, trustworthy, and regulation-compliant IoMT infrastructures that protect patient safety and uphold public trust.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used the tool Writefull integrated in Overleaf in order to spot mistakes and to have suggestions about technical terms. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

CRediT authorship contribution statement

Islam Hentous: Writing – review & editing, Writing – original draft, Methodology, Investigation, Data curation, Conceptualization; **Valentino Merlino:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology; **Tayeb Kenaza:** Writing – review & editing, Validation, Supervision, Project administration; **Saïd Mahmoudi:** Writing – review & editing, Validation, Supervision, Project administration; **Dario Allegra:** Writing – review & editing, Visualization, Validation, Supervision, Project administration, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] R. Lohiya, A. Thakkar, Application domains, evaluation data sets, and research challenges of IoT: a systematic review, IEEE Internet Things J. 8 (2021) 8774–8798. https://doi.org/10.1109/JIOT.2020.3048439

[2] R. Chataut, A. Phoummalayvane, R. Akl, Unleashing the power of IoT: a comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0, Sensors 23 (2023). https://doi.org/10.3390/s23167194

[3] J. Ding, M. Nemati, C. Ranaweera, J. Choi, IoT connectivity technologies and applications: a survey, IEEE Access 8 (2020) 67646–67673. https://doi.org/10.1109/ACCESS.2020.2985932

[4] A. Souri, A. Hussien, M. Hoseyninezhad, M. Norouzi, A systematic review of IoT communication strategies for an efficient smart environment, Trans. Emerg. Telecommun. Technol. 33 (2019). https://doi.org/10.1002/ett.3736

[5] S. Pattar, R. Buyya, K. Venugopal, S.S. Iyengar, L. Patnaik, Searching for the IoT resources: fundamentals, requirements, comprehensive review, and future directions, IEEE Commun. Surv. Tutor. 20 (2018) 2101–2132. https://doi.org/10.1109/COMST.2018.2825231

[6] V. Merlino, D. Allegra, Energy-based approach for attack detection in IoT devices: a survey, Internet Things 27 (2024) 101306. https://doi.org/10.1016/j.iot.2024.101306

[7] X. Chen, C.-M. Yang, Y. Nan, Z. Zheng, An empirical study of high-risk vulnerabilities in IoT systems, IEEE Internet Things J. 12 (2025) 1590–1601. https://doi.org/10.1109/JIOT.2024.3506976

[8] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (2019) 2702–2733. https://doi.org/10.1109/COMST.2019.2910750

[9] A. Al-Boghdady, K. Wassif, M. El-Ramly, The presence, trends, and causes of security vulnerabilities in operating systems of IoT's low-end devices, Sensors 21 (2021). https://doi.org/10.3390/s21072329

[10] J.-P.A. Yaacoub, H.N. Noura, O. Salman, A. Chehab, Ethical hacking for IoT: security issues, challenges, solutions and recommendations, Internet Things Cyber-Phys. Syst. (2023). https://doi.org/10.1016/j.iotcps.2023.04.002

[11] H.F. Atlam, G. Wills, IoT security, privacy, safety and ethics, Internet Things (2019). https://doi.org/10.1007/978-3-030-18732-3_8

[12] H. Yang, S. Kumara, S. Bukkapatnam, F. Tsung, The internet of things for smart manufacturing: a review, IISE Trans. 51 (2019) 1190–1216. https://doi.org/10.1080/24725854.2018.1555383

[13] B. Yuan, J. Wan, Y.-H. Wu, D.-Q. Zou, H. Jin, On the security of smart home systems: a survey, J. Comput. Sci. Technol. 38 (2) (2023) 228–247.

[14] M. Al-rawashdeh, P. Keikhosrokiani, B. Belaton, M. Alawida, A. Zwiri, IoT adoption and application for smart healthcare: a systematic review, Sensors 22 (2022). https://doi.org/10.3390/s22145377

[15] K. Kakhi, R. Alizadehsani, H.M.D. Kabir, A. Khosravi, S. Nahavandi, U.R. Acharya, The internet of medical things and artificial intelligence: trends, challenges, and opportunities, Biocybern. Biomed. Eng. (2022). https://doi.org/10.1016/j.bbe.2022.05.008

[16] Z.B. Akhtar, A.T. Rawol, Enhancing cybersecurity through AI-powered security mechanisms, IT J. Res. Dev. (2024). https://doi.org/10.25299/itjrd.2024.16852

[17] R. Somasundaram, M. Thirugnanam, Review of security challenges in healthcare internet of things, Wirel. Netw. 27 (8) (2021) 5503–5509.

[18] Health insurance portability and accountability act of 1996, 1996, (Public Law 104-191, 110 Stat. 1936). United States. Available at: https://www.hhs.gov/hipaa/ (accessed 2025-08-12).

[19] Regulation (EU) 2016/679 of the European parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016, (Official Journal of the European Union, L 119, 4 May 2016). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 2025-08-12).

[20] Regulation (EU) 2017/745 of the European parliament and of the council on medical devices, 2017, (Official Journal of the European Union, L 117, 5 May 2017). Available at: https://eur-lex.europa.eu/eli/reg/2017/745/oj (accessed 2025-08-12).

[21] Personal information protection and electronic documents act, 2000, (S.C. 2000, c. 5). Canada. Available at: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/ (accessed 2025-08-12).

[22] Lei Geral de Proteção de Dados Pessoais (LGPD), 2018, (Law No. 13,709, of 14 August 2018). Brazil. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (accessed 2025-08-12).

[23] Act on the protection of personal information, 2003, (Act No. 57 of 2003 (as amended)). Japan. Available at: https://www.ppc.go.jp/en/legal/ (accessed 2025-08-12).

[24] Personal data protection act 2012, 2012, (No. 26 of 2012). Singapore. Available at: https://sso.agc.gov.sg/Act/PDPA2012 (accessed 2025-08-12).

[25] A.A. El-Saleh, A.M. Sheikh, M.A.M. Albreem, M.S. Honnurvali, The internet of medical things (IoMT): opportunities and challenges, Wirel. Netw. 31(1) (2025) 327–344. https://doi.org/10.1007/s11276-024-03764-8.

[26] P. Mishra, G. Singh, Internet of medical things healthcare for sustainable smart cities: current status and future prospects, Appl. Sci. 13 (15) (2023) 8869.

[27] L. Bracciale, P. Loreti, G. Bianchi, Cybersecurity vulnerability analysis of medical devices purchased by national health services, Sci. Rep. 13 (1) (2023) 19509.

[28] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, et al., The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, Br. Med. J. - BMJ 372 (2021) n71.

[29] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, Security and privacy in the medical internet of things: a review, Secur. Commun. Netw. 2018 (1) (2018) 5978636.

[30] S.K. Kharroub, K. Abualsaud, M. Guizani, Medical IoT: a comprehensive survey of different encryption and security techniques, in: 2020 International Wireless Communications and Mobile Computing (IWCMC)(2020) 1891–1896.

[31] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the internet-of-medical-things (IoMT) systems security, IEEE Internet Things J. 8 (11) (2020) 8707–8718.

[32] M. Elhoseny, N.N. Thilakarathne, M.I. Alghamdi, R.K. Mahendran, A.A. Gardezi, H. Weerasinghe, A. Welhenge, Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions, Sustainability 13 (21) (2021) 11645.

[33] R.U. Rasool, H.F. Ahmad, W. Rafique, A. Qayyum, J. Qadir, Security and privacy of internet of medical things: a contemporary review in the age of surveillance, botnets, and adversarial ML, J. Netw. Comput. Appl. 201 (2022) 103332.

[34] H. Wu, H. Han, X. Wang, S. Sun, Research on artificial intelligence enhancing internet of things security: a survey, IEEE Access 8 (2020) 153826–153848.

[35] A. Barnawi, S. Gaba, A. Alphy, A. Jabbari, I. Budhiraja, V. Kumar, N. Kumar, A systematic analysis of deep learning methods and potential attacks in internet-of-things surfaces, Neural Comput. Appl. 35 (25) (2023) 18293–18308.

[36] F. Alwahedi, A. Aldhaheri, M.A. Ferrag, A. Battah, N. Tihanyi, Machine learning techniques for IoT security: current research and future vision with generative AI and large language models, Internet Things Cyber-Phys. Syst. 4 (2024) 167–185.

[37] S. Messinis, N. Temenos, N.E. Protonotarios, I. Rallis, D. Kalogeras, N. Doulamis, Enhancing internet of medical things security with artificial intelligence: a comprehensive review, Comput. Biol. Med. 170 (2024) 108036.

[38] D. Koutras, G. Stergiopoulos, T.K. Dasaklis, P. Kotzanikolaou, D. Glynos, C. Douligeris, Security in IoMT communications: a survey, Sensors 20 (2020). https://doi.org/10.3390/s20174828

[39] S.F. Ahmed, S. Sharmin, S.A. Kuldeep, A. Lameesa, M.S.B. Alam, G. Liu, A.H. Gandomi, Transformative impacts of the internet of medical things on modern healthcare, Results Eng. (2024). https://doi.org/10.1016/j.rineng.2024.103787

[40] F. Al-turjman, M.H. Nawaz, U. Ulusar, Intelligence in the internet of medical things era: a systematic review of current and future trends, Comput. Commun. 150 (2020) 644–660. https://doi.org/10.1016/j.comcom.2019.12.030

[41] P. Manickam, S.A. Mariappan, S. Murugesan, S. Hansda, A. Kaushik, R. Shinde, S.P. Thipperudraswamy, Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare, Biosensors 12 (2022). https://doi.org/10.3390/bios12080562

[42] S.F. Ahmed, M.S.B. Alam, S. Afrin, S.J. Rafa, N. Rafa, A.H. Gandomi, Insights into internet of medical things (IoMT): data fusion, security issues and potential solutions, Inf. Fusion 102 (2023) 102060. https://doi.org/10.1016/j.inffus.2023.102060

[43] J.B. Awotunde, R. Jimoh, S. Folorunso, E. Adeniyi, K.M. Abiodun, O. Banjo, Privacy and security concerns in IoT-based healthcare systems, Internet Things (2021). https://doi.org/10.1007/978-3-030-75220-0_6

[44] M. Adil, M.K. Khan, N. Kumar, M. Attique, A. Farouk, M. Guizani, Z. Jin, Healthcare internet of things: security threats, challenges, and future research directions, IEEE Internet Things J. 11 (2024) 19046–19069. https://doi.org/10.1109/JIOT.2024.3360289

[45] I.A. Khatib, A. Shamayleh, M. Ndiaye, Healthcare and the internet of medical things: applications, trends, key challenges, and proposed resolutions, Informatics 11(3) (2024) 47.

[46] R. Dwivedi, D. Mehrotra, S. Chandra, Potential of internet of medical things (IoMT) applications in building a smart healthcare system: a systematic review, J. Oral Biol. Craniofacial Res. 12 (2) (2022) 302–318.

[47] F. Al-Turjman, M.H. Nawaz, U.D. Ulusar, Intelligence in the internet of medical things era: a systematic review of current and future trends, Comput. Commun. 150 (2020) 644–660.

[48] L. Sun, X. Jiang, H. Ren, Y. Guo, Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application, IEEE Access 8 (2020) 101079–101092.

[49] G. Balhareth, M. Ilyas, B. Alkanjar, AI for IOMT security: a survey of intrusion detection systems, architectures, attacks and challenges, Int. J. Artif. Intell. Appl. (2024). https://doi.org/10.5121/ijaia.2024.15604

[50] M.S. Aslam, A. Altaf, F. Iqbal, N. Nigar, J.C. Galán, D.G. Aray, I. de la Torre Díez, I. Ashraf, Novel model to authenticate role-based medical users for blockchain-based IoMT devices, PLOS One 19 (2024). https://doi.org/10.1371/journal.pone.0304774

[51] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the internet-of-medical-things (IoMT) systems security, IEEE Internet Things J. 8 (2020) 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653

[52] L. Dzamesi, N. Elsayed, A review on the security vulnerabilities of the IoMT against malware attacks and DDoS, (2025). arXiv:2501.07703

[53] C. Liptak, S. Mal-Sarkar, S. Kumar, Power analysis side channel attacks and countermeasures for the internet of things, IEEE Phys. Assur. Insp. Electron. (2022) 1–7. https://doi.org/10.1109/PAINE56030.2022.10014854

[54] M. Siddiqi, W. Serdijn, C. Strydis, Zero-power defense done right: shielding IMDs from battery-depletion attacks, J. Signal Process. Syst. 93 (2020) 421–437. https://doi.org/10.1007/s11265-020-01530-5

[55] N.M. Thomasian, E. Adashi, Cybersecurity in the internet of medical things, Health Policy Technol. 10 (2021) 100549. https://doi.org/10.1016/J.HLPT.2021.100549

[56] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, R. Boutaba, Man-in-the-middle attack mitigation in internet of medical things, IEEE Trans. Ind. Inform. 18 (2022) 2053–2062. https://doi.org/10.1109/TII.2021.3089462

[57] A. Jahangeer, S. Bazai, S. Aslam, S. Marjan, M. Anas, S.H. Hashemi, A review on the security of IoT networks: from network layer's perspective, IEEE Access 11 (2023) 71073–71087. https://doi.org/10.1109/ACCESS.2023.3246180

[58] J.-P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, Securing internet of medical things systems: limitations, issues and recommendations, Future Gener. Comput. Syst. 105 (2020) 581–606. https://doi.org/10.1016/j.future.2019.12.028

[59] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, L. Coventry, Phishing simulation exercise in a large hospital: a case study, Digit. Health 8 (2022). https://doi.org/10.1177/20552076221081716

[60] R. Hireche, H. Mansouri, A.-S.K. Pathan, Security and privacy management in internet of medical things (IoMT): a synthesis, J. Cybersecur. Priv. 2 (3) (2022) 640–661. https://www.mdpi.com/2624-800X/2/3/33. https://doi.org/10.3390/jcp2030033

[61] U. Tariq, I. Ullah, M.Y. Uddin, S.J. Kwon, An effective self-configurable Ransomware prevention technique for IoMT, Sensors 22 (2022). https://doi.org/10.3390/s22218516

[62] C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: International Conference on Evaluation and Assessment in Software Engineering, 2014, pp. 1–10.

[63] Mendeley, 2025, https://www.mendeley.com/reference-management/reference-manager/.

[64] Connected Papers, 2025, https://www.connectedpapers.com/.

[65] F. Ding, H. Li, F. Luo, H. Hu, L. Cheng, H. Xiao, R. Ge, DeepPower: non-intrusive and deep learning-based detection of IoT Malware using power side channels, in: ACM Asia Conference on Computer and Communications Security, 2020, pp. 33–46.

[66] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, M. Prvulovic, EDDIE: EM-based detection of deviations in program execution, in: Proceedings of the 44th Annual International Symposium on Computer Architecture, 2017, pp. 333–346.

[67] N. Garg, I. Shahid, E. Avllazagaj, J. Hill, J. Han, N. Roy, Thermware: toward side-channel defense for tiny IoT devices, in: International Workshop on Mobile Computing Systems and Applications, 2023, pp. 81–88.

[68] N. Sehatbakhsh, A. Nazari, M. Alam, F. Werner, Y. Zhu, A. Zajic, M. Prvulovic, REMOTE: robust external Malware detection framework by using electromagnetic signals, IEEE Trans. Comput. 69 (3) (2019) 312–326.

[69] H.A. Khan, N. Sehatbakhsh, L.N. Nguyen, R.L. Callan, A. Yeredor, M. Prvulovic, A. Zajić, IDEA: intrusion detection through electromagnetic-signal analysis for critical embedded and cyber-physical systems, IEEE Trans. Dependable Secure Comput. 18 (3) (2019) 1150–1163.

[70] H.A. Khan, N. Sehatbakhsh, L.N. Nguyen, M. Prvulovic, A. Zajić, Malware detection in embedded systems using neural network model for electromagnetic side-channel signals, J. Hardw. Syst. Secur. 3 (2019) 305–318.

[71] S. Khan, A. Akhunzada, A hybrid DL-driven intelligent SDN-enabled malware detection framework for internet of medical things (IoMT), Comput. Commun. 170 (2021) 209–216.

[72] A. Albasir, K. Naik, R. Manzano, Toward improving the security of IoT and CPS devices: an AI approach, Digit. Threats Res. Pract. 4 (2) (2023) 1–30.

[73] H. Alrubayyi, M.S. Alshareef, Z. Nadeem, A.M. Abdelmoniem, M. Jaber, Security threats and promising solutions arising from the intersection of AI and IoT: a study of ioMT and IoET applications, Future Internet 16 (3) (2024) 85.

[74] S.H. Almotiri, AI driven IOMT security framework for advanced malware and ransomware detection in SDN, J. Cloud Comput. 14 (1) (2025) 19.

[75] A.I. Newaz, A.K. Sikder, M.A. Rahman, A.S. Uluagac, Healthguard: a machine learning-based security framework for smart healthcare systems, in: 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS), IEEE, 2019, pp. 389–396.

[76] L. Ben Amor, I. Lahyani, M. Jmaiel, AUDIT: anomalous data detection and isolation approach for mobile healthcare systems, Expert Syst. 37 (1) (2020) e12390.

[77] D. Gupta, O. Kayode, S. Bhatt, M. Gupta, A.S. Tosun, Hierarchical federated learning based anomaly detection using digital twins for smart healthcare, in: 2021 IEEE 7th International Conference on Collaboration and Internet Computing (CIC), IEEE, 2021, pp. 16–25.

[78] N.I. Haque, A.A. Khalil, M.A. Rahman, M.H. Amini, S.I. Ahamed, Biocad: bio-inspired optimization for classification and anomaly detection in digital healthcare systems, in: IEEE International Conference on Digital Health, IEEE, 2021, pp. 48–58.

[79] P.V. Astillo, D.G. Duguma, H. Park, J. Kim, B. Kim, I. You, Federated intelligence of anomaly detection agent in IoTMD-enabled diabetes management control system, Future Gener. Comput. Syst. 128 (2022) 395–405.

[80] A. Sundas, S. Badotra, S. Bharany, A. Almogren, E.M. Tag-ElDin, A.U. Rehman, HealthGuard: an intelligent healthcare system security framework based on machine learning, Sustainability 14 (19) (2022) 11934.

[81] V.V. Raje, S. Goel, S.V. Patil, M.D. Kokate, D.A. Mane, S. Lavate, Realtime anomaly detection in healthcare IoT: a machine learning-driven security framework, J. Electr. Syst. 19 (3) (2023) 192–202.

[82] S. Rani, S. Kumar, A. Kataria, H. Min, SmartHealth: an intelligent framework to secure IoMT service applications using machine learning, ICT Express 10 (2) (2024) 425–430.

[83] L. Song, H. Lan, J. Du, K. Wang, W. Kang, Application of intelligent internet of things technology in the security monitoring system of power internet of things network, Discov. Internet Things 5 (1) (2025) 1–15.

[84] H. Goumidi, S. Pierre, Real-time anomaly detection in IoMT networks using stacking model and a healthcare-specific dataset, IEEE Access 13 (2025) 70352–70365.

[85] G. Thamilarasu, A. Odesile, A. Hoang, An intrusion detection system for internet of medical things, IEEE Access 8 (2020) 181560–181576.

[86] S.R. Addula, M.K. Meesala, P. Ravipati, G.S. Sajja, A hybrid autoencoder and gated recurrent unit model optimized by honey badger algorithm for enhanced cyber threat detection in IoT networks, Secur. Priv. 8 (6) (2025) e70086. https://doi.org/10.1002/spy2.70086

[87] A. Heidari, M.A.J. Jamali, Internet of things intrusion detection systems: a comprehensive review and future directions, Clust. Comput. 26 (2022) 3753–3780. https://doi.org/10.1007/s10586-022-03776-z

[88] P. Kulshrestha, T.V.V. Kumar, Machine learning based intrusion detection system for IoMT, Int. J. Syst. Assur. Eng. Manag. 15 (2023) 1802–1814. https://doi.org/10.1007/s13198-023-02119-4

[89] A.A. Hady, A. Ghubaish, T. Salman, D. Unal, R. Jain, Intrusion detection system for healthcare systems using medical and network data: a comparison study, IEEE Access 8 (2020) 106576–106584. https://ieeexplore.ieee.org/document/9109651/. https://doi.org/10.1109/ACCESS.2020.3000421

[90] S. Manimurugan, S. Al-Mutairi, M.M. Aborokbah, N. Chilamkurti, S. Ganesan, R. Patan, Effective attack detection in internet of medical things smart environment using a deep belief neural network, IEEE Access 8 (2020) 77396–77404.

[91] G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J.C. Ribeiro, J. Rodriguez, An anomaly-based intrusion detection system for internet of medical things networks, Electronics 10 (21) (2021) 2562.

[92] I. Essop, J.C. Ribeiro, M. Papaioannou, G. Zachos, G. Mantas, J. Rodriguez, Generating datasets for anomaly-based intrusion detection systems in IoT and industrial IoT networks, Sensors 21 (4) (2021) 1528.

[93] J.D. Lee, H.S. Cha, S. Rathore, J.H. Park, M-IDM: a multi-classification based intrusion detection model in healthcare IoT, Comput. Mater. Contin. 67 (2) (2021) 1537–1553.
[94] J.B. Awotunde, K.M. Abiodun, E.A. Adeniyi, S.O. Folorunso, R.G. Jimoh, A deep learning-based intrusion detection technique for a secured IoMT system, in: International Conference on Informatics and Intelligent Applications, Springer, 2021, pp. 50–62.
[95] I. Siniosoglou, P. Sarigiannidis, V. Argyriou, T. Lagkas, S.K. Goudos, M. Poveda, Federated intrusion detection in NG-IoT healthcare systems: an adversarial approach, in: IEEE International Conference on Communications, IEEE, 2021, pp. 1–6.
[96] I. Idrissi, M. Boukabous, M. Grari, M. Azizi, O. Moussaoui, An intrusion detection system using machine learning for internet of medical things, in: International Conference on Electronic Engineering and Renewable Energy Systems, Springer, 2022, pp. 641–649.
[97] Y. Li, S.-m. Ghoreishi, A. Issakhov, Improving the accuracy of network intrusion detection system in medical IoT systems through butterfly optimization algorithm, Wirel. Pers. Commun. 126 (3) (2022) 1999–2017.
[98] K. Gupta, D.K. Sharma, K.D. Gupta, A. Kumar, A tree classifier based network intrusion detection model for internet of medical things, Comput. Electr. Eng. 102 (2022) 108158.
[99] K. Ramana, A. Revathi, A. Gayathri, R.H. Jhaveri, C.V.L. Narayana, B.N. Kumar, WOGRU-IDS–an intelligent intrusion detection system for IoT assisted wireless sensor networks, Comput. Commun. 196 (2022) 195–206.
[100] R. Chaganti, A. Mourade, V. Ravi, N. Vemprala, A. Dua, B. Bhushan, A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things, Sustainability 14 (19) (2022) 12828.
[101] S. Saif, P. Das, S. Biswas, M. Khari, V. Shanmuganathan, HIIDS: hybrid intelligent intrusion detection system empowered with machine learning and meta-heuristic algorithms for application in IoT based healthcare, Microprocess. Microsyst. (2022) 104622.
[102] M. Akshay Kumaar, D. Samiayya, P.M. D.R. Vincent, K. Srinivasan, C.-Y. Chang, H. Ganesh, A hybrid framework for intrusion detection in healthcare systems using deep learning, Front. Public Health 9 (2022) 824898.
[103] D. Misra, Mish: a self regularized non-monotonic activation function, (2019). arXiv:1908.08681
[104] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, M. Dinesh, An investigation and comparison of machine learning approaches for intrusion detection in IoMT network, J. Supercomput. 78 (15) (2022) 17403–17422.
[105] I.A. Khan, N. Moustafa, I. Razzak, M. Tanveer, D. Pi, Y. Pan, B.S. Ali, XSRU-IoMT: explainable simple recurrent units for threat detection in internet of medical things networks, Future Gener. Comput. Syst. 127 (2022) 181–193.
[106] M. Alalhareth, S.-C. Hong, An improved mutual information feature selection technique for intrusion detection systems in the internet of medical things, Sensors 23 (10) (2023) 4971.
[107] O. Taouali, S. Bacha, K. Ben Abdellafou, A. Aljuhani, K. Zidi, R. Alanazi, M.F. Harkat, Intelligent intrusion detection system for the internet of medical things based on data-driven techniques, Comput. Syst. Sci. Eng. 47 (2) (2023).
[108] N. Faruqui, M.A. Yousuf, M. Whaiduzzaman, A. Azad, S.A. Alyami, P. Liò, M.A. Kabir, M.A. Moni, SafetyMed: a novel IoMT intrusion detection system using CNN-LSTM hybridization, Electronics 12 (17) (2023) 3541.
[109] M. Norouzi, Z. Gürkaş-Aydın, Ö.C. Turna, M.Y. Yağci, M.A. Aydin, A. Souri, A hybrid genetic algorithm-based random forest model for intrusion detection approach in internet of medical things, Appl. Sci. 13 (20) (2023) 11145.
[110] M. Alalhareth, S.-C. Hong, An adaptive intrusion detection system in the internet of medical things using fuzzy-based learning, Sensors 23 (22) (2023) 9247.
[111] M. Alalhareth, S.-C. Hong, Enhancing the internet of medical things (IoMT) security with meta-learning: a performance-driven approach for ensemble intrusion detection systems, Sensors 24 (11) (2024) 3519.
[112] P.G. Shambharkar, N. Sharma, Deep learning-empowered intrusion detection framework for the internet of medical things environment, Knowl. Inf. Syst. (2024) 1–50.
[113] I. Ioannou, P. Nagaradjane, P. Angin, P. Balasubramanian, K.J. Kavitha, P. Murugan, V. Vassiliou, GEMLIDS-MIOT: a green effective machine learning intrusion detection system based on federated learning for medical IoT network security hardening, Comput. Commun. 218 (2024) 209–239. https://linkinghub.elsevier.com/retrieve/pii/S0140366424000793. https://doi.org/10.1016/j.comcom.2024.02.023
[114] J. Li, M.S. Othman, H. Chen, L.M. Yusuf, Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning, J. Big Data 11 (1) (2024) 36. https://doi.org/10.1186/s40537-024-00892-y
[115] Z. Sun, G. An, Y. Yang, Y. Liu, Optimized machine learning enabled intrusion detection 2 system for internet of medical things, Frankl. Open 6 (2024) 100056.
[116] U. Zukaib, X. Cui, C. Zheng, D. Liang, S.U. Din, Meta-fed IDS: meta-learning and federated learning based fog-cloud approach to detect known and zero-day cyber attacks in IoMT networks, J. Parallel Distrib. Comput. 192 (2024) 104934.
[117] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, M. Ilyas, Stacking ensemble deep learning for real-time intrusion detection in IoMT environments, Sensors 25 (3) (2025) 624.
[118] A. Nasayreh, H.M. Khalid, H.K. Alkhateeb, J. Al-Manaseer, A. Ismail, H. Gharaibeh, Automated detection of cyber attacks in healthcare systems: a novel scheme with advanced feature extraction and classification, Comput. Secur. 150 (2025) 104288.
[119] A.A. Mawgoud, A.I. Karadawy, B.S. Tawfik, A secure authentication technique in internet of medical things through machine learning, (2019). arXiv:1912.12143
[120] S. Pirbhulal, N. Pombo, V. Felizardo, N. Garcia, A.H. Sodhro, S.C. Mukhopadhyay, Towards machine learning enabled security framework for IoT-based healthcare, in: International Conference on Sensing Technology, IEEE, 2019, pp. 1–6.
[121] H. Rathore, C. Fu, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, Z. Yu, Multi-layer security scheme for implantable medical devices, Neural Comput. Appl. 32 (2020) 4347–4360.
[122] S. Kute, A.V. Shreyas Madhav, A.K. Tyagi, A. Deshmukh, Authentication framework for healthcare devices through internet of things and machine learning, in: International Conference on Evolutionary Computing and Mobile Sustainable Networks, Springer, 2022, pp. 399–415.
[123] M.A. Almaiah, F. Hajjej, A. Ali, M.F. Pasha, O. Almomani, A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS, Sensors 22 (4) (2022) 1448.
[124] P.K. Sadhu, V.P. Yanambaka, A. Abdelgawad, Physical unclonable function and machine learning based group authentication and data masking for in-hospital segments, Electronics 11 (24) (2022) 4155.
[125] P.K. Sadhu, V.P. Yanambaka, A. Abdelgawad, MC-multi PUF based lightweight authentication framework for internet of medical things, in: IEEE World Forum on Internet of Things, IEEE, 2022, pp. 1–6.
[126] M. Adil, M.K. Khan, M.M. Jadoon, M. Attique, H. Song, A. Farouk, An AI-enabled hybrid lightweight authentication scheme for intelligent IoMT based cyber-physical systems, IEEE Trans. Netw. Sci. Eng. 10 (5) (2022) 2719–2730.
[127] F.J. Alruwaili, S.P. Mohanty, E. Kougianos, ALBA: novel anomaly location-based authentication in IoMT environment using unsupervised ML, in: Internet of Things. Advances in Information and Communication Technology, Springer, 2023, pp. 424–432.
[128] M. Hazratifard, V. Agrawal, F. Gebali, H. Elmiligi, M. Mamun, Ensemble siamese network (ESN) using ECG signals for human authentication in smart healthcare system, Sensors 23 (10) (2023) 4727.
[129] S.A. El-Moneim Kabel, G.M. El-Banby, L.A. Abou Elazm, W. El-Shafai, N.A. El-Bahnasawy, F.E.A. El-Samie, A.A. Elazm, A.I. Siam, M.A. Abdelhamed, Securing internet-of-medical-things networks using cancellable ECG recognition, Sci. Rep. 14 (1) (2024) 10871.
[130] Y.D. Al-Otaibi, K-nearest neighbour-based smart contract for internet of medical things security using blockchain, Comput. Electr. Eng. 101 (2022) 108129.
[131] R. Kumar, P. Kumar, R. Tripathi, G.P. Gupta, A.N. Islam, M. Shorfuzzaman, Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems, IEEE Trans. Ind. Inform. 18 (11) (2022) 8065–8073.
[132] E. Ashraf, N.F.F. Areed, H. Salem, E.H. Abdelhay, A. Farouk, FIDChain: federated intrusion detection system for blockchain-enabled IoT healthcare applications, in: Healthcare, Vol. 10, MDPI, 2022, p. 1110.
[133] R.A. Alsemmeari, M.Y. Dahab, A.A. Alsulami, B. Alturki, S. Algarni, Resilient security framework using TNN and blockchain for IOMT, Electronics 12 (10) (2023) 2252.

[134] J. Dutta, D. Puthal, PoAh 2.0: AI-empowered dynamic authentication based adaptive blockchain consensus for IoMT-edge workflow, Future Gener. Comput. Syst. 161 (2024) 655–672.
[135] S. Khan, M. Khan, M.A. Khan, M.A. Khan, L. Wang, K. Wu, A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems, IEEE J. Biomed. Health Inform. (2025) 1–14.
[136] M. Anjum, N. Kraiem, H. Min, A.K. Dutta, Y.I. Daradkeh, S. Shahab, Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning, Sci. Rep. 15 (1) (2025) 7589.
[137] B.R. Bezanjani, S.H. Ghafouri, R. Gholamrezaei, Privacy-preserving healthcare data in IoT: a synergistic approach with deep learning and blockchain, J. Supercomput. 81 (4) (2025) 533.
[138] S. Rani, A. Kataria, S. Kumar, P. Tiwari, Federated learning for secure IoMT-applications in smart healthcare systems: a comprehensive review, Knowl.-Based Syst. 274 (2023) 110658.
[139] S. Dadkhah, E.C.P. Neto, R. Ferreira, R.C. Molokwu, S. Sadeghi, A.A. Ghorbani, CICIoMT2024: a benchmark dataset for multi-protocol security assessment in IoMT, Internet Things 28 (2024) 101351.
[140] S. Alsubai, V. Karovič, A. Almadhor, A.A. Hejaili, R.A. Juanatas, G.A. Sampedro, Future-proofing AI models in IoMT environment: adversarial dataset generation and defense strategies, Digit. Twins Appl. 2 (1) (2025) e70010.
[141] S. Rahman, S. Pal, A. Fallah, R. Doss, C. Karmakar, RAD-IoMT: robust adversarial defense mechanisms for IoMT medical image analysis, Ad Hoc Netw. 178 (2025) 103935.
[142] O. Subasi, J. Cree, J. Manzano, E. Peterson, A critical assessment of interpretable and explainable machine learning for intrusion detection, (2024). arXiv:2407.04009
[143] V.Z. Mohale, I.C. Obagbuwa, A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity, Front. Artif. Intell. 8 (2025) 1526221.
[144] I.D. Mienye, G. Obaido, N. Jere, E. Mienye, K. Aruleba, I.D. Emmanuel, B. Ogbuokiri, A survey of explainable artificial intelligence in healthcare: concepts, applications, and challenges, Inform. Med. Unlocked 51 (2024) 101587.
[145] Y. Ning, M. Liu, N. Liu, Advancing ethical AI in healthcare through interpretability, Patterns 6 (6) (2025).
[146] D. Bhusal, R. Shin, A.A. Shewale, M.K.M. Veerabhadran, M. Clifford, S. Rampazzi, N. Rastogi, SoK: modeling explainability in security analytics for interpretability, trustworthiness, and usability, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES '23, Association for Computing Machinery, New York, NY, USA, 2023. https://doi.org/10.1145/3600160.3600193