Discover Applied Sciences

Review

IoMT landscape: navigating current challenges and pioneering future research trends

Badraddin Alturki[1] · Qasem Abu Al-Haija[2] · Rayan A. Alsemmeari[1] · Abdulaziz A. Alsulami[3] · Ali Alqahtani[4] · Bandar M. Alghamdi[1] · Sheikh Tahir Bakhsh[5] · Riaz Ahmed Shaikh[6]

Received: 7 September 2024 / Accepted: 14 November 2024
Published online: 18 December 2024

Abstract
Technological advancement drives the growth of the Internet of Things (IoT) applications in many fields, such as smart homes, smart cities, smart grids, and healthcare. IoT in healthcare is called the Internet of Medical Things (IoMT), which provides remote patient treatment using information and communications technology. This new telemedicine technology simplifies the regular and effective communication between medical and computing devices. Critical motivations for adopting the IoMT are reduced cost, increased quality of life, and timely medical intervention. IoMT is significant because it enables continuous, real-time patient monitoring during routine everyday activities using a variety of wearables and sensors. With big data, IoMT technology makes excellent use of Machine Learning (ML) to support disease detection and health condition prediction, alerting patients and healthcare providers. Many research studies have been conducted to explore several aspects of IoMT and its applications in the real world. However, it is challenging to comprehend all the techniques and solutions proposed by the research community. Therefore, this survey sheds light on some crucial aspects of IoMT technology and explores the potential research gaps and directions the research community could tackle. The survey examines and discusses the characteristics of IoMT standards, protocols, and types. It then delves into the layers of IoMT and distinguishes them into fog and edge. The studies published under each type were explored, and the limitations of these works were highlighted. The research gaps and directions on IoMT approaches and technology were also highlighted. With such findings and research directions, further research endeavors could be carried out to address the issues and existing limitations in the IoMT.

1 Introduction

Smart electronic devices and telemedicine are widely used in people's daily lives. Telemedicine refers to the remote treatment of patients using information and communication technology. Emerging telemedicine trends such as Medical cyber-physical systems (MCPS) facilitate regular and efficient interactions between medical and computing devices [1]. A Cyber-Physical System (CPS) integrates networking, physical processes, computers, and physical components, enabling seamless interactions between cyber services and physical components [2]. Incorporating

✉ Qasem Abu Al-Haija, qsabuhaija@just.edu.jo | [1]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia. [2]Department of Cybersecurity, Faculty of Computer & Information Technology, Jordan University of Science and Technology, PO Box 3030, Irbid 22110, Jordan. [3]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia. [4]Department of Networks and Communications Engineering, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia. [5]Department of Computer Science, Cardiff Metropolitan University, Western Avenue, Cardiff CF5 2YB, UK. [6]School of Computing Sciences, University of East Anglia, Norwich, UK.

the Internet of Things (IoT) in medical care has become increasingly popular in the era of 5G technology. Many medical and healthcare applications, for example, remote health monitoring, elderly care, fitness programs, and even metaverse-based healthcare [3] have emerged due to the capability of many portable devices like mobile phones to integrate medical-related functions and easy internet access. These devices provide an efficient and effective way to combine medication at home with healthcare centers and keep patients who require special care under real-time observation. To achieve this, medical devices can be integrated into the Internet of Medical Things (IoMT) ecosystem. IoMT is an ecosystem that connects patients and medical activity at any time. With the assistance of 5G and IPv6, the IoMT can play a crucial role in medical diagnoses and treatments.

One of the key objectives of implementing the IoMT is reduced costs, increased quality of life, and timely medical intervention. A significant benefit of IoMT is the ability to use efficient scheduling. It also provides seamless and secure communication between the patient and the healthcare provider. IoMT supports real-time, reliable monitoring and early diagnosis. Utilizing public network topology, patients' health records can be processed and stored on the cloud or locally, facilitating delivering real-time health services.

The IoMT aims to provide efficient solutions for delivering medical healthcare services, such as personalized devices for diagnosis, telemedicine systems, and electronic record systems. The importance of IoMT comes from the need to continuously observe patients in real-time during normal daily activities with the help of sensors and wearable devices. The data collected from such observation is vital to diagnose and predict health conditions in the long term, and it is important to observe the trends at both personal and social levels. Developing coherent and high-quality healthcare services becomes easy by envisioning such a trend. Furthermore, integrating IoMT into healthcare services helps provide faster and more cost-effective care, improves the patient experience, and saves healthcare resources. Moreover, the IoMT facilitates the customization and prioritization of healthcare services based on patient's needs and/or health conditions.

The IoMT technology uses Artificial Intelligence (AI) to support disease detection and health condition prediction, alerting patients and healthcare providers [4]. A significant benefit from such a transformation is the change in medical diagnosis, which has shifted from a manual, reactive, and time-consuming method to a more intelligent, automated, and proactive one. Medical care services become more effective by combining IoMT nodes and AI algorithms involving Deep Learning (DL) and Machine Learning (ML), and more recently, the new federated learning-based models have been applied to improve the healthcare systems in the IoMT [5]. Applying these algorithms efficiently can provide successful prediction models with the highest accuracy and precision, which increases healthcare services' efficacy and save many lives. However, the study of the potential of smart IoMT is still undergoing in both research and industry, and more work is yet to be done to use the enabling technologies and increase the involvement of these solutions in all aspects of the healthcare ecosystem.

As the IoMT is a multi-faceted field of research, comprehending the concepts and principles is challenging, especially for new areas. Research in IoMT could be tackled from several perspectives, including data processing, modeling, prediction, and security. For someone new to the area, there is always a need to survey articles that summarize the state-of-the-art and provide directions for moving forward with the research. Although several surveys have been published recently, the focus was on highlighting the latest development and proposal without sufficient emphasis on individual studies and subfields' limitations. This paper addresses this issue and critically analyzes the related scholarly publication in IoMT. Unlike existing surveys, this paper discusses IoMT-related literature and highlights the contribution and limitations of each article.

Additionally, research gaps and directions for further research are given at the end of each section. With such a critical analysis, we hope the research community can use some of these ideas.

Section 2 provides an overview of IoMT structures, protocols, and standards. It illustrates the major components of IoMT systems. Section 3 discusses existing techniques in edge computing, including limitations and research directions for IoMT systems. Section 4 addresses fog computing and its related research techniques, analysis of existing techniques, evaluation criteria, limitations, and research directions. Section 5 emphasizes IoMT processing techniques that could be conducted globally in a centralized location or distributed in local nodes. Section 6 provides an overall summary, identifies potential constraints, and concludes the paper by highlighting the main findings from related literature.

2 The IoMT structures and standards

Figure 1 shows the major components of IoMT systems as proposed by the Continua Health Alliance. The figure shows that the system consists of four layers: Interoperability, Application Hosting Devices (AHD), WAN Devices, and Health Record Devices (HRD). This system is a simplified architecture that embodies the interaction between the different components and devices within the IoMT. In the Interoperability layer, sensors and patient-attached devices collect readings about vital signals [6]. These devices are wearable and, most of the time, are resource constrained. Therefore, the data they collect are sent immediately to the hosting device(s) in the next layer, i.e., Application Hosting Devices. The communication between the Interoperability layer's devices and the device in the next layer uses Wi-Fi technology. Each sensor and wearable device are embedded with wireless hardware to transfer the data into the hosting devices in the AHD layer. Smartwatches, portable ECGs, and thermometers are examples of Interoperability devices that collect data about the patient's health condition. The AHD layer consists of several devices that have capabilities higher than the Interoperability layer, such as laptops and smartphones. Furthermore, the connection between the devices in the AHD and Interoperability layers is performed by either Wireless Body Area Networks (WBAN) or Wi-Fi [7]. These devices are used as local storage for data from the sensors and devices in the Interoperability layer. The third layer is the WAN devices layer. It collects data from several systems and stores them in one location, such as a corporate office, government office, or WAN data storage. Analytical processing and predictive modeling are normally conducted in this layer as the devices have the processing power and memory capacity to run sophisticated algorithms like deep learning to build different models. The WAN Devices layer is connected to the AHD layer using WAN technology such as PPPoE, Frame Relay, DSL, or Fibre Optic. In the fourth layer, called the Health Record Device (HRD), the data are relayed into a shared online data center in the cloud to be accessed over the Internet. Other types of services are also provided by this layer, like frontend analysis and modeling. The HRD is connected with the WAN Devices layer.

Another framework was proposed, which resembles the popular network TCP/IP framework and stacks the system into four layers: Transport, Network, 6 LoWPAN Adaptation, and Link & Physical [8]. Figure 2 shows the structure of this framework. In the application layer, several protocols and application programming interfaces are defined. This set of protocols includes well-known applications like HTTP, SSL, and COAP. These protocols facilitate the interaction between user-related applications and the network module in the operating system. Using these protocols, the application layer collects, prepares, formats, and packs the data before passing them into the transport layer. Control Protocol (TCP)s, User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), are used in the transport layer to encapsulate the data with the necessary information for application-to-application communication between the communicating peers. Whether to use TCP or UDP relies on the nature of the application used by the communicating pair. TCP or UDP should be used if the communicating nodes need a reliable session [9].

The destination and source addresses are added to the header in the transport layer. The data from the application layer is encapsulated in segments, each with the same header and information about the source and destination ports. The data are then passed down into the network layer, where another addressing information will be attached to each segment's header and encapsulated into user datagrams. In IoMT, IPv6 is used to assign both source and destination

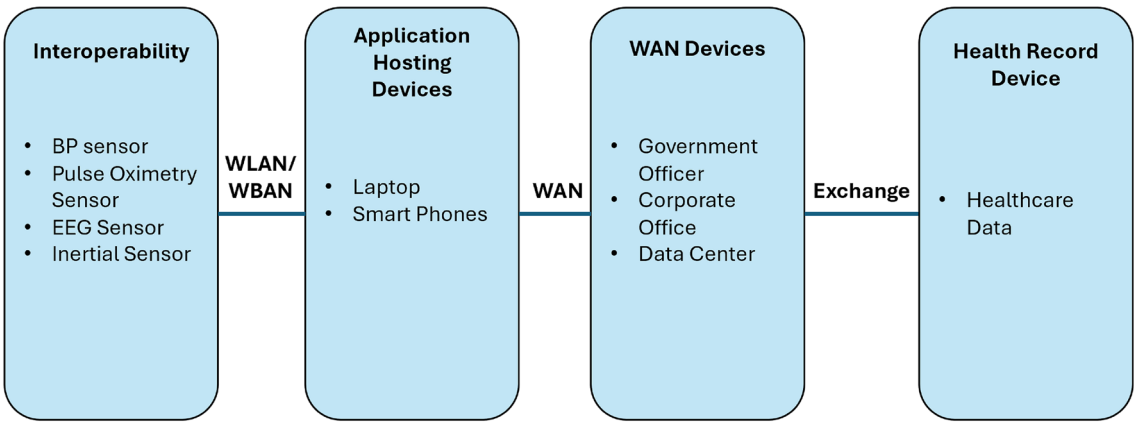

Fig. 1 The components of IoMT by the continua health alliance

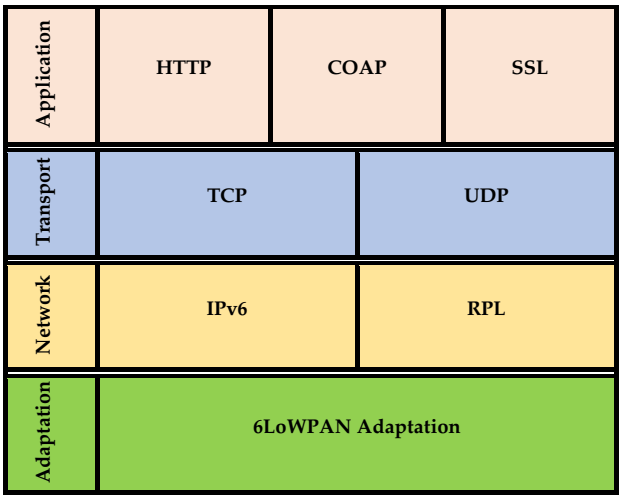

Fig. 2 Resembling the popular network TCP/IP framework and stacks

addresses. Another protocol type is defined in the network layer, which is the RPL responsible for routing the datagrams from the source to the destination. Such a routing mechanism guarantees end-to-end delivery of the data. After adding the IP addressing and routing information, the datagrams are passed down to the adaptation layer. This layer defines the power Wireless Personal Area Network, which optimizes the transmission of the IPv6 packets in 802.11.15.4 frames. This standard is suitable for IoMT sensors as it is low cost, low power, low bit rate, and short range. The data frames are converted into the binary form at the link and Physical layer and encoded into electrical signals that travel through transmission media between source and destination. Encapsulation, which happens at the sender end, passes data from the application layer down to the physical layer while attaching additional information to the header. Data travels from the physical layer to the application layer, and the respective header information is removed at the receiver end. This process is called decapsulation [10].

2.1 IoMT Data types and protocols

Data from IoMT devices and sensors contain a wide range of information, such as address, radio, historical, and command data. These devices often operate in real time, necessitating timely and efficient data processing. Address data consists of the node's physical and logical addresses attached to the data packets. These addresses help to track data trajectories from source to destination. Radio data records the technology-specific information for each communicating pair and is characterized by different packet structures. Understanding the specific structure of these packets is crucial for optimizing communication protocols. These data are usually generated by Radio Frequency Identification Module (RFID), Bluetooth, LoRA, and ZigBee. Furthermore, IoMT ecosystems generate historical data, this information can include usage patterns, device status, and environmental factors, describing the events of different processing and interactions between the sensors, edge devices, and systems. Among these historical data, the commands sent from controllers to actuators are used to do some tasks, like sending a signal to a wearable device to recalibrate or a notification about the new condition to the healthcare center [11].

Due to the heterogeneous nature of IoMT systems, the data collected is highly dimensional, which adds extra burden to the processing and analysis. Furthermore, the various components produce unstructured data types like text, images, and symbols, which makes the analysis and modeling more challenging. It is important to implement effective data preprocessing models to manage this complexity. Furthermore, transmitting this data to wireless networks makes them susceptible to noise, loss, and attacks. Such threats may negatively affect the quality and reliability of data and related models. Therefore, addressing these issues when addressing IoMT data is essential. IoMT's heterogeneity is not limited to data verity and communication technology but also includes protocol diversity. These protocols are not restricted to ZigBee, RFID, LoRA, and TCP/IP. In IoMT, the processes of data acquisition, manipulation, analysis, and modeling are influenced by several factors. This involves several applications that require decision-making, security, and prediction. The heterogeneous protocols must communicate the information needed to decide resiliently and smoothly. However, this is challenging since the standard differences may make it difficult for some protocols to cooperate. Standardizing protocols could improve interoperability among IoMT devices, facilitating smoother communication. For example, an

IP-based hub could not directly exchange packets with a Bluetooth-based IoT-Connected Inhaler, and a converter could be needed [12].

IoMT needs to address data security and privacy in light of heterogeneous protocols. An ECG device running well-secured protocols could become vulnerable when cooperating with less secure protocols. Therefore, IoMT must guarantee that the data exchanged among different protocols is secure and private. The diversity, privacy, and security of data exchanged between IoMT components impact predictive modeling. As pointed out, the variety of data comes at the cost of high dimensionality, extensive pre-processing, and type incompatibility [13]. Furthermore, data privacy and security might become issues when dealing with diverse protocols and technologies. For instance, attackers can manipulate, hijack, and falsify the data in a vulnerable node. Establishing robust security measures at each node can help mitigate these risks. This adversely affects the accuracy of predictive modeling built based on this data.

3 Existing research in IoMT

The application of IoMT hugely relies on big data collected from sensors that are directly or indirectly attached to the human body [14]. Vital data are collected from these sensors in real-time simultaneously among hundreds or thousands of medical things. With such enormous amounts of data collected, they must be stored in servers with resources sufficient to process and analyze them. However, the cost of collecting and storing data is high. Thus, it is imperative to make a trade-off between efficiency in terms of cost and effectiveness in terms of thoroughness. Several approaches have been proposed to provide solutions that effectively use collected data. The following sections explore these approaches more.

3.1 Edge computing

Edge computing, called the Edge of Things (EoT), is an IoT model that embodies the middle layer between sensors and cloud layers. The EoT connects the IoT gateways and IoT devices' terminal endpoints [15]. Several studies related to healthcare EoT data analytics have been proposed [16–18].

3.1.1 Studies in edge computing

An edge-assisted framework was proposed by [19], which controls the parameters of mobile sensors to identify anomalies in the collected signals in real time. Using a probabilistic approach, the framework addresses battery-imposed constraints. A use case evaluated it using vital signs like respiration rate, heart rate, and oxygen saturation from a Photoplethysmogram (PPG) signal. Experimental evaluation shows that the framework can effectively trade between low sensing energy consumption and high anomaly detection accuracy. However, preserving the battery comes at the cost of signal and data quality, which is important in real-time scenarios. These scenarios need a continuous data stream that keeps the sensors and backend systems busy. Consequently, reducing energy consumption could interrupt the data stream, which reduces data quality and sufficiency.

The HiCH model, proposed in [16], is a hierarchical computing architecture that used for IoT-based health monitoring systems. The architecture tends to increase reliability, punctuality, and availability of services and overcomes intermittent network connectivity with the centralized cloud-based IoT. It also tries to improve accuracy and adapts to topology and operating environment changes. The architecture comprises two main components: data sensing and data analytics. HiCH relies on features extracted from fog and cloud computing data to conduct the data analytics and modeling designed to manage healthcare IoT systems. However, the study's centralized approach lacks the resiliency to adapt to topology changes that might happen in IoMT systems due to patient mobility and a harsh operating environment. The architecture overlooks the potential data loss in such an environment in case of connectivity disruptions due to bottlenecks that a centralized gateway might introduce.

To overcome bottlenecks at the gateway level, the study by [17] suggested a Smart e-Health Gateway to position the gateways at the network's edge strategically. To assess the efficacy of the proposed solution, the UT-GATE, a Smart e-Health Gateway prototype, was built where a set of higher-level features have been used. A case study was conducted to show the system's efficiency and relevance by integrating an IoT-based Early Warning Score (EWS) for health monitoring. However, relying on the smart gateway is vulnerable to single-point-of-failure. Such a hierarchy also makes it impractical to deploy real-time monitoring without addressing connectivity disruption, transmission delay, and network

congestion. Data security and privacy are other concerns when applying centralized solutions, as the intruders could compromise the smart gateway, which puts the data and system at risk.

The study's security concern was addressed by [18], which proposed a novel Edge of Things (EoT) framework. Fully homomorphic encryption was employed to preserve data privacy in the EoT framework. A distributed clustering method was developed to collect and analyze the enormous and heterogeneous data in the EoT devices. A case study was conducted using patient biosignal data to show the efficacy of the proposed framework. Although the framework improved the analysis response time, the data's completeness was compromised due to the aggregation and summarization of the data. Consequently, incomplete data adversely affects the efficacy of patients' health monitoring and response.

BodyEdge, a human-centric architecture, was proposed by [20]. For healthcare applications. The architecture involves a mobile client module and a performing edge gateway. The gateway supports multi-radio communication to collect and process data from different scenarios. The gateway guarantees a flexible, robust, and adaptive healthcare service by exploiting components from public and private cloud environments. The efficacy of the proposed architecture was evaluated in terms of reduced processing time and transmitted data. The evaluation was conducted through an actual implementation on different hardware platforms, which shows that the BodyEdge is an efficient and cost-effective option for healthcare-related situations. However, relaying the processing burden to the gateway will lead to a bottleneck, which causes intermittent connectivity and disrupts the processing.

IoT and Edge Cloud were combined [21] for medical data retrieval. Such integration provides a secure healthcare monitoring framework that integrates the NDN-based IoT with the edge cloud. The framework improves the efficiency of medical data retrieval by exploiting the capabilities of NDN and strengthens the signature and ciphertext to support the security of medical data delivery. The framework was assessed quantitatively, which shows that the framework reduced the latent retrieval of medical data and the cost significantly compared with the existing solution. However, the cloud's integration with the edge is governed by the connection quality, which might experience many disruptions due to the patient's mobility.

Edge and cloud computing were exploited in the study conducted by [22]. Convolutional Neural Network (CNN) was used to create a classification model that conducts the classifier's heavy tasks to the servers on the cloud side and outsources the hypothesis function to the edge. This hierarchy helps to improve the response time. The proposed model's applicability was demonstrated by a case study on ECG classifications whose performance was evaluated regarding response time and accuracy. However, machine learning classifiers are static as they rely on one-time training to build the model. This is unsuitable for dynamic environments like IoMT, where patients are mobile and topology is ephemeral.

To address the problem of static classifiers in dynamic environments like IoMT, agile learning was proposed by [23] to build the EdgeCNN architecture, which utilizes the data generated and exchanged between edge and cloud computing for healthcare data. With the adaptation capability, deep learning was used as an inference method running on the edge layer to facilitate real-time analysis and diagnosis. This reduces learning latency significantly and improves network I/O, preserving cloud resources for massive data and large user groups. Accordingly, the cost of maintaining and building cloud platforms will be reduced. The intuition is that the system can make decisions faster by making data analytics closer to the data source. However, hosting a resource-hungry model like deep learning in resource-limited devices at the edge layer of IoMT makes deploying the system for real-world applications that need real-time operation difficult. Additionally, data security and reliability are some of the concerns that influence the performance of such data-driven modeling.

A secure framework for SDN-based Edge computing was proposed by [24]. To address the security concerns in IoMT ecosystems. The framework protects edge devices and preserves the privacy of sensitive patient data. A lightweight authentication scheme was used to authenticate the IoMT devices at the Edge layer. Once authenticated, edge devices collect data from the patients they are attached to and send them to the edge servers for further processing and analysis. An SDN controller connected edge components (sensors and servers) and balanced the network load. However, incorporating SDN renders the entire system vulnerable to many attacks that tend to disrupt network operations and redirect the traffic in such a way that creates bottlenecks. This bottleneck makes it difficult for the system to work as a real-time application. To support real-time applications, an energy-efficient edge-based healthcare support system (EESE-HSS) was proposed by [25] and applied to diabetic patients with cardiovascular disease. The proposed system employs the hierarchical computing architecture that Cloud Edge provides to cater to swift diagnosis during emergencies. Therefore, deep learning was used at the edge nodes to enable quick decisions and satisfy emergencies. However, deep understanding is resource-hungry, making it unsuitable for edge nodes with limited resources and insufficient data.

3.1.2 Limitations and research directions for edge computing in IoMT

The wide range of devices and nodes in edge computing that run different protocols and standards makes it challenging to deal with the diverse data, creating compatibility, consistency, and privacy problems. The nodes are connected to patients in the edge computing layer of IoMT infrastructure. These nodes are portable, which means they rely on batteries as a power source. Such portability means that these devices need light, affecting the battery capacity. Therefore, battery efficiency is an important aspect that needs to be focused on. Although several studies were conducted to address the issue of battery limitation, they overlook the unique characteristics of IoMT devices that require a real-time feed of data and resource-intensive contents that these devices might acquire. Some edge IoMT nodes and sensors are dedicated to observing critical health conditions. They must be synchronized with the control center in real-time to allow a healthcare provider to deliver the service on time. The real-time operation requires that edge nodes always be active, which depletes the battery quickly.

In addition, the portability of IoMT edge nodes causes intermittent connection as patients move around and sometimes become out of the network's coverage. Such disconnection disrupts the operation of the sensors and the transmission of data. This significantly complicates the analysis and predictive modeling as the data received on the processing side will be incomplete. Relying on incomplete data adversely affects the accuracy of analytics and modeling. Therefore, edge-related studies must consider patients' mobility when designing IoMT solutions.

On the other hand, the nature of data exchanged between edge devices and backend servers in the IoMT ecosystem necessitates sufficient bandwidth allocation to accommodate vital data sent/received at a high rate. This is imperative when dealing with life-related decisions that need synchronous and online analytics and prediction. Also, the intermittent connection might be caused by the noise emitted from a harsh environment that the patient might be in or from the co-located devices nearby. Such noise disrupts and distorts the signals carrying vital data, which leads to incorrect, incomplete, and inaccurate readings from the biosensors. As such, the IoMT solutions must be robust enough to work in such harsh environments.

3.2 Fog computing

Fog computing brings several benefits to healthcare such as reduced latency, location awareness, improved quality of service, real-time monitoring, and improving privacy. Fog computing architecture enables fast data transmission between IoT devices, which reduces communication delays especially for critical healthcare data. Location awareness allows for processing data closer to IoT devices, which helps for better understanding of the environment surrounding the patient. Furthermore, fog computing improves quality of service, as it addresses several changes, for example in network, fog computing reduces network congestion. In addition, fog computing allows for real-time monitoring, which leads to better response [26].

In the following subsections, we delve into fog computing. We will elaborate on characteristics and types before we explore studies related to the application of fog computing in IoMT.

3.2.1 Characteristics of fog computing

Fog computing expands cloud capabilities and offers the advantages of on-demand storage, network, and computing resources. It differs from the cloud in proximity to end-users, support for user mobility, and dense geographical distribution. The Cloud computing approach could not support these features because of its distance from end-users and centralized structure. The primary features of fog computing can be outlined as follows:

- As fog computing is located at the network's edge, it is closer to the end-user generating data. This indicates that Fog and IoT are on the same LAN, enabling them to exchange data faster. This helps us reduce delays, latency, and jitter, which is crucial for delay-sensitive applications such as emergency services and healthcare delivery. Dense Geographical Distribution: The fog computing approach of greater geographical distribution has numerous advantages over centralized cloud deployment.
- Support for Mobility: Fog computing supports the mobility of users and provides location awareness. It is made possible by geographical distribution and locating it at the network's edge. This location gives fog computing network and context information collected by traffic, analytics, and several IoT devices. Location awareness is key to healthcare service providers supporting users' mobility and offering a range of personalized mobile applications.

- These features provide a significant advantage of fog computing compared to the cloud computing approach. Because of geographical distribution and vicinity to end-users, Fog supports users' location awareness and mobility, reduces delay, latency, and jitter, eliminates data transmission in the network's infrastructure, and enhances encrypted data's flexibility, scalability, and security. However, Fog's computing has several constraints in resource such as limitations in computational power, memory, and energy resources therefore it cannot replace cloud computing [27].

3.2.2 IoMT fog-cloud computing

Fog computing is used to allow computing to be performed directly at the network's edge, which provides new services and applications, particularly for the Internet's future. For instance, commercial edge routers advertise the number of cores, processor speed, and built-in network storage. Such routers may become new servers. Infrastructures or facilities in fog computing that may provide resources for services at the network edge are called fog nodes. Fog nodes can be resource-poor devices like routers, set-top-boxes, access points, base stations, switches, resource-rich machines, and end devices like IOx and Cloudlet. Cloudlet is a resource-rich machine, and it is a small data center that provides computational resource closer to the edge devices, this allows of reducing the latency [28].

Managing private data centers for customers often utilizes the cloud computing model, where payment is based on data usage. To maintain the massive aggregation of data centers, the factors influencing data center efficiency must exhibit greater predictability to support high utilization with adequate performance. This includes leveraging cost-effective power sources across different locations, as well as optimizing storage and networking resources [29]. These optimizations can be achieved by using fog computing, which allows services and computation to be closer to IoT devices, which reduces the response time and improves efficiency [30]. Fog Computing facilitates the interplay of diverse applications and services within the Fog and the cloud in data management. It operates closer to the consumer, on the network edge, avoiding delays and failure in the network and leading to quicker decision-making in healthcare delivery [31].

Fog computing's function in big data analytics utilizes networking, storage, and computation of data, as well as virtualization and multi-tenancy, which are attributes the same as the cloud. There are a few differences in the functioning of both applications. The Fog considers the applications and features that were deficient in the cloud. It aids in geo-distributed applications such as monitoring pipelines and sensors associated with environmental data. It also enables the distribution of control systems on a large scale and fast mobile applications. With all these excellences, Fog complements the cloud rather than a substitution [20]. There are fog computing nodes (micro clouds) near the data source. It reduces the requirement of massive storage, processes a large amount of data before reaching the cloud, and reduces data communication duration and cost. It connects the IoT devices and the cloud data center by propelling the storage, networking, and cloud computing services near the end of the IoT devices [31].

In summary, from these two general architectures, it may be noted that data and applications are processed in the cloud in a centralized manner, which is time-consuming. In the fog case, it operates on the network's edge, and processing takes less time, thus overcoming delays. In clouds, bandwidth is expected because all data is transmitted over cloud channels (Internet). Alternatively, Fog does not demand more bandwidth as every bit of information is aggregated at certain access points within the sensor network rather than sending data over cloud channels. In clouds, servers can be located at remote locations, resulting in slow response time and scalability issues. Fog gateways or devices can be deployed at the network edge, thus overcoming response time and scalability. Hence, fog computing gateways provide more efficiency and reliability and help overcome latency issues in cloud-based healthcare application environments.

3.2.3 Studies in fog computing

Four criteria are proposed to evaluate the existing work for fog computing. The first criterion is heterogeneity, where fog nodes should provide multiple communication protocols to collect data from various IoT devices. The second criterion is scalability, so fog systems should handle increasing users. The fog platform must be able to deal with a huge number of IoT devices and users. Furthermore, they should be able to include many applications and fog nodes. The fog platform should be operational on such a large scale. The third criterion is Mobility Support, in which fog computing should support the user's mobility and provide location-specific information. This is achieved by geographical distribution and its location at the edge network. The fourth criterion is security, in which all IoT devices may pose a risk that could be exploited to harm users or their privacy. It is an important aspect of the fog system. The fog environment should safeguard personal information not accessible by a third party.

3.2.4 Analysis of existing techniques and evaluation criteria in fog computing

A fog-based healthcare architecture (FHA) was proposed by [32], which deploys a fog gateway at the network's edge to monitor a patient's health in real-time. ZigBee technology is used to connect the patient's health condition, mobile-based wearable sensors collect real-time data through the ZigBee link, and data is forwarded to the Tele-lab server (TLS). Patients' data are analyzed through a Laboratory Information Database (LIDB) module, which sends the information to the cloud server for storage and backup. In this system, the TLS transmits data over the communication channel and relies on FHA to manage the congestion. When FHA predicts the critical condition, it immediately sends data to the fog gateway to raise an emergency alert and to the cloud server to update the patient's record. However, the study was built based on the assumption that the communication channel is dependable and has no data loss during the data transmission. This does not hold due to the transient nature of the IoMT networks and the patient's mobility and dynamic topology. Consequently, data that reaches the gateway might not be complete. Although the proposed architecture was designed to deal with sensors' heterogeneity, it used fixed architecture in its simulation, which makes it outdated when topology changes.

The need for a transition from clinic-centered healthcare to patient-centered was discussed in [33]. This could be achieved by connecting hospitals, patients, and services into a layered e-health ecosystem. The layers include end nodes, fog, and cloud, which facilitate efficient handling of the big data generated by the system's components. The study used multiple standards at the interface level to deal with a vast number of sensor devices and support fog nodes' heterogeneity. Although the authors discussed scalability in detail in this paper, they did not show how to apply it in their proposed architecture. There is no discussion of mobility support in this paper. The authors show the significance of protecting and securing patients' information. The architecture supports multi-layer security measures for access control, encryption, and authentication.

The study in [34] proposed an Adaptive Heuristic Edge assisted Fog Computing design (AHE-FCD) to improve the processing of health data at the edge and fog layers. The authors indicated that using AHE-FCD reduces latency, increases data privacy, and improves real-time analysis by relocating data processing closer to the source. In addition, AHE-FCD can optimize resource utilization and enable scalability and flexibility when handling large healthcare data. Although the proposed model addressed latency and processing concerns, it could bring additional complexity when managing data in distributed systems.

A detailed review of the implementation of fog computing in healthcare services was provided by [31]. The study investigated the different cases of fog computing being used in healthcare informatics. The study categorizes the use cases based on specific fog device applications and functions. It discusses the processing and analytics at the network and fog levels. The study concluded that fog computing supports many activities in healthcare. Data analysis at higher network tiers is needed to overcome IoT constraints and fulfill the need to aggregate data. Although the study showed that a common infrastructure could be used by sensor devices to transfer their data to more comprehensive applications using standardized protocols, it did not show the exact mechanism to deal with the heterogeneous environment. The introductory study discussed fog computing's ability to enhance the scalability of a system. Nevertheless, no technique was proposed. The authors described the importance of mobility and security in a fog environment but did not show how to apply them in their work.

As Healthcare 4.0 systems enable the use of fog computing, the study in [35] proposed an efficient resource discovery model that can handle data within fog computing environments. The proposed model was designed based on a peer-to-peer (P2P) network architecture. Moreover, it addressed several problems, such as high latency, privacy concerns, and scalability issues. The high latency is mitigated by moving processing of data and storage near to the IoT sensor nodes instead of relying on cloud servers. This also allows for improving privacy, as the data is processed locally within fog nodes rather than the cloud. The proposed model improves scalability because the P2P architecture ensures the handling of large volumes of data. Therefore, it obtained benefit from P2P architecture; however it uses static peer systems, which does not allow for removal and adding peers dynamically.

The effect of incorporating IoT in healthcare was investigated by [36]. It was found that fog computing helps provide sufficient storage, processing, and networking resources. Fog also improves real-time analysis and supports online decision-making. Furthermore, the fog device's data collected by sensors can be managed immediately while minimizing latency and jitter. Two scenarios, "Daily Monitoring and Healthcare Service Provisioning" and "Extended eCall Service Delivery," were investigated considering the heterogeneity of communication protocols that allow data aggregation from different heterogeneous IoT devices. However, the fog environment's scalability was overlooked, which is crucial as the heterogeneity implies the interoperability between many devices and sensors that grow exponentially in real-world

deployment to support mobility and allow data gathering from different IoT technologies. Security and privacy concerns are also overlooked, which could have severe consequences for the entire system.

The FedHealthFog model was proposed in [37], which integrates federated learning and fog computing. The federated learning eliminates storing data in a central sever and instead it stores data in local devices. FedHealthFog was used in healthcare systems to enable connected wearables devices, such as smartwatches to monitor health. Therefore, collected data can be processed locally which allows for faster response and protects patient privacy. The proposed model solves the problem of conventional models that relieve a central server which causes slow process of the healthcare data. In addition, it uses less energy compared with conventional models. FedHealthFog may face challenges with unclear or uncertain data, which could disturb the decision-making processes in healthcare systems.

The authors of [38] proposed architecture to enable the efficient processing and storage of data to enhance the existing smart meter infrastructure. In their proposed architecture for the fog computing platform, smart meters are gathered to process a cluster that acts as a data node. Among these data nodes, one will be chosen to function as a master node. The master node is responsible for managing the file system. It is also responsible for storing metadata that holds the needed data, such as the file name and the storage location. However, the study does not show how to deal with the nodes' heterogeneity on the fog or cloud layers. Nevertheless, one of the advantages of this solution is that the architecture has a Plug-and-Play feature, which reduces the need for manual configuration. Consequently, the scalability criteria are met. The mobility support was not discussed. Even though the authors showed the importance of security and privacy when aggregating data to the cloud, they did not implement any security measures.

Researchers in [39] proposed R2AM model, which was designed to manage resource allocation in IoT transportation system through fog computing. IoT transportation systems require processing data collected from e.g., sensors, vehicles traffic cameras, GPS devices, in real-time and they involve critical decision-making. The collected data is placed in a queue for processing by fog nodes. Data is assigned to a fog node based on its processing capacity, so a node with higher capability has the priority to handle the data. The fog computing was used to process the data collected nearby fog devices to reduce load in cloud and enables low energy consumption. A limitation of the R2AM model is that it does not account for the range of capabilities and distances of communication devices, which could affect the scalability.

The authors of [40] introduced an architecture for big data analysis in smart cities. They proposed hierarchical Fog Computing architecture. The main objective of their work is to support a large number of infrastructures and services in future smart cities. Their architecture consists of four layers. Layer one is the Cloud for Data Management, which has a data center that gathers data from the intermediate layer. Layer two is the Intermediate Computing Node for Event Recognition, which is connected to many edge devices that govern the community-level sensors. Layer three is the edge device for feature extraction. It is responsible for detecting possible risk patterns on the received data streams from sensors and extracting features for computing at the higher layer. Layer four is the Sensing Network, consisting of numerous sensory nodes deployed at public infrastructures to monitor condition changes over time. The proposed architecture can support fast, providing intelligence and great performance in future smart cities.

In a distributed fog computing environment, an optimization policy for multi-user small cell clustering was proposed in [41]. The authors use a small cell clustering network to reduce power consumption and manage resource sharing. The load is distributed among small cell clusters. Their simulation results showed that the users were satisfied, and the consumption of communications power was reduced. Heterogeneity is proposed in their system, where each small cell cluster has various devices. The authors addressed the scalability of the clusters according to the requirements of computation requests. Mobility and security were not described.

The authors of [42] propose architecture for resource allocation that allows efficient workload distribution over the fog and the cloud layer. The authors proposed their design model to handle resource allocation issues in the fog paradigm. They designed the proposed architecture in a cloud-fog environment. Therefore, the architecture has three layers. The first layer is the client layer, the second is the fog layer, and the third is the cloud layer. The authors implemented the algorithm in the client and the fog layer to serve the clients with the required resources. The request will be directed to the cloud if no resource is available in the fog layer.

Latency in the fog layer of IoMT was also investigated by [41], and a 3-tier fog-assisted health monitoring architecture was proposed. All sensors, such as medical, environmental, and actuators, exchange the data with the Fog layer's application, where they are fused and processed. As data are locally analyzed, network traffic is minimized, preserving the bandwidth and decreasing the latency. Storing data locally also protects security and maintains the privacy of patients' information.

Preserving the resources within the fog layer's IoMT layer was investigated in [42]. Employing a task scheduling algorithm prioritizes the tasks properly based on their relevance. The study developed a Task Classification and

Virtual Machine Categorization (TCVC) method that prioritizes task significance. The tasks were categorized into high-importance, medium-importance, and low-importance tasks based on the patient's health status. MAX-MIN scheduling algorithm was employed to determine the performance of the proposed method. However, the method does not consider the task size when estimating the priority, which hinders the full utilization of the fog layer's resources. The 3-tier approach was also used in [43]. To build an analytical healthcare IoT model. By combining reinforcement learning and fuzzy logic in the fog computing environment, network latency was decreased. Patient health data were collected by sensors and sent to the fog layer, where they were prepared and used for training the model. The model then classifies the new readings as high-risk, low-risk, and normal. The purpose of reinforcement learning is to support real-time decision-making and prioritize time-sensitive data. Nonetheless, the study ignores task size when prioritizing resources. It is also unclear how the model decides whether data is time sensitive. Relying on a fixed definition does not fit the dynamic nature of health status, changing the context.

An energy-efficient fog-to-cloud architecture was used by [44]. To reduce energy consumption in IoMT devices. This architecture works in three modes to preserve sensors' battery energy: periodic, sleep-renew–renew and continue. The IoMT sensors are divided into several clusters, each with a dedicated cluster head such that cluster members use the cluster head as their gateway to the cloud and are connected to gateways called cluster heads. The cluster heads forward data to a respective fog, which is processed and then forwarded to the cloud for further processing. This technique enabled all sensing modes, which collected the patient data according to their health condition. However, cluster heads in this architecture are sign-point-of-failure and bottlenecks that cause data loss. Such data loss is caused by faulty cluster heads or mobility of the nodes within a cluster, which sometimes becomes unreachable to the centroid.

An efficient analytical model was proposed in [45] to reduce computational complexity regarding processing power and memory and to suit the resource constraints in IoMT. A network of queues that help in estimating minimum computing resources was integrated into the model. The gateway sends sensitive data to a private cloud to protect patients' data. In contrast, non-sensitive data is sent to fog nodes connected to a public cloud where thorough data analytics is conducted. However, the model assumes that communication channels are stable, and data delivery is dependable, which does not hold when the patient is mobile. Healthcare sensors work in harsh environments.

A 5-tier architecture [46] was proposed to process and analyze the data generated by different devices and equipment in IoMT. This architecture supports real-time event detection and shows the alerts on monitoring dashboards run at the fog layer. Nodes in the fog layer receive and process data collected from sensors through gateways before they are transmitted to the cloud for additional processing. Time-sensitive healthcare applications can make real-time decisions by relying on the fog layer for processing and analyzing data. However, the architecture's multi-layer nature creates additional overhead on the system as it needs extra work when passing data between layers. This adversely affects the efficiency of the architecture and delays the response in real-time applications. A detection model [47] was created in the fog layer to notify people about real-time fall activity. The model used the One-Class Support Vector Machine (OC-SVM). A new kernel matrix calculation technique was developed and incorporated into the classifier for real-time applications. The caregivers can get real-time notification despite losing the cloud and fog node connection. Although the kernel efficiently calculates the model's parameters, it does not account for the noises generated during a patient's mobility or the harsh environment.

The fog-based model for predicting, monitoring, and controlling the real-time risks of remote diabetic patients based on their physiological condition was proposed by [48]. By training a J48 decision tree, the risk level of the diabetic patient can be predicted. Multiple parameters like blood glucose levels, ECG, and physical activities were used as input parameters to train the model and support high accuracy. However, the model does not consider the special nature of data that arrives at the fog layer contaminated with noises. This could mislead the model and decrease the detection accuracy. Smart e-Health Gateways for IoMT were investigated in [17], which could support many services like real-time data processing, local storage, and embedded data mining. These gateways were incorporated into the fog layer and strategically positioned between the sensor nodes and the cloud. The model overcomes the challenges related to energy consumption, mobility, reliability, and scalability issues by relaying the processing to the fog layer. However, gateways could be a single point of failure that causes much data loss. Table 1 summarizes the studies related to fog computing based on the named criteria.

An improvement for the IoMT health monitoring system was proposed in [49], which employs fog computing at smart gateways to perform tasks such as distributed storage, embedded data mining, and notification service at the network's edge. The features were obtained from cardiac disease data from the electrocardiogram (ECG). ECG signals were analyzed in smart gateways with extracting features, such as heart rate, P wave, and T wave, through a flexible template based on

Table 1 Fog computing studies are categorized based on several criteria

Refs	Category	Heterogeneity	Scalability	Mobility	Security
[32]	Healthcare	✓	×	✓	✓
[33]		×	✓	✓	×
[34]		✓	✓	✓	✓
[31]		✓	×	✓	✓
[35]		✓	✓	×	✓
[36]		×	×	×	×
[37]		✓	✓	✓	✓
[38]	Smart Living	×	✓	×	×
[39]		✓	×	✓	×
[40]		×	×	×	×
[50]	Energy Consumption	✓	×	×	×
[51]	Resource Management	✓	×	×	×

a lightweight wavelet transform mechanism. However, analyzing data at smart gateways creates additional overhead on these nodes, which causes time delays.

Transferring computing intelligence from the cloud to the fog network was utilized in [36], which lowers the response time and minimizes network failures. The servers in the fog layer relay all protocol conversions, data storage, processing, and evaluation to the cloud and only focus on decision-making. Therefore, faster and more accurate treatment delivery, reduced medical costs, and improved doctor-patient interaction could be achieved. However, fetching the cloud data increases Fog's time to detect and/or predict a serious condition. A low-cost health IoMT system that integrates end-node sensors with a fog layer to provide continuous remote monitoring of ECG together with automatic analysis and notification was proposed by [25]. The sensors collect data about body temperature, respiration rate, and ECG and transmit them to a smart gateway where healthcare providers can access them. The data are represented in a form suitable for automatic decision-making. However, sending data about vital signs introduces a risk of noise and dropped packets, harming the user and the data quality.

A fog-assisted-IoT IoT-enabled patient health monitoring model has been proposed by [52]. The idea was to utilize fog computing at the smart gateway to process the massive amount of data collected by healthcare-related sensors at the end nodes close to patients. The Bayesian belief network algorithm was used to construct the classifier. Event triggering-based data transmission method was implemented to process real-time patient data at the fog layer. The temporal mining concept analyzes adversity by calculating the patient's temporal health index. However, temporal features do not accurately reflect the context in which data is collected. This negatively affects the data quality and the model's accuracy.

A Reduced Variable Neighborhood Search (RVNS) based Sensor Data Processing Framework (REDPF) [53] was proposed to enhance the reliability of data transmission and processing speed between the nodes and fog layer in IoMT systems. The framework was used to evaluate the health status of older people. The framework provides reliable data transmission and rapid data processing by adopting self-adaptive filtering, fault tolerant data transmission, and data-load-reduction processing. Therefore, it significantly improves the efficacy of IoMT applications. Self-adaptive filtering that recollects lost data is achieved by using the RVNS model to extract important information from raw data at fog devices. However, the study assumes that the data retention period at sensory devices is sufficient to hold the data until recollection is successful. This does not hold for resource-restricted devices in IoMT that have no sufficient space or memory to hold data for long periods.

In the study carried out by [54], the security of fog-driven IoT healthcare systems was investigated. Two security parameters (authentication and key agreement) have been explored. Specifically, a three-party authenticated key agreement protocol from bilinear pairings was proposed. The security model was formally proved so it can be used to protect fog nodes deployed in remote and unprotected places. However, attackers could hijack a legitimate user account and easily break into the system. In such a case, the data and services will be fully or partially accessible to the attacker, who could compromise the integrity of the data and the privacy of the patient's information.

The cognitive Fog (CF) model [55] was developed to safeguard the integrity of the data exchanged among the nodes in IoMT. The model provides secure data transmission between smart healthcare services and allows people to opt in and out of running processes, utilizing new processes when necessary and providing security for Fog's operational processes system. The proposed Ensemble learning security showed better performance compared with K-Nearest Neighbor (K-NN),

Density-Based Spatial Clustering of Applications with Noise (DBSCAN), and Decision Trees (DT) when classifying the data as normal or suspicious.

Fog layers have been employed to enhance IoT-based healthcare systems' capabilities, and they have demonstrated their worth by providing fast response time and low latency. However, such development poses a significant challenge in preserving users' privacy and addressing security/privacy issues. Being in an infant stage, such technology has invariably become more prone to privacy issues. Therefore, the study by [56] proposed an e-healthcare framework that deals with electronic medical records (EMRs) in the fog layer while preserving data privacy. However, the heterogeneity of data and services at the fog layer was overlooked, resulting in the risk of unauthorized parties exposing data by exploiting vulnerabilities in Fog's weekly secured services.

A multi-modal fog-assisted system [48] was proposed to support remote patients with diabetes. The system combines data from multiple vital sensors measuring heart rate, ECG, and blood sugar. The data processing is conducted at the fog layer instead of the sensors, which preserves the resources at the sensory layer. The sensor's battery lifetime is prolonged by offloading the processing on the fog layer. The J48 decision tree was utilized to predict the diabetes risk level with higher classification accuracy. An emergency alert is generated immediately for preventive actions by using fog computing. However, making decisions at the fog level involves some delay, which is not recommended for time-sensitive and life-threatening applications. A virtual machine (VM) partitioning technique [57] IoMT services' security at the fog layer was proposed to be reconsolidated. The Elliptic Curve Cryptography technique created the output token for user authentication. This authentication method was implemented into identity management to prevent security breaches. However, the attacker could take over a legitimate identity and utilize it to gain access to the system, where he can decrypt the data and access the resources freely.

3.2.5 Limitations and research directions for fog computing in IoMT

In general, fog computing aims to bridge the gap between IoT and cloud computing. It distributes the processing among resources, which enables the comprehensive analysis of a huge amount of data while maintaining the efficient utilization of the resources at the sensory layer. This is important for IoMT as the end nodes will be freed up and only dedicated to acquiring the data and communicating with other components. By integrating fog technology into the IoMT infrastructure, the workload will be relayed to devices with higher capacity and stronger processing power. However, the research community has addressed several issues regarding data analytics and predictive modeling in fog computing for IoMT.

The compatibility issue between the distributed infrastructure components is a major issue that needs further investigation. This is due to a lack of standardization in interoperability between the IoMT's fog devices. The fog devices manufactured by different vendors run different software and protocols. This creates interoperability issues as these protocols are not necessarily compatible. Although there is ongoing research to address such an issue, most studies tackled the problem from the application perspective and overlooked the nature of the data. Some devices use the IPv4 protocol, whereas others run the IPv6. To ensure that data prepared to be one protocol can pass through a route containing devices that run the other protocol, a tunneling mechanism must be in place. Such tunneling requires that data be packed in datagrams of a size suitable for both protocols. This might be challenging with the heterogeneous and multi-type data generated in IoMT. There is a need to highlight the data compatibility aspect in the fog computing layer of IoMT.

The lack of standardization in IoMT fog layer devices has another complication related to the susceptibility to attacks that exploit the vulnerabilities in one or more protocols to penetrate the well-secured nodes. Although several solutions have been proposed to secure the data transmission within the fog layer in IoMT, most ignore the multi-faceted nature of the data, combining (non-compatible) types like numerical, textual, and image. Unlike other IoT applications, devices in the fog layer of IoMT must distinguish and isolate the noise data caused by wearable sensors' non-stationary nature on the patient side.

4 IoMT processing

Processing data in IoMT could be conducted globally in a centralized location or distributed in local nodes. Processing data globally needs all nodes to send data to a central location, i.e., a server in the cloud. Distributed processing, on the other hand, is an approach where the data are processed in local nodes. The research community has investigated both approaches to make IoMT applicable in real-world deployment and addressed the issues that hinder the efficacy of such approaches.

4.1 Distributed processing

Researchers proposed a high-reliability and low-latency framework for Internet of Medical Things (IoMT) applications [58]. This framework uses an edge computing layer composed of Fog nodes controlled and managed by a Software-Defined Networking (SDN) system. The SDN system has distributed controllers and OpenFlow switches with limited resources. Blockchain technology is used to ensure secure decentralization. Based on their current workload, the framework includes a data offloading algorithm that allocates different processing and computing activities to the OpenFlow switches. Additionally, a traffic model was proposed to analyze and model traffic in different network parts. Simulations and a testbed were used to test the proposed algorithm. However, offloading based on workload only does not allocate resources properly, as it reflects the critical nature of the tasks. This is why some tasks are time-critical, and others are not, and treating both types of tasks negatively impacts the response time of the IoMT systems.

IoMT is vulnerable to many security threats in distributed environments, including internal and external attacks. Therefore, an adaptive security context framework was proposed in [59]. The data exchange between various components of the IoMT be properly tracked. The framework achieves accountability by tracking information propagation between services and devices in the system. However, auditing the local node activities is challenging because intruders use legitimate identities to conduct tasks within the internal system. They can also access and manipulate data in auditing files, which results in concealing and erasing these data. Data leakage and collusion attacks are among the threats that could cause the distributed IoMT. As such, the Privacy Protector framework [60] investigated the challenges during data collection. The framework employs secret sharing and repairs mechanisms, particularly in cases of data loss or compromise, to safeguard the privacy of patients data. The Slepian-Wolf-coding-based secret sharing (SW-SSS) was utilized to implement the concept. A distributed database consisting of multiple cloud servers was utilized to ensure that the privacy of patients' data remains protected as long as one of the servers is uncompromised. The solution assumes that compromising one server does not impact the other server in the distributed infrastructure. This does not hold, as the compromised server could share manipulated data with other servers in the distributed database. The attacker also could compromise all other servers if he managed to penetrate the system.

The study by [61] The integration of EHR and IoT into a highly heterogeneous system of devices, network standards, platforms, types of data, and connectivity while maintaining secure and private data. The proposed solution utilizes biometric-based blockchain technology with the EHR system. It introduced a mechanism that utilizes a patient's fingerprint to secure patients' access control on their EHRs without compromising their privacy and identity. A secure distributed healthcare system (SDHCARE) is designed to uniquely identify patients and enable them to control and secure access to their EHRs that are exchanged and synchronized between distributed healthcare providers. However, the solution does not consider the threats that could alter the data within a local node. This is important since attackers could use authenticated identities to steal, manipulate, or delete the data.

Addressing the security concerns in distributed healthcare IoT solutions was investigated by [62]. The study proposed a health data aggregation scheme as a privacy-preserving solution that securely gathers health data from multiple sources and guarantees fair incentives for contributing patients. Signature techniques were employed to ensure fair incentives for patients. In addition, noises were added to the health data for privacy. Boneh-Goh-Nissim cryptosystem and Shamir's secret sharing were combined to safeguard data obliviousness, security, and fault tolerance. The study asserts that noise follows a certain distribution that may differ from reality as the noise could be random and vary based on the context.

The authors of [63]. They demonstrated the challenges that fog computing faces for time-critical IoT applications regarding latency and energy efficiency requirements. Due to the availability of data and computing resources, it is promising to take advantage of applying intelligence in the system operations. This paper proposes human- and device-driven intelligence to reduce latency and energy consumption. In this paper, two case studies are used to demonstrate their technique. The first case study uses machine learning to identify the users' behaviors, and then the algorithm performs an adaptive low-latency MAC layer scheduling between sensor devices. It uses adaptive sampling and high-resolution data only whenever needed. ML module determines human activities, which can trigger the MAC-layer scheduler to allocate a timeslot to the requesting sensor(s). Three ML classifiers are used, i.e., decision tree, Support Vector Machine (SVM), and Gaussian Naive Bayes (GNB). In the second case study, they designed an algorithm to take advantage of nearby multiple fog nodes where the end-user device can perform an intelligent offloading task. In fog, nodes are deployed in a dense environment. The paper considers an end user with independent tasks; each task can be offloaded to a CPU of any fog node or locally processed by the end user's CPU.

Authors in [64] proposed an IoMT architecture approach to reduce the fog layer's computation. Their approach is implemented based on two phases of ML; first, ML is used to detect the priority of employees' medical records in a workplace. Therefore, an employee with a record with stress data is considered a priority record; in contrast, an unstressed record is a non-priority record. A priority record is transmitted to a second ML to classify the cause of stress. In the meantime, non-priority records are sent to the cloud for archiving. They compared the performance of several ML models, but the artificial neural network (ANN) showed the best F1-score value, reaching 99.97%. In the study, the authors assumed that the priority records usually happen to be less than non-priority records, which could be true in some applications. However, with more priority records, more records will be directed to the fog, which could lead to computation overhead. Table 2 summarizes the techniques that are utilized in literature.

4.2 Limitations and research directions for distributed processing in IoMT

Distributed computing allows for simplifying the processing and analyzing of a high-volume of data generated in the IoMT. It handles that by dividing the massive data into smaller samples, each managed by a dedicated machine/service. Distributed infrastructures like Hadoop Distributed File System (HDFS) are the main enablers for distributed big data analytics in IoMT [65]. Existing research on big data distributed analytics and predictive modeling caters to efficient processing and low-cost deployment. However, the main challenge of such distributed processing is the insufficiency and incompleteness of data when broken down into smaller chunks. For the IoMT ecosystem, data insufficiency and completeness are crucial for accurately diagnosing critical health conditions. Building analytical and predictive decisions requires fully available data, especially for those with urgent and critical health conditions.

Nevertheless, such a challenge is overlooked by the ongoing research in IoMT, as they assume that the subsets are as descriptive as the original data with the same distribution and characteristics. This does not hold, as the data selection for each subset is not necessarily even. The subsets are built by randomly selecting data instances from the original data set. Random sampling does not guarantee that samples represent the same distribution and characteristics as the original data.

Scaling IoMT solutions at large could bring further practical challenges, especially when managing the flow of large data into multiple devices. The IoMT generates a vast amount of health data, therefore it requires enabling scalable network architectures. In addition, using devices from different manufacturers increases the complexity of the interoperability of those devices, especially without standardization of protocols. Handling ethical issues of patient data is also considered a challenge in IoMT. As IoMT architecture allows for collecting sensitive patient information, this increases the risk of privacy and security problems. Patients have concerns about their information and want to know how their data is handled and controlled. Sharing patient data with a third party could lead to unauthorized access or misuse of their data, this should be carefully addressed at the time when designing IoMT systems [66].

On the other hand, the distributed processing in IoMT relies mostly on wireless communication to support patient portability and mobility. However, such mobility could disrupt the operation of the network. Consequently, the collaborative analysis and prediction will be adversely affected as the aggregation will not be aware of data lost due to intermittent signals. Furthermore, the distributed processing can be interrupted due to hardware or software failure in the distributed file system architecture. The collaborative analysis must know of any loss or changes in network components and topology changes.

4.3 Centralized processing

In their paper, referenced as [67], the authors presented architecture for integrating IoT-based healthcare systems in a cloud environment. The proposed platform runs the framework on fog computing. The study collects health data from sensors and securely transmits it to near-edge devices. These devices then transfer the data to the cloud, making it accessible to healthcare professionals. The system employs an authentication and authorization mechanism for all devices and maintains records of those devices. It also utilizes asynchronous communication between the applications and data servers in the cloud environment. However, this approach does not support critical IoMT applications that require real-time data.

In their research paper [68], proposed a fog-assisted information model that delivers healthcare services through IoT devices as a cloud service. This model is designed to manage heart patient data effectively received through user requests. It addresses the data processing issue that does not consider the requirements of a centralized cloud environment. The proposed solution suits deadline-oriented cloud applications like health monitoring, where low latency is

Table 2 The techniques and tools used by existing research

Ref.	Performance	Evaluation tools	Experimental evaluation	Strength
[63]	Energy consumption, Latency	OpenMote-CC2538 platforms provide Contiki-OS with built-in sensors -Raspberry Pi 3 is the gateway.	Results show that the average delay in urgent-high and urgent-medium states is about 90 ms, which is many folds better than the original ones (1000 ms)	Used for designing fog computing that maps with the requirements of IoT applications. Device-driven and human-driven intelligence is considered a feasible solution.
	Energy consumption, Latency	Simulation	The result shows that energy consumption & latency are reduced significantly when the number of nearby fog nodes increases.	
[41]	Energy consumption, Latency, Bandwidth expenditure	The application is hosted on the Fog Server and is run using the Raspberry Pi Zero W board. The operating system uses the Python script. The applications support the Message Queuing Telemetry Transport (MQTT)	Local data processing has many advantages, such as reduced latency and low bandwidth costs, affecting the total cost.	The proposed gateway has the main features that help the fog computing system to perform well.
[42]	Latency	CloudSim Simulation	The simulation results indicated that the method demonstrated the best cooperation between AET, AWT, and AFT compared to scheduling algorithms such as SJS, FCFS, and MAX-MIN.	The proposed scheduling technique helped in the real-time monitoring of the remote healthcare system.
[43]	Latency	Ifogsim simulator +-SPARK	Virtualization and the machine learning approach reduce the network latency between the Fog and cloud for different physical topological arrangements.	A hybrid fuzzy logic and reinforcement learning approach can enhance the current healthcare IoT and cloud-based fog computing.
[38]	Energy consumption, Latency	iFogSim	The results were compared to those observed for the existing processes regarding end-to-end delay, throughput, and energy consumption. The proposed methods reduced energy consumption by 30–40%. Simulation results of the FC-IoMT were compared to the earlier techniques. The FC-IoMT was effective as it collected all data from the biosensors and assigned the patient's request to the bio-fog and the bio-cloud-based architecture.	This technique allowed the sensing modes to collect patient data, depending on their health condition.
[45]	Number of computing resources Response time	A JMT simulator was installed on the machine with an Intel Core i5 CPU, 2.40 GHz, 4 GB memory, and 250 GB permanent storage.	The study presents the results derived from the simulation & the queuing model for demonstrating how the proposed model displayed effective & dynamic scalability using minimal computing resources (FC nodes, private and public VM nodes) for the incoming workload prompted by the body sensor or IoMT devices for satisfying the imposed SLA response time (2.5 ms)	Analytical and simulation results showed that this model predicted the system's response time based on various workload conditions. It could accurately estimate the number of computing resources required so that the health data services can perform satisfactorily.

Table 2 (continued)

Ref.	Performance	Evaluation tools	Experimental evaluation	Strength
[41]	Latency	The Kafka cluster, Storm topology, and MongoDB database (or Neo4j graph database) provide a faster query execution time.	N\A	By processing a large amount of the healthcare data streams at the network edge near the data sources, one can decrease the network traffic and increase the latency of the time-sensitive healthcare services & applications.
[47]	Bandwidth, Latency	MATLAB mobile app for transmitting the accelerometer data from the smartphone to a fog node.	They evaluated this model on real-world fall data. It could accurately classify 100% of the falls. The fall detection technique used the fog computing concept, significantly decreasing the data sent to the cloud from 900 values (10,799 bytes) to 5 values (59 bytes) every 6s.	This framework offered real-time fall detection as it analyzed the accelerometer data at the fog node instead of a cloud node.
[48]	Latency, Bandwidth efficiency, Classification accuracy of the Fog compared to cloud computing.	The smartphone is equipped with Snapdragon 410 Quad-Core, which is 450 MHz, has 2 GB memory, and a J48Graft classifier.	J48Graft displayed a high classification accuracy of 98.56% compared to other baseline techniques. It utilized fog computing as the intermediary layer, which helped to achieve mobility, local data storage, scalability, and interoperability. Experimental results indicated fog computing had a lower latency, higher bandwidth efficiency, and more classification accuracy than cloud computing.	They effectively predicted the risky blood glucose levels in diabetic patients.
[17]	Energy efficient, Latency, Mobility	The complete system was implemented, from the development of the cloud services to the software-hardware demonstration of the Smart e-Health Gateway prototype.	This concept provided an IoT-based health monitoring system that enhances intelligence, mobility, energy efficiency, interoperability, and security.	The authors evaluated the smart gateways at the network edge for developing high-level services such as real-time local data processing, local storage, and embedded data analysis based on fog computing. They presented different case scenarios that used smart healthcare IoT systems.

crucial. However, when a large amount of data is received, it creates a bottleneck at the cloud edge, which can increase response time.

A framework that coordinates processing between the edge and cloud has been developed by integrating the characteristics of both platforms [69]. This framework uses historical information and network-wide knowledge at the cloud center to guide edge computing units in achieving the performance needs of heterogeneous wireless IoT networks. The study highlights the synergies and differences between cloud and edge processing, including main features, key enablers, and big data analytics challenges. However, coordinating between the edge and cloud incurs additional expenditure, which can lead to increased delay.

A cluster-based hierarchical approach [70] that preserves energy and monitors the patients was proposed. The approach provides a cluster head to gather data from other cluster members by organizing the monitoring devices into clusters of equal sizes. The cluster head sends the data to a centralized base station. The approach outlines the power consumption cluster members in several states: idle, sleep, awake, and active. However, the approach does not consider a particular device's capacity, making it unfair to treat cluster members equally. It is also essential to consider the proximity to the cluster head when calculating the load. An advanced federated learning framework [71] was built to train deep neural networks for modeling data collected from sensors in the IoMT. Most powerful server training operations are managed by executing model training in the cloud. The sparsification of activations and gradients significantly reduces the communication overhead. However, data collected at sensors are naturally heterogeneous, which needs to be pre-processed before it becomes suitable for modeling. This adds another layer of overhead that delays the real-time response, which is crucial for sensitive and critical healthcare applications.

4.4 Limitations and Research directions for centralized processing in IoMT

As the centralized processing in IoMT gathers all information required into one location, it addresses incomplete data distributed in different locations. Accordingly, the accuracy of data analysis and predictive modeling is high. However, the enormous data collected from multiple IoMT sensors and nodes puts a heavy load on the analysis machine and requires more time. This is an issue for the applications that need real-time interaction and might be unable to work promptly. These applications need a prompt response, especially when dealing with patients with critical conditions. Therefore, centralized analysis needs to make the trade-off between thorough processing and efficiency. Nevertheless, such compromise is ignored by most of the related studies, and they focus on how to collect as much data as possible to support accurate decisions.

On the other hand, the data in centralized IoMT systems are collected from different types of devices that produce different data types. Consequently, the different data types must be federated into one set to facilitate centralized processing. Yet, merging incompatible data is an extra overhead that adversely affects the system's efficiency. Such an overhead exacerbates real-time systems' latency, which is unacceptable in IoMT applications that deal with patients with critical conditions. Although some centralized processing studies try to address the issue by carrying out data fusion and preprocessing offline before retraining, this might not be sufficient in real-time applications that need a prompt response from the service provider based on developing a patient's health condition. Additionally, retraining is another overhead that might disrupt the analysis, especially with highly dynamic environments like IoMT. The dynamic environment triggers retraining more frequently. As such, it is imperative that IoMT applications can resiliently receive, pre-process, and integrate the incoming data without causing any additional overhead or disrupting normal operation.

4.5 Analysis techniques

Increased time delay for data transmission due to the large volume of data and multiple hops counts between IoT devices and cloud servers, can render healthcare data inadequate and irrelevant for end-users. Healthcare applications that are sensitive to time constraints require genuine data. Traditional cloud servers cannot meet healthcare IoT devices and end-users minimum latency requirements. Computation latency, communication latency, and network latency need to be minimized for IoT data transmission to reduce high latency. Fog computing (FC) can provide storage, processing, and data analysis from cloud computing to network edges to reduce high latency. An analytical model based on a hybrid fuzzy-based reinforcement learning algorithm [72] has been proposed to address the high latency issue due to the large volume of data that causes network congestion. The proposed solution aims to reduce the high latency on the Internet of Medical Things (IoMT). The FC analytical model utilizes a fuzzy inference system and reinforcement learning to extract

features and select them. However, the dynamic nature of IoMT makes it unsatisfactory to train the model only once, as the system's topology changes continuously. Therefore, the model should adapt to such changes.

The privacy-preserving analytics model [73] was built to provide privacy protection for IoMT systems. The model adopts kHealth, a personalized digital healthcare information system for disease monitoring. Likewise [74], proposed a random forest-based model for real-time, remote health monitoring (IoMT). The model was trained using data lying in the cloud. However, one-time training is unsuitable for real-time applications with dynamic IoMT environments. The Decision Tree, Random Forest, and Naive Bayes machine learning classifiers were used [75]. To diagnose Parkinson's disease based on IoMT sensors. The IoT-based node receives the data and offers a faster classification solution to help with decision-making. However, offloading the sensors' decision is an additional overhead that drains the sensor's memory, CPU, and battery.

A Grey Filter Bayesian Convolution Neural Network (GFB-CNN) model was proposed in [76] to address two significant issues in heterogeneous IoMT sensors: connectivity and convergence between communicating parties, such as between patients and hospitals. The accuracy rate of medical data analysis was improved by introducing the volume alignment softmax CNN algorithm in the GFB-CNN method. However, relying on Bayesian filters has an underlying assumption that the data follows Bayesian distribution. This does not hold for data generated in harsh environments like IoMT. In such a case, the method could be suboptimal. A Fuzzy Rule-based Neural Classifier [77] was developed to diagnose the disease and identify its severity. It is a cloud-based Mobile IoMT that monitors, predicts, and diagnoses serious diseases. As part of this framework, a systematic approach was used to generate diabetes disease and related medical data using the UCI dataset and medical sensors. However, determining the severity of the disease requires real-time updates on the patient's status, which might not be applicable when patients are in remote locations with no streamlined data feed.

In a study by [78], researchers developed a user-dependent data mining approach using IoT technology to classify offline human activity. They also created a robust and precise human activity recognition model. The proposed model uses a dataset containing records of vital signs and body motion from ten volunteers with different profiles, each performing twelve physical activities for human activity recognition purposes. The researchers studied machine learning algorithms like Artificial Neural Network (ANN), K-NN, DT, RF, and SVM. However, they found that static data is not suitable for modeling dynamic environments where patients are mobile. The researchers also investigated Collaborative Machine Learning in IoMT by presenting a holistic multi-layer architecture [79]. This architecture enables real-time actionable insights, ultimately improving patients' and healthcare providers' decision-making powers. To demonstrate the feasibility of the architecture, a case study was conducted on ECG-based arrhythmia detection using deep learning and Convolutional Neural Network (CNN) methods distributed across endpoint IoT Devices, Edge (Fog) nodes, and Cloud servers. However, the multilayer architecture is unsuitable for real-time applications due to the need to exchange and convert data between layers. In such collaborative efforts, compatibility becomes an issue [79]. Also, in [80], a Deep Learning-based Internet of Health Framework for detecting Alzheimer Patients was proposed. The framework comprises three main components: a recurrent neural network-based Alzheimer prediction scheme, an ensemble approach combining CNN and NLP, and an IoT-based assistance mechanism for elderly patients. However, the ensemble approach is insufficient as it requires investigating data from different perspectives.

4.6 Existing works in IoMT

The authors in [81] proposed a framework for creating sustainable and secure IoMT solutions. Their work aimed to focus on the issues regarding sustainability and security in the medical field. They used a case study to assess the effectiveness of their study; they carried out the case study in a private medical clinic. They implemented an IoMT system for monitoring patients, particularly their vital signs. Their results show that they achieved positive results when they implemented an IoMT system that can meet sustainability and security requirements. Also, their case study has findings that include monitoring patients' vital signs in real-time. This helped them improve care quality and detect some complications in the early phases. They have used two types of datasets, including simulated and clinical datasets, to analyze and test the framework's performance. They achieved an accuracy of 89%. The researchers in [82] reviewed state-of-the-art techniques to secure IoT systems when transmitting, collecting, and storing data. They have explored several security requirements and challenges behind the designs; also, they reviewed several security techniques to make the IoMT systems more secure. The authors tried to describe what the researchers have done in the field and the current proposals, outlining several future trends and research challenges. The study in [83] proposed an intrusion detection system (IDS) with two algorithms, including AdaBoost and particle swarm optimization, to detect and classify records regarding malware in health platforms. They used a dataset called NSL-KDD with instances of 125,973 and features of 41; the dataset is divided

into two parts: 20% for training and 805 for testing. They have identified 12 features that are relevant for detecting intrusion by using particle swarm optimization. Their IDS has shown effectiveness in detecting attacks like Probe attacks, Root-to-local (R2L), User-to-root (U2R), and Denial of Service (DoS). They compared their results with naïve Bayes and KNN (K-Nearest Neighbours). Their results were promising, and the AdaBoost achieved the highest value in accuracy of 98.5% and recall of 96.67%.

The work in [84] reviews several papers on the Internet of Medical Things (IoMT) to explore customized intelligence, connectivity, and healthcare systems. Also, they explored other cutting-edge technologies like blockchain, artificial intelligence, cloud computing, and big data that support healthcare services to be more personalized and convenient. They discussed the technologies in the healthcare domain that exist in the literature. They covered topics about connected health and smart health, bibliometric analysis, and the global market; they discussed the healthcare industry's evolution from 1.0 to 5.0. Also, they pointed out important aspects of the next step in healthcare, which will be focusing on a patient-centric approach and a personalized one. Furthermore, healthcare architecture based on IoMT is introduced, which helps prioritize security integrated with devices. They outlined research challenges and future trends that will help researchers before delving into the field. The authors in [85] stated that a few researchers have focused on bio-inspired, combined with IoT. Therefore, they started reviewing papers in this field by providing an overview of IoT based on bio-inspired, explaining how this concept started, and exploring and discussing the status, ecosystem, advantages, future trends, and challenges of bio-inspired IoT. They mentioned bio-inspired solutions, including robotics, Materials and structures, sustainability and energy, healthcare, and optimization. They stated that bio-inspired techniques can help the IoT system to be more scalable and durable. Their paper might be useful for researchers trying to get information about bio-inspired IoT.

The researchers' aim in [85] was to address the issues of data fusion in the field of IoMT, also discussing the security challenges and possible solutions that are lacking in the existing works. They stated that the data collected from IoMT devices can affect the accuracy of predictions due to quantity, quality, and relevance. There is an algorithm called Epilepsy seizure detector-based Naive Bayes (ESDNB) that has achieved an accuracy of 99.53–99.99%, which is considered the highest obtained value in the IoMT. The data collection, protection, and storage methods should be improved based on their analyses. Several future research trends mentioned, including cross-platform methods when detecting the malware, can be considered as future work that can tackle the heterogeneous environment of IoMT systems. The research in [86] proposed a framework that helps refine the classification activities of people and detect the wellness related to the people's routines. Based on their findings, the framework has improved the accuracy of classifying individuals' activities. Their researchers have integrated the sensor data fusion based on IoMT into multimodal data processing to implement patterns of daily living activities and detect anomalies. Their model, AiCareLiving, is based on IoMT and artificial intelligence. This model's objective is to get low false positives when detecting anomalies and predicting; their model achieved the highest accuracy of around 95%.

Authors in [64] proposed an IoMT architecture approach to reduce the fog layer's computation. Their approach is implemented based on two phases of ML; first, ML is used to detect the priority of employees' medical records in a workplace. Therefore, an employee with a record with stress data is considered a priority record; in contrast, an unstressed record is a non-priority record. A priority record is transmitted to a second ML to classify the cause of stress. In the meantime, non-priority records are sent to the cloud for archiving. They compared the performance of several ML models, but the artificial neural network (ANN) showed the best F1-score value, reaching 99.97%. In the study, the authors assumed that the priority records usually happen to be less than non-priority records, which could be true in some applications. However, with more priority records, more records will be directed to the fog, which could lead to computation overhead.

Authors in [87] proposed a resilient security framework for the IoMT model. Their framework is implemented by combining a Tri-layered Neural Network (TNN) and a blockchain model. TNN is used to capture cyberattacks from patient data collected by medical sensors. Therefore, malicious data is dropped from the IoMT architecture while normal data is transmitted to the blockchain in the fog layer for data integrity and immutability. The TNN achieved a 99.99% F1-score, and the blockchain met the expected performance. The research assumes that the TNN operates close to the sensor layer of IoMT; however, it does not provide details on how the TNN functions within that layer.

Authors in [88] introduced meta-learning to enhance ensemble-based IDS for the IoMT. They compared the accuracy performance of their proposed model, ME-IDS, with Stack-IDS, a Distributed Intrusion Detection System for the IoT (DIS-IoT), and an Ensemble Deep Learning Intrusion Detection System (EDL-IDS). The comparison results demonstrated that the research proposed model, ME-IDS, achieved the highest accuracy across different numbers of features, ranging from 5 to 45. The authors used a dataset called WUSTL-EHMS-2020 and discussed the number of features used. However, they did not provide details about the number of samples for each label in the dataset.

Authors in [89] proposed a novel IDS technique named the SafetyMed, which merges CNN and LSTM models. Therefore, their proposed model can defend against sequential and grid-structured malicious data. The average accuracy of the proposed model was 97.63%. SafetyMed is considered a comprehensive model; however, combining CNN and LSTM could increase the complexity of the model. The research in [90] compared various ML models, which are K-NN, NB, SVM, ANN, and DT, used as IDS for IoMT. They evaluated the performance of each ML model using the Bot-IoT dataset. According to the authors' findings, DT achieved the best performance, reaching 100% accuracy compared to the other ML models.

Authors in [91] presented an IDS implemented based on a deep learning approach for the IoMT. Their model leverages combining features extracted from network flow and patient biometrics to enhance its accuracy. They handled the imbalanced dataset using a cost-sensitive learning approach. The proposed model accuracy reached an accuracy of 99% with combined features. However, it achieved 95% with network features and 89% with patient biometrics. The authors focused on cyberattacks injected into the IoT gateway and the cloud network. Authors in [92] also combined the features extracted from network flow and patient biometrics when designing their IDS model for IoMT. The proposed IDS was implemented using a particle swarm optimization (PSO) deep neural network (DNN). The PSO was used for feature selection, and DNN was used to detect intrusions. However, the accuracy of the proposed model reached 96%, which is less than the research in [91], which achieved 99%, as mentioned. This study in [93] presented an IDS implemented based on fuzzy learning and LSTM for IoMT. The fuzzy logic adjusts the number of training epochs, eliminating underfitting and overfitting. As a result, it enhances the accuracy of the model. However, adjusting the number of epochs alone is insufficient to prevent overfitting and underfitting fully. Authors in [94] proposed an IDS used in the fog layer for IoMT. Their model addresses the limitations of traditional IDSs built into embedded devices or cloud systems. Therefore, the model combines host and network attack detection using several classifiers that utilize adaptive online settings, which enable updating and learning in real time to avoid retraining the model. The model reached approximately 100% accuracy. Table 3 shows the summary of the works that have been discussed above.

In [95], the authors explored the integration of Artificial Intelligence (AI) for the Internet of Medical Things (IoMT), which combines AI techniques with old medical technologies, resulting in what is known as AIoMT. AIoMT has achieved vast momentum, specifically due to the COVID-19 epidemic, due to its ability to renovate healthcare sections through the real-time collection, processing, and interpretation of massive capacities of patient data. Such data is acquired by different AIoMT devices supplied with smart sensors to tailor patient treatment and improve overall healthcare proficiency. On the other hand, data security, device compatibility, and regulatory obstacles must be solved. The authors have also referred to open research concerns that require more exploration to reinforce the nonstop advancement and effective utilization of AIoMT in healthcare.

In [96], the contributors proposed a distinctive approach for addressing coronary artery disease prediction models that use AI and IoMT. Their proposed model uses real-time physiological data from connected devices such as heart rate monitors and ECGs via IoMT to render tailored risk assessments. Also, the model utilizes advanced AI algorithms, such as TabNet for feature selection and catBoost for categorical data, to enhance the prediction accuracy while lowering model overfitting. To ensure that the model is adaptable across populations, the model has been trained on wide and diverse datasets. This real-time data processing facilitated the instant predictions to modernize preventive healthcare situations. By allowing for rapid and precise risk assessments, the approach enables the creation of individualized preventive treatment measures, thereby improving cardiovascular health outcomes.

In [97], the authors presented a hybrid methodology for examining IoMT applications in the medical libraries of Pakistan. They collected quantitative data from 63 librarians, and in-depth interviews with 10 librarians show that IoT devices such as smart air conditioners, fire alarms, hand sanitizer dispensers, automated notifications, and smart gates are rarely used. Benefits include cost savings, remote access, and increased security, while drawbacks include high expenditures, data security difficulties, integration requirements, and a shortage of experienced workers. This study, the first thorough survey in Pakistan, intends to help libraries integrate IoT technology in emerging nations.

In [98], the authors investigated the use of wearable sensors in the IoMT to collect real-time health data. However, even small instruments have limits, leaving raw data susceptible to inaccuracies. Data refining is critical before processing, but current approaches can be difficult or resource intensive. This research provides a unique two-tier, lightweight data fusion technique tailored for IoMT wearables and server modules. Each device applies local data fusion to its sensor data to increase accuracy, utilizing lessons from previously sent data. This method may even deal with unexpected physiological changes like heart attacks. Furthermore, an overall data blending step on the server can help enhance the system's accuracy by removing redundant data obtained by adjacent devices. Simulations exhibit that this two-tier procedure substantially raises the data accuracy and precision.

Table 3 Summary of existing works in IoMT

Study	Authors (Year)	Methods	Results/findings
[81]	Villegas-Ch et al. (2023)	Case study implemented IoMT system for patient monitoring, simulated and clinical datasets.	Achieved 89% accuracy, improved care quality, early complication detection
[82]	Bhushan et al. (2023)	Review of state-of-the-art security techniques	Outlined security requirements, challenges, and future trends
[83]	Sun et al. (2024)	AdaBoost, Particle Swarm Optimization, NSL-KDD dataset	Achieved 98.5% accuracy and 96.67% recall with AdaBoost
[84]	Mishra et al. (2023)	Review of IoMT, blockchain, AI, cloud computing, big data	Discussed evolution from healthcare 1.0–5.0, future patient-centric approach
[85]	Alabdulatif et al. (2023)	Review of bio-inspired IoT	Explored status, advantages, challenges, and future trends
[11]	Ahmed et al. (2024)	Epilepsy seizure detector-based Naive Bayes (ESDNB)	Achieved 99.53–99.99% accuracy, suggested improvements in data handling
[86]	Ghayvat et al. (2024)	AiCareLiving model, sensor data fusion, sensor event-triggered activation dataset	Achieved around 95% accuracy, low false positives in anomaly detection
[87]	Alsemmeari et al. (2023)	TNN + blockchain	TNN: 99.99% F-1 score, blockchain achieves expected performance
[88]	Alalhareth et al. (2024)	ME-IDS	High accuracy
[89]	Faruqui et al. (2023)	SafetyMed	Average accuracy: 97.63%, DT: 100%
[90]	Binbusayyis et al. (2022)	ML	99% (combined features), 95% (network features), 89% (patient biometrics)
[91]	Ravi et al. (2023)	Deep learning-based IDS	Accuracy: 99%
[92]	Chaganti et al. (2022)	IDS with PSO and DNN	Accuracy: 96%
[93]	Alalhareth et al. (2023)	IDS with fuzzy learning and LSTM	Depends on features No.
[94]	Hameed et al. (2021)	IDS in the fog layer	Approximately 100%

While the IoMT revolutionized healthcare by providing real-time patient data, centralized cloud storage introduces dangers. Therefore, the investigators in [99] suggested a new and safe approach that integrates IoT and blockchain technologies to establish a decentralized intelligent medical system. Blockchain technology has improved system security by eliminating centralized single points of failure and recovering data integrity through its immutable ledger. Besides, this research emphasized a comprehensive comparative analysis of preceding models that employ blockchain to secure IoMT systems, concentrating on imperative issues such as system design, data integrity approaches, secure information exchange, and granular access control. Moreover, in this research, the authors provided a clue about the existing security challenges, open research problems, and research gaps. Their work provided a fundamental roadmap for researchers examining this pioneering approach to IoMT data security.

Due to the initialization of wearable health monitors, IoMT connectivity has expanded considerably through the apparent increase in connected devices that provide nonstop health intuitions and life-saving warnings for irregularities. Therefore, the research developed in [100] reported a three-layer architectural design to meet the Quality of Service (QoS) requirements of IoMT networks. The proposed design utilizes the indispensable IEEE 802.11 WLAN technologies (such as multi-link operation (MLO) for ultra-low latency) to ensure real-time communication. To assess MLO performance, a case study of ambient assisted living (AAL) has been used where it exhibited the effectiveness of the MLO module. Furthermore, their proposed architectural design usefulness has been assessed for several other latency-critical healthcare applications (beyond AAL), including remote operations, e-consultations, and even pandemic response efforts.

In a similar perspective, the authors in [101] studied how integrating AI and IoMT has improved digital health and diagnosis. This integration was later renamed to AIoMT. AIoMT facilitates real-time data analysis from wearable medical devices and smart sensors, ensuring more adapted and effective medical care systems. The collected data is further processed through big data, mobile internet, cloud computing, microelectronics, and PowerAI apps to improve the medical care system by producing prompt outcomes and providing instantaneous drug supply. They also reported on various AIoMT devices to realize the full potential of AIoMT. They highlighted the importance of ensuring proper data security and interoperability and overcoming regulatory difficulties. Finally, by resolving such significant issues, intelligent IoMT technology can be used to replace outdated healthcare systems.

The authors in [96] introduced a heart disease prediction model that spans cholesterol checks to state-of-the-art machine learning algorithms. The existing studies in the field of heart disease prediction via machine learning models like TabNet and CatBoost seem to uncover many crucial gaps that need deeper probing. One is the pooling of data information, especially unstructured data like medical imaging and clinical notes, leading to improvement in the accuracy of predictions. Moreover, even datasets from different parts of the US have been used in numerous models to make predictions specifically on data from certain states or localities leading to concern about the possibility of generalizing how well these models perform in predicting healthcare outcomes equally for wider population structure requiring external validation. Additionally, real-time monitoring and adaptability will need improvement because as it stands the current implementations only go so far into ongoing learning while receiving new data inputs much of which emanate from wearable devices. In addition, while TabNet provides interpretability tools, better enabling us to explain predictions is a high priority for clinicians who wish to trust and utilize these models effectively in clinical practice.

Other potential target areas to fill gaps include: (1) addressing missing or incomplete data by developing methodologies robust to missing data; and (2) focusing on more longitudinal analyses since the vast majority of current published studies are cross-sectional in nature (without proper considerations for time-varying effects and changing risk factor distributions). The inclusion of patient-reported outcomes and preferences could add new dimensions to model predictions that may enrich patient engagement in their own healthcare plans. Advancing these recommendations will vastly improve the power of ML models in heart disease prediction, resulting in improved patient outcomes and more personalized healthcare strategies. Although the authors state that machine learning-generated features are incorporated, they did not explain how a comprehensive explanation of what exact techniques are used for feature generation (e.g., PCA, feature selection methods), the idea of "derived features" is confusing and lacks evaluation metric orientation. A brief explanation of the metrics to calculate model performance (accuracy, precision, recall, F1-score, AUC-ROC) is discussed, but it misses how hyperparameter tuning is done to optimize.

4.7 IoMT applications and case studies

The IoMT includes a wide range of applications ranging from mobile health (mHealth) application to complex remote monitoring setups and smart healthcare environments. The mHealth [102] is system that has cloud storage, secure data management and real-time participant interaction including wearable devices. In other words, the application has the

following abilities such as obtaining streams of health data, interpret the data, trigger actions, and provide feedback. Another application is called Remote Biomarker Detection [103] that is affordable and self-sufficient sensing gadget depending on a galvanic cell structure for detecting H2S that allows monitoring of non-invasive and integration of wearable. Hybrid RFID-IoT Scrub Distribution [104] tracks the usage of medical scrub via RFID and IoT to enhance control of infection and reduce cross-contamination in hospitals. IoT-Based Disease Prediction [105] utilizes ML and Arduino/ESP8266 sensors to collect and analyze symptoms of a patient and essentials for accurate diagnosis of telemedicine. Table 4 summarizes the IoMT applications by considering the technologies used and the purpose of each application.

To fully understand the practical IoMT applciations real world case studies can provide important insights into the way that these technologies are developed in several environments of healthcare. Several examples that are based on IoMT applications will be presented that ranges from remote patient monitoring to smart post surgical and inhalers monitoring tools. These case studies show the advantages of IoMT in healthcare that are enhanced patient outcomes, cost savings and increased independency. Table 5 is a summary of the case studies that has the case study, the description and the outcome. The summarized information in Table 5 has been adapted from [106] that provides an in-depth analysis of IoMT implementations in healthcare settings.

4.8 Limitations and research directions for techniques in IoMT

The studies on intelligent techniques used for modeling and analyzing the data acquired from the IoMT can be categorized based on the topology and functionality. The techniques are categorized into cloud-based and ad-hoc from a topology perspective. From the literature survey, it can be noticed that most of the techniques rely on cloud services to offload the heavy analytical processing to the backend platform. This helps to preserve the computational and energy resources on the sensors at the edge network, which prolongs these sensors' lifetime and guarantees interrupted services. However, reliable communication needed to achieve synchronization and real-time interaction can be difficult due to the patient's mobility and the harsh environment in which IoMT works. Likewise, the analytics on the cloud side may impose an additional cost, making it sometimes not appealing for both customer and service provider to rely on.

Furthermore, outsourcing the analytics and modeling in IoMT creates privacy and security concerns. This can be observed from several studies focusing on this issue and trying to address the problem by proposing techniques that provide secure communication channels between end nodes and backend servers on the cloud side. However, these solutions overlook the possibility that attacks could originate from nodes inside the network, which is challenging as they could falsify the data at the local node. This approach neutralizes the conventional attack detection and protection strategies that rely on observing data as they travel through the communication channel. Therefore, more innovative techniques are needed to thwart the internal threats in IoMT.

On the other hand, the modeling techniques in IoMT are categorized based on learning strategies into shallow and deep learning. In shallow learning, existing studies use several algorithms like SVM and DT. However, these algorithms lack the resiliency and ability to deal with a huge amount of data. These algorithms need much work in the pre-processing phase to prepare data and make them suitable for modeling. This is crucial, especially with data generated in IoMT, whose types are heterogeneous. Although some studies addressed this issue by employing deep learning methods and algorithms when building the models, this approach's main challenge is the availability of labeled data. Big data is difficult to manage, making the labeling more complicated, especially when data comes from multiple sources, which could contain conflicting and inconsistent labels. Such inconsistency is problematic when dealing with supervised learning, which degrades the model's performance. AI-driven IoMT has several challenges in terms of data privacy and power consumption at the edge of the network that need to be addressed. However, it offers tremendous benefits that can be tackled by researchers regarding real time data processing and immediate responses that can enhance healthcare systems by providing real time monitoring and alerting systems, cost reduction, and improving decision making.

Furthermore, the energy consumption of sensor devices for IoMT is another challenge that researchers should focus on to efficiently continuously monitor patient's health condition while managing the energy consumption during data transmission. As the sensors devices are recourse constrained several techniques can be developed to adjust the sampling rate based on the critical condition of the patient such as continuous monitoring during emergencies, sleep awake mode and periodic sampling during less critical periods. Additionally, in future research, it is crucial to investigate deeper into energy harvesting solutions in which sensor devices generate their power by capturing and converting ambient energy from their environment such as solar, mechanical energy and thermal. Generating sustainable energy is important to enhance IoMT systems.

Table 4 IoMT Applications

Application	Technologies	Purpose
mHealth	Cloud, Wearable Devices	Real-time health data monitoring and feedback.
Remote Biomarker Detection	Galvanic Cell Structure, Wearables	Non-invasive biomarker detection (H2S), supporting wearable integration.
Hybrid RFID-IoT Scrub Distribution	RFID, IoT	Infection control and reducing hospital cross-contamination.
IoT-Based Disease Prediction	Machine Learning, Arduino/ESP8266 Sensors	Collecting patient symptoms for accurate telemedicine diagnosis.

Table 5 Real-world IoMT implementations in Healthcare

Study	Facility	Solution	Key outcomes
Remote Patient Monitoring for Chronic Disease	Partners HealthCare	RPM system for chronic heart disease patients using wearables to track vital signs.	• Reduced hospital readmissions • Improved medication compliance • Cost savings
Smart Inhalers for Asthma Management	Cleveland Clinic	Smart inhalers with sensors for tracking usage and environmental triggers for asthma patients.	• Increased medication adherence • Fewer asthma attacks • Higher patient satisfaction
IoMT in Post-Surgical Care	Johns Hopkins Hospital	Wearable sensors for monitoring vital signs to detect post-surgical complications.	• Early detection of complications • Shorter hospital stays • Increased patient empowerment
Diabetes Management with Continuous Glucose Monitors	Mayo Clinic	Continuous glucose monitors for real-time blood glucose tracking and analysis.	• Better glycemic control • Reduced hypoglycemic events • Higher patient engagement
Telehealth and Remote Monitoring for Elderly Care	Kaiser Permanente	IoMT devices for monitoring elderly patients in assisted living facilities. IoMT system with fall detectors and heart monitors.	• Improved health outcomes • Greater independence for patients • Reduced caregiver burden

5 Conclusions

This survey explored research on the techniques and models proposed for IoMT, emphasizing the limitations of each proposed method. The survey began by discussing the characteristics of IoMT standards, protocols, and types. A detailed analysis of research papers on adopting fog and edge computing for IoMT was provided. For each study, the proposed method, technique, or model is described, followed by its limitations and suggestions for further improvement. A thorough discussion about research directions and gaps regarding different IoMT approaches and technologies was provided such that further research endeavors could be carried out to address these issues and limitations. IoMT applications would prevail by addressing those limitations, and trust in automated healthcare services would increase. The emerging trends in IoMT will facilitate the interactions between patients on the customer side and medical devices and computing devices on healthcare service size. Reduced cost, increased quality of life, and timely medical intervention are among the immediate outcomes of adopting IoMT. Future work in IoMT could be focused on enhancing security and data privacy, electromagnetic compatibility issues, synchronization, and real-time interaction, and integrating AI and Machine Learning.

Author contributions B.A.T and Q.A.: Conceptualization, Methodology, Investigation; RA.A., A.A.A., and AA.: Validation, Formal analysis, Software; B.A.G, S.T.B, and R.A.S.: Resources, Visualization, Software. All authors contributed to Writing—original draft, review & editing, and Funding acquisition. All authors have read and agreed to the published version of the manuscript.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

1. Sun Y, Du X, Niu S, Zhou SA. Lightweight attribute-based Signcryption Scheme based on cloud-fog assisted in Smart Healthcare. PLoS ONE. 2024;19:e0297002. https://doi.org/10.1371/journal.pone.0297002.
2. Huanca F, Torres M, Rodriguez-Fernandez M, Núñez F. A cyber–physical system for real-time physiological data monitoring and analysis. IEEE Internet Things J. 2024;11:28918–30. https://doi.org/10.1109/JIOT.2024.3404220.
3. Damar S, Koksalmis GH. A bibliometric analysis of metaverse technologies in healthcare services. Service Bus. 2024;18:223–54. https://doi.org/10.1007/s11628-024-00553-3.
4. Batra P, Dave DM. Revolutionizing healthcare platforms: the impact of ai on patient engagement and treatment efficacy. Int J Sci Res. 2024;13:273–80. https://doi.org/10.21275/SR24201070211.
5. Rauniyar A, Hagos DH, Jha D, Håkegård JE, Bagci U, Rawat DB, Vlassov V. Federated learning for medical applications: a taxonomy, current trends, challenges, and future research directions. IEEE Internet Things J. 2023;11:1–1. https://doi.org/10.1109/JIOT.2023.3329061.
6. Azizan A, Ahmed W, Razak AHA. Sensing health: a bibliometric analysis of wearable sensors in healthcare. Health Technol (Berl). 2024;14:15–34. https://doi.org/10.1007/s12553-023-00801-y.
7. Ali O, Abdelbaki W, Shrestha A, Elbasi E, Alryalat MAA, Dwivedi YK. A systematic literature review of artificial intelligence in the healthcare sector: benefits, challenges, methodologies, and functionalities. J Innov Knowl. 2023;8:100333. https://doi.org/10.1016/j.jik.2023.100333.
8. Khalil Maysa, Al-Haija Qasem Abu. Samir Ahmad healthcare IoT networks using LPWAN. Low-power wide area network for large scale internet of things. New Delhi: CRC; 2024.
9. Pergolizzi J Jr., LeQuang JAK, Vasiliu-Feltes I, Breve F, Varrassi G. Brave new healthcare: a narrative review of digital healthcare in American medicine. Cureus. 2023. https://doi.org/10.7759/cureus.46489.
10. Osama M, Ateya AA, Sayed MS, Hammad M, Pławiak P, Abd El-Latif AA, Elsayed RA. Internet of medical things and healthcare 4.0: trends, requirements, challenges, and research directions. Sensors. 2023;23:7435. https://doi.org/10.3390/s23177435.
11. Ahmed SF, Alam MS, Bin; Afrin S, Rafa SJ, Rafa N, Gandomi AH. Insights into internet of medical things (IoMT): data fusion, security issues and potential solutions. Inform Fusion. 2024;102:102060. https://doi.org/10.1016/j.inffus.2023.102060.

12. Aski VJ, Dhaka VS, Parashar A, kumar S, Rida I. Internet of things in healthcare: a survey on protocol standards, enabling technologies, WBAN architectures and open issues. Phys Commun. 2023;60:102103. https://doi.org/10.1016/j.phycom.2023.102103.
13. Kamalov F, Pourghebleh B, Gheisari M, Liu Y, Moussa S. Internet of medical things privacy and security: challenges, solutions, and future trends from a new perspective. Sustainability. 2023;15:3317. https://doi.org/10.3390/su15043317.
14. Putra KT, Arrayyan AZ, Hayati N, Damarjati C, Bakar A, Chen H-C. A review on the application of internet of medical things in wearable personal health monitoring: a cloud-edge artificial intelligence approach. IEEE Access. 2024. https://doi.org/10.1109/ACCESS.2024.3358827.
15. Aldribi A, Singh A, Bresa J. Edge of things inspired robust intrusion detection Framework for scalable and decentralized applications. Comput Syst Sci Eng. 2023;46:3865–81. https://doi.org/10.32604/csse.2023.037748.
16. Azimi I, Anzanpour A, Rahmani AM, Pahikkala T, Levorato M, Liljeberg P, Dutt N. Hierarchical fog-assisted computing architecture for healthcare IoT. ACM Trans Embedded Comput Syst. 2017;16:1–20. https://doi.org/10.1145/3126501.
17. Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, Liljeberg P. Exploiting smart E-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Future Generat Comput Syst. 2018;78:641–58. https://doi.org/10.1016/j.future.2017.02.014.
18. Alabdulatif A, Khalil I, Yi X, Guizani M. Secure edge of things for smart healthcare surveillance framework. IEEE Access. 2019;7:31010–21. https://doi.org/10.1109/ACCESS.2019.2899323.
19. Yu X, Lu H, Yang X, Chen Y, Song H, Li J, Shi W. An adaptive method based on contextual anomaly detection in internet of things through wireless sensor networks. Int J Distrib Sens Netw. 2020;16:155014772092047. https://doi.org/10.1177/1550147720920478.
20. Pace P, Aloi G, Gravina R, Caliciuri G, Fortino G, Liotta A. An edge-based Architecture to support efficient applications for Healthcare Industry 4.0. IEEE Trans Industr Inf. 2019;15:481–9. https://doi.org/10.1109/TII.2018.2843169.
21. Wang X, Cai S. Secure healthcare monitoring framework integrating NDN-Based IoT with edge cloud. Future Generat Comput Syst. 2020;112:320–9. https://doi.org/10.1016/j.future.2020.05.042.
22. Azimi I, Takalo-Mattila J, Anzanpour A, Rahmani AM, Soininen J-P, Liljeberg P. Empowering Healthcare IoT Systems with Hierarchical Edge-Based Deep Learning. In: Proceedings of the Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies; ACM: New York, NY, USA. 2018;63–68.
23. Yu J, Fu B, Cao A, He Z, Wu D. A Hybrid Architecture for Agile Learning of Healthcare Data from IoT Devices. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). Piscataway: IEEE; 2018. p. 852–9.
24. Li J, Cai J, Khan F, Rehman AU, Balasubramaniam V, Sun J, Venu P. A secured framework for SDN-based edge computing in iot-enabled healthcare system. IEEE Access. 2020;8:135479–90. https://doi.org/10.1109/ACCESS.2020.3011503.
25. Abirami S, Chitra P. Energy-efficient edge based real-time healthcare support system. 2020;117:339–68.
26. Agnihotri AK. Healthcare technology evolution and adoption of fog computing in healthcare: review, issue and challenges. J Pharm Negat Results. 2023. https://doi.org/10.47750/pnr.2023.14.S02.172.
27. Alsadie D. Artificial intelligence techniques for securing fog computing environments: trends, challenges, and directions F. IEEE Access. 2024. https://doi.org/10.1109/ACCESS.2024.3463791.
28. Abdulazeez DH, Askar SK. Offloading mechanisms based on reinforcement learning and deep learning algorithms in the fog computing environment. IEEE Access. 2023;11:12555–86. https://doi.org/10.1109/ACCESS.2023.3241881.
29. Panwar SS, Rauthan MMS, Barthwal VA. Systematic review on effective energy utilization management strategies in cloud data centers. J Cloud Comput. 2022;11:95. https://doi.org/10.1186/s13677-022-00368-5.
30. Alsemmeari RA, Dahab MY, Alturki B, Alsulami AA, Alsini R. Towards an effective service allocation in fog computing. Sensors. 2023;23:7327. https://doi.org/10.3390/s23177327.
31. Kraemer FA, Braten AE, Tamkittikhun N, Palma D. Fog computing in healthcare–a review and discussion. IEEE Access. 2017;5:9206–22. https://doi.org/10.1109/ACCESS.2017.2704100.
32. Tahir S, Bakhsh ST, Alghamdi R, Abulkhair M. Fog-based healthcare architecture for wearable body area network. J Med Imaging Health Inf. 2017;7:1409–18. https://doi.org/10.1166/jmihi.2017.2152.
33. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT EHealth: promises and challenges of IoT in medicine and healthcare. Future Generation Comput Syst. 2018;78:659–76. https://doi.org/10.1016/j.future.2017.04.036.
34. Kaliyaperumal K. Adaptive heuristic edge assisted fog computing design for healthcare data optimization. J Cloud Comput. 2024;13:127. https://doi.org/10.1186/s13677-024-00689-7.
35. Roy I, Mitra R, Rahimi N, Gupta B. Efficient Non-DHT-based rc-based architecture for fog computing in healthcare 4.0. IoT. 2023;4:131–49. https://doi.org/10.3390/iot4020008.
36. Andriopoulou F, Dagiuklas T, Orphanoudakis T. Integrating IoT and fog computing for healthcare service delivery. In: Components and services for IoT platforms. Cham: Springer International Publishing; 2017. p. 213–32.
37. Tripathy SS, Bebortta S, Chowdhary CL, Mukherjee T, Kim S, Shafi J, Ijaz MF. FedHealthFog: a federated learning-enabled approach towards healthcare analytics over fog computing platform. Heliyon. 2024;10:e26416. https://doi.org/10.1016/j.heliyon.2024.e26416.
38. Yan Y, Su WA. Fog computing solution for advanced metering infrastructure. In proceedings of the 2016 IEEE/PES transmission and distribution conference and exposition (T&D). Piscataway: IEEE; 2016. p. 1–4.
39. Atiq HU, Ahmad Z, Uz Zaman SK, Khan MA, Shaikh AA, Al-Rasheed A. Reliable resource allocation and management for IoT transportation using fog computing. Electron (Basel). 2023;12:1452. https://doi.org/10.3390/electronics12061452.
40. Tang B, Chen Z, Hefferman G, Wei T, He H, Yang QA. Hierarchical Distributed Fog Computing Architecture for Big Data Analysis in Smart Cities. In Proceedings of the Proceedings of the ASE BigData & SocialInformatics 2015. ACM: New York.2015;1–6.
41. Vilela PH, Rodrigues JJPC, Solic P, Saleem K, Furtado V. Performance evaluation of a fog-assisted IoT solution for e-Health applications. Future Generation Comput Syst. 2019;97:379–86. https://doi.org/10.1016/j.future.2019.02.055.
42. Aladwani T. Scheduling IoT Healthcare tasks in Fog Computing based on their importance. Procedia Comput Sci. 2019;163:560–9. https://doi.org/10.1016/j.procs.2019.12.138.

43. Shukla S, Hassan MF, Jung LT, Awang A, Khan MK. A 3-Tier architecture for network latency reduction in healthcare internet-of-things using fog computing and machine learning. In Proceedings of the Proceedings of the 2019 8th International Conference on Software and Computer Applications. ACM: New York. 2019;522–528.
44. Tahir S, Bakhsh ST, Abulkhair M, Alassafi MO. An energy-efficient fog-to-Cloud internet of Medical things Architecture. Int J Distrib Sens Netw. 2019;15:155014771985197. https://doi.org/10.1177/1550147719851977.
45. El Kafhali S, Salah K. Performance modelling and analysis of internet of things enabled Healthcare Monitoring systems. IET Networks. 2019;8:48–58. https://doi.org/10.1049/iet-net.2018.5067.
46. Badidi E, Moumane K. Enhancing the processing of healthcare data streams using fog computing. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC). IEEE. 2019;1113–1118.
47. Shrivastava R, Pandey M. Real time fall detection in fog computing scenario. Cluster Comput. 2020;23:2861–70. https://doi.org/10.1007/s10586-020-03051-z.
48. Devarajan M, Subramaniyaswamy V, Vijayakumar V, Ravi L. Fog-assisted personalized healthcare-support system for remote patients with diabetes. J Ambient Intell Humaniz Comput. 2019;10:3747–60. https://doi.org/10.1007/s12652-019-01291-5.
49. Gia TN, Jiang M, Rahmani A-M, Westerlund T, Liljeberg P, Tenhunen H. Fog computing in healthcare internet of things: a case study on ECG feature extraction. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing. IEEE. 2015;356–363.
50. Oueis J, Strinati EC, Sardellitti S, Barbarossa S. Small cell clustering for efficient distributed fog computing: a multi-user case. In Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall). IEEE. 2015;1–5.
51. Agarwal S, Yadav S, Yadav AK. An efficient architecture and algorithm for resource provisioning in fog computing. Int J Inform Eng Electron Bus. 2016;8:48–61. https://doi.org/10.5815/ijieeb.2016.01.06.
52. Verma P, Sood SK. Fog assisted-IoT enabled patient health monitoring in smart homes. IEEE Internet Things J. 2018;5:1789–96. https://doi.org/10.1109/JIOT.2018.2803201.
53. Wang K, Shao Y, Xie L, Wu J, Guo S. Adaptive and fault-tolerant data processing in healthcare IoT based on fog computing. IEEE Trans Netw Sci Eng. 2020;7:263–73. https://doi.org/10.1109/TNSE.2018.2859307.
54. Jia X, He D, Kumar N, Choo K-KR. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Netw. 2019;25:4737–50. https://doi.org/10.1007/s11276-018-1759-3.
55. Al-Khafajiy M, Otoum S, Baker T, Asim M, Maamar Z, Aloqaily M, Taylor M, Randles M. Intelligent control and security of fog resources in healthcare systems via a cognitive fog model. ACM Trans Internet Technol. 2021;21:1–23. https://doi.org/10.1145/3382770.
56. Saha R, Kumar G, Rai MK, Thomas R, Lim S-J. Privacy ensured ${e}$ -healthcare for fog-enhanced IoT based applications. IEEE Access. 2019;7:44536–43. https://doi.org/10.1109/ACCESS.2019.2908664.
57. Awaisi KS, Hussain S, Ahmed M, Khan AA, Ahmed G. Leveraging IoT and fog computing in healthcare systems. IEEE Internet Things Magazine. 2020;3:52–6. https://doi.org/10.1109/IOTM.0001.1900096.
58. Muthanna A, Ateya A, Khakimov A, Gudkova A, Abuarqoub I, Samouylov A, Koucheryavy K. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. J Sens Actuator Networks. 2019. https://doi.org/10.3390/jsan8010015.
59. Sangpetch O, Sangpetch A. security context framework for distributed healthcare IoT platform. 2016;71–6.
60. Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiquzzaman M. PrivacyProtector: privacy-protected patient data collection in IoT-based healthcare systems. IEEE Commun Mag. 2018;56:163–8. https://doi.org/10.1109/MCOM.2018.1700364.
61. Scholarworks U, Al Baqari S, Baqari MR, S A. M.R. Sdhcare: Secured distributed healthcare system. Information. 2020. Theses. 6.
62. Tang W, Ren J, Deng K, Zhang Y. Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. IEEE Internet Things J. 2019;6:8714–26. https://doi.org/10.1109/JIOT.2019.2923261.
63. La QD, Ngo MV, Dinh TQ, Quek TQS, Shin H. Enabling intelligence in fog computing to achieve energy and latency reduction. Digit Commun Networks. 2019;5:3–9. https://doi.org/10.1016/j.dcan.2018.10.008.
64. Alsemmeari A, Yehia Dahab R, Alturki M, Alsulami B;A. Priority detector and classifier techniques based on ML for the IoMT. Computers Mater Continua. 2023;76:1853–70. https://doi.org/10.32604/cmc.2023.038589.
65. Yıldırım E, Cicioğlu M, Çalhan A. Fog-cloud architecture-driven internet of medical things framework for healthcare monitoring. Med Biol Eng Comput. 2023;61:1133–47. https://doi.org/10.1007/s11517-023-02776-4.
66. Abbas T, Khan AH, Kanwal K, Daud A, Irfan M, Bukhari A, Alharbey R. IoMT-based healthcare systems: a review. Comput Syst Sci Eng. 2024;0:1–10. https://doi.org/10.32604/csse.2024.049026.
67. Thota C, Sundarasekar R, Manogaran G, R V. Centralized fog computing security platform for IoT and cloud in healthcare system. In: Fog Computing. IGI Global; p. 365–78.
68. Gill SS, Arya RC, Wander GS, Buyya R. Fog-based smart healthcare as a big data and cloud service for heart patients using IoT. 2019;1376–83.
69. Sharma SK, Wang X. Live data analytics with collaborative edge and cloud processing in wireless IoT networks. IEEE Access. 2017;5:4621–35. https://doi.org/10.1109/ACCESS.2017.2682640.
70. Yang G, Jan MA, Menon VG, Shynu PG, Aimal MM, Alshehri MD. A centralized cluster-based hierarchical approach for green communication in a smart healthcare system. IEEE Access. 2020;8:101464–75. https://doi.org/10.1109/ACCESS.2020.2998452.
71. Yuan B, Ge S, Xing WA. Federated learning framework for healthcare IoT devices. 2020.
72. Shukla S, Hassan MF, Khan MK, Jung LT, Awang A. An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. PLoS ONE. 2019;14:e0224934. https://doi.org/10.1371/journal.pone.0224934.
73. Sharma S, Chen K, Sheth A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Comput. 2018;22:42–51. https://doi.org/10.1109/MIC.2018.112102519.
74. Kaur P, Kumar R, Kumar MA. Healthcare monitoring system using random forest and internet of things (IoT). Multimed Tools Appl. 2019;78:19905–16. https://doi.org/10.1007/s11042-019-7327-8.
75. Panda S, Panda G. Intelligent classification of IoT Traffic in healthcare using machine learning techniques. In Proceedings of the 2020 6th International Conference on Control, Automation and Robotics (ICCAR). IEEE. 2020; 581–585.
76. Patan R, Pradeep Ghantasala GS, Sekaran R, Gupta D, Ramachandran M. Smart healthcare and quality of service in IoT using grey filter convolutional based cyber physical system. Sustain Cities Soc. 2020;59:102141. https://doi.org/10.1016/j.scs.2020.102141.

77. Kumar PM, Lokesh S, Varatharajan R, Chandra Babu G, Parthasarathy P. Cloud and IoT based disease prediction and diagnosis system for healthcare using fuzzy neural classifier. Future Generat Comput Syst. 2018;86:527–34. https://doi.org/10.1016/j.future.2018.04.036.
78. Subasi A, Radhwan M, Kurdi R, Khateeb K. IoT Based mobile healthcare system for human activity recognition. In Proceedings of the 2018 15th Learning and Technology Conference (L&T). IEEE. 2018; 29–34.
79. Farahani B, Barzegari M, Aliee FS. Towards collaborative machine learning driven healthcare internet of things. In Proceedings of the Proceedings of the International Conference on Omni-Layer Intelligent Systems. ACM: New York. 2019;134–140.
80. Sharma S, Dudeja RK, Aujla GS, Bali RS, Kumar N. DeTrAs: deep learning-based Healthcare Framework for IoT-Based assistance of Alzheimer patients. Neural Comput Appl. 2020. https://doi.org/10.1007/s00521-020-05327-2.
81. Villegas-Ch W, García-Ortiz J. Urbina-Camacho I framework for a secure and sustainable internet of medical things, requirements, design challenges, and trends F. Appl Sci. 2023;13:6634. https://doi.org/10.3390/app13116634.
82. Bhushan B, Kumar A, Agarwal AK, Kumar A, Bhattacharya P, Kumar A. Towards a secure and sustainable internet of medical things (IoMT): requirements, design challenges, security techniques, and future trends. Sustainability. 2023;15:6177. https://doi.org/10.3390/su15076177.
83. Sun Z, An G, Yang Y, Liu Y. Optimized machine learning enabled intrusion detection 2 system for internet of medical things. Frankl Open. 2024;6:100056. https://doi.org/10.1016/j.fraope.2023.100056.
84. Mishra P, Singh G. Internet of medical things healthcare for sustainable smart cities: current status and future prospects. Appl Sci. 2023;13:8869. https://doi.org/10.3390/app13158869.
85. Alabdulatif A, Thilakarathne NN. Bio-inspired internet of things: current status, benefits, challenges, and future directions. Biomimetics. 2023;8:373. https://doi.org/10.3390/biomimetics8040373.
86. Ghayvat H, Awais M, Geddam R, Tiwari P, Löwe W. Revolutionizing healthcare: IoMT-enabled digital enhancement via multimodal ADL data fusion. Inform Fusion. 2024;111:102518. https://doi.org/10.1016/j.inffus.2024.102518.
87. Alsemmeari RA, Dahab MY, Alsulami AA, Alturki B, Algarni S. Resilient security framework using TNN and blockchain for IoMT. Electron (Basel). 2023;12:2252. https://doi.org/10.3390/electronics12102252.
88. Alalhareth M, Hong S-C. Enhancing the internet of medical things (IoMT) security with meta-learning: a performance-driven approach for ensemble intrusion detection systems. Sensors. 2024;24:3519. https://doi.org/10.3390/s24113519.
89. Faruqui N, Yousuf MA, Whaiduzzaman M, Azad A, Alyami SA, Liò P, Kabir MA, Moni MA. SafetyMed: a novel IoMT intrusion detection system using CNN-LSTM hybridization. Electron (Basel). 2023;12:3541. https://doi.org/10.3390/electronics12173541.
90. Binbusayyis A, Alaskar H, Vaiyapuri T, Dinesh M. An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. J Supercomput. 2022;78:17403–22. https://doi.org/10.1007/s11227-022-04568-3.
91. Ravi V, Pham TD, Alazab M. Deep learning-based network intrusion detection system for internet of medical things. IEEE Internet Things Mag. 2023;6:50–4. https://doi.org/10.1109/IOTM.001.2300021.
92. Chaganti R, Mourade A, Ravi V, Vemprala N, Dua A, Bhushan BA. Particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things. Sustainability. 2022;14:12828. https://doi.org/10.3390/su141912828.
93. Alalhareth M, Hong S-C. An adaptive intrusion detection system in the internet of medical things using fuzzy-based learning. Sensors. 2023;23:9247. https://doi.org/10.3390/s23229247.
94. Hameed SS, Selamat A, Abdul Latiff L, Razak SA, Krejcar O, Fujita H, Ahmad Sharif MN, Omatu S. A hybrid lightweight system for early attack detection in the IoMT Fog. Sensors. 2021;21:8289. https://doi.org/10.3390/s21248289.
95. KE Fahim, K Kalinaki, W Shafik. Electronic Devices in the artificial intelligence of the internet of medical things (AIoMT). In Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things. 2023.
96. Baseer KK, Sivakumar K, Veeraiah D, Chhabra G, Kumar Lakineni P, Jahir Pasha M, Gandikota R, Harikrishnan G. Healthcare Diagnostics with an adaptive deep learning Model Integrated with the internet of medical things (IoMT) for Predicting Heart Disease. Biomed Signal Process Control. 2024;92:105988. https://doi.org/10.1016/j.bspc.2024.105988.
97. Asim M, Arif M, Rafiq M, Nawaz MA, Ahmad R. Investigating applications of internet of things in medical libraries of Pakistan: an empirical study. J Acad Librariansh. 2024;50:102925. https://doi.org/10.1016/j.acalib.2024.102925.
98. Jan MA, Zhang W, Khan F, Abbas S, Khan R. Lightweight and smart data fusion approaches for wearable devices of the internet of medical things. Inform Fusion. 2024;103:102076. https://doi.org/10.1016/j.inffus.2023.102076.
99. Raj A, Prakash S. Privacy preservation of the internet of medical things using Blockchain. Health Serv Outcomes Res Methodol. 2024;24:112–39. https://doi.org/10.1007/s10742-023-00306-1.
100. Qadri YA, Jung H, Niyato D. Towards the internet of medical things for real-time health monitoring over Wi-Fi. IEEE Netw. 2024;38:1–1. https://doi.org/10.1109/MNET.2024.3352598.
101. W Shafik. Wearable Medical electronics in artificial intelligence of medical things. In Handbook of Security and privacy of AI-enabled healthcare systems and internet of medical things. 2023.
102. CB S, M DK. Accessibility study of MHealth systems based on the internet of things (IoT). Tamjeed J Healthc Eng Sci Technol. 2023;1:14–23. https://doi.org/10.59785/tjhest.v1i1.7.
103. Huang W, Ding Q, Wang H, Wu Z, Luo Y, Shi W, Yang L, Liang Y, Liu C, Wu J. Design of Stretchable and Self-Powered sensing device for portable and remote Trace biomarkers detection. Nat Commun. 2023;14:5221. https://doi.org/10.1038/s41467-023-40953-z.
104. Maïzi Y, Bendavid Y. Hybrid RFID-IoT simulation modeling approach for analyzing Scrubs' distribution solutions in operating rooms. Bus Process Manage J. 2023;29:1734–61. https://doi.org/10.1108/BPMJ-12-2022-0658.
105. Siddiqui SA, Ahmad A, Fatima N. IoT-based disease prediction using machine learning. Comput Electr Eng. 2023;108:108675. https://doi.org/10.1016/j.compeleceng.2023.108675.
106. Al Khatib I, Shamayleh A, Ndiaye M. Healthcare and the internet of medical things: applications, trends, key challenges, and proposed resolutions. Informatics. 2024;11:47. https://doi.org/10.3390/informatics11030047.