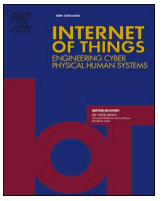
Internet of Things 39 (2026) 102008

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.sciencedirect.com/journal/internet-of-things



Intrusion detection system for IoMT in smart hospitals: a systematic literature review

Sadia Fatima [a], Muhammad Ismail Kashif [a], Khadija Tuz Zahra [a], Muhammad Adnan [b,*]

[a] National College of Business Administration and Economics, Sub campus Multan, Pakistan
[b] School of Architecture, Built Environment, Computing, and Engineering, Birmingham City University, United Kingdom

ARTICLE INFO

Keywords:
Intrusion detection systems (IDS)
Internet of medical things (IoMT)
Healthcare IoMT security
Privacy protection
Decentralized learning
Primary cybersecurity threats
Edge computing
Federated learning (FL)

ABSTRACT

With the quick development of smart healthcare, the Internet of Medical Things (IoMT) has emerged as a paradigm-changing technology. It connects wearable devices, smart sensors, and medical systems to enable real-time, patient-centric care. To protect these life-saving systems, their security is essential and often requires the use of specific Intrusion Detection Systems (IDS). However, such solutions have yet to address complex medical networks. A systematic literature review is conducted to reveal the current state and future trends in the IDS framework for IoMT. The 32 studies identified in prominent digital databases were selected for in-depth qualitative and quantitative analysis. The total number of datasets used in the selected studies is 11; some of these achieve high accuracy (98%-99.9%). The frequently used models are XG Boost (XGB), K-Nearest Neighbors (KNN), Artificial Neural Network (ANN), and Convolutional Neural Network. (CNN). IDS with AI methods, primarily ML, DL, and hybrid models, are very much popular. High accuracy and low latency are the priorities of such systems. However, most are poorly adapted to IoMT energy and resource constraints. This review aims to bridge the gap between algorithmic innovations and clinical utilities. Numerous frameworks also overlook privacy, real-time implementation, and regulatory compliance. We advocate for context-aware systems that center on patient safety.

1. Introduction

1.1. Key issues

The use of IoMT devices has significantly improved patient care and operational efficiency [1,2]. These devices enable real-time monitoring, automated data collection, and remote patient management, thereby enhancing the efficiency of healthcare delivery [3,4]. However, the widespread adoption of interconnected devices has also created considerable security risks [5,6], making IDS crucial [7,8]. As smart hospitals increasingly implement IoMT technologies, the threat of advanced cyberattacks aimed at these devices also rises. A single compromised device could act as a gateway for infections to spread throughout the hospital's network [9]. The primary challenge lies in the heterogeneity of IoMT devices [10], which vary in hardware specifications, communication protocols,

* Corresponding author.
E-mail addresses: sadiafatima258@gmail.com (S. Fatima), ismailkashif@ncbae.edu.pk (M.I. Kashif), KhadijaZahra@ncbaemultan.edu.pk (K.T. Zahra), muhammad.adnan@bcu.ac.uk (M. Adnan).

https://doi.org/10.1016/j.iot.2026.102008

Available online 13 July 2026

and operating systems [11]. What is more, diversity makes it infeasible to deploy a single IDS across all devices, as embedded devices have highly compact computational resources that may make it difficult to run sophisticated security mechanisms [12]. It not only compromises the security of individual devices but also risks the entire hospital network, as weak nodes can serve as entry points for breaches to spread [13]. Furthermore, the varying lifecycles of IoMT devices, ranging from a few months to a couple of years, lead to recurring maintenance and compatibility issues [14].

Lack of procedures is a significant issue that needs to be addressed in IoMT devices [15]. These devices can implement different security standards (as manufacturers are independent of one another, but security levels vary) [16]. It not only provides potential points of entry for an assailant but also makes articulating a coherent security model difficult [17]. Without a unified framework for security controls, we see an increase in exploitable vulnerabilities [18,19]. Inconsistent firmware patches and vendor support compound this, leaving critical systems unsupported and vulnerable [20,21].

The resource-constrained nature of IoMT devices poses significant challenges to deploying IDS [22,23]. Therefore, the requirements for lightweight IDS for IoMT devices are more demanding [24]. The limited computing and storage capacities of such devices prevent them from effectively handling and analyzing information, thereby making them highly susceptible to various attacks [25].

1.2. Research gap

It is widely recognized that the IoMT environment, by itself, poses challenges for IDS. Cybercriminals are constantly evolving, challenging defenders to develop more complex strategies that evade traditional detection methods [26]. Researchers are exploring DL technologies and ML methods to improve attack detection [27,28] due to the diverse nature of data generated by IoMT sensors. However, these solutions may not be ideal for IoMT settings [29]. General-purpose ML models may not be suitable given the varied sensor data structures and the real-time processing required; these models must be customized for each domain [30].

1.3. Significance of the study

IDSs for smart hospitals must consider resource limitations and real-time requirements; therefore, it is necessary to develop a lightweight and flexible IDS for IoMT devices [31]. IDS is expected to support secure monitoring and end-to-end protection in 5G scenarios through edge computing [32]. Moreover, novel approaches such as FL (that is, where several parties train a common model together, but do not share raw data directly) and Graph Neural Networks (GNNs) have shown the potential for improving IDS performance in a privacy- and compliance-preserving manner [19,33].

1.4. Primary contribution of this study

A primary contribution of this study is the comparative analysis of the papers published in 2020–2025.

- A comprehensive Systematic Literature Review (SLR) that focuses on the aspects of IDS in IoMT.
- Unlike previous reviews, this study focuses only on the specific requirements and issues of IoMT security rather than treating it as an overall security problem or a subset of IoT.
- We provide a discussion of IoMT-specific datasets, attacks, and privacy issues.
- Performance analysis (accuracy, latency, resource efficiency) of different IDS models (ML and DL based IDS models, hybrid) is compared.
- Proposes future research directions focused on developing lightweight, interpretable, and context-aware IDS frameworks suitable for clinical deployment.
- Combines technical considerations with real-world issues, providing a road map to how IoMT security can be improved in healthcare systems.

1.5. Research objectives

This review aims to identify key cybersecurity threats in smart hospitals. The purpose is to evaluate how effectively IDS mitigates them using measurable indicators such as mitigation efficiency and reduction in attack success. A comparison will be made between ML, DL, and Hybrid IDS models. It is based on quantifiable performance metrics, detection rate, latency, computational overhead, scalability, and ability to adapt in clinical environments. The review will investigate the limitations of IoMT devices stemming from their limited processing power, memory, energy, and bandwidth. This would influence the effectiveness and real-time responsiveness of IDS. It will also evaluate proposed decentralized (without a central device) or privacy-preserving techniques, such as FL. Also, the study will analyze performance enhancements resulting from edge-enabled IDS architectures, focusing on response time and throughput. The review will then highlight the quantifiable research gaps in terms of privacy, energy efficiency, interoperability, and regulatory compliance. It also provides comparative, evidence-based guidance for lightweight, interpretable, clinically deployable IDS frameworks.

1.6. Research questions

RQ1. What are the primary cybersecurity threats faced by IoMT devices in smart hospitals?
RQ2. How can IDS help to mitigate Cybersecurity threat risks?
RQ3. How do resource limitations in IoMT devices affect the design and performance of IDS in smart hospital environments?
RQ4. How can decentralized learning be leveraged to develop privacy-preserving IDS for IoMT in smart hospitals?
RQ5. What role does edge computing play in enhancing real-time IDS performance in smart hospitals?

1.7. The structure of the SLR

There are six sections in all. The main issue, gaps in the literature, objectives, research questions, and the motivation behind the study were all covered in detail in the introduction. Addressing the main concerns, IDS strategy types, performance, deployment challenges, and scalability approaches in the context of IoMT-based smart hospital settings, the review's research questions are addressed. The Materials and Methods section follows the PRISMA 2020 framework to systematically identify, screen, and analyze 32 high-quality research articles retrieved from multiple academic databases. The Result section critically discusses the findings with respect to the defined research questions, evaluates the efficiency of IDS in IoMT medical ecosystems, and identifies deployment limitations. The rest of the Discussion is a detailed critique. It is essential in the Future Directions that the IDSs be employed in real time, incorporating more sophisticated AI-based algorithms, privacy-preserving solutions, and standardized evaluations. The Conclusion states that IDSs have been critically discussed to secure the IoMT-based medical infrastructure, along with the existing limitations and challenges.

1.8. Limitations

Due to the technological and practical limitations of medical settings, IDS in the IoMT) Intelligent hospitals face significant limitations [34,35]. First and foremost, IoMT devices have limited memory, storage, and processing power, rendering comprehensive IDS models impractical and necessitating lighter solutions that often compromise detection accuracy [36,37]. IDS efficiency is further constrained by the adjustment between detection accuracy and performance [38]. Additionally, IDS often misses real threats and generates false alarms, causing operational disruptions, alert fatigue in the healthcare industry, and increased vulnerabilities, especially during critical downtime in environments like intensive care units [37,39,40]. Another issue is scalability, as the rapid growth of networked medical devices overwhelms IDS with an enormous volume of data that is impossible to analyze in real time [41]. Inconsistent security practices across vendors create further compatibility concerns with the many IT systems used in hospitals, such as older-generation Electronic Health Record (EHR) systems. This results in broken ecosystems in which resources must be manually checked and integrated, and thus cannot be accessed automatically [42–44]. Adaptable IDS Features: Adaptability in IDS is crucial to learning evolving threats [45,46]. AI and ML techniques are not feasible due to the lack of data and processing resources in IoMT environments. Finally, the validation and generalization of IDS for IoMT is impeded by a lack of benchmark datasets [47,48].

1.8.1. Methodological limitations

This research is not without limitations. The studies analyzed in the included systematic reviews and meta-analyses may have been affected by publication bias, reflecting a tendency to report positive outcomes. Limited access to commercial IDS datasets poses a challenge to evaluating IDS performance in real-world IoMT scenarios.

1.9. Study comparison

Table 1 compares this study with three previous reviews, focusing on its unique contributions and added value, highlighting differences in focus, methodologies, and key insights, and demonstrating the advancement in IoMT IDS research.

Table 1
The table compares this study with three previous reviews to highlight its added value.

Study	Focus	Key features	Limitations	Contribution of this study
[49]	Focus on automated detection of cyberattacks in IoMT using DL models	Applies DL for cyber attack detection in IoMT, but lacks a comprehensive review of IDS models	Focuses on a specific aspect (DL) but does not offer a broad comparison of various IDS techniques in IoMT	This study offers a broad, comparative analysis of IDS models across ML, DL, and hybrid approaches, filling in the gaps of isolated research on individual models
[50]	Focus on ensemble learning-based IDS for IoMT.	Uses traditional ensemble learning methods (Random Forest, XG Boost, etc.) for IDS, but does not address the evolving nature of cybersecurity threats in IoMT	Does not provide a systematic review of existing IDS models or their performance in real-world IoMT environments	The proposed study evaluates the current state of IDS in IoMT, identifying gaps, datasets, and future research directions, which are not covered in this ensemble learning-focused study.
[51]	IDS in IoMT	Integrates IoMT into healthcare systems and connects devices such as wearable sensors and medical instruments for health data collection and analysis.	Limited coverage of specific IoMT challenges	Comprehensive review of IoMT, examining concepts, deployment, technologies, and applications with a focus on future directions.

Table 2 presents a comparison between the proposed study and the closest prior work. A table covers the papers from 2023 to 2025. It is compared in terms of scope, years covered in the study, and other parameters.

2. Materials and methods

2.1. Systematic literature review methodology

The systematic approach was then applied to identify, evaluate, and synthesize relevant studies on IoMT IDS for this study's literature review. The aim was to map the evolution and current state of IDS in healthcare environments supported by IoMT technology and to identify potential research gaps in this context.

A comprehensive search was carried out using electronic databases, including:

- ScienceDirect
- ACM Digital Library
- Taylor & Francis
- Springer
- IEEE Xplore

Studies focusing on IDS specifically designed or evaluated for IoMT environments in healthcare or smart hospitals. Papers discussing threat models, attack types, or security challenges specific to IoMT. Research presenting novel IDS frameworks, algorithms, or evaluation metrics applicable to smart hospital infrastructure.

Fig. 1 highlights the names of databases from which the papers are selected and evaluated for the literature review of the current research. A total of five databases are included to identify relevant papers for the proposed study.

Table 2
Reviewed studies and the distinct contribution of the proposed study.

Reference	Scope	Years covered	No of studies	Focus on smart hospitals	Focus on FL/Edge
[52]	Cybersecurity in healthcare systems, IoMT IDS	Up to 2023	Not explicitly stated	Yes	No
[50]	IoMT network security using ensemble learning for intrusion detection	Up to 2024	Not explicitly stated	Yes	No
[53]	Medical IoMT technology for remote health monitoring and device management	Recent advancements	Not explicitly stated	Yes	No
[54]	Intrusion detection in IoMT networks using meta-learning methods	2020-2024	Not explicitly stated	Yes	No
[51]	(IoMT) in healthcare, with an emphasis on technologies, applications, and future challenges	2020–2023	Not explicitly stated	Yes	Yes
[55]	IDS in the IoMT environment, focusing on AI-based, ML, and DL methods	2018 - April 2024	28 studies	Yes	Yes
[56]	Intrusion detection in IoMT networks using (FL)	Not Mentioned Clearly	Not explicitly stated	Yes	Yes
[49]	Detecting cyberattacks in IoMT using ML & DL	2020-2024	Not explicitly stated	Yes	Yes
[57]	IDS for resource-constrained IoMT using SaaS(Software as a Service)	Recent 2024	Not explicitly stated	Yes	yes
[58]	FL in healthcare, especially for privacy-preserving.	2020–2024	Not explicitly stated	Yes	yes
[50]	Enhances IoMT IDS using ensemble learning with multiple base models	Recent 2024	Not explicitly stated	Yes	No
[59]	Reviews IoMT in healthcare, including technologies, applications, challenges, and IoMT-enabled architectures	2014–2023	116 studies selected	Yes	Yes
[60]	Focus on IDS for IoMT	Recent developments in IoMT (up to 2023)	Several studies reviewed	Yes	Yes
[61]	Use of FL in cybersecurity, including attack detection and privacy preservation	2021–2024	Not explicitly stated	Yes	Yes
[52]	Focus on cybersecurity intrusion detection in healthcare	Recent 2023	Not explicitly stated	Yes	No
[62]	IoMT security architecture for addressing security issues and threats	2020–2023	64 studies included	Yes	Yes
The proposed study	The study focuses on IDS in the IoMT and on how the interaction between FL and Edge Computing plays a role.	2020-May,2025	32	Yes	Yes

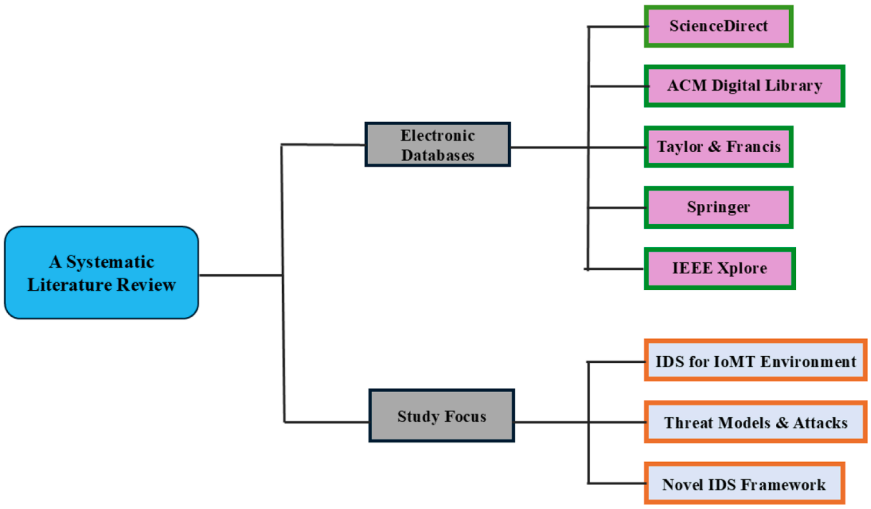


Fig. 1. Electronic databases included in extracting papers for literature review.

2.2. Prisma guidelines

This literature review follows the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines [63] to ensure a transparent and replicable process for selecting and analyzing relevant studies on IDS in IoMT.

In Fig. 2, a PRISMA diagram outlines the methodological process for identifying, appraising, and selecting research papers for quality analysis. The search date range for the articles is 2020–2025. In the beginning, a total of 239 papers were gathered from five primary databases (Science Direct, ACM Digital Library, Taylor & Francis, Springer, and IEEE Xplore). After discarding 113 duplicate reports from the various database searches (a duplicate record was selected randomly from any one database). We had 126 records available for screening at this point. The Titles and Abstracts were then screened for relevance to the research topic. The 64 papers

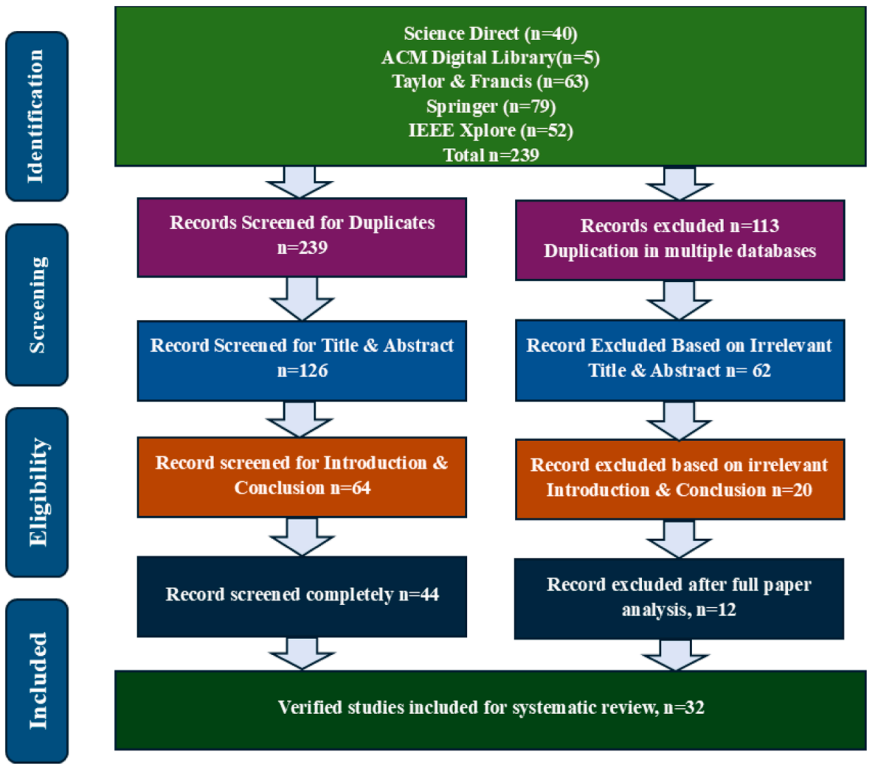


Fig. 2. PRISMA flow diagram illustrating the study selection process for the SLR.

remained for additional assessment after 62 were removed in this phase because they did not support the study's goals. The Introduction and Conclusion sections of these 64 papers were then evaluated. Twenty papers were eliminated after this analysis because they did not meet the inclusion criteria. The 44 papers were left for full-text review at this point. The last 12 papers were further disqualified for failing to meet the eligibility requirements after a thorough examination of the complete papers, including all sections. In the end, 32 studies that met the inclusion criteria were included in the qualitative synthesis.

2.3. Keywords used

Intrusion Detection Systems (IDS), Internet of Medical Things (IoMT), Healthcare IoMT Security, Privacy Protection, decentralized learning, primary cybersecurity threats, edge computing, FL.

2.4. Sources searched

Table 3 provides an overview of the literature search strategy used across five prominent research databases: ScienceDirect, ACM Digital Library, Taylor & Francis, Springer, and IEEE Xplore. It lists the specific search strings used to retrieve articles related to IDS in the context of smart hospitals and the IoMT. The table also contains the number of search results from each database (239 articles) and specifies the publication date range to be covered (2020–2025).

2.5. Bibliographic analysis

Table 4 reflects a comprehensive summary of the bibliographic information for selected studies published between 2024 and 2025. It includes key details to aid in identifying and referencing relevant research articles.

2.6. Most cited research articles

The bar chart titled "Citation" displays the citation counts for different authors or groups of authors, derived from selected articles in a systematic literature review. A bar's height signifies the number of times its publication has been cited. Of particular interest are [64] and [65], which took the lead with a high citation of approximately 582 and 566, respectively. By considering the second-highest in citations [66], who has 436 citations and is considered the third highest in citation record. Others, such as [67] and [68], they have their citations above 300. In contrast, [53] has the fewest citations on the chart, at approximately 5. Generally, this graph represents the relative influence and scholarly recognition of each paper quite well, providing important insights into how much each has been cited, which can help assess quality in the literature review process.

Fig. 3 represents the top ten reviewed studies with the highest number of citations. The reviewed paper. It is considered at the top with 582 citations.

2.7. Citation record

Table 5 highlights the number of citations of each selected paper for review. The citation count across the reviewed studies ranges from 5 to 582.

2.8. Inclusion and exclusion criteria

2.8.1. Inclusion criteria

- To reflect recent developments, studies released between 2020 and 2025 were included.

Table 3
Sources were searched across multiple databases, using the following search string.

Database	Search string	Search results	Duration
Science Direct	[All "intrusion detection system"] AND [All: "Smart Hospitals"] AND [All: "Cyber Attacks"] Research Articles	40	2020-2025
ACM Digital Library	[All: [all: intrusion detection]] AND [All: [all: IoT in smart hospitals]] AND [All: [all: federated learning]]	5	2020-2025
Taylor & Francis	[All: intrusion detection system] AND [All: iomt]	63	2020-2025
Springer	[All: Threat detection in smart healthcare]AND [All: Edge computing intrusion detection for IoMT] Articles+ Research Articles+ Subject (IoMT)	79	2020-2025
IEEE Xplore	("All Metadata": cyber security attacks) AND ("All Metadata": intrusion detection) AND ("All Metadata": internet of medical things) Journals	52	2020-2025
Total		239	

Table 4
Bibliographic data of selected studies from 2024–2025.

Reference	Database	DOI
(R. M. Czekster et al., 2025)	ScienceDirect	https://doi.org/10.1016/j.iot.2024.101437
[54]	ScienceDirect	https://doi.org/10.1016/j.jpdc.2024.104934.
[52]	Science Direct	https://doi.org/10.1016/j.ijcip.2023.100658
[50]	Science Direct	https://doi.org/10.1016/j.jer.2024.12.003
[49]	ACM	https://doi.org/10.1016/j.cose.2024.104288
[55]	Springer	https://doi.org/10.1007/s10462-024-11101-w
[56]	IEEE	https://doi.org/10.1109/TCE.2025.3544885
[57]	IEEE	https://doi.org/10.1109/JIOT.2023.3327024
[58]	IEEE	https://doi.org/10.1109/JIOT.2023.3325822

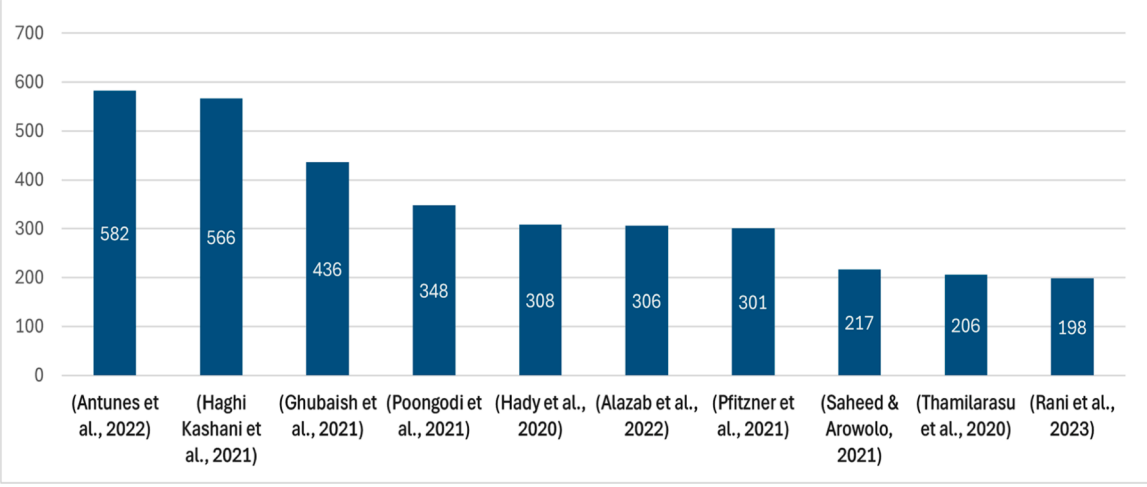


Fig. 3. Top 10 most cited papers in selected studies.

- Due to language proficiency, only English-language publications were included.
- The studies that were specifically relevant to the goals or research questions were included.
- To ensure credibility, only peer-reviewed papers from reputable journals were included.
- To maintain relevance, only studies that focus on IDS in the context of IoMT were included.

2.8.2. *Exclusion criteria*

- Studies released before 2020 were not included because they do not fall within the selected time frame.
- Due to language barriers, studies published in languages other than English were not included.
- To keep things focused, papers that did not answer the research questions or objectives properly were disqualified.
- Studies without empirical data, abstracts, and non-peer-reviewed sources were not included.
- The studies focusing on generic IoT (Internet of Things) were excluded, as they do not address the specific challenges and requirements of IoMT.

Fig. 4 clarifies the Inclusion and exclusion criteria for selecting research studies. Multiple parameters were used in this process, which are clearly defined in the figure.

2.9. *Record extraction*

Several research studies have been conducted in the past related to IDS for IOMT in smart hospitals. To select the study, databases are Science Direct, ACM Digital Library, Taylor & Francis, Springer, and IEEE Xplore. While extracting data from the 32 studies we reviewed, we aligned each study with the research question(s) it addressed. The RQ categories were overlapping rather than mutually exclusive because a single study could provide evidence for multiple research questions. As a result, the total of the per-RQ counts might surpass the overall number of included studies.

Table 5
Citation record of selected research papers.

Title	Author	Year	Citation
Federated Learning for Healthcare: Systematic Review and Architecture Proposal	[64]	2022	582
A systematic review of IoT in healthcare: Applications, techniques, and trends	[65]	2021	566
Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security	[66]	2021	436
Smart healthcare in smart cities: wireless patient monitoring system using IoT	[67]	2021	348
Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study	[68]	2020	308
Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions	[69]	2022	306
Federated Learning in a Medical Context: A Systematic Literature Review	[70]	2021	301
Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms	[71]	2021	217
An Intrusion Detection System for Internet of Medical Things	[72]	2020	206
Federated learning for secure IoMT applications in smart healthcare systems: A comprehensive review	[61]	2023	198
Deep Learning in the Security of the Internet of Things	[73]	2022	180
Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets, and Cloud–Fog–Edge architectures	[60]	2023	137
Internet of medical things: A systematic review	[51]	2023	127
An investigation and comparison of machine learning approaches for intrusion detection in the IoMT network.	[74]	2022	98
Edge-Based Hybrid System Implementation for Long-Range Safety and Healthcare IoT Applications	[75]	2021	97
Intelligent Intrusion Detection Based on Federated Learning for Edge-Assisted Internet of Things	[76]	2021	88
Federated Learning for Healthcare Applications	[58]	2024	76
AI-driven IoT for smart health care: Security and privacy issues	[77]	2022	73
Improving the Accuracy of Network Intrusion Detection Systems in Medical IoT Systems through Butterfly Optimization Algorithm	[78]	2021	52
Attack Detection for Medical Cyber-Physical Systems: A Systematic Literature Review	[79]	2023	42
Meta-IDS: Meta-Learning-Based Smart Intrusion Detection System for Internet of Medical Things (IoMT) Network	[54]	2024	37
An Intelligent and Explainable SaaS-Based Intrusion Detection System for Resource-Constrained IoMT	[57]	2024	35
A comparative study of cybersecurity intrusion detection in healthcare systems	[52]	2024	22
A comprehensive and systematic literature review on intrusion detection systems in the Internet of Medical Things: current status, challenges, and opportunities	[55]	2025	20
Automated detection of cyber attacks in healthcare systems: A novel scheme with advanced feature extraction and classification	[49]	2025	17
Internet of things in Healthcare: a conventional literature review	[59]	2023	16
Improving Security Architecture of Internet of Medical Things: A Systematic Literature Review	[80]	2023	16
Internet of Things (IoTs) Security: Intrusion Detection using Deep Learning	[81]	2021	11
Enhancing IoMT network security using ensemble learning-based intrusion detection systems	[50]	2024	6
A Resource-Efficient Federated Learning Framework for Intrusion Detection in IoMT Networks	[56]	2025	6
Dynamic risk assessment approach for analysing cybersecurity events in medical IoT networks	[53]	2025	5

2.10. Quality assessment

Evaluation of quality gauges the calibre of the papers selected for systematic reviews. To evaluate the chosen paper's quality, SLR uses a quality assessment process. A questionnaire intended to gauge the caliber of the chosen paper is used in this SLR. An evaluation of quality was conducted in the prior mapping research [82,83]

a) The research study discussed the primary cybersecurity threats faced by IoMT devices in smart hospitals. The possible answers in this regard were "Yes" (+ 1), "Partially" (+ 0.5), and "No"(0).
b) The research study clearly expresses that the IDS helps to mitigate Cybersecurity threats. The possibility of answers in this regard will be “Yes” (+ 1), “Partially” (+ 0.5), and “No” (0).
c) The research study clearly discusses the resource limitations in IoMT devices. The possibility of answers in this regard will be “Yes” (+ 1), “Partially” (+ 0.5), and “No” (0).

Continue4a) CORE rating conference papers and SCImago Journal Rank (SJR) lists will be used to assess the responses to these questions. The table displays potential options for journals and conferences.

2.10.1. SCImago journal rank

The journals' quality reputation is gauged by the SCImago Journal Rank (SJR).

2.10.2. Quality criteria SJR sources ranking score

In Table 6, the quality of the selected literature can be evaluated to ascertain its relevance to the journal.

Table 7 presents the quality assessment of the 32 selected papers, with columns "a, b, and c" detailing the questions used for quality assessment. Column "d" represents the Quartile of each paper (Q1-Q4), which is further discussed in Table 6.

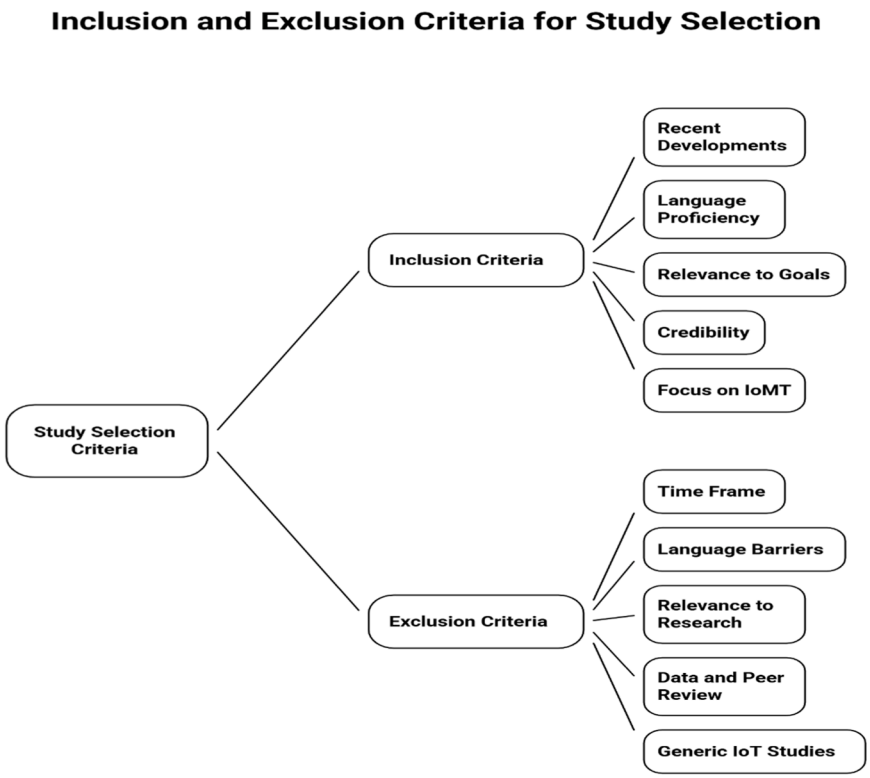


Fig. 4. Inclusion and exclusion criteria for the selection of research studies.

Table 6
Criteria for source ranking score of selected studies.

Source type	Ranking classification	Assigned quality score
Journal	Q1	2
	Q2	1.5
	Q3 or Q4	1
	Not indexed in SJR	0
Conference	CORE A	2
	CORE B	1.5
	CORE C	1
	Not listed in CORE ranking	0

2.11. Final record included

To refine the final selection of records, several electronic databases, including Science Direct, ACM Digital Library, Taylor & Francis, Springer, and IEEE Xplore, were systematically searched using multiple keywords relevant to the main topic. Most of the reviewed papers scored highly in the quality assessment, with several achieving the full 5 out of 5, indicating detailed research aims, solid methodologies, strong future relevance, and reputable publication venues. Papers such as [70] and [80] exemplified this standard. Some papers, e.g., [79] and [50], had a minimum rating of 4, indicating minor restrictions, generally in methodological transparency or future relevance. Overall, the studies included are of strong literature in this systematic review.

2.12. Criteria for judging risk of bias

A total of 32 studies were identified to meet the requirements of the literature review. The 5-bias domains (D1–D5) are rated for each study, with these outcomes categorized as High, Some concerns, and Low. Parsing the domains and providing a brief caption for the plot:

Table 8 is based on the criteria used to evaluate the risk of bias in selected studies. It highlights the complete criteria by domain (D1–D5) and then the overall risk.

Regarding the risk of bias in the included studies shown in Fig. 5, each study was rated as high, low, or moderate risk across the

Table 7
Quality assessment table of all selected studies from 2020–2025.

Sr No	References of selected studies	Source	Year	Quality assessment				
				a	b	c	d	a+b+c+d=Score
1	[79]	Survey	2023	1	1	1	2	5
2	[54]	Journal	2024	1	0.5	1	2	4.5
3	[73]	Journal	2022	1	0.5	1	2	4.5
4	[68]	Journal	2020	1	0.5	1	2	4.5
5	[69]	Journal	2022	1	0.5	1	2	4.5
6	[70]	Journal	2021	1	1	1	2	5
7	[72]	Journal	2020	1	1	1	2	5
8	[84]	Journal	2020	1	1	1	2	5
9	[71]	Journal	2021	1	1	1	2	5
10	[53]	Journal	2025	1	1	1	2	5
11	[55]	Journal	2025	1	1	1	2	5
12	[74]	Journal	2022	1	1	1	1.5	4.5
13	[77]	Journal	2022	1	1	1	1.5	4.5
14	[51]	Journal	2023	1	1	1	2	5
15	[75]	Journal	2021	1	1	1	2	5
16	[67]	Journal	2021	1	1	1	1.5	4.5
17	[81]	Journal	2021	1	1	1	1	4
18	[65]	Journal	2021	1	1	1	2	5
19	[66]	Journal	2021	1	1	1	2	5
20	[56]	Journal	2025	1	1	1	2	5
21	[57]	Journal	2024	1	1	1	2	5
22	[49]	Journal	2025	1	1	1	2	5
23	[78]	Journal	2021	1	1	1	1.5	4.5
24	[64]	Journal	2022	1	1	1	2	5
25	[58]	Journal	2024	1	1	1	2	5
26	[59]	Journal	2023	1	1	1	2	5
27	[52]	Journal	2024	1	1	1	2	5
28	[61]	Journal	2023	1	1	1	2	5
29	[60]	Journal	2023	1	1	1	2	5
30	[50]	Journal	2024	1	1	1	1	4
31	[76]	Journal	2021	1	1	1	1.5	4.5
32	[80]	Journal	2023	1	1	1	2	5

Table 8
Criteria of risk of bias with domains and evaluation.

Domain	Evaluation
D1: Bias from Randomization	Evaluates whether randomization was appropriate to avoid bias in selection. A + is for randomization, - denotes some concerns (problems), X means no randomization.
D2: Interventions Cause Deviation that Leads to Bias	Investigate whether IDS systems or Edge FL applications were consistently used. A '+ ' refers to applied consistently; '-' represents not applied consistently, and X=not consistently applied.
D3: Bias from Missing Data	Tests the possible impact of missing data (e.g, device logs, training data) on the results. (+) no missing, (-) significant amounts of missing; (X) very adversely affected results.
D4: Bias in Outcome Measurement	Focuses on the reliability and validity of IDS efficacy assessments. A '+' represents dependable results, '-' represents inconsistency, and 'X' means poor measurement.
D5: Bias in Reported Results	Examine if only statistically significant results were published. A '+' denotes that all results were reported; a '-' indicates selective reporting, and X means that selective reporting occurred.
Overall:	By examining these, we can develop a more holistic understanding of the study design, implementation, and reporting that may affect the reliability of the findings. Apart from the direct risks of performance and detection bias, more effort may also need to be directed towards reducing other biases in these fields so that we can have less biased, more reliable, and generalizable evidence regarding the effectiveness of IDS for IoMT.

following five principal domains. Regarding randomization bias, most studies were ranked as low risk, indicating appropriate strategies for randomization to prevent selection bias. Nonetheless, there was some suggestion that bias may have occurred due to a departure from the intended intervention. That indicates that, in some instances, studies had significant difficulty delivering the same interventions, potentially affecting the results. It is also a concern in some studies that one may be looking at bias due to missing outcome data (i.e., attrition bias), where reasons for data loss or dropout might have affected the study results. Measurement bias in the outcome was a second domain, with some studies at high risk of bias due to inconsistent measurement or recording. Finally, reporting bias in the selection of reported results was also described, notably in studies that selectively reported positive results, potentially leading to overestimation of efficacy.

In Fig. 6, the domains assess various aspects of study methodology: (D1) bias arising from randomization and (D2) bias due to

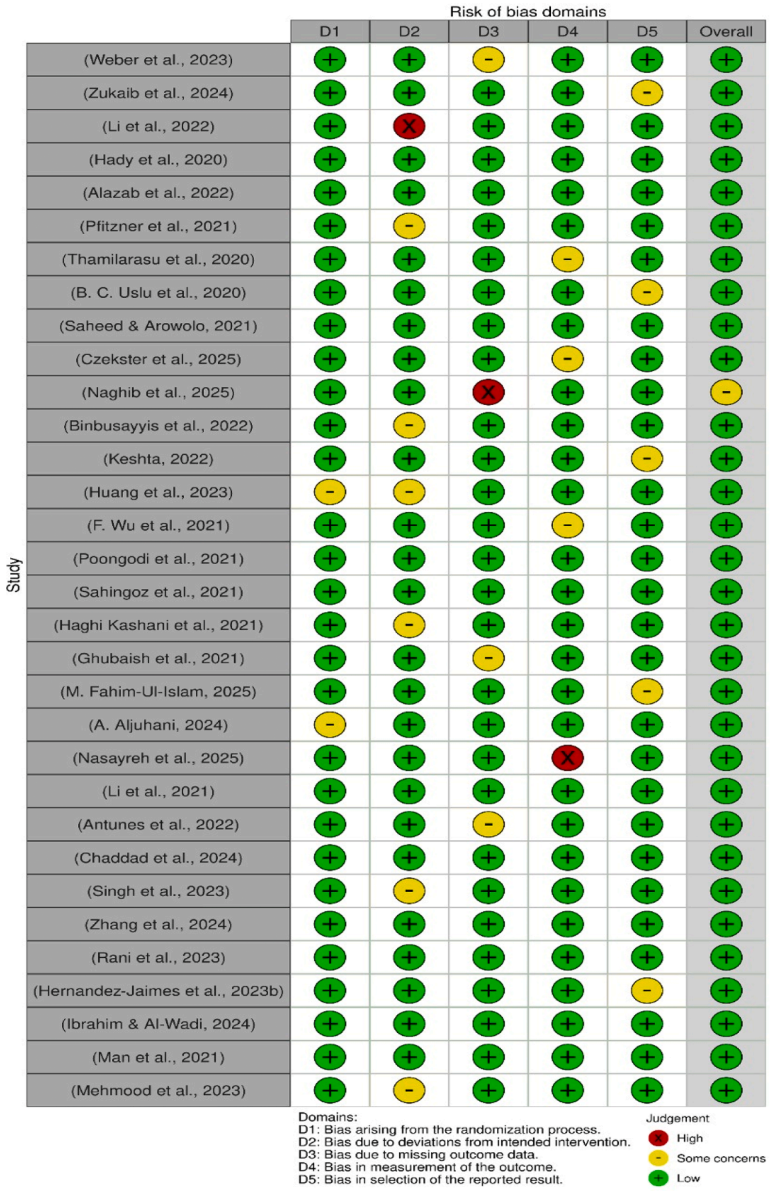


Fig. 5. Risk of bias assessment for quality evaluation of included studies. The chart shows the evaluation of five bias domains (D1 to D5) across the studies, with indicators representing low risk (green), some concerns (yellow), and high risk (red) for each domain, as well as the overall risk of bias for each study.

deviations from the intended intervention. The (D3) bias due to missing outcome data, (D4) bias in the measurement of outcomes, and (D5) bias in the selection of reported results. Each domain is rated as low, some concerns, or high risk, providing a comprehensive view of the methodological quality and reliability of the studies included in the review.

3. Results

Table 9 presents the results of the research questions, summarizing the analytical findings derived from the selected research studies and addressing the key hypotheses or inquiries posed in the study. These results provide insights into the research outcomes, supporting or refuting the proposed theories or objectives.

Table 10 highlights commonly used datasets, their accuracy comparisons, and the ML/DL models used on them. It also includes the strengths and weaknesses of the datasets.

Fig. 7 presents a comparison among multiple datasets and commonly used ML/DL Models, along with their accuracies. It also clarifies the difference in accuracy between the balanced and imbalanced BOT-IOT datasets.

While multiple datasets are often used for IoMT benchmarking, as shown in Table 10, only a few of them capture true medical realism. The public benchmark datasets (e.g., CICIDS2017, NSL-KDD, and Bot-IoT) remain the most widely used. They are readily available and provide high-accuracy values in the published literature [52,74,76]. Their clinical relevance and ability to mimic real healthcare settings remain inadequate. On the other hand, some datasets, such as WUSTL-EHMS 2020 and ECU-IoHT, contain actual or partial hospital IoT data, thereby adding greater medical realism [49,52].

However, the number and scale of such medically grounded datasets are limited. This imbalance poses a major concern for IoMT clinical deployment, as IDS models trained and validated on non-medical datasets may report overestimated performance metrics that do not generalize in the healthcare domain. Thus, the unavailability of standardized, medically realistic benchmark datasets impacts the credibility, comparability, and clinical applicability of IoMT security solutions.

3.1. Taxonomy diagram

Fig. 8 shows the security framework for the (IoMT), defined by a multi-faceted taxonomy that addresses the unique challenges of healthcare environments. The Detection Paradigm dictates the threat identification method, ranging from deterministic approaches like Signature-Based IDS, which relies on static rule-searching for known attacks, and Specification-Based IDS, using predefined behavior profiles for medical devices, to probabilistic approaches like Anomaly-Based IDS, which employs ML/DL-based techniques for behavior modeling to detect unknown attack theories. Many recent systems rely on a Hybrid IDS to integrate all the mentioned methods. Deployment The Deployment Architecture specifies the placement and capability of a system that includes DL-IDS (Deep Learning-based Intrusion Detection System) with ultra-lightweight models for real-time protection on light-weighted devices, supplemented with GW(Gateway)/Fog/Edge IDS for protecting against attacks (e.g., DDoS) having low-latency requirements, and CL/HD-IDSS (Centralized Learning/Hybrid Distributed-Intrusion Detection and Security System(s)) support testing in computation-intensive environments like FL aggregation. These systems can also be organized as a Cooperative IDS to facilitate coordinated cross-node attack and intrusion detection in a large hospital environment. Lastly, the Intelligence Model yields analytical power from essential ML models that rely on feature engineering to state-of-the-art DL models with high accuracy, and also leverages FL to achieve privacy-preserving collaboration, without centralized data. A critical component of the IoMT is Edge AI/Tiny ML for real-time detection and Explainable AI (XAI) to build trust with clinician users and meet healthcare regulations. This holistic method, in turn, provides a comprehensive, efficient, and privacy-enhanced threat defense for the entire IoMT ecosystem.

4. Discussion

RQ1. What are the primary cybersecurity threats faced by IoMT devices in smart hospitals?

IoMT devices are exposed to a variety of cybersecurity risks that can significantly affect patient well-being and data accuracy. One of the major challenges is data security, as IoMT devices store and transmit private patient information, making them a potential target for hackers seeking to steal PHI (Protected Health Information) [67,81]. Another significant risk is Man-in-the-Middle (MITM) attacks, in which adversaries may eavesdrop on and even modify communication between IoMT devices and central servers, resulting in unauthorized access or data tampering [68,81].

Moreover, all types of DoS and DDoS attacks are major threats, as they can flood IoMT devices with malicious traffic. In this situation, critical facilities may be unavailable, and hospital services may be disrupted [81]. Device hijacking is a further risk in which hackers leverage IoT devices' vulnerabilities to gain control, taking over and infiltrating hospital networks [68,81]. There are also numerous reports of malware and ransomware attacks. Where malicious software can penetrate a hospital's IoMT systems, encrypt data while holding the hospital to ransom, leading to expensive loss of operational use [81]. Additionally, insecure interfaces are common in many IoMT devices, further worsening security issues. More often than not, these devices use insecure, outdated security practices, which can expose them to attack [81].

There are several weaknesses and limitations in the majority of surveyed studies on IoMT security in smart hospitals. One of the main limitations is that existing IDSs focus either on data flow or on biometric information to carry out the defense. However, none of them combine both into a complete defense [81]. Furthermore, scalability is an issue, and many solutions are not tailored to managing large-scale, dynamically evolving, and non-IID data generated by numerous IoMT devices across diverse healthcare settings [67]. Another significant limitation is the lack of testing in real-world scenarios, with most models built on idealized datasets such as NSL-KDD, which do not fully capture the sophisticated nature of real-world IoMT attacks in hospitals [81]. Regarding the contradictions here, some studies indicate a high detection capability against known attacks. While others can hardly detect unknown or rare (zero-day) attacks due to skewed data patterns and inadequate training [54,68]. This lack of granularity, inherent inconsistencies, and other deficiencies underscore the necessity for holistic, scalable, and flexible security frameworks. Those are capable of mitigating dynamic and diverse cybersecurity threats in healthcare IoMT settings.

This work presents a new perspective on security requirements in smart hospital scenarios by highlighting the importance of lightweight, flexible, and privacy-preserving IDS frameworks. It is this pressing need to move away from traditional, generic IDS models towards lightweight, flexible, and legally compliant solutions. Those have been explicitly tailored for smart hospital IoMT infrastructures, which motivates the novelty.

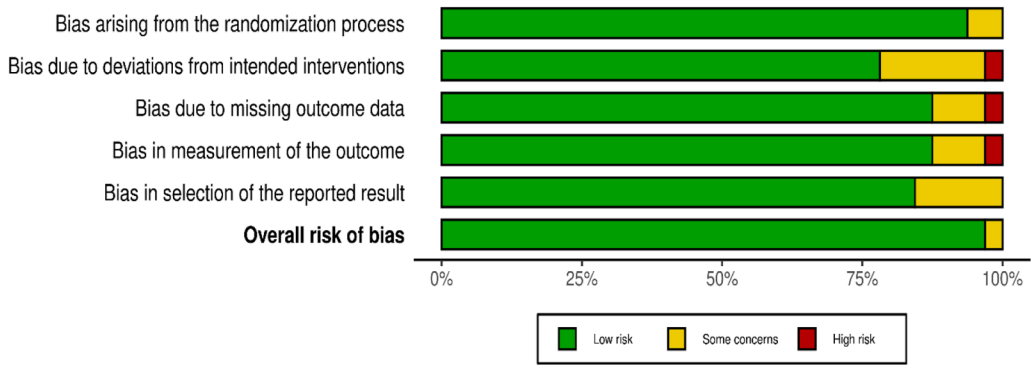


Fig. 6. This chart illustrates the evaluation of the risk of bias across five key domains (D1 to D5).

As shown in Table 11, the deployment and use of interconnected medical devices increase the risk that intelligent healthcare systems will be affected by cybersecurity threats. It includes ransomware threats, data breach risks, and device hijacking. That all of them exist in a world where legacy protocols, constrained device resources, and uneven security standards abound does not help matters. The state-of-the-art advancements in attention are centered on AI-based intrusion detection, lightweight real-time monitoring, and privacy-preserving solutions, such as FL, to mitigate these concerns. In particular, to provide strong, high-quality health protection in difficult situations with limited resources, a paradigm shift towards full-stack security from the hardware level up to the cloud level should be achieved.

Among the 32 selected studies, the 14 studies mainly concern DDoS, MitM, and Ransomware threats. These are recognized as among the highest risks affecting the availability of smart hospital services. The other 10 studies relate to data privacy, leakage, and storage lifecycle; a clear trend is evident towards adopting Federated Learning (FL) and decentralized frameworks. In addition, 5 studies provide specialized insights about hardware vulnerabilities of resource-constrained edge devices, legacy protocols, and unprotected emergency systems. Finally, 3 studies point towards the emergence of specialized risks, such as Adversarial AI.

RQ2. How can IDS help to mitigate Cybersecurity threat risks?

IDS provides strong assistance in coping with cyber threats for a smart hospital, as it offers early detection and response to attack patterns. IDSs can track network traffic in real time to detect anomalous behavior, such as man-in-the-middle attacks, DoS attacks, or device hijacking, and intervene quickly before these threats cause significant damage [81]. Through anomaly-based detection, the IDS can recognize previously unknown threats, such as zero-day attacks, by detecting behaviors that deviate from normal behavior [67]. In addition, IDS can help protect patient data by implementing access controls and preventing rogue devices from handling sensitive patient information [54]. IDS based on FL can enhance data privacy by training models on devices and not sharing users' personal information, thereby protecting IoMT networks with high detection accuracy [81]. On the whole, IDS enhances the security of IoMT systems through continuous surveillance, detection, and response to cyber threats, thereby minimizing data breaches, system downtime, and unauthorized access.

The IDS is necessary to mitigate cybersecurity risks in smart hospitals; however, some weaknesses, limitations, and contradictions have been identified in the literature. One weakness is that many IDSs focus exclusively on network-based and biometric data security, with little or no integration between the two to provide a comprehensive defense [76]. This division leaves open potential blind spots when facing complex cyber threats that could potentially exploit both data flows. One of the major shortcomings of most IDS solutions is their failure to scale efficiently when processing the large, dynamic data generated by heterogeneous IoMT devices in a hospital. One of the most common examples in FL-based IDS is non-IID data, along with resource constraints, which occur in healthcare-related IoTM devices [54]. In addition, we found inconsistencies when comparing the effectiveness of different IDS methodologies. Some studies report high precision in detecting known attack types; however, they do not detect new or zero-day attacks, which are difficult to categorize with conventional training techniques [66]. This paradox highlights a deficiency in the existing IDS: imbalanced datasets and insufficient training prevent systems from adapting to novel threats. These limitations require better models that can properly operate in the complex space of smart hospital scenarios to achieve, at least against all APT vectors, more robust detection.

This paper presents a novel approach to enhancing IDS in smart hospitals by addressing the main drawbacks of existing models. Comparison to Existing IDS Although current IDS are primarily targeted at network or biometric data security. We highlight that both may be combined in an integrated approach to face multi-dimensional cyber threats. It also sheds light on the potential problems of scalability and non-IID data in FL-based IDS, which are typically expected in resource-limited healthcare IoMT systems. By proposing more adaptive and scalable IDS solutions, this study aims to improve real-time threat detection and data privacy. It also ensures robust security across diverse IoMT devices in smart hospitals.

According to Table 12, contemporary intrusion detection techniques in smart healthcare systems focus on developing adaptive,

Table 9
Results of the research questions based on the selected research paper.

Reference	Year	Primary cybersecurity threats in IoMT	Cybersecurity threats mitigation in IoMT	IoMT resource limitations in smart hospitals	Decentralized learning techniques in IoMT security	Role of edge computing in enhancing IDS performance
[55]	2025	Data breaches, device hijacking, DDoS (Distributed Denial of Service), ransomware, malware, MitM (Man-in-the-Middle), SQL (Structured Query Language) injection, extortion, firmware attacks	Strong security protocols, continuous monitoring, regular updates, designing IDS (Artificial Intelligence, ML, DL based), decentralized detection.	Low memory, low computational and storage capabilities, energy constraints, and inability to apply traditional security methods.	FL approaches are discussed to overcome privacy and computation constraints. Decentralized learning minimizes data transfer to central servers. Models train locally on individual and edge devices. Raw data remains on local devices, enhancing privacy.	The integration of edge-fog-cloud architectures in IoMT enhances latency reduction, real-time data processing, and localized IDS deployment, while introducing challenges related to interoperability, scalability, and security across layers.
[81]	2021	Malware and ransomware attacks Unauthorized access and data breaches threaten. Multi-layered attacks complicate security measures in IoMT systems.	ML-based IDS improves intrusion detection by leveraging advanced algorithms. Achieved Accuracy:99.90 %, F1 Score: 99.90%, Recall:99.90%, Precision: 99.90%.	Limited resources restrict IoMT security. Network connectivity issues hinder device communication and data transfer. Energy constraints impact device longevity and operational efficiency.	FL preserves data privacy by keeping data local, while collaborative learning enhances IoMT security through shared insights without compromising confidentiality.	Edge computing facilitates real-time security, enabling faster threat detection and response, which significantly strengthens the system's resilience.
[67]	2021	The paper explicitly mentions DDoS attacks as extremely dangerous in the context of smart healthcare systems.	ML-IDS improves IDS by using machine learning algorithms, while regular updates ensure the continuous enhancement of IoMT security by addressing new threats and vulnerabilities.	Low resources limit security High cost restricts protection.	FL preserves privacy by keeping data decentralized, while collaborative learning enhances security by enabling shared insights without compromising sensitive information.	Real-time, local threat response enhances IoMT security by enabling immediate action at the edge, reducing latency, and improving the system's ability to detect and mitigate attacks quickly.
[76]	2021	Unauthorized access risks and malware/ ransomware threats pose significant challenges to IoMT security, compromising data integrity and system functionality if not effectively mitigated.	ML-based IDS protection Regular updates are vital. FedACNN. It employs a convolutional neural network (CNN) model. Accuracy: 99.12%, Precision: 99.50%, Recall:99.10%, F1 Score: 99.40%.	Limited resources, high cost.	FL enables secure model training without sharing raw data. Clients use local data to train models in edge networks. Attention mechanisms enhance parameter aggregation in decentralized learning. Decentralized techniques improve security and privacy in IoMT applications.	It reduces latency in network communication services. Edge computing enhances data privacy protection. It alleviates bandwidth limitations of traditional cloud computing.
[66]	2021	Network attacks include Man-in-the-Middle and sniffing attacks. Attacks aim to steal or fabricate patient data. Security in IoMT systems is a major challenge.	ML/AI-based detection Encryption authentication protocols.	IoMT sensors have processing and storage limitations. Need lightweight security.	Decentralized learning techniques enhance IoMT systems' security. Improve data confidentiality and integrity. Techniques include ML and blockchain technology. These methods tolerate attacks like Denial-of-Service.	Local data processing Real-time threat response.
[54]	2024	Successful attacks can lead to severe consequences, including loss of patient lives.	ML-based IDS detection Encryption, strong authentication. WUSTL-EHMS-2020: 99.47%	Low power, memory limits Need lightweight security addressing challenges	(FL) aims to protect privacy by keeping data local.	Local, real-time processing Supports dynamic environments.

(*continued on next page*)

Table 9 (*continued*)

Reference	Year	Primary cybersecurity threats in IoMT	Cybersecurity threats mitigation in IoMT	IoMT resource limitations in smart hospitals	Decentralized learning techniques in IoMT security	Role of edge computing in enhancing IDS performance
			IoTID20: 99.98% WUSTL-IIOT-2021: 99.99% Remarkable accuracy rates of 99.57%, 99.93%, and 99.99% for signature-based detection. Techniques include signature-based rules and network-traffic anomalies.	such as environmental variations and diverse data sources, which are critical for deployment in real-world scenarios.		
[68]	2020	Data breaches, device compromise Patient safety at risk.	ML-based IDS detection Real-time threat response. Accuracy: 93.50%, F1 Score: 92.60%, Precision: 92.80%, Recall: 92.60%.	Limited power, memory Traditional security is unsuitable.	FL ensures privacy by enabling local training on devices, where sensitive data stays on the device rather than being transferred to centralized servers, significantly reducing the risk of data.	Real-time edge processing Low latency, fast response.
[59]	2023	Cybersecurity threats include data breaches and unauthorized access. Vulnerabilities in devices can lead to exploitation by attackers.	ML-based IDS systems Real-time intrusion response Encryption and authentication are essential.	IoT healthcare applications face energy efficiency challenges. Security and privacy issues hinder patient data management.	Localized model training Privacy-preserving learning.	On-device threat analysis Fast, low-latency response.
[51]	2023	Unauthorized data access Device integrity compromise. IoMT systems face risks of data abuse and misappropriation. Sensitive health data is vulnerable to hijacking and tampering.	ML-based IDS solutions Encryption and authentication.	Limited processing and memory Resource-heavy security is unfit. Insufficient policies for data privacy and security in IoMT.	FL enhances privacy. Localized model training.	Real-time local processing.
[78]	2021	Unauthorized data access Device attacks risk safety.	Mitigate IDS using an Artificial Neural Network (ANN). A Butterfly Optimization Algorithm (BOA).Best Model - BOA-ANN): 93.27% accuracy.	Limited power, memory Traditional security is unsuitable.	FL secures data by keeping it decentralized on local devices, ensuring that sensitive information never leaves the device.	On-device threat detection Real-time response enabled.
[61]	2023	Unauthorized access, malware Network/data integrity threats	Encryption, IDS, and authentication Secure data, device integrity. IoMT-based datasets with Accuracy:99.90%, F1 Score: 99.80%, Precision: 99.90%, Recall: 99.80%	Limited power and memory Security implementation challenges	FL enhances privacy by avoiding centralized data compilation. Keyless techniques, such as blockchain, secure IoMT systems. FL supports collaboration among hospitals for model training.	Real-time threat response
[64]	2022	Data leaks, malware, and weak networks.	It is a decentralized methodology that enables the distributed training of ML models. FL helps systems better align with regulatory requirements and improves trustworthiness and data sovereignty.	Low power, memory, and storage.	Local training enhances privacy by keeping data on the device, allowing models to be trained without transmitting sensitive information to centralized servers, thereby reducing the risk of data breaches.	Fast response and low latency are achieved by processing data locally or at the edge, minimizing delays and enabling real-time decision-making.
[69]	2022	Data breaches, malware, and network risks.	Encryption, IDS, and authentication.	Low power, memory, and battery constraints in IoMT devices limit the complexity and efficiency of IDS.	Core focus is on (FL) as a decentralized data concept.	Real-time detection, low latency.

(*continued on next page*)

Table 9 (*continued*)

Reference	Year	Primary cybersecurity threats in IoMT	Cybersecurity threats mitigation in IoMT	IoMT resource limitations in smart hospitals	Decentralized learning techniques in IoMT security	Role of edge computing in enhancing IDS performance
[70]	2021	Unauthorized access, malware.	Encryption, IDS, and authentication. Electronic health records (EHR) data are used. Accuracy: 99.40%.	Low power, memory, and battery limits.	Local training, privacy, and security. FL focuses on the client-server model and model aggregation.	On-site processing, fast detection.
[58]	2024	Unauthorized access, malware, and network flaws.	Encryption, IDS, and authentication work together to ensure data privacy, detect intrusions, and verify authorized access, forming a comprehensive security framework for IoMT systems.	Low CPU, memory, and battery.	FL enhances data privacy in IoMT. FL trains local models without sharing raw data. Security risks include backdoor and Byzantine attacks.	Local processing, fast response.
[50]	2024	Data theft, device tampering, and DoS (Denial of Service) attacks.	Mitigation is achieved by developing a robust IDS using an Ensemble Learning approach. Accuracy: 0.9960 (or 99.60%) Time Completion: 12.42.	Low power, memory, battery.	FL plays a crucial role in enhancing data privacy by enabling decentralized model training.	Local processing enables fast response times by performing data analysis and decision-making directly on the device or at the edge of the network, reducing the need to send data to centralized servers.
[71]	2021	Unauthorized access, malware, and DoS attacks.	Encryption, IDS, and authentication. Deep Recurrent Neural Networks (DRNN) with traditional ML Accuracy: 99.96% (on the NSL-KDD dataset) Detection Rate (Recall): 99.96% False Alarm Rate: 0.04%.	Limited power, memory, and battery.	FL enhances privacy. Localized model training.	Edge computing is the natural deployment location for such a system to maximize its performance and ensure the real-time response required for critical medical systems.
[75]	2021	Unauthorized access.	Encryption, IDS, and authentication. Achieved minimal delay (11.5 ms) with LoRa (Long Range) and BLE (Bluetooth Low Energy) hybrid network. Accuracy:99.90%.	Low power, memory, and battery.	FL plays a crucial role in enhancing data privacy by enabling decentralized model training.	Local processing, fast threat detection.
[53]	2025	Unauthorized access, malware, and DoS attacks.	Strong encryption, advanced IDS, robust authentication.	Constraints in processing power, memory, and battery life.	The study focuses on the physical networking and energy solution for long-range communication..	Real-time threat detection by processing data closer to the source, enhancing overall security.
[77]	2022	Unauthorized access and data breaches in the interconnected ecosystem.	AI-based solutions and ensuring legal/ethical compliance. Key mitigation approaches: Strong encryption methods. Access control mechanisms. Using Blockchain for secure data sharing and privacy preservation.	limited computational capabilities and restricted battery life. These limitations pose a challenge to implementing complex security algorithms and robust encryption directly on the devices.	Emphasizing user feedback loops and collaborative training among edge devices.	Fog and Edge computing are essential for real-time data analytics and for supporting a large number of sensors and devices. Deploying IDS logic (AI models) closer to the data source (the edge) directly reduces latency and improves overall system performance.
[74]	2022	Threats stem from inherent security and privacy issues related to the IoMT architecture. The use of obsolete systems creates security	ML-based IDS, KNN (K-Nearest Neighbors), SVM (Support Vector Machine), ANN (Artificial Neural Network) Autoencoder Accuracy: 99.98% (on BoT-IoT	Need for efficient algorithms on constrained devices for limited battery life or memory of the devices.	Allows multiple devices to train ML models while keeping their data local collaboratively.	The approach addresses challenges such as data privacy, communication efficiency, and resource constraints, thereby

(*continued on next page*)

Table 9 (*continued*)

Reference	Year	Primary cybersecurity threats in IoMT	Cybersecurity threats mitigation in IoMT	IoMT resource limitations in smart hospitals	Decentralized learning techniques in IoMT security	Role of edge computing in enhancing IDS performance
		vulnerabilities that attract attackers.	dataset) Detection Rate (Recall): 99.99% False Alarm Rate: 0.03%			facilitating effective ML in edge environments.
[57]	2024	DDoS, MitM, ransomware, data breaches. Include malicious attacks and unauthorized access that exploit vulnerabilities in the network and devices.	Edge-deployed SaaS IDS using PSO (Particle Swarm Optimization), ML/DL, SHAP (Shapley Additive Explanations). Explainable AI (XAI) using(Shapley Additive explanations) SHAP values for transparency. (Hybrid IDS using PSO-Ensemble): Accuracy: 99.99% (on IoMT-IDS dataset) F1-Score: 99.98%.	Focus on reducing computational load using feature engineering. Deploying the heavy-lifting logic on the edge (to be near the source) and as a SaaS (to offload processing from individual devices).	use of edge computing and Software-as-a-Service (SaaS) deployment at the edge. Centralized/SaaS-based IDS deployed at the edge. Decentralized Learning Techniques like Federated.	Core to the approach, used for efficient local processing. This edge deployment is crucial for enhancing efficiency by performing analysis close to the source, reducing latency, and ensuring real-time response for intrusion detection.
[72]	2020	Connected medical devices create new attack surfaces, introducing a multitude of security and privacy concerns. Attacks can cause significant physical harm and life-threatening damage to patients.	Mitigation is achieved by designing a novel mobile agent-based IDS. The system uses distributed intrusion and anomaly detection algorithms that can run directly on low-powered devices. Values for Best Model IDS: True Positive Rate (Detection Rate): 99.98% (achieved by the system) False Positive Rate: 0.01%	Lightweight mobile agents to improve system efficiency and resiliency.	The paper designs and implements a novel mobile agent-based IDS that utilizes distributed intrusion and anomaly detection algorithms.	It effectively leverages edge computing principles to enable real-time monitoring and detection, thereby enhancing IDS performance by reducing latency and improving response time.
[84]	2020	Threats like unauthorized access to data, data breaches, and attacks that disrupt service continuity.	Structured layered IoMT architecture. Mitigation is integrated across the five-layer architecture.	The limited capacity of IoMT devices in terms of battery life, storage, and processing power is a major technical challenge.	Edge, Fog, and Mist Computing (Remote Services Layer).	Edge Computing. Edge computing is used to provide real-time processing, reduce latency, and manage the high volume of data from sensors.
[60]	2023	Unauthorized access, data breaches, outdated software, weak encryption, and unpatched vulnerabilities.	AI-powered IDS (ML/DL) detects anomalies, improves response, and adapts to IoMT challenges. It analyses high-performing models. IDS research often reports high accuracy (e.g., >99%) using ML/DL models.	Resource constraints necessitate lightweight, cloud-fog-edge adaptable IDS architectures.	Discussed in the context of distributed edge computing and data locality for privacy.	Crucial for reducing latency and improving IDS scalability in IoMT. Edge and Fog computing are vital for real-time IDS deployment and enhanced performance by reducing latency by performing detection closer to the data source.
[79]	2023	Challenges include device heterogeneity and diverse connectivity types. Common attacks reviewed.	Focus on an anomaly-based detection approach using various ML/DL models. Anomaly detection (44% of studies), followed by signature-based detection (18%).	Highlight constraints in energy, processing; IDS must be low-power and efficient.	Not explicitly addressed; implies need for contextual, adaptive detection strategies.	Deploying IDS logic at the edge (gateways or local networks) is critical for real-time detection.
[49]	2025	Smart device vulnerabilities, APTs (Advanced Persistent Threats), fake data injection, and	Proposes an LSTM (Long Short-Term Memory)-KNN-PCA (Principal Component Analysis) hybrid model for real-time anomaly detection	Addresses efficiency by using PCA-based feature reduction to reduce computational load.	edge computing, cloud nodes, and distributed data handling.	Edge Computing. Edge deployment would enable the proposed LGBM classifier to analyze traffic closer to the IoMT devices,

(*continued on next page*)

Table 9 (*continued*)

Reference	Year	Primary cybersecurity threats in IoMT	Cybersecurity threats mitigation in IoMT	IoMT resource limitations in smart hospitals	Decentralized learning techniques in IoMT security	Role of edge computing in enhancing IDS performance
		unauthorized control of IoMT devices.	with high accuracy. MI-LGBM): Accuracy: 99.98% (on various IoMT datasets) F1-Score: 99.98%			reducing latency and ensuring a real-time response.
[73]	2022	Vulnerabilities stemming from heterogeneity, low-security architecture, and connectivity risks.	Architecture and connectivity risks. Advocates DL-based IDS using anomaly detection and predictive analysis across applications, performance is reported to be as high as 99.99%	Highlights limitations of edge device memory/CPU (Central Processing Unit); suggests model optimization.	DL models trained to adapt at the edge level; implicit decentralized capability.	Key component enabling local intelligent decision-making and faster threat detection. Edge computing reduces latency in Intrusion Detection Systems (IDS). Edge computing supports scalable and flexible IDS architectures.
[65]	2021	Privacy threats, side-channel attacks, and unauthorized access.	Encryption, authentication, k-anonymity, public-key cryptosystems. The Security-based research category was the most frequent in the review, with 37% of the 146 selected articles.	The dynamic nature of IoMT environments poses resource challenges. Energy, bandwidth, computation, and storage constraints.	Local edge processing Fog computing Distributed scheduling and resource allocation Privacy-preserving data handling.	Proposed to overcome cloud latency and enable real-time decisions. Fog computing. Edge computing allows for latency and bandwidth utilization criteria.
[56]	2025	DoS, DDoS, ransomware, and MitM attacks on smart medical devices.	FL with KANConvNet (Kanban Convolutional Network), robust aggregation, and meta-learning. 99.98% (outperforms traditional KANConvNet and Federated CNN models). Loss Reduction: 6.75% lower loss compared to FedCNN.	Addressed using a lightweight FL model and reduced memory usage.	Core of the proposed system; FL used for private, distributed model training.	The entire FL framework is designed to run efficiently on the edge, where the consumer sensor devices are located. This deployment reduces latency and enables real-time attack detection, significantly enhancing the IDS's performance in a decentralized manner.
[52]	2024	Healthcare systems are prime targets for cyber attackers, leading to loss of patient data, disruption of surgical anesthesia, or even patient death. Common threats include ransomware (e.g., WannaCry, Conti) and attacks that exploit poorly secured IoMT devices, such as insulin pumps.	ML/DL models (e.g., XGB, LGB) enhanced by the Maximum Information Coefficient (MIC) feature selection method XGB Accuracy (WUSTL-EHMS-2020): 95.01% Accuracy (CICIDS2017): 99.76%.	Limited memory, processing power, battery life, and bandwidth.	FL with encryption is suggested as a solution for collaborative IDS across multiple medical institutions.	IDS can be deployed on cloud-based IoMT edge network-assisted devices. This deployment model allows for dynamic adjustment of computing resource allocation based on the current load, leading to more efficient utilization.
[80]	2023	Discusses threats such as data breaches, unauthorized access, and malware. The implementation of security controls addresses the identified vulnerabilities.	Talks about security frameworks, encryption, access control, and monitoring.	Mentions IoMT devices having limited computing, storage, and battery capacity. Insufficient power supply affects device performance and reliability.	Emphasizes local computation and monitoring. Promotes modular security controls adaptable to different IoMT nodes.	lightweight security mechanisms due to the limited processing power and memory of IoMT devices.

Table 10
Commonly used datasets in reviewed studies with quantitative metrics and their weaknesses and strengths.

Reference	Dataset	Dataset type	Medical realism	Model	Preprocessing	Features	Metrics	Latency	Weakness	Strength
[52]	CICIDS2017	Public Benchmark	N/A	Extreme Gradient Boosting (XGB)	Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), & LSTM + (CNN)	78	Accuracy = 95.01% F1= 95.01%, Precision= 94.94%, Recall= 95.01%	×	R epetitive lines affecting performance	Mainly includes benign and 14 common types of cyber attacks.
[76]	NSL-KDD	Public Benchmark	N/A	CNN Convolutional Layer (CL-CNN), Federated Adaptive Convolutional Neural Network (FedACNN) & Federated Averaging (FedAVG) (CNN)	Numerical encoding of character-based feature attributes Normalization of data values between	41	CNN (CL-CNN) Accuracy: 99.65% FedACNN Accuracy: 99.12% FedAVG (CNN) Accuracy: 98.90%	Low	Requires preprocessing before training models	It excludes redundant records, reducing classifier bias
[49]	WUSTL-EHMS 2020	Real Hospital IoT Data	High	KNN	Principal Component Analysis (PCA) for feature reduction	×	A chieved highest accuracy: 99.90%	×	C hallenges with the backpropagation algorithm instability	The proposed model achieved 99.9% accuracy in detecting threats.
[74]	Bot-IoT	Public Benchmark	N/A	KNN, Naïve Bayes, SVM (Support Vector Machine), ANN, and DT (Decision Trees)	Data Normalization & Data Transformation	46	KNN Imbalanced data Accuracy: 100% Balanced Data: Accuracy: 99.80%	×	C lass imbalance in the dataset	Publicly available for research purposes in 2018
[52]	ECU-IoHT	Real Hospital IoT Data	Partial	XGB, SVM, KNN, DT, DGBT (Decision Gradient Boosting Tree), RF, LGBM (Light Gradient Boosting Machine), LSTM, LSTM+CNN, GRU	The MIC (Maximal Information Coefficient) method for analyzing non-linear relationships.	fewer features	XGB got higher accuracy: 99.39%, F1: 99.37%, Recall: 99.39, Precision:99.37%	×	F ewer features	contains patient biometric data such as temperature, blood pressure, and heart rate
[49]	TON-IoT	Simulated Data	N/A	KNN	PCA for feature reduction,	×	K NN had an accuracy of 99.98%	Not defined clearly	There are 10 classifications, which makes the classification process difficult.	The model achieves amazing accuracy.

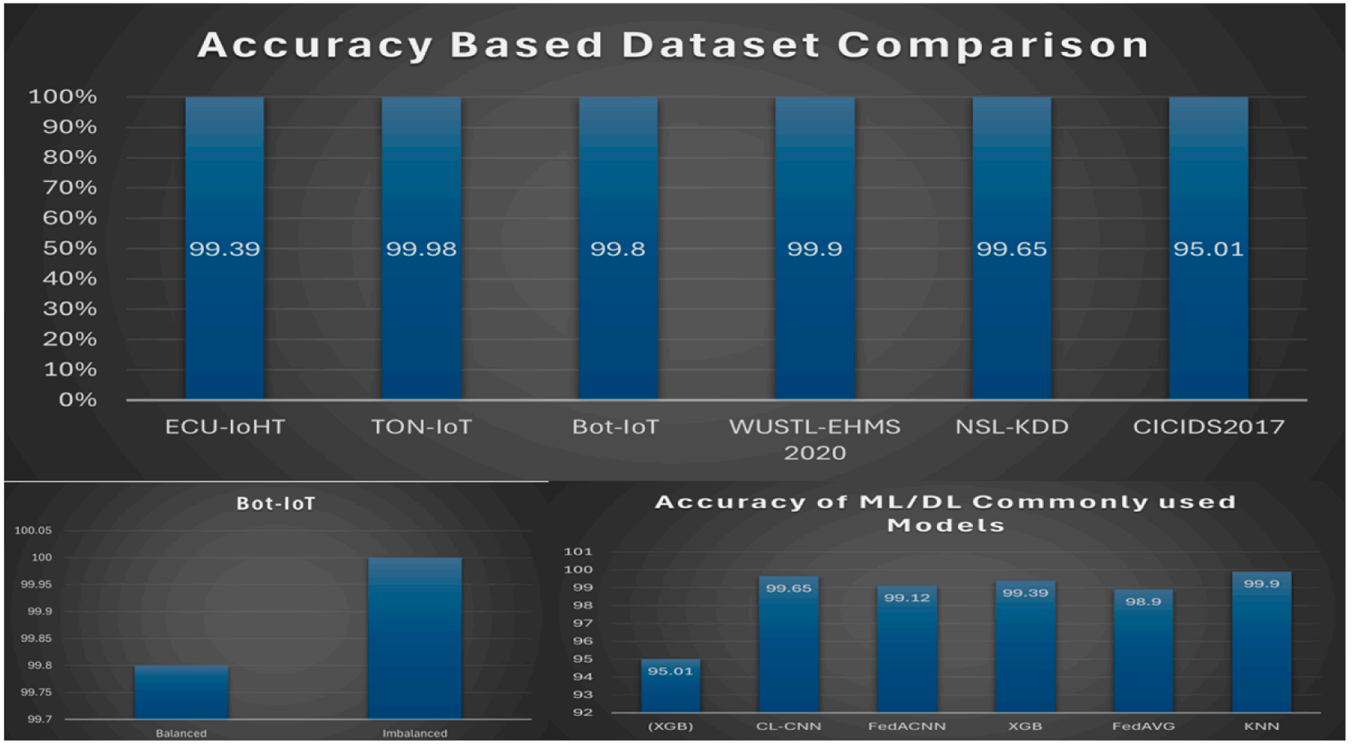


Fig. 7. Accuracy and model-based comparison between commonly used datasets and models.

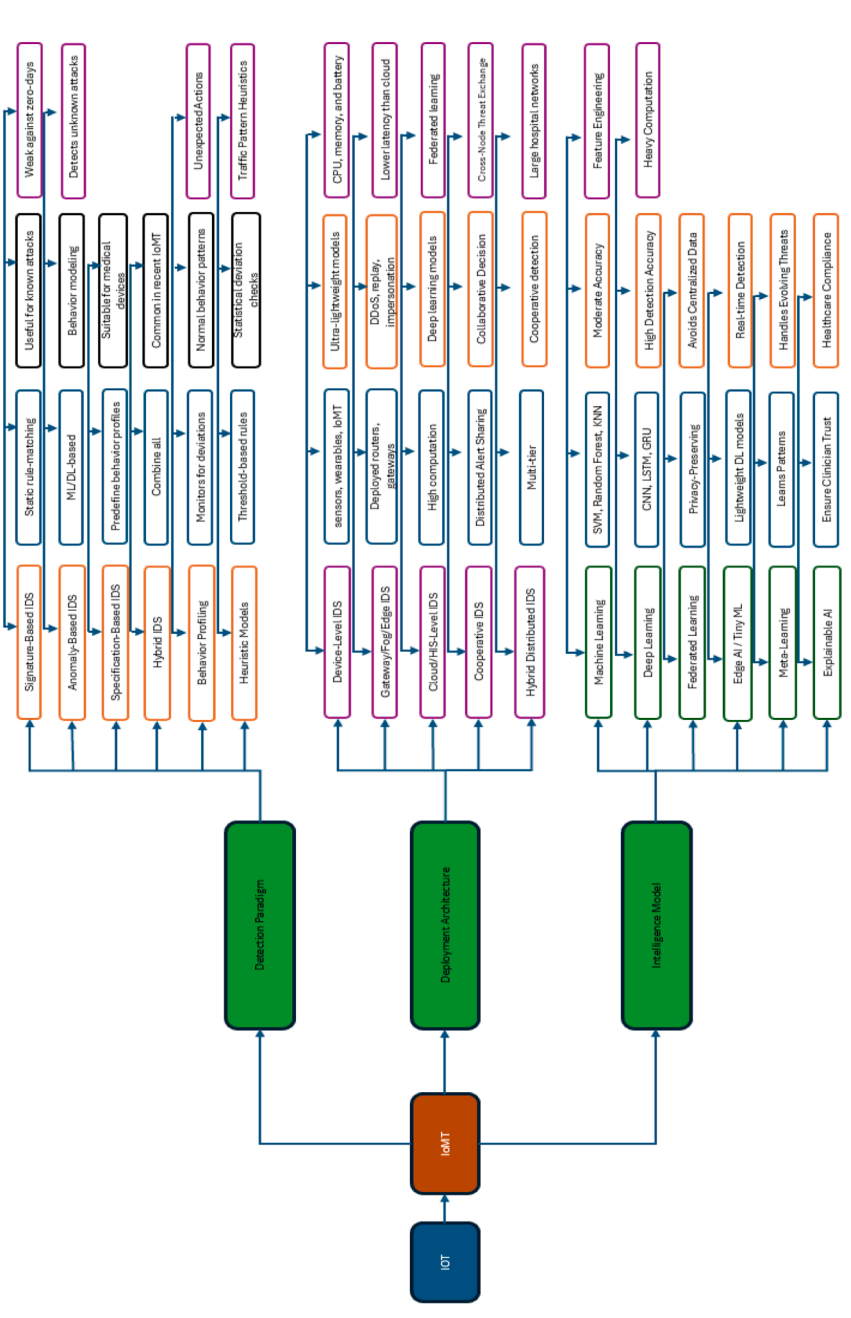


Fig. 8. Taxonomy diagram of IDS in IoMT.

Table 11
A critical analysis and comparative synthesis of RQ1.

References	Primary cybersecurity threats	Critical insights & trends	Comparative syntheses
[55]	Ransomware, device hijacking, MitM, DDoS, and firmware exploits.	AI-based IDS needed for heterogeneous and constrained IoMT.	Emphasizes the need for tailored, lightweight AI-IDS in critical environments.
[65]	Eavesdropping, replay attacks, and weak legacy devices.	Calls for stronger encryption, standardization, and access control.	Highlights risks from legacy tech and the lack of IoMT security standardization.
[56]	DoS/DDoS, adversarial ML, cloud vulnerabilities.	FL is proposed to protect privacy in AI training.	Suggests privacy-preserving ML as key to scalable, secure IoMT.
[77]	Access control flaws, data leaks, adversarial AI (Artificial Intelligence).	Advocates for regulatory frameworks and AI-aware security models.	Urges the architectural and governance standards.
[74]	Data injection, impersonation, and outdated protocols.	ML-based anomaly detection is recommended.	Reinforces ML for detecting novel threats in dynamic IoMT networks.
[57]	DDoS, ransomware, and healthcare data breaches.	IDS must be efficient and privacy-preserving.	Balances performance needs with data protection in hospital networks.
[72]	Fake data injection, message tampering.	A lightweight, mobile-agent-based IDS is proposed.	Emphasizes low-power, real-time solutions for constrained devices.
[84]	Unsecured communication, network attacks.	Multi-layered defenses across 5 smart hospital layers are suggested.	Systems-level design required for full-spectrum defense.
[60]	Data breaches, MitM, and ransomware.	Economic risks and high breach costs stressed.	IoMT security must include cost-effective, high-impact protections.
[79]	Insider threats, protocol vulnerabilities.	Real-time IDS critical for medical CPS.	Shows IDS must handle both device-level and system-wide threats.
[49]	Malware, weak encryption, insecure interfaces.	Inadequate IDS makes systems easy targets.	Highlights the urgent need for robust device-level security mechanisms.
[73]	Weak edge-device security and encryption gaps.	Need for intelligent continuous monitoring systems.	Emphasizes vulnerable edge nodes needing intelligent safeguards.
[53]	Malware, data exfiltration, MitM.	Simulation-based risk modeling is recommended.	Recommends dynamic risk management alongside IDS.
[75]	Latency and poor interoperability.	Gateway vulnerabilities and delayed detection risks flagged.	Reinforces edge/cloud hybrid risks requiring distributed IDS.
[71]	Hijacking, impersonation, and DoS.	Conventional methods fail in IoMT due to overhead.	Lightweight custom defenses are needed over traditional IT solutions.
[50]	Device tampering, injection attacks.	Focus on zero-day readiness and system lifecycle risks.	Advocates advanced IDS to detect evolving vulnerabilities.
[64]	Privacy violations in data sharing.	FL is recommended to avoid centralized data.	Reinforces decentralized AI as a privacy-centric solution.
[70]	Re-identification, federated data risks.	Privacy-preserving training is essential in diverse environments.	Focus on trust models and privacy in federated AI.
[69]	Phishing, malware, zero-days.	FL reduces risk from centralized storage.	Supports AI with privacy built into the learning architecture.
[58]	Data breaches, info leakage.	FL encouraged.	Centralized AI models are discouraged for privacy-sensitive healthcare.
[61]	Data theft, identity spoofing.	Communication vulnerabilities demand real-time protection.	Federated frameworks protect distributed IoMT data.
[78]	DoS, data manipulation.	AI-IDS is vital for detecting traffic anomalies.	IDS systems need to address both data and traffic layer threats.
[51]	Unencrypted transmissions, data integrity.	Network-level security is needed in layered architectures.	Stresses secure comms as first-line defense in smart hospitals.
[59]	Wearable device threats, public network leaks.	Secure data-sharing protocols are lacking.	Integration of wearables increases network exposure.
[81]	Malware, data leakage.	DL-based IDS proposed.	Promotes adaptive AI systems for evolving threats.
[68]	Manipulated biometric data, delayed response.	Hybrid datasets improve IDS robustness.	Combines biometric + network features for holistic detection.
[54]	APTs, MITM, signature-evasion.	Meta-learning for adaptive IDS defense.	Emphasizes intelligent adaptation in high-threat scenarios.
[66]	Replay attacks, MedRadio sniffing, cloud DoS.	Threats are mapped across collection, transmission, and storage.	Lifecycle-based threat modeling for end-to-end security.
[76]	Node-level malware, edge attacks.	Highlights risk from distributed processing.	Edge-focused IDS systems are needed for real-time detection.
[67]	Unsecured emergency systems.	Low-power design leaves gaps in defense.	Urges resilient emergency IoMT architectures.
[80]	Malware, physical device tampering.	Highlights the insecurity of low-cost medical IoMT.	Emphasizes physical security and secure hardware.
[52]	SQL injection, malware, DDoS, and device compromise.	Warns of weak device design and authentication protocols.	Stresses full-stack protection from hardware to network.

Table 12
A critical analysis and comparative synthesis of the RQ2.

References	Mitigation strategy (IDS Focus)	Critical insights and trends	Comparative syntheses
[55]	AI-based hybrid IDS for malware, ransomware, and DDoS.	Real-time, adaptive IDS is crucial for device-level protection.	IDS must evolve with the complexity of threats and system heterogeneity.
[65]	IDS for anomaly detection in IoMT traffic.	Enforces privacy, trust, and secure interoperability.	Essential for maintaining secure medical communications.
[56]	FL (FedIoMT) IDS	Preserves privacy, supports decentralized updates.	Suited for dynamic, resource-constrained smart hospitals.
[77]	AI-enhanced IDS for AI IoMT environments.	Addresses data leaks and algorithm manipulation.	IDS must incorporate intelligent, regulatory-aware features.
[74]	ML-based anomaly IDS (e.g., KNN, ANN)	Learns normal patterns, flags novel attacks.	Proactive defense against emerging threats in IoMT.
[57]	DL + PSO + SHAP-based IDS at edge (SaaS)	Feature selection + model explainability.	Resource-efficient, interpretable IDS for real-time defense.
[72]	Mobile-agent IDS with ML and regression	Hierarchical, lightweight, context-aware IDS.	Ideal for low-power devices and real-time analytics
[84]	IDS in a 5-layer smart hospital architecture	Layered defense strategy, early detection	Emphasizes design-level IDS integration
[60]	AI-based cloud–fog–edge IDS	Detects zero-days, enhances scalability	Distributed IDS ensures continuous, adaptive protection
[79]	IDS for protocol and insider threat detection	Real-time alerts in Medical CPS	IDS tailored for MCPS complexity improves patient safety
[49]	LSTM + KNN anomaly classifier	Reduces false positives, enhances response speed	Hybrid models optimize IDS in health-critical networks
[73]	DL-enhanced IDS across diverse networks	Protocol-independent adaptability	Broad applicability for evolving medical IoMT environments
[53]	IDS + simulation for dynamic risk models	Reduces overload, enables scenario prioritization	Integrates threat modeling into operational IDS use
[75]	Edge-based IDS (implied)	Localized processing reduces latency	Effective in intermittent connectivity environments
[71]	DRNN + RF/KNN-based IDS	Detects spoofing, DoS, and data breaches	IDS must scale to detect diverse, stealthy attacks
[50]	Ensemble ML IDS (RF, XG Boost)	Real-time anomaly classification	Balances accuracy with interpretability in smart hospitals
[64]	Federated IDS (privacy-preserving)	Data stays local while detecting intrusions	Aligns cybersecurity with healthcare regulations
[70]	IDS in FL frameworks	Monitors cross-institutional threats	Points to gaps in current federated IDS implementations
[69]	Federated DL IDS	Real-time, privacy-safe collaboration	Combines decentralization with AI adaptability
[58]	FL-enhanced IDS (indirectly supported)	Risk mitigation without centralization	Protects sensitive data while maintaining detection accuracy
[61]	Federated IDS for traffic surveillance	Improves resilience and privacy	Decentralized IDS supports real-time detection in IoMT
[78]	AI + Butterfly Optimization IDS	High-accuracy abnormality detection	AI-enhanced IDS is effective for both known and unknown threats
[51]	IoMT-focused network IDS	Early anomaly warning system	Improves hospital data/system continuity and integrity
[59]	Real-time network behavior analysis	Prevents manipulation of patient data	Enhances operational security in connected hospital systems
[81]	DL-powered IDS for adaptive security	Early warning in constrained environments	Critical for resource-limited IoMT settings
[68]	Hybrid IDS (biometric + network data)	Manages reliability in real-time monitoring	Combines physical and digital security perspectives
[54]	Meta-learning-based IDS	Detects zero-day and evolving threats	Combines signature + anomaly models for greater coverage
[66]	Multi-layered IDS (collection, transmission, storage)	Emphasizes lightweight, adaptive IDS design	Calls for device-aware IDS to fit IoMT constraints
[76]	FedACNN IDS with attention mechanism	Real-time edge-level detection	Minimizes data exposure and communication overhead
[67]	IDS in emergency IoMT systems (implied)	Mitigates device misuse, ensures health data integrity	Highlights the IDS needs in real-time medical contexts
[80]	Real-time anomaly-based IDS	Early threat alerts in healthcare networks	Supports operational continuity and data protection
[52]	Behavioral IDS for IoMT	Monitors traffic, flags known/unknown attacks	Comprehensive monitoring is needed for healthcare reliability

resource-light, and privacy-aware solutions to address evolving threats. These solutions increasingly rely on AI and ML for anomaly detection, reducing false positives and providing real-time protection. Lightweight federated solutions are also more appealing, since they can run on less resource-intensive devices without sacrificing data privacy. Modern-day architects are focusing on distributed, layered, context-aware approaches, such as explainability, risk modeling, and edge-level detection. It ensures the secure and resilient IoMT infrastructures.

Of the 32 studies, 13 focus on AI-driven Anomaly Detection. These studies prove that hybrid ML/DL models are the building blocks of real-time detection of known and zero-day attacks. The remaining 8 papers promote Privacy-Preserving and Federated IDS frameworks. Taken together, these suggest that decentralized mitigation is the solution for aligning cybersecurity with healthcare regulation. Additionally, 7 studies highlight Edge-Based and Resource-Efficient mitigation. Finally, across the 4 studies, Architectural and Multi-Layered defense was noted as suggesting that IDS mitigation is most effective when employed within 5-layer hospital designs or in conjunction with dynamic risk modeling.

RQ3. How do resource limitations in IoMT devices affect the design and performance of IDS in smart hospital environments?

Resource constraints of IoMT devices are heavily shaping the architecture and performance of IDS in smart hospital settings. There are limitations to using sophisticated IDS models, including computational overhead, large-scale data storage, and real-time analysis. Accordingly, IDS solutions for such devices generally have to be lightweight, resource-bound, and efficient, which inevitably compromises detection accuracy and real-time performance [54]. Moreover, in Resource-constrained Contexts, making IDS solutions scalable to the large amount of dynamic data produced by many connected devices is a challenge [76]. As a result, many of these IDS models contain simplified algorithm structures or predesigned rules that are not capable of identifying complex and newly deployed threats [66]. Although resource-conscious IDS is indispensable for smart hospital IoMT devices, the reviewed literature reveals some weaknesses, limitations, and contradictions. Many of the IDS models designed for IoMT settings have been developed using simple ML algorithms or attack signatures (which are well-suited for resource-constrained devices but lack robustness in detecting APTs) [76]. Non-IID data and imbalanced datasets further degrade the performance of IDS, especially when handling real-time data from heterogeneous groups of medical devices [81].

These challenges are further exacerbated by device diversity. The heterogeneity of IoMT devices, with varying computational and storage capabilities, poses challenges to deploying a one-size-fits-all IDS solution [54]. Furthermore, there is evidence that some models contradict one another in terms of performance. The resource-efficient models achieved high detection accuracy in a standard lab but were unsuccessful in real-world, dynamic hospital environments due to the complexity of big data [67]. These contradictions highlight the need to develop more flexible, scalable IDS solutions with minimal resource requirements that can control threats in the rapidly changing IoMT healthcare domain.

This paper presents a new viewpoint on scalable frameworks that can be accurate and do not impose overhead on medical devices. By concentrating on an energy-efficient, adaptive, and distributed IDS approach based on FL, optimization, and edge/fog computing.

The resource limitations, including power, processing, and memory resources, are identified in Table 13 as one of the major challenges facing the deployment of traditional advanced IDS in an IoMT device. To bypass these requirements, more recent works have instead turned to decentralized, lightweight (energetically efficient) IDS designs. These reduce computational load while compromising the detection performance. Techniques such as FL, model simplification, edge computing, and feature reduction are frequently used to achieve optimal IDS performance in resource-constrained environments. Accuracy, real-time response, device compatibility, and security must be balanced to enable effective and scalable smart healthcare systems.

Among the 32 studies, 11 fall under the categories of Algorithm Simplification and Feature Engineering. The other 9 focus on decentralized and Federated Learning (FL) as a possible local solution to training load. The other 8 studies support Edge/Fog Offloading and Network-Level Detection. Lastly, 4 studies highlight Operational Safety and Real-Time Responsiveness, which state that IDS complexity must never hinder critical medical functions or emergency responsiveness.

RQ4. How can decentralized learning be leveraged to develop privacy-preserving IDS for medical IoMT in smart hospitals?

Decentralized learning, particularly FL, can be used to construct privacy-preserving IDS for IoMT devices in smart hospitals by enabling collaborative model training without sharing sensitive patient data. It does not transmit raw medical data, thereby preserving patient privacy while allowing the IDS to learn from numerous data sources. FL enables IoMT devices with limited resources to participate in training, thereby implementing privacy-preserving methods in the IDS without performance degradation [54]. Additionally, decentralized learning reduces data privacy and security concerns, since distributed models are less susceptible to unauthorized access or data leaks than centralized storage. This is significant, especially in smart hospitals, where patient data is extremely sensitive and subject to strict regulations [67]. Moreover, decentralized learning enables real-time learning and adaptation to the environment in which the IDS is deployed. It can efficiently detect new cyber threats while keeping sensitive medical data private.

Regarding the reviewed studies, there are marked shortcomings, constraints, or contradictions. One primary limitation is the high communication overhead in FL, where many model updates must be sent to the central server. This is a difficult task in an IoMT environment with limited resources and can cause delays in identifying intrusions [76]. Another challenge that limits the applicability of IDS in IoMT-based smart hospitals is the diversity of IoMT devices, with heterogeneous built-in computational capabilities. While some devices struggle to process and update IDS models on the go efficiently, this hampers scalability [67]. Moreover, although FL enhances privacy, it does not solve the problem of protecting model parameters in secure aggregation, as adversaries may modify model updates during the upload process [81]. Some studies report conflicting results regarding the accuracy of FL for intrusion

Table 13
A critical analysis and comparative synthesis of the RQ3.

Reference (APA)	Resource limitation issues	Critical insights and trends	Comparative syntheses
[55]	Limited power, memory, and computing; real-time IDS infeasible	Need for lightweight IDS optimized for healthcare IoMT	Traditional IDSs are impractical; tailored models are needed
[65]	Low-power devices cannot run intensive algorithms.	Cloud/edge reliance introduces privacy risks	Performance-security trade-off is the key challenge
[56]	High memory/CPU cost of IDS unsuited for IoMT	FL-based IDS reduces energy/memory by 93%	Demonstrates FL's feasibility in constrained settings
[77]	Devices lack bandwidth/processing for AI-IDS.	Offloading causes latency/privacy issues	Advocates lightweight, adaptive IDS designs
[74]	Deep models are unsuitable for low-power devices	Suggests simple ML models for real-time use	Realistic IDS must balance accuracy and complexity
[57]	Devices cannot run complex models locally.	SaaS edge-based IDS + PSO for lightweight ops	Hybrid deployments help bypass local constraints
[72]	WBANs cannot handle heavy cryptography/ IDS.	Mobile agents + distributed learning minimize load	Decentralized models scale better with minimal device load
[84]	Embedded layers constrained by compute limits.	Security mechanisms must be infrastructure-aware	Embedding IDS into smart hospital layers is effective
[60]	AI-IDS is often too large for IoMT	Fog/edge computing + lightweight algorithms help	Stresses preprocessing and model compression
[79]	Wearables cannot support IDS logic.	Network-based IDS is preferred over device-level	Network-level focus offloads detection from devices
[49]	Insufficient memory/CPU in devices	PCA + KNN is used to lower the resource burden	Feature reduction improves efficiency significantly
[73]	Edge nodes cannot run complex IDS.	Lightweight DL-based IDS with minimal overhead needed	Recommends custom DL for constrained edge setups
[53]	MioT (Medical Internet of Things) cannot host a full-featured IDS	Simulation-based threat modeling to reduce live load	Accepts a delay in detection to preserve resources
[75]	IoMT devices offload to edge gateways.	Gateway-level IDS reduces local device pressure	Edge is a viable layer for preliminary intrusion analysis
[71]	Devices cannot support deep IDS models.	Optimized DRNN + feature selection ensures fit	Adaptive DL models must be scaled down for IoMT
[50]	Power/memory limits block high-end IDS.	Simpler models balance speed and resource usage	Ensemble models offer a balance between accuracy and load
[64]	FL assumes resource availability is not always present	Local model updates still strain weak devices	Highlights the gap in FL assumptions vs. practical feasibility
[70]	Devices cannot handle complex federated training.	Calls for lightweight, consistent FL IDS across sites	Heterogeneity complicates unified IDS deployment
[69]	Communication overhead limits IDS updates.	FL mitigates the central load, but optimization is needed	FL improves scalability, still needs tuning
[58]	Constrained devices struggle even with FL.	Optimization is needed even for minimal models	Shows FL is not plug-and-play in resource-limited IoMT
[61]	Diverse devices complicate IDS standardization.	Decentralized lightweight IDS models proposed	IDS must adapt to mixed device capabilities
[78]	Devices cannot process high-dimensional data.	Optimization (e.g., Butterfly) enhances IDS speed	Meta-heuristics help trim overhead effectively
[51]	IoMT lacks processing for IDS frameworks.	Simple, fast IDS needed for timely detection	Heavy models fail; need task-specific IDS algorithms
[59]	Memory/power limits restrict IDS deployment.	IDS must avoid interfering with medical function	Safety must not be compromised by IDS complexity
[81]	DL-based IDS too heavy for hospitals	Edge integration or model simplification is needed	Leaner DL models critical for IoMT use cases
[68]	Devices cannot handle continuous monitoring.	Combining data sources selectively improves efficiency	Streamlining input can optimize IDS performance
[54]	Power constraints limit anomaly-based IDS.	Meta-IDS is designed for low-latency use	Requires trade-offs in accuracy for efficiency
[66]	Wearables cannot handle traditional IDS.	Lightweight, custom architectures are necessary	Device-aware IDS development is essential
[76]	High training loads are unsuitable for local devices	FL + attention mechanisms optimize cost	Communication efficiency must be factored in
[67]	Emergency devices must be minimal and fast	Complex IDS disrupts emergency responsiveness	Simplicity prioritized for real-time systems
[80]	Storage and power limits persist.	IDS must match hardware constraints	Lightweight IDS ensures security does not impair operation
[52]	IDS needs often exceed IoMT capacity	Rule-based or hybrid models are practical	Flexibility over sophistication in model design

Table 14
A critical analysis and comparative synthesis of the RQ4.

References	Decentralized learning approach	Critical insights and trends	Comparative syntheses
[55]	FL implied	FL enables privacy-preserving IDS but faces challenges like data heterogeneity and device limitations.	Calls for optimization of FL for resource-constrained smart hospitals
[65]	Implied FL	Decentralization reduces cloud dependency and privacy risks	Supports decentralized IDS as a future direction for privacy compliance
[56]	FL (FedIoMT + KANConvNet)	Enables local training, high accuracy, low latency, and scalability	Demonstrates a practical, privacy-focused decentralized IDS model
[77]	Implied Edge Intelligence	Distributed intelligence helps secure data without central exposure	Implies that decentralization supports privacy and real-time response
[74]	Suggests FL	Centralized ML lacks privacy; FL is noted as a potential solution	Encourages future work toward FL integration in IDS pipelines
[57]	Edge SaaS (Not FL)	Offloading improves efficiency, but lacks full decentralization	Complementary to FL through the distributed deployment of lightweight models
[72]	Mobile-agent Distributed IDS	Shared IDS logic reduces per-node load and aligns with decentralized concepts.	Promotes distributed detection even without FL
[84]	Distributed Infrastructure	Lightweight IDS embedded at various layers	Suggests infrastructure-level decentralization instead of cloud reliance
[60]	Distributed + Hybrid AI	Fog-edge layers balance latency and compute limits	Supports layered distributed learning for healthcare IDS scalability
[79]	Distributed IDS (Implied)	Network-layer detection avoids device-level overload	Advocates for decentralized IDS focused on energy-efficient monitoring
[49]	Suggests FL in the future	Current ML models are centralized; decentralization is proposed for privacy.	Future IDS must integrate FL to enhance security and compliance.
[73]	Distributed/Edge-Implied FL	Localized analysis preserves privacy and boosts IDS speed	Edge and distributed models are natural complements to FL-based IDS
[53]	Implied Decentralization	Simulation supports distributed adaptation to threats	FL aligned with the proposed responsive, resource-aware IDS architecture
[75]	Edge-based Distributed Analysis	Edge infrastructure supports decentralized detection	Emphasizes foundational readiness for decentralized IDS systems
[71]	Suggests FL	Central ML methods have privacy limitations	Points to decentralization as the next step for secure IDS
[50]	Implied FL	Real-time detection requires privacy-respecting local learning	Encourages exploration of decentralized learning under privacy constraints
[64]	Use FL	FL ensures compliance and collaborative threat detection	Strong support for FL as an ideal decentralized learning model
[70]	Use FL	Highlights benefits (privacy) and challenges (heterogeneity, comms)	Identifies FL as feasible but needing refinement for real-world IoMT
[69]	Use FL	FL offers scalable IDS without centralizing sensitive data	Affirms FL's value in securing healthcare infrastructure
[58]	FL Usage	FL enables generalizable, privacy-compliant IDS across systems	Supports FL as the backbone of modern, decentralized IDS in hospitals
[61]	Use FL	Local learning protects privacy and allows secure collaboration	Aligns FL with responsive IDS models
[78]	Suggests Distributed Learning	Reduces central load and improves control over data	Distributed IDS is preferred in hospital networks for speed and privacy
[51]	Decentralized Analysis Suggested	Local data analysis reduces breach risk	Aligns with decentralized architecture for privacy-respecting IDS
[59]	Suggests FL	Reduces data movement, suits confidentiality-sensitive settings	Promotes decentralized IDS for critical care data protection
[81]	Central DL with implied decentralization	Heavy models unsuitable for IoMT; lightweight FL alternatives needed	Emphasizes efficiency gains via decentralization
[68]	Suggests FL for future IDS	Calls for a distributed model training to enhance privacy and performance	Future-ready for FL integration across medical nodes
[54]	Implied FL + Meta-IDS	Privacy-aware IDS could benefit from decentralized training	FL could scale meta-learning for smart hospital IDS
[66]	Hybrid/Distributed Frameworks Suggested	Centralized systems are not suitable for IoMT	Decentralized learning offers resilience, performance, and privacy
[76]	FL (FedACNN)	FL reduces latency, enhances privacy, and increases accuracy	Strong implementation showing edge-compatible, decentralized IDS
[67]	Suggests Decentralized Learning	Emergency healthcare benefits from localized data analysis	Ideal environment for real-time decentralized IDS
[80]	Supports Decentralized Learning	Enables IDS model updates without exposing patient data	Decentralized systems suit dynamic hospital IoMT scenarios
[52]	FL	Scalable, adaptive IDS that meets privacy laws	Recommends FL as a privacy-first, resilient IDS framework

detection, with some models performing well in controlled environments but falling short in real-world settings (where the data distribution is not IID) [54]. These conflicts emphasize the difficulties that remain in realizing privacy preservation in IDS within the context of a dynamic and complex medical IoMT.

We investigate decentralized learning, including federated IDS as a privacy-friendly paradigm for smart hospital IoMT. Recent studies demonstrate that FL can achieve up to 93.27% detection accuracy without sharing raw patient data [78]. The literature under-explores its combination with edge and fog computing for scalability, latency, and device-overhead balancing [60,75], and focuses on decentralized, regulation-compliant, and adaptive IDS models that address heterogeneity and resource-constrained challenges.

Table 14 elaborates on the importance of decentralized learning techniques, especially FL, in protecting patient privacy and securing IoMT systems, which is becoming more widely acknowledged. These approaches reduce the risks of data exposure and latency by providing local data processing without transmitting personal data to central servers. FL implementations face challenges such as resource constraints, communication expense, and device diversity, while offering promising benefits. To address these problems, research favors a decentralized IDS model that is lightweight, edge-friendly, and hybrid (balancing scalability with privacy and performance). These models are particularly appropriate for the sensitive and dynamic environment of smart healthcare.

Among 32 studies, 15 studies indicate that FL enables local training of IDS models on medical devices or edge gateways. The other 10 papers belong to Distributed Edge-Gateway and Multi-Layered Architectures. Although these studies do not always refer to a decentralized approach as FL, they benefit from decentralizing analysis to reduce dependence on the cloud. Lastly, 7 studies show that decentralization is a Future Requirement for Scalability and Resilience.

RQ5: What role does edge computing play in enhancing real-time IDS performance in smart hospitals?

Edge computing significantly improves the real-time performance of IDS in smart hospitals. It facilitates data processing and analytics near IoMT devices, where data is generated, rather than transferring it to centralized cloud servers. As a result, the proposed decentralized method reduces the latency of transmitting data to a central server for analysis and detection, resulting in faster response times [76]. In a smart hospital environment, where low latency and immediacy are key, edge computing enables local data processing on IoMT devices. It includes medical sensors and wearables to prevent breaches [67]. By migrating heavy computation to edge devices, hospitals can alleviate network traffic congestion and complexity. It provides an efficient deployment strategy for IDS on heterogeneous devices with different capabilities. Additionally, edge computing provides data privacy and retention, allowing sensitive patient data to be processed locally without transmitting it to external servers. It is essential for preserving patients' privacy regulations [66].

Although edge computing greatly improves the real-time performance of IDS in smart hospitals, some weaknesses, limitations, and contradictions remain in the literature. There are several shortcomings, such as the limited resources of edge devices, which can struggle to handle sophisticated IDS models or massive data analysis. Although edge computing supports local processing, the computational capacity of edge devices is bounded, and complex IDS models may not be achievable. It causes attacks to go undetected or benign traffic to be detected [54]. Another shortcoming lies in the non-uniformity of hospital equipment's, with a large number of IoMT devices and their different processing capacities, the performance levels of IDS may vary in the network [81]. Additionally, there are inconsistencies in the operation of edge computing-based IDS across different devices on non-IID data. Some of the works argue that FL and other decentralized strategies. FL can alleviate these problems, while others claim that distributed learning still faces issues with privacy-preserving data aggregation and model convergence [76]. Such inconsistencies and constraints indicate the need for IDS solutions that are more adaptable, resource-conscious, and scalable in the smart hospital environment.

The novelty of the proposed Work lies in combining edge computing and IDS in smart hospitals for real-time threat detection. In contrast to classical cloud-based systems, we focus on edge-local data processing, eliminating the need to offload patients' private data to the cloud. It thus minimizes latency and protects patients' privacy by keeping sensitive patient data on-site. By handling resource-constrained devices and diverse IoMT environments, this solution scales dynamically to deliver fast IDS performance in real time. That is resulting in more effective detection without violating data security and regulatory obligations.

Fig. 9 illustrates Edge Computing and FL in IoMT IDS, enabling decentralized, privacy-preserving processing of healthcare data at the network edge. This interaction improves real-time intrusion detection while optimizing resource efficiency and maintaining patient privacy.

We need fast IDS performance in a smart hospital and edge computing environments. Previous work has demonstrated that edge-based anomaly detection reduces detection latency [85]. However, most of the literature disregards FL integration due to privacy concerns and does not provide specific verification for medical IoMT use [56,76]. This work not only provides new insights into designing a scalable, lightweight, and clinically viable framework for a smart hospital but also accounts for characteristics that reduce latency and computational overhead. IDS is decentralized yet regulation-compliant at the edge, and it also specifies how the edge should cooperate seamlessly with the cloud in deploying IDS at scale.

Table 15 focuses on real-time, privacy-preserving IDS in IoMT contexts, made possible in large part by edge computing. Edge-based IDS alleviates reliance on the cloud, accelerates threat identification, and reduces latency by processing data closer to devices, especially in resource-constrained medical environments. Localized computation, bandwidth savings, and enhanced patient data privacy can be achieved without burdening device hardware through a decentralized architecture. Edge computing has been a part of scalable and responsive smart healthcare security, as evidenced by state-of-the-art trends that incorporate edge computing alongside FL, mobile agents, and lightweight AI.

The 14 papers are under Latency Reduction and Offloading in the selected 32 studies. The other 11 studies demonstrate the synergy between Edge and Decentralized Learning. These researchers demonstrate that edge nodes are the best candidates for the physical layer for Federated Learning (FL). Last, 7 studies identify edge integration as the Essential Path to future Scalability.

4.1. Concrete suggestions

The paper elucidates the key technologies and methodologies for enhancing IDS in IoMT-based systems. In particular, it focuses on lightweight IDS models that run efficiently on resource-constrained medical devices. This can be achieved through methods such as pruning and quantization, which maintain high accuracy without overwhelming device resources.

XAI needs to be an integral part of clinical decision-making for transparency and trust in AI, and healthcare systems should enforce the use of XAI-based IDS solutions to promote accountability. FL is proposed as a solution to protect patient data and support collaborative model training, and health organizations are encouraged to deploy FL to reduce the potential of data exposure. Emerging 6 G networks will enab real-time IDS performance through high bandwidth and ultra-low latency. Smart hospitals need to plan for the infrastructure required for 6G-enabled IDS implementation.

Last but not least, open and interoperable IDS will help achieve seamless security across different IoMT devices. That can be ensured if regulatory authorities mandate consideration of interoperability standards to ensure consistent protection across the entire IoMT ecosystem.

Table 16 presents the experimental solutions to the research questions, detailing the systematic methods and approaches used to investigate and answer them through controlled experiments.

5. Future directions

There is scope for future studies on the development of lightweight, IoMT-device-specific IDS that operate in real time to support resource-constrained IoMT devices in smart hospitals. The goal is to get them to work with as little latency and power consumption as possible. Stress aims to accelerate the adoption of FL mechanisms, which enable decentralized training on edge or fog nodes, enhancing data privacy by eliminating the need for a central system. Integrating XAI solutions with IDS systems will also be essential to provide transparency, interpretability, and trust in anomalous detection results, enabling their adoption by medical specialists. IDS systems should be modular and resilient, functioning dynamically across layers, cloud-fog-edge, with intelligent trade-offs between detection accuracy and computational load as well as energy efficiency. Future work should focus on addressing the challenge of connecting IDS to heterogeneous IoMT devices and the current hospital IT system to ensure reliable cooperation. Furthermore, due to the presence of non-independent and identically distributed (non-IID) data and device heterogeneity, which are common in practical IoMT scenarios, there is a need for robust IDS models. A promising future direction for IDS is to improve its robustness to adversarial attacks and zero-day threats through continual learning and adaptive strategies. Domain-specific real hospital testbed and public IoMT datasets are required to evaluate the performance of IDS in a practical environment. In the future, IDS designs and deployments should comply with strict privacy regulations (e.g., HIPAA, GDPR) and place an ethical emphasis on design.

Table 17 presents the proposed future research directions, along with the reviewed studies that address these aspects, and the last column summarizes the remaining gaps.

Table 18 is all about mapping privacy regulations, such as GDPR, with the IDS through Federated Learning (FL).

Lightweight AI models can be implemented to perform real-time monitoring and anomaly detection. They provide early intervention or post-event analysis against the faults (malfunctions) occurring in the medical device. This can lead to more secure data communication and storage practices in IOMT environments, potentially helping organizations fulfill regulatory compliance [55]. Given the importance of data privacy requirements for future real deployments, the system should also comply with data privacy regulations [54]. The Meta-IDS is designed with mechanisms in place to accomplish this. Patient data protection is a critical requirement in healthcare under GDPR and HIPAA. Federated learning protects privacy and intellectual property by allowing on-device processing of data, which means that raw data never leaves the original site [70]. Regulatory compliance is a crucial step in the IoMT security process for enhancing patient safety and care delivery when properly instituted and authenticated [55].

Fig. 10 highlights the future directions of IDS in the Internet of Medical Things (IoMT) for smart hospitals, focusing on advancements in real-time threat detection, integration with AI, and enhanced cybersecurity measures

6. Conclusion

In this study, we investigate cyber threats in IoMT devices and explore the relationship between smart hospitals and the IoMT medical environment. We follow standard threat modeling notations to identify them, then explore the challenges that affect IoMT security and examine how IDS can address them. This analysis discovers several main cybersecurity threats, such as data breaches, MiTM attacks, DoS attacks, and device hijacking, that could threaten patient safety and data confidentiality. These are further exacerbated by security weaknesses in many IoMT devices, including weak authentication schemes and insecure communication interfaces.

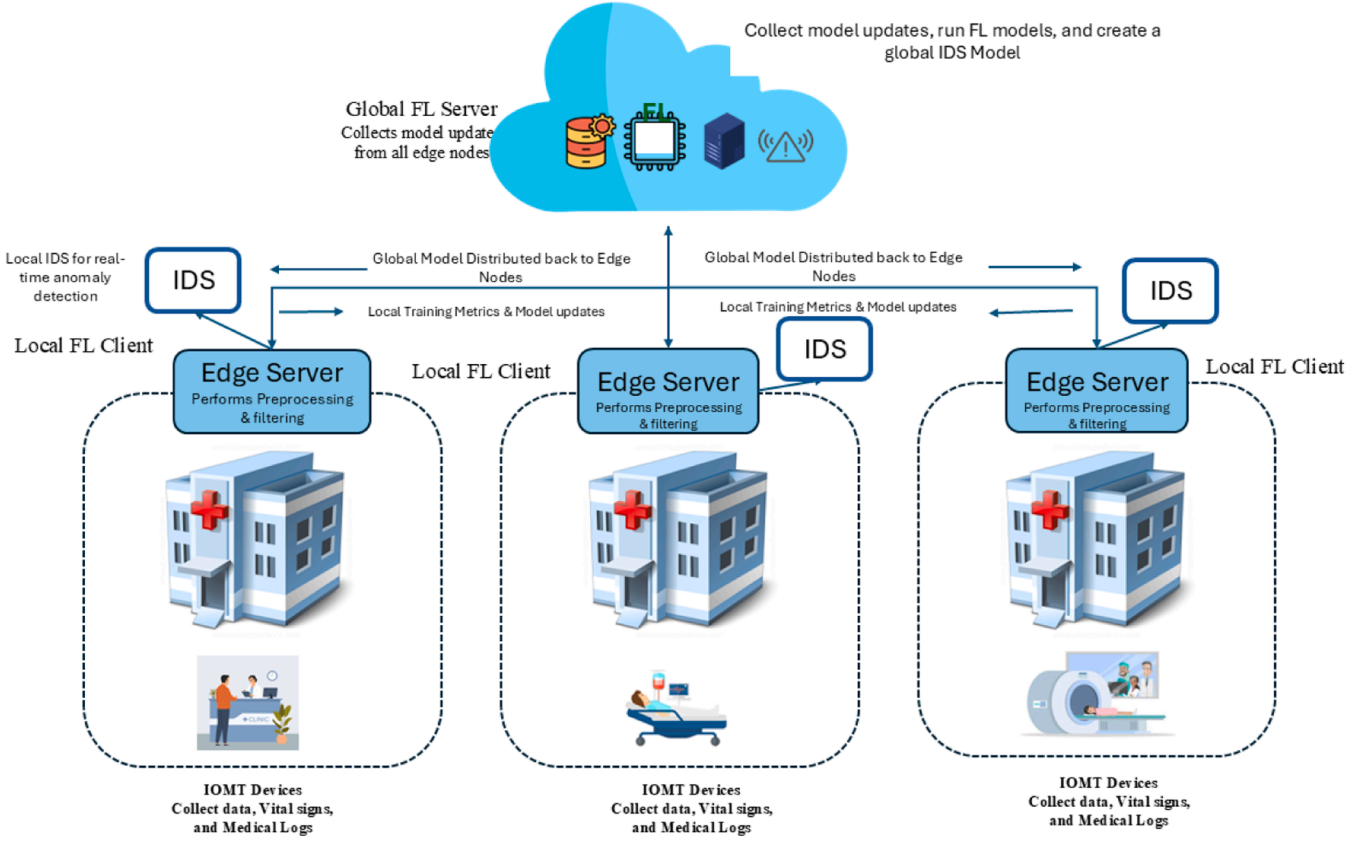


Fig. 9. 3 The edge computing and FL interaction within IoMT IDS.

Table 15
A critical analysis and comparative synthesis of the RQ5.

References	Edge computing role in real-time IDS	Critical insights and trends	Comparative syntheses
[55]	Enables localized analysis; reduces latency.	Edge-based IDS is crucial for resource-limited IoMT	Emphasizes the need for lightweight, real-time models at the edge
[65]	Minimizes reliance on the cloud for real-time response.	Edge enhances privacy and processing speed	Supports edge as an infrastructure layer for secure IDS
[56]	Combines edge + FL in FedIoMT.	Lightweight edge models reduce latency and preserve privacy.	Real-world example of scalable, private IDS at the edge.
[77]	Edge mitigates cloud latency/privacy risks.	Supports local analysis for faster, secure threat response.	Aligns with edge-aware smart healthcare architectures.
[74]	Edge suggested reducing the detection delay.	Implies edge feasibility for IoMT IDS	Highlights offloading as a solution to central bottlenecks
[57]	SaaS-based IDS deployed at the edge	Offloads heavy IDS tasks from constrained devices	Practical application of edge computing in real-time IDS
[72]	Mobile agents operate like edge logic.	Distributed nodes reduce communication overhead	Implied edge-compliant design supports responsive IDS
[84]	Edge ensures timely anomaly detection.	Reduces network congestion, enables immediate action	Architecture-oriented view promotes edge-integrated IDS
[60]	Fog-edge-cloud tiers support scalable IDS.	Real-time performance benefits from edge proximity	Advocates a hybrid layered architecture for IDS deployment
[79]	Offloads processing from constrained devices	Edge improves IDS responsiveness in MCPS	Edge integration is necessary for wearable device support
[49]	Edge computing is expected to support faster ML-IDS	Need for low-latency detection systems	Future direction: embed ML-based IDS in edge nodes
[73]	Edge reduces latency and increases privacy.	Enables fast, local anomaly detection in hospitals	Edge meets healthcare's dual need: speed and data protection
[53]	Edge suggested for responsive risk mitigation.	Distributed setup enhances threat response time	Calls for edge-aware threat simulation in IDS design
[75]	Edge gateways lower processing delay (11.5 ms)	Real-time filtering boosts scalability	Concrete metrics show the edge's performance in smart hospitals
[71]	Edge is implied to enhance latency-sensitive detection	Local processing would optimize DRNN-based IDS	Suggests edge integration as a future enhancement
[50]	Edge is implied to support fast threat response	Avoids overburdening IoMT with heavy IDS tasks	Recommends edge for real-time ML-based IDS
[64]	Edge supports FL training locally.	Local model updates protect privacy and enable fast detection	Integrates privacy and latency through edge + FL framework
[70]	Edge suggested via distributed learning systems.	Local servers act as privacy-aware IDS hubs	Decentralized IDS via edge gateways improves speed/privacy
[69]	Edge enhances FL-based IDS.	Enables fast local analysis and secure collaboration	Strong case for edge as core to scalable healthcare IDS
[58]	Edge implied in privacy-aware decentralized learning.	Local processing increases IDS robustness	Edge preserves privacy and boosts responsiveness
[61]	Performs detection at gateways/devices	Maintains speed and local privacy in smart hospitals	Strong endorsement for edge-integrated IDS design
[78]	Suggests optimized local algorithms	Local computation supports lightweight IDS	Edge supports fine-tuned, real-time detection strategies
[51]	Local analysis improves IDS responsiveness.	Edge avoids cloud delays and lowers bandwidth use	Ideal for hospitals with time-sensitive data pipelines
[59]	Edge minimizes transmission overhead and enables fast IDS.	Traffic is analyzed directly at the device/gateway level	Edge supports autonomous, real-time threat mitigation
[81]	Edge could run lightweight DL models.	Improves performance in IoMT, where full DL is too heavy	Edge offers a viable path for deploying simplified IDS
[68]	Distributed design aligns with edge potential.	Improves data locality, detection accuracy	Suggests that edge integration would enhance IDS performance
[54]	Edge integration hinted at for scalable IDS	Meta-IDS benefits from distributed, low-latency logic	Future work: combine edge + meta-learning for IoMT IDS
[66]	Local processing is emphasized for fast detection	Edge reduces data transit delays and enhances safety	Supports edge for low-power, real-time medical IDS
[76]	FedACNN runs IDS on edge nodes.	Reduces latency, improves system privacy	A working model combining edge + FL for real-time detection
[67]	Edge is suitable for emergency diagnosis systems	Enables real-time response in ambulances, remote care	Recommends edge for time-critical, location-flexible IDS
[80]	Edge offloads data from the cloud to the device level	Reduces detection time in smart hospital networks	Edge reduces latency, essential for continuous monitoring
[52]	Edge ensures real-time, bandwidth-saving IDS.	Supports a hybrid edge-rule-based approach	Aligns edge with critical care responsiveness and privacy

Table 16
Experimental solutions to research questions.

Question No.	Keyword	Problem	Solution	Experimental solution
RQ1	Lightweight IDS for IoMT	Absence of lightweight, real-time, explainable IDS tailored for resource-constrained IoMT devices; existing IDS are overly complex, energy-intensive, and centralized.	Design in lightweight, real-time, explainable IDS optimized for IoMT.	Evaluate the efficiency and accuracy of IDS in real-time hospital IoMT scenarios.
RQ2	Accuracy vs. Energy Efficiency	Minimal focus on balancing detection accuracy and energy efficiency; adaptive IDS across the edge, fog, and cloud layers remains underexplored.	Develop adaptive IDS frameworks that balance accuracy and energy efficiency across layers.	Simulate IDS performance across cloud, fog, and edge to measure energy-accuracy trade-offs.
RQ3	Medical Datasets & Legacy Integration	Scarcity of real-world, domain-specific medical datasets; limited practical implementations or integration with legacy systems.	Create and validate realistic hospital-specific testbeds and datasets.	Deploy IDS on real hospital testbeds with legacy system integration.
RQ4	Privacy & FL	Privacy, trust, compliance, and ethical AI are often overlooked; FL is promising but rarely integrated with explainable models.	Leverage FL for decentralized, privacy-preserving IDS with explainable AI.	Implement FL-based IDS with XAI (Explainable Artificial Intelligence) in distributed hospital IoMT environments.
RQ5	Edge Computing in IDS	Edge computing is underutilized, with limited empirical deployments; challenges include real-time constraints, energy limitations, and integration with healthcare infrastructure.	Utilize edge computing to enable efficient, real-time IDS.	Empirically deploy IDS at edge nodes to validate real-time and energy efficiency in hospitals.

In response to the research questions, this study shows that IDS can substantially reduce cybersecurity threats in smart hospitals through early warnings and rapid decision-making. IDS models, especially those using anomaly-based detection, can discover novel threats (i.e., zero-days) by detecting anomalous behavior patterns.

The scalability issues remain, as many existing IDS proposals are inefficient at processing the large and ever-evolving volume of data produced by IoMT devices due to resource constraints (e.g., limited CPU power and memory). These limitations necessitate lightweight IDS solutions that balance performance and footprint.

Furthermore, the work also points out the prospect of FL in constructing privacy-preserving IDS. With FL, models can be trained without sharing raw patient data with the server, thereby maintaining privacy while still enhancing security. Likewise, the emergence of Edge Computing has a profound impact on improving such real-time IDSs' performance. It enables low-latency responses by processing data at or near its point of origin in the network. It guarantees faster threat detection and a lower risk of service outages. However, there are various challenges to the practical deployment of such learning paradigms, including high communication overhead, resource-constrained edge devices, and non-IID data.

Altogether, this review highlights the need for flexible, scalable, and resource-efficient IDS systems capable of managing the complexities of the IoMT environment in smart hospitals. In the future, it will be necessary to address limitations in data privacy, resource constraints, and interoperability to design efficient, lightweight, clinically deployable IDS frameworks. Leveraging the latest technologies, such as Federated Learning and Edge Computing, can help smart hospitals strengthen their cybersecurity. These ultimately uphold patient care and the integrity of healthcare networks.

CRediT authorship contribution statement

Sadia Fatima: Writing – original draft, Methodology, Formal analysis, Conceptualization. **Muhammad Ismail Kashif:** Visualization, Supervision, Resources, Methodology. **Khadija Tuz Zahra:** Methodology, Investigation, Data curation, Conceptualization. **Muhammad Adnan:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Methodology, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no competing financial or personal interests that could have appeared to influence the research, analysis, or conclusions presented in this manuscript.

Table 17
Proposed research direction, papers that already go in this direction, and the gap that remains.

Suggested future directions	Lack of studies	Critical gap for IoMT clinical deployment
Lightweight, Real-time, Customized IDS for IoMT Devices	Challenges in deploying IDS in IoMT environments [55]. IoMT security requires lightweight, real-time, and customized IDS to handle diverse device environments effectively [80]. Current IDS models may lack transparency and trust. The paper addresses the need for advanced IDS solutions [57]. Lightweight, real-time, and customized IDS are crucial for securing resource-constrained IoMT devices and addressing their unique vulnerabilities [50].	This gap is critical as it can risk patient data, delay interventions, and reduce trust in IoMT systems [55]. IoMT must ensure secure, trusted, and timely remote patient care while safeguarding health data [80]. IoMT must ensure real-time, integrated, and remote health monitoring to support timely interventions and improve healthcare quality [57]. IoMT must provide real-time, adaptive security to protect patient safety and counter evolving cyber threats [50].
Federated Learning for Decentralized Training	Federated Learning enables decentralized training by allowing IoMT devices to learn from distributed data collaboratively [54]. Federated Learning lacks access to real medical devices for experimentation [79]. Limited exploration of real-world FL applications in healthcare [61]. Limited exploration of vertically split data in federated learning [70]. Need for improved model training on edge devices [55]. High computational cost and time consumption hinder FL adoption [69].	IoMT must enable real-time, privacy-preserving model updates while ensuring regulatory compliance, secure collaboration, and efficient resource use [54]. Federated Learning must ensure privacy-preserving, adaptable, and secure IoMT deployments while supporting diverse medical device interactions [79]. Federated Learning must ensure secure, privacy-preserving, and efficient decentralized training to support collaborative and safe IoMT healthcare operations [61]. Federated Learning must ensure privacy-preserving, collaborative, and real-time IoMT analytics to support personalized and secure patient care [70]. Federated Learning must ensure secure, privacy-preserving, and compliant IoMT operations while minimizing data transfer and reducing breach risks [55]. Federated Learning must ensure privacy-preserving, trustworthy, and efficient IoMT deployments with real-time threat detection [69].
Incorporation of XAI Techniques in IDS	Lack of XAI in IDS for IoMT [72]. Need for integrating XAI to enhance user trust in IDS [71]. Few proposals addressing XAI integration in intrusion detection systems [60]. AI models treated as black boxes lack transparency [57].	XAI must provide transparent, interpretable, and adaptive IoMT intrusion detection to enhance trust, reduce false positives, and support regulatory compliance [72]. XAI must ensure transparent, trustworthy, and unbiased IoMT intrusion detection to support clinical decision-making, regulatory compliance, and patient data protection [71]. XAI must provide transparent, explainable, and trustworthy IoMT intrusion detection to enhance understanding of anomalies and address legal and ethical concerns [60]. XAI must ensure transparent, interpretable, and trustworthy ML-based IDS for IoMT, enhancing security and administrator understanding [57].
Modular and Adaptive IDS Frameworks	Lack of modular IDS frameworks and real-time integration [55] Need for innovative frameworks using AI and machine learning [50]. Limited research on adaptive and hybrid models [60]. Need for more exploration in legal, ethical, and AI techniques [74].	Modular and adaptive IDS frameworks must ensure flexible, scalable, and continuous IoMT security while efficiently responding to evolving threats [50,55]. Modular and adaptive IDS must provide flexible, real-time, and efficient IoMT security across diverse medical devices while responding to evolving cyber threats [60]. Modular and adaptive IDS must ensure flexible, real-time, and reliable IoMT security to protect patient data, support diverse devices, and enhance network resilience [74].
Integration of IDS with Heterogeneous IoMT Devices	Current studies lack integration of IDS with heterogeneous IoMT devices [54].Lack of focus on unified intrusion detection across diverse devices [72]. Lack of standardized protocols for IDS in heterogeneous IoMT systems [49]. There is a lack of studies on IDS integration with heterogeneous IoMT devices [55]. Current studies focus on traditional systems rather than heterogeneous IoMT. It needs comprehensive solutions addressing diverse IoMT device vulnerabilities [57]. Heterogeneous devices present unique cybersecurity challenges [69].	Integration must ensure secure, real-time, and adaptable IoMT monitoring to protect patient data, comply with regulations, and optimize resource use [54]. Integration must provide continuous, secure, and real-time IoMT monitoring to protect patient safety, improve diagnostics, and detect network intrusions [72]. Integration must ensure the development of secure, reliable, and robust IoMT systems that protect patient data and enable rapid responses to cyber threats [49]. Integration must ensure secure, compliant, and scalable IoMT systems that provide real-time monitoring, protect patient data, and enhance healthcare reliability [55]. Integration must provide secure, real-time, and efficient IoMT monitoring that ensures comprehensive threat detection and fosters trust in clinical decision-making [57]. Integration must ensure secure, real-time, and device-specific IoMT monitoring with privacy-preserving

(*continued on next page*)

Table 17 (*continued*)

Suggested future directions	Lack of studies	Critical gap for IoMT clinical deployment
		and customized defenses to mitigate cyber threats effectively [69].
Handling Non-IID Data and Device Heterogeneity	Device heterogeneity poses significant challenges in attack detection [79]. Non-IID data poses challenges in federated learning applications [70]. Non-IID data leads to low model accuracy and convergence issues [76]. Device heterogeneity in IoMT is not extensively studied [60].	IoMT must address non-IID data and device heterogeneity through standardized and tailored intrusion detection strategies for effective healthcare deployment [79]. IoMT must handle non-IID data and device heterogeneity through federated learning to ensure comprehensive, secure, and efficient patient data analysis [70]. Non-IID data and device heterogeneity must be addressed through federated learning to ensure accurate, secure, and collaborative IoT healthcare deployments [76]. IoMT must manage diverse devices and non-IID data to ensure adaptable, secure, and real-time patient monitoring in clinical environments [60].
Enhancing IDS Resilience Against Zero-Day Threats	Signature-based methods are ineffective against zero-day attacks [54]. Limited datasets hinder effective zero-day threat detection strategies. Future research should focus on MCPS-specific datasets for zero-day threats [79]. Current methodologies do not adequately address zero-day attack detection [71]. Limited research on dynamic adaptation for zero-day threat resilience [50]. Current studies inadequately address zero-day attack detection [60]. Limited research on IDS resilience against zero-day threats exists [69].	Enhancing IDS resilience ensures adaptive, accurate, and efficient detection of zero-day threats to protect patient data in resource-constrained IoMT environments [54]. Enhancing IDS resilience protects IoMT from zero-day threats, ensures continuous operation, safeguards patient data, and fosters trust and regulatory compliance [79]. Enhancing IDS resilience protects sensitive medical data, addresses IoMT-specific vulnerabilities, mitigates zero-day threats, and ensures continuous healthcare operations [71]. Enhancing IDS resilience with ensemble models ensures adaptive, robust, and effective detection of zero-day threats in IoMT environments [50]. Enhancing IDS resilience with AI ensures adaptive, robust detection of unknown threats, safeguarding patient data, and maintaining trust in IoMT systems [60]. Enhancing IDS resilience ensures robust detection of zero-day threats, protects sensitive IoMT data, maintains trust, and supports regulatory compliance [69].
Development of Domain-Specific Testbeds and Publicly Available IoMT Datasets	Lack of domain-specific testbeds for IoMT [79]. There is a pressing need for domain-specific testbeds [60]. More comprehensive datasets could enhance intrusion detection systems [49]. More research is needed to create diverse IoMT datasets [55]	Domain-specific testbeds and medically realistic datasets are critical for accurate IoMT attack detection, reliable benchmarking, and safe clinical deployment [79]. Domain-specific testbeds and diverse datasets enable realistic IoMT simulations, improving IDS evaluation, threat understanding, and clinical security deployment [60]. Domain-specific testbeds and publicly available datasets advance IoMT security by enabling robust model evaluation, benchmarking, and standardized clinical deployment [55,49]
Ensuring Privacy Regulations (e.g., HIPAA, GDPR) Compliance and Ethical Principles in IDS Design	Ethical principles must guide IDS design for privacy protection [55,60]. Compliance with HIPAA and GDPR is crucial for IoMT security [80] Federated learning enables IoMT compliance with GDPR and HIPAA, protecting patient privacy while supporting secure clinical data use [70]. HIPAA and GDPR are essential for securing patient data [58].	Compliance with HIPAA, GDPR, and ethical regulations is vital for securing IoMT devices and ensuring trustworthy clinical deployment [60]. IDS design must ensure patient data confidentiality and integrity, comply with HIPAA/GDPR, and employ secure, privacy-preserving methods for clinical IoMT deployment [55]. Compliance with HIPAA/GDPR and ethical IDS design ensures confidentiality, integrity, and secure clinical deployment of IoMT systems [80]. Federated Learning ensures compliance with GDPR and HIPAA by upholding data minimization and sharing insights without compromising patient privacy [70]. Compliance with HIPAA and GDPR is essential for securing patient data and ensuring safe IoMT clinical deployment [58].

Table 18
A mapping table between privacy regulations and IDS via FL.

Privacy principle (GDPR / HIPAA)	Evidence level	Supporting study	Mapping to FL-based IDS
Data Privacy & Data Protection (GDPR)	Implicit / Design Implication Only	[58]	FL-based IDS reduces direct access to sensitive information by storing raw data on local devices and sharing only model parameters, thereby facilitating the deployment of privacy-preserving IDS.
Data Minimization (GDPR)	Implicit / Design Implication Only	[58]	Because IDS training occurs locally, only model updates are shared, reducing exposure of raw user or patient data.
Confidentiality & Privacy Protection (GDPR)	Implicit / Design Implication Only	[70]	By keeping sensitive healthcare or IDS data on client devices, FL minimizes exposure risks and aligns conceptually with GDPR privacy requirements by ensuring that such data is not transferred or stored elsewhere.
Regulatory Constraints & Privacy Compliance Context (GDPR / HIPAA)	Implicit / Design Implication Only	[64]	By allowing models to be trained locally, FL overcomes the limitations of traditional ML and reduces the need for centralized data sharing, which conceptually mitigates privacy concerns related to GDPR/HIPAA.

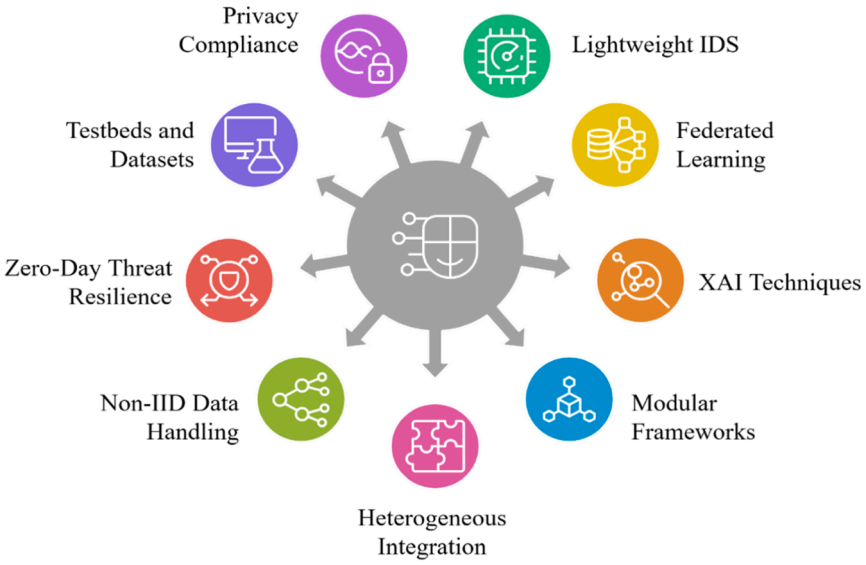


Fig. 10. Future directions of IDS in IOMT in smart hospitals.

Appendix

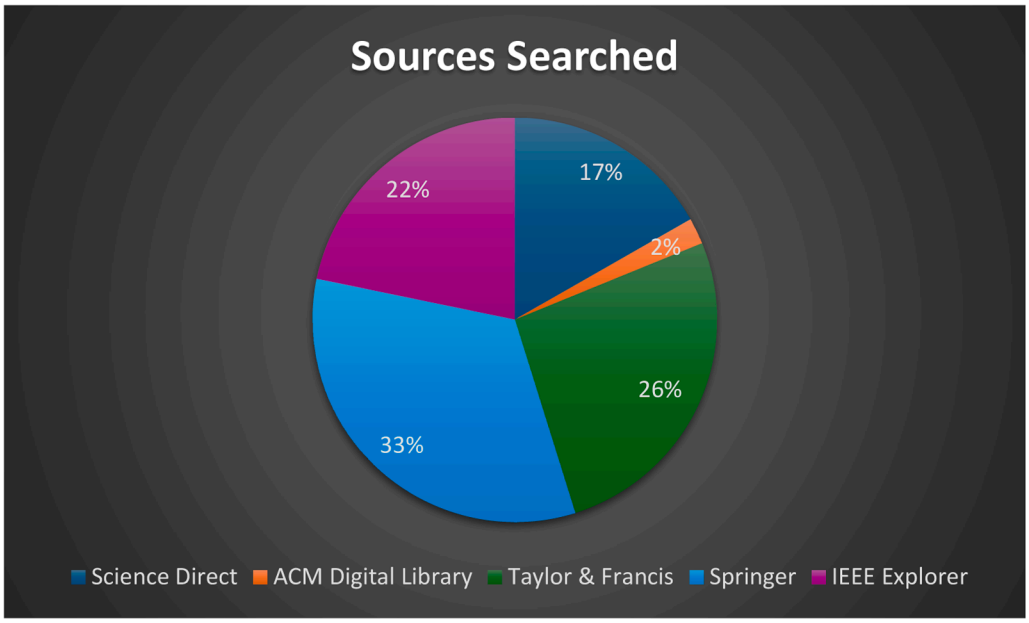


Fig. A1. Sources were searched for the relevant research articles.

Fig. A1 highlights the sources that were searched across multiple databases to identify relevant research articles. A comprehensive search strategy was employed to ensure the inclusion of all pertinent studies.

Table A1
Screening process, based on multiple parameters.

Phase	Process	Selection criteria	Science Direct	ACM Digital Library	Taylor & Francis Online	Springer	IEEE Xplore	Total
1	Searching	Keywords	40	5	63	79	52	239
2	Screening	Repeated Studies	26	4	25	41	30	126
3	Further screening	Title + Abstract	10	3	14	19	18	64
4	Further screening	Introduction and Conclusion	8	2	12	10	12	44
5	Evaluation	Complete Article	4	2	10	4	12	32

Table A1 outlines a systematic literature review screening process that spans several academic databases. This process unfolds in five distinct phases, which start with initial keyword searches.

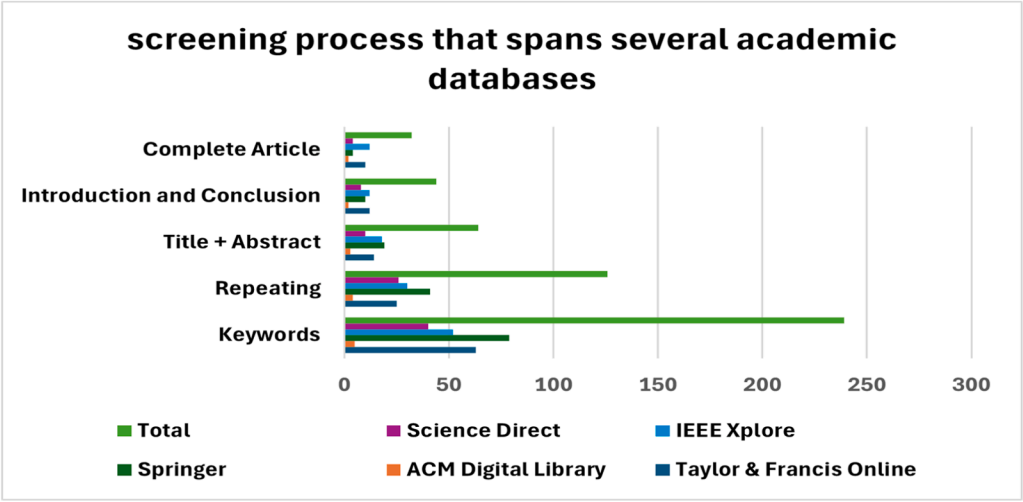


Fig. A2. Selection criteria based on keywords, title, abstract, introduction, conclusion, and complete analysis.

Fig. A2 shows that the selection criteria for including research articles were based on a detailed evaluation of several key components to ensure the relevance and quality of the studies.

Data availability

Data will be made available on request.

References

[1] M. Habibur, M.H. Hasan, M.S. Sadik, M. Estehad, M. Rahatul, P. Kumar, A. Rahman, Impact of Internet of Things (IoT) on healthcare in transforming patient care and overcoming operational challenges, J. Angiother. 8 (11) (2024) 1–8.
[2] D.K.A.A. Rizk, H.M. Hosny, S. ElHorbety, A.-B. Salem, Smart hospital management systems based on Internet of Things: challenges, intelligent solutions and functional requirements, Int. J. Intell. Comput. Inform. Sci. 22 (1) (2022) 32–43.
[3] M. Afa, M. Alam, M. Enam, AI-infused respiratory diagnostics: a new era in healthcare. Security and Privacy in Internet of Things*, CRC Press, 2025, pp. 22–28, https://doi.org/10.1201/9781003606055-11.
[4] P. Bhambri, A. Khang, Managing and monitoring patients' healthcare using AI and IoT technologies. Driving Smart Medical Diagnosis Through AI-Powered Technologies and Applications, IGI Global, 2024, pp. 1–23.
[5] A. Reyes-Menendez, J. Saura, P. Palos-Sanchez, Cybersecurity and the Internet of Things: anticipating the leverage of cyber crimes with interconnected devices. The Evolution of Business in the Cyber Age, Apple Academic Press, 2020, pp. 263–291.
[6] B. Buyuktanir, Ş. Altinkaya, G. Karatas Baydogmus, et al., Federated learning in intrusion detection: advancements, applications, and future directions, Cluster. Comput. 28 (2025) 473, https://doi.org/10.1007/s10586-025-05325-w.
[7] N. Ahmad, M. Alam, Cybersecurity challenges for social, ad-hoc, and sensor networks in the Internet of Things. Security and Privacy in Internet of Things, CRC Press, 2024, pp. 269–287, https://doi.org/10.1201/9781003528982-12.
[8] E. Biermann, E. Cloete, L.M. Venter, A comparison of intrusion detection systems, Comput. Secur. 20 (8) (2001) 676–683.
[9] O.C. Edo, D. Ang, P. Billakota, J.C. Ho, A zero trust architecture for health information systems, Health Technol. (Berl) 14 (1) (2024) 189–199.
[10] M. Alam, Z. Ashraf, P. Singh, B. Pandey, K. Rehman, L. Aldasheva, Deep learning techniques for intrusion detection systems in healthcare environments, in: 2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2025, pp. 105–111, https://doi.org/10.1109/CSNT64827.2025.10968425.
[11] B. Shanmugam, S. Azam, Risk assessment of heterogeneous IoMT devices: a review, Technologies (Basel) 11 (1) (2023) 31.
[12] O.I. Abiodun, E.O. Abiodun, M. Alawida, R.S. Alkhawaldeh, H. Arshad, A review on the security of the Internet of Things: challenges and solutions, Wirel. Pers. Commun. 119 (2021) 2603–2637.
[13] K. Srivastava, K. Faist, B. Lickert, K. Neville, N. McCarthy, M. Fehling-Kaschek, A. Stolz, Assessment of the impact of cyber-attacks and security breaches in diagnostic systems on the healthcare sector, in: 2024 IEEE International Conference on Cyber Security and, Resilience (CSR), 2024.
[14] G. Pradyumna, R.B. Hegde, K. Bommegowda, T. Jan, G.R. Naik, Empowering healthcare with IoMT: evolution, machine learning integration, security, and interoperability challenges, IEEE Access. 12 (2024) 20603–20623.
[15] M. Rahman, H. Jahankhani, Security vulnerabilities in existing security mechanisms for iomt and potential solutions for mitigating cyber-attacks, Inform. Secur. Technol. Controll. Pandem. (2021) 307–334.
[16] H. Boyes, M.D. Higgins, An overview of information and cyber security standards, J. ICT Standardi. 12 (1) (2024) 95–134.
[17] M. Anisetti, C. Ardagna, M. Cremonini, E. Damiani, J. Sessa, L. Costa, Security threat landscape, White Paper Secur. Threats (2020).
[18] M.A.I. Mallick, R. Nath, Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments, World Sci. News 190 (1) (2024) 1–69.
[19] C. Zhong, A. Sarkar, S. Manna, M.Z. Khan, A. Noorwali, A. Das, K. Chakraborty, Federated learningguided intrusion detection and neural key exchange for safeguarding patient data on the Internet of Medical Things, Int. J. Mach. Learn. Cybern. 15 (12) (2024) 56355665, https://doi.org/10.1007/s13042024022692.
[20] García, M.R., Betts, K., & Ponce, E. (2025). Identifying the key vulnerabilities in the warehouses of the future.

[21] S. Mittal, S. Dhand, T.M.N. Luu, Intrinsic vulnerabilities of RPA systems. Intelligent Robotic Process Automation: Development, Vulnerability and Applications, IGI Global Scientific Publishing, 2025, pp. 75–104.
[22] A. Berguiga, A. Harchay, A. Massaoudi, HIDS-IoMT: a deep learning-based intelligent intrusion detection system for the internet of medical things, IEEE Access. (2025).
[23] A. Salehpour, M.A. Balafar, A. Souri, An optimized intrusion detection system for resource-constrained IoMT environments: enhancing security through efficient feature selection and classification, J. Supercomput. 81 (6) (2025) 783.
[24] 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.
[25] M. Ozaif, S. Mustajab, M. Alam, Navigating challenges in IoT: applications, limitations, tools and open research direction, in: 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT), Jabalpur, India, 2024, pp. 525–531, https://doi.org/10.1109/CSNT60213.2024.10546141.
[26] A. Thakkar, R. Lohiya, A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges, Arch. Comput. Methods Eng. 28 (4) (2021) 3211–3243.
[27] Y.L. Khaleel, M.A. Habeeb, A. Albahri, T. Al-Quraishi, O. Albahri, A. Alamoodi, Network and cybersecurity applications of defense in adversarial attacks: a state-of-the-art using machine learning and deep learning methods, J. Intell. Syst. 33 (1) (2024) 20240153.
[28] N.S. Musa, N.M. Mirza, S.H. Rafique, A.M. Abdallah, T. Murugan, machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions, IEEE Access 12 (2024) 17982–18011.
[29] G. Zachos, G.M., K. Porfyrakis, J.ManuelCamõesSobral de Bastos and J. Rodriguez, (2025) Anomaly-based intrusion detection for IoMT networks: design, implementation, dataset generation, and ML algorithms evaluation.
[30] M. Nkoom, S.G. Hounsinou, G.V. Crosby, Securing the internet of robotic things: a comprehensive review on machine learning-based intrusion detection, J. Cyber Secur. Technol. (2024) 1–50.
[31] 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.
[32] A.N. Lone, S. Mustajab, M. Alam, A comprehensive study on cybersecurity challenges and opportunities in the IoT world, Secur. Privacy 6 (6) (2023) e318, https://doi.org/10.1002/spy2.318.
[33] M.P. Uddin, Y. Xiang, M. Hasan, J. Bai, Y. Zhao, L. Gao, A systematic literature review of robust federated learning: issues, solutions, and future research directions, ACM. Comput. Surv. 57 (10) (2025) 1–62.
[34] N. Alhumam, M.H. Rahman, A. Aljughaiman, A comprehensive review on cybersecurity of digital twins issues, challenges, and future research directions, IEEE Access. (2025).
[35] H. Ullah, S. Manickam, M. Obaidat, S.U.A. Laghari, M. Uddin, Exploring the potential of metaverse technology in healthcare: applications, challenges, and future directions, IEEE Access. 11 (2023) 69686–69707.
[36] I. Rozlomii, A. Yarmilko, S. Naumenko, Data security of IoT devices with limited resources: challenges and potential solutions, Doors 3666 (2024) 85–96.
[37] S. Yılmaz, E. Aydogan, S. Sen, A transfer learning approach for securing resource-constrained iot devices, IEEE Trans. Inform. Forensics. Secur. 16 (2021) 4405–4418.
[38] C. Slimani, L. Morge-Rollet, L. Lemarchand, D. Espes, F. Le Roy, J. Boukhobza, A study on characterizing energy, latency and security for intrusion detection systems on heterogeneous embedded platforms, Future Gener. Comput. Syst. 162 (2025) 107473.
[39] D.P. Sharma, A. Habibi Lashkari, M. Parizadeh, Defining cybersecurity in healthcare. Understanding Cybersecurity Management in Healthcare: Challenges, Strategies and Trends, Springer, 2024, pp. 35–54.
[40] 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 (Basel) 10 (21) (2021) 2562.
[41] E.K. Oikonomou, R. Khera, Designing medical artificial intelligence systems for global use: focus on interoperability, scalability, and accessibility, Hellenic J. Cardiol. 81 (2025) 9–17.
[42] A.H. Adepoju, A. Eweje, A. Collins, B. Austin-Gabriel, Framework for migrating legacy systems to next-generation data architectures while ensuring seamless integration and scalability, Int. J. Multidisc. Res. Growth Eval. 5 (6) (2024) 1462–1474.
[43] D. Ajish, Streamlining cybersecurity: unifying platforms for enhanced defense, Int. J. Inform. Technol. Res. Appl. 3 (2) (2024) 48–57.
[44] Hou, X., Zhao, Y., Wang, S., & Wang, H. (2025). Model context protocol (mcp): Landscape, security threats, and future research directions. *arXiv preprint arXiv: 2503.23278*.
[45] Ö. Aslan, S.S. Aktuğ, M. Ozkan-Okay, A.A. Yilmaz, E. Akin, A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions, Electronics (Basel) 12 (6) (2023) 1333.
[46] N. Vemuri, N. Thaneeru, V.M. Tatikonda, Adaptive generative AI for dynamic cybersecurity threat detection in enterprises, Int. J. Sci. Res. Arch. 11 (1) (2024) 2259–2265.
[47] W.N. Ismail, M.M. Hassan, H.A. Alsalamah, G. Fortino, CNN-based health model for regular health factors analysis in internet-of-medical things environment, IEEE Access. 8 (2020) 52541–52549.
[48] B. Kaur, S. Dadkhah, F. Shoeleh, E.C.P. Neto, P. Xiong, S. Iqbal, P. Lamontagne, S. Ray, A.A. Ghorbani, Internet of things (IoT) security dataset evolution: challenges and future directions, Internet Things 22 (2023) 100780.
[49] 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. (2025) 150, https://doi.org/10.1016/j.cose.2024.104288.
[50] M. Ibrahim, A. Al-Wadi, Enhancing IoMT network security using ensemble learning-based intrusion detection systems, J. Eng. Res. (Ponta Grossa) (2024), https://doi.org/10.1016/j.jer.2024.12.003.
[51] C. Huang, J. Wang, S. Wang, Y. Zhang, Internet of medical things: a systematic review, Neurocomputing 557 (2023), https://doi.org/10.1016/j.neucom.2023.126719.
[52] Y. Zhang, D. Zhu, M. Wang, J. Li, J. Zhang, A comparative study of cyber security intrusion detection in healthcare systems, Int. J. Crit. Infrastr. Prot. (2024) 44, https://doi.org/10.1016/j.ijcip.2023.100658.
[53] R.M. Czekster, T. Webber, L.B. Furstenau, C. Marcon, Dynamic risk assessment approach for analysing cybersecurity events in medical IoT networks, Internet Things 29 (2025), https://doi.org/10.1016/j.iot.2024.101437.
[54] U. Zukaib, X. Cui, C. Zheng, M. Hassan, Z. Shen, Meta-IDS: meta-learning-based smart intrusion detection system for internet of medical things (IoMT) network, IEEE Internet. Things. J. 11 (13) (2024) 23080–23095, https://doi.org/10.1109/jiot.2024.3387294.
[55] A. Naghib, F.S. Gharehchopogh, A. Zamanifar, A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities, Artif. Intell. Rev. 58 (4) (2025), https://doi.org/10.1007/s10462-024-11101-w.
[56] A.C. M. Fahim-Ul-Islam, M.G.R. Alam, S.S. Maidin, A_Resource-Efficient_Federated_Learning_Framework_for_Intrusion_Detection_in_IoMT_Networks.pdf, >, IEEE Trans. Consum. Electron. (2025).
[57] A.A. A. Aljuhani, P. Kumar, A. Jolfaei, An intelligent and explainable SaaS-based intrusion detection system for resource-constrained IoMT, IEEE Internet. Things. J. 11 (15) (2024) 25454–25463, https://doi.org/10.1109/JIOT.2023.3327024.
[58] A. Chaddad, Y. Wu, C. Desrosiers, Federated learning for healthcare applications, IEEe Internet. Things. J. 11 (5) (2024) 7339–7358, https://doi.org/10.1109/jiot.2023.3325822.
[59] B. Singh, D. Lopez, R. Ramadan, Internet of things in healthcare: a conventional literature review, Health Technol. (Berl) 13 (5) (2023) 699–719, https://doi.org/10.1007/s12553-023-00771-1.
[60] M.L. Hernandez-Jaimes, A. Martinez-Cruz, K.A. Ramírez-Gutiérrez, C. Feregrino-Uribe, Artificial intelligence for IoMT security: a review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures, Int. Things 23 (2023) 100887, https://doi.org/10.1016/j.iot.2023.100887.

[61] S. Rani, A. Kataria, S. Kumar, P. Tiwari, Federated learning for secure IoMT-applications in smart healthcare systems: a comprehensive review, Knowl. Based. Syst. (2023) 274, https://doi.org/10.1016/j.knosys.2023.110658.
[62] S. Mehmood, R. Amin, J. Mustafa, M. Hussain, F.S. Alsubaei, M.D. Zakaria, Distributed denial of services (DDoS) attack detection in SDN using optimizer-equipped CNN-MLP, PLoS. One 20 (1) (2025) e0312425, https://doi.org/10.1371/journal.pone.0312425.
[63] M.L. Rethlefsen, M.J. Page, PRISMA 2020 and PRISMA-S: common questions on tracking records and the flow diagram, J. Med. Libr. Assoc. JMLA 110 (2) (2022) 253.
[64] R.S. Antunes, C. André da Costa, A. Küderle, I.A. Yari, B. Eskofier, Federated learning for healthcare: systematic review and architecture proposal, ACM. Trans. Intell. Syst. Technol. 13 (4) (2022) 1–23, https://doi.org/10.1145/3501813.
[65] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, E. Mahdipour, A systematic review of IoT in healthcare: applications, techniques, and trends, J. Netw. Comput. Appl. 192 (2021), https://doi.org/10.1016/j.jnca.2021.103164.
[66] 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) (2021) 8707–8718, https://doi.org/10.1109/jiot.2020.3045653.
[67] M. Poongodi, A. Sharma, M. Hamdi, M. Maode, N. Chilamkurti, Smart healthcare in smart cities: wireless patient monitoring system using IoT, J. Supercomput. 77 (11) (2021) 12230–12255, https://doi.org/10.1007/s11227-021-03765-w.
[68] 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://doi.org/10.1109/access.2020.3000421.
[69] M. Alazab, S.P. Rm, P. M, P.K.R. Maddikunta, T.R. Gadekallu, Q.-V Pham, Federated learning for cybersecurity: concepts, challenges, and future directions, IEEE Trans. Industr. Inform. 18 (5) (2022) 3501–3509, https://doi.org/10.1109/tii.2021.3119038.
[70] B. Pfitzner, N. Steckhan, B. Arnrich, Federated learning in a medical context: a systematic literature review, ACM. Trans. Internet. Technol. 21 (2) (2021) 1–31, https://doi.org/10.1145/3412357.
[71] Y.K. Saheed, M.O. Arowolo, Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms, IEEE Access. 9 (2021) 161546–161554, https://doi.org/10.1109/access.2021.3128837.
[72] G. Thamilarasu, A. Odesile, A. Hoang, An intrusion detection system for internet of medical things, IEEE Access. 8 (2020) 181560–181576, https://doi.org/10.1109/access.2020.3026260.
[73] Y. Li, Y. Zuo, H. Song, Z. Lv, Deep learning in security of internet of things, IEEE Internet. Things. J. 9 (22) (2022) 22133–22146, https://doi.org/10.1109/jiot.2021.3106898.
[74] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, M. Dinesh, An investigation and comparison of machine learning approaches for intrusion detection in the IoMT network, J. Supercomput. 78 (15) (2022) 17403–17422, https://doi.org/10.1007/s11227-022-04568-3.
[75] F. Wu, C. Qiu, T. Wu, M.R. Yuce, Edge-based hybrid system implementation for long-range safety and healthcare IoT applications, IEEE Internet. Things. J. 8 (12) (2021) 9970–9980, https://doi.org/10.1109/jiot.2021.3050445.
[76] D. Man, F. Zeng, W. Yang, M. Yu, J. Lv, Y. Wang, Q. Jiang, Intelligent intrusion detection based on federated learning for edge-assisted internet of things, Secur. Commun. Netw. 2021 (2021) 1–11, https://doi.org/10.1155/2021/9361348.
[77] I. Keshta, AI-driven IoT for smart health care: security and privacy issues, Inform. Med. Unlocked 30 (2022), https://doi.org/10.1016/j.imu.2022.100903.
[78] 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) (2021) 1999–2017, https://doi.org/10.1007/s11277-021-08756-x.
[79] S.B. Weber, S. Stein, M. Pilgermann, T. Schrader, Attack detection for medical cyber-physical systems–a systematic literature review, IEEE Access. 11 (2023) 41796–41815, https://doi.org/10.1109/access.2023.3270225.
[80] M. Mahmood, M.I. Khan, Ziauddin, H. Hussain, I. Khan, S. Rahman, M. Shabir, B. Niazi, Improving security architecture of internet of medical things: a systematic literature review, IEEE Access. 11 (2023) 107725–107753, https://doi.org/10.1109/access.2023.3281655.
[81] O.K. Sahingoz, U. Cekmez, A. Buldu, Internet of Things (IoTs) security: intrusion detection using deep learning, J. Web Eng. (2021), https://doi.org/10.13052/jwe1540-9589.2062.
[82] I.A. Ali, W.A. Bukhari, M. Adnan, M.I. Kashif, A. Danish, A. Sikander, Security and privacy in IoT based smart farming: a review, Multimed. Tools. Appl. (2024), https://doi.org/10.1007/s11042-024-19653-3.
[83] S. Ouhbi, A. Idri, J.L. Fernández-Alemán, A. Toval, Requirements engineering education: a systematic mapping study, Requir. Eng. 20 (2) (2015) 119–138, https://doi.org/10.1007/s00766-013-0192-5.
[84] B.C. Uslu, E. Okay, E. Dursun, Analysis of factors affecting IoT-based smart hospital design, J. Cloud. Comput. (Heidelb) 9 (1) (2020) 67.
[85] Ngo, M.V., Chaouchi, H., Luo, T., & Quek, T.Q.S. (2020). *Adaptive anomaly detection for IoT data in hierarchical edge computing* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2001.03314.