Review



# IoMT Landscape: Navigating Current Challenges and Pioneering Future Research Trends

Badraddin Alturki , Qasem Abu Al-Haija * , Rayan A. Alsemmeari , Abdulaziz A. Alsulami , Ali Alqahtani , Bandar M. Alghamdi , Sheikh Tahir Bakhsh , Riaz Ahmed Shaikh

Posted Date: 16 May 2024

doi: 10.20944/preprints202405.1056.v1

Keywords: internet of medical things; artificial intelligence; wearables and sensors; fog computing; edge computing

*Review*

# IoMT Landscape: Navigating Current Challenges and Pioneering Future Research Trends

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

[1] Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; baalturki@kau.edu.sa (B.A.); bmmalghamdi@kau.edu.sa (B.A.);
[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; ralsemmeari@kau.edu.sa (R.A.A.); aaalsulami10@kau.edu.sa (A.A.A.)
[4] Department of Networks and Communications Engineering, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia; asalqahtany@nu.edu.sa (A.A.);
[5] Department of Computer Science, Cardiff Metropolitan University, Western Avenue, Cardiff CF5 2YB, UK; sbakhsh@cardiffmet.ac.uk
[6] School of Computing Sciences, University of East Anglia, UK; riaz-ahmed.shaikh@uea.ac.uk
* Correspondence: qsabuhaija@just.edu.jo

**Abstract.** Smart electronic devices and telemedicine are widely used in humans' daily lives. This provides remote treatment of patients using information and communications technology. New telemedicine technologies, such as the Internet of Medical Things (IoMT), make it easier for medical and computing devices to communicate regularly and effectively. Critical motivations for adapting 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, the IoMT technology makes excellent use of Artificial Intelligence (AI) to support disease detection and health condition prediction, alerting patients and healthcare providers. Many research studies have been conducted to explore various 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 technologies 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 technologies 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.

**Keywords:** internet of medical things; artificial intelligence; wearables and sensors; fog computing; edge computing

## 1. Introduction

Smart electronic devices are widely used in humans' daily life and telemedicine. Telemedicine refers to the remote treatment of patients using information and communications technology. Emerging telemedicine trends such as Medical cyber-physical systems (MCPS) facilitate regular and efficient interactions between medical devices 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 the Internet

 doi:10.20944/preprints202405.1056.v1



of Things (IoT) in medical care has become increasingly popular in the era of 5G technology. Many medical and healthcare applications like elderly care, fitness programs, remote health monitoring, 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. Various medical devices can be integrated into the Internet of Medical Things (IoMT) ecosystem to achieve this. IoMT is an ecosystem that connects patients and any medical activity at any time. With the assistance of 5G and IPv6, the IoMT can play a crucial role in various medical diagnoses and treatments.

One of the key objectives of implementing the IoMT is reduced cost, increased quality of life, and timely medical intervention. The IoMT is one of the key advantages of adopting the IoMT as a scheduling tool. Furthermore, seamless and secure communication between the patient and the healthcare provider is a significant factor in today's IoMT. They guarantee reliable and uninterrupted healthcare service delivery on time, which provides real-time monitoring and early diagnosis. With the help of 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 various 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 various 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.

With big data, the IoMT technology makes excellent use of 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 initiative-taking 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 increase healthcare services' efficacy and save many lives. However, the study of the potential of smart IoMT is still in its infancy 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. That is, 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 indications 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 could use some of these ideas. This paper is organized as follows: Section 2 includes IoMT structures, protocols, and standards— and section 3 discusses existing techniques in IoMT in edge computing. Fog computing and its related

 doi:10.20944/preprints202405.1056.v1



research techniques and limitations are given in Section 4. Section 5 emphasizes IoMT processing techniques. Section 6 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. 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 various vital signals [6]. These devices are wearable and, most of the time, are resource-constrained. Therefore, the data they collect is sent immediately to 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 is equipped with wireless capability, transferring 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 comprises multiple devices with capabilities higher than the Interoperability layer. These devices include Laptops, PCs, PDAs, and Terminals. 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 the data from the sensors and devices in the Interoperability layer. The second layer in this framework is the WAN devices layer. It acquires data from multiple systems and stores them in one location, which could be 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—these store locations and platforms. 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 using the xHRN Interface.

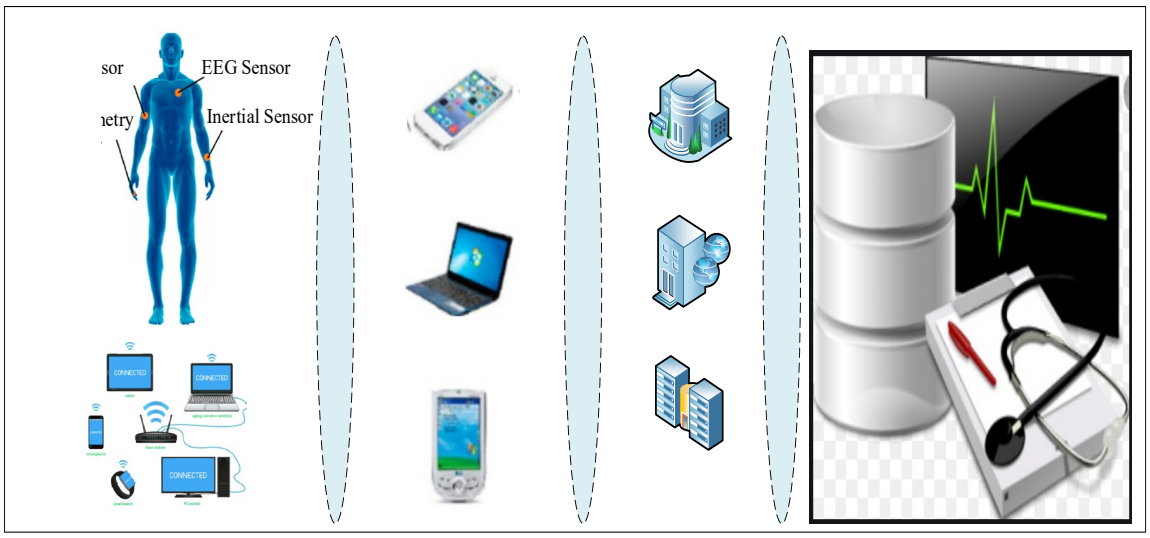


**Figure 1.** The components of IoMT by the Continua Health Alliance.

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

 doi:10.20944/preprints202405.1056.v1



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].

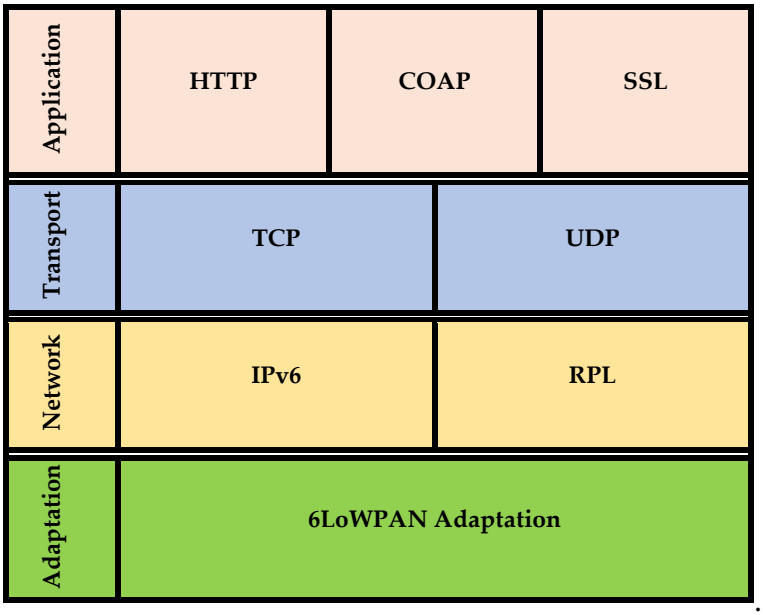


**Figure 2.** Resembling the popular network TCP/IP framework and stacks.

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 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 the 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. 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

 doi:10.20944/preprints202405.1056.v1



is characterized by different packet structures. This is because these data are usually generated by various technologies like Radio Frequency Identification Module (RFID), Bluetooth, LoRA, and ZigBee. Furthermore, IoMT ecosystems generate historical data 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. Furthermore, transmitting these 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, data acquisition, manipulation, analysis, and modeling are some factors that govern data acquisition, manipulation, analysis, and modeling. This involves several applications that require decision-making, security, and prediction. The heterogeneous protocols must communicate the information needed to make a decision resiliently and smoothly. However, this is challenging since the standard differences may make it difficult for some protocols to cooperate. 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. This adversely affects the accuracy of predictive modeling built based on these 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]. The vital data are collected from these sensors in real-time simultaneously among hundreds or thousands of medical things. With such enormous 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] [17] [18].

#### 3.1.1. Studies in Edge Computing

An edge-assisted framework was proposed by [15], which controls the parameters of mobile sensors. Using a probabilistic approach, the framework tries to identify the anomalies in the collected

 doi:10.20944/preprints202405.1056.v1



signals in real time, given battery-imposed constraints. The framework was evaluated by a use case utilizing various 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.

HiCH proposed a hierarchical computing architecture for IoT-based health monitoring systems. [16]. 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 changes in topology and operating environment. 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 strategically position the gateways at the network's edge. 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 [19] 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 various 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.

The IoT and Edge Cloud were combined. [20] For medical data retrieval. Such integration provides a secure healthcare monitoring framework integrating 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 medical data retrieval latency and cost significantly compared with the existing solution. However, the

 doi:10.20944/preprints202405.1056.v1



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 [21]. 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 [22] 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 [23] 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 [24] 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.

 doi:10.20944/preprints202405.1056.v1



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.

## 4. FOG COMPUTING

Deployments of fog computing at the edge of the network enable efficiency, security, network scalability, availability, reliability, and maintainability in the cloud computing paradigm. Due to these features, fog computing devices have been deployed in various application areas, notably in healthcare. [25]. 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.

### *4.1. 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, dense geographical distribution, and support for user mobility. 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, 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 various 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 power is limited, and thus, it cannot replace cloud computing. Because of its proximity to the user and geographical distribution, it can support the users' mobility, provide location awareness, and decrease delay, latency, and jitter, eliminating data transmission in the network infrastructure and ensuring enhanced

 doi:10.20944/preprints202405.1056.v1



security of encrypted data. As Fog's computing power is limited, it will not replace cloud computing. [26].

### *4.2. IoMT Fog-Cloud Computing*

Fog computing is recommended to enable computing directly at the network's edge that may provide 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 is a "cloud-in-a-box" that can be used by mobile devices nearby. [27].

Managing private data centers for customers often uses the cloud computing model, and the pay is based on data usage. To maintain the massive aggregation of the data centers, the data centers' factors must have a higher predictability of massive aggregation, allowing high use with adequate work performance, utilization of inexpensive power in various locations, appropriate storage, and networking. [28]. Combining all these qualities can be brought under one platform, the Internet of Things (IoT) or Fog Computing. [29]. Fog Computing facilitates the interplay of various 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. [30].

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. [19]. 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. [30].

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 delay. 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.

### *4.3. 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 aggregate data from heterogeneous 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

 doi:10.20944/preprints202405.1056.v1



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 that is not accessible by a third party.

### *4.4. Analysis of Existing Techniques and Evaluation Criteria in Fog Computing*

A fog-based healthcare architecture (FHA) was proposed by [31], 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 [32]. 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 various 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 by [33] indicated that deploying smart e-health gateways at the network's edge will enable health monitoring in hospital environments. They concluded that fog gateways must be strategically positioned to provide high-level services, including local storage, real-time analysis, data mining, etc. The purpose of the proposed smart gateway is to manage sensor network operations and remote healthcare centers. It also manages scalability, energy efficiency, and reliability. However, the study overlooks the possibility that any failure at the gateway would cause a major disruption to the system. Although redundant gateways solve such a single point of failure, they create additional overhead and complexity when selecting the gateway. The paths to different gateways must be prioritized to address such an issue based on criteria like the number of hops, bandwidth, and signal-to-noise ratio (SNR).

A detailed review of the implementation of fog computing in healthcare services was provided by [30]. 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.

 doi:10.20944/preprints202405.1056.v1



As part of the OpSIT project, the smart Fog was integrated with cloud computing. [34] To support healthcare applications. The proposed smart healthcare system's architecture comprises three layers: sensors, Fog, and cloud. The validity of this architecture was evaluated using several use cases. However, it is not clear on which criteria the architecture was evaluated. Additionally, the multi-layer architecture creates additional overhead due to the interfacing and compatibility issues when data passes through various components.

The effect of incorporating IoT in healthcare was investigated by [35], and 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.

A consumer-centric IoT services approach was investigated in [36], which utilizes fog computing to create an architecture for connected vehicles with M2M gateway and Road Side Units. The authors discussed M2M Data Analytics with Semantics, discovery, and connected vehicles' management as a consumer-centric IoT. The study proposed an architecture for utilizing vehicles as the infrastructures for computation and communication, called Vehicular Fog Computing. It supports mobility, allowing the mobile stations to write, read, and even update sensor configuration. Such an architecture suits IoMT, matching the need for mobile stations like ambulances and reliable and robust communication with the healthcare center. Their study results showed huge potential improvement in computation, communication, and capacity, which the vehicular fog platform can recognize. The computational performance can be improved dramatically by vehicular fog computing compared to conventional systems because it benefits from individual vehicles' currently underutilized computational resources. 37]. However, the study overlooks the heterogeneity of this kind of network.

Furthermore, scalability was not considered when designing the solution, which becomes an issue with this architecture. Security is another aspect that this study has not considered, which adversely affects the reliability of the communication channels and the consistency and credibility of the data. Security is not discussed in their work.

The authors of [38] proposed an 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.

The use of fog technology to support a smart living environment and improve the user's experience was discussed in [39]. The integration between fog components like Fog Edge Node, Fog Server, and Foglet was investigated to determine to what extent they support the heterogeneity of IoMT. The study concluded that latency could be reduced if data processing were carried out within the fog scope. However, the analysis overlooks the density of IoMT devices, which could cause a lot of congestion and bottlenecks when the number of nodes in the fog layer increases. Such a scalability issue hurts the latency.

 doi:10.20944/preprints202405.1056.v1



Latency in the fog layer of IoMT was also investigated by [40], 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 [41] 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 [42] 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 not clear 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 [43] 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 sing-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 [44] 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 are 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 [45] was proposed to process and analyze the data generated by various 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 [46] was created in the fog layer to notify people about fall activity in real-time. 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 a real-time notification despite losing the cloud and fog node connection. Although

 doi:10.20944/preprints202405.1056.v1



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 monitoring, predicting, and controlling the real-time risks of remote diabetic patients based on their physiological condition was proposed by [47]. By training a J48 decision tree classifier, 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 arrive 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 51], which employs fog computing at smart gateways to perform various tasks such as embedded data mining, distributed storage, 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 features extracted, such as heart rate, P wave, and T wave, through a flexible template based on a lightweight wavelet transform mechanism. However, analyzing data at smart gateways creates additional overhead on these nodes, which causes time delays.

**Table 1.** Fog Computing studies are categorized based on several criteria.

| Ref | Category | Heterogeneity | Scalability | Mobility | Security |
|---|---|---|---|---|---|
| **[31]** | Healthcare | ✓ | × | ✓ | ✓ |
| **[32]** | | × | ✓ | ✓ | × |
| **[33]** | | ✓ | × | × | ✓ |
| **[30]** | | ✓ | × | ✓ | ✓ |
| **[34]** | | × | × | × | × |
| **[35]** | | × | × | × | × |
| **[36]** | Connected Vehicles | × | × | ✓ | × |
| **[37]** | | × | × | ✓ | × |
| **[38]** | Smart Living | × | ✓ | × | × |
| **[39]** | | ✓ | × | × | × |
| **[48]** | | × | × | × | × |
| **[49]** | Energy Consumption | ✓ | × | × | × |
| **[50]** | Resource Management | ✓ | × | × | × |

The concept of transferring the computing intelligence from the cloud to the fog network was utilized in [35], 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

 doi:10.20944/preprints202405.1056.v1



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 methodology is implemented to process the patient's real-time 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 Neighbourhood 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 fault-tolerant data transmission, self-adaptive filtering, and data-load-reduction processing. Therefore, it significantly improves the efficacy of IoMT applications. Self-adaptive filtering that recollects lost data is achieved using the RVNS algorithm to refine valuable information from raw sensing 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 proofed 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. Ensemble learning was utilized to create the model to classify the data as normal or suspicious. However, the ensemble-based model was unsuitable for the dynamic nature of IoMT systems and user mobility. Therefore, attackers could use the concept of drift to avoid detection.

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 the Fog's weekly secured services.

A multi-modal fog-assisted system [57] 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 [58] was proposed to reconsolidate IoMT services' security at the fog layer. The Elliptic Curve Cryptography technique created the output token for user authentication. This authentication method was implemented into identity management to prevent security breaches.

 doi:10.20944/preprints202405.1056.v1



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.

### *4.5. 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 various (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.

## 5. 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.

### *5.1. Distributed Processing*

Researchers proposed a high-reliability and low-latency framework for Internet of Medical Things (IoMT) applications [60]. 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 various 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.

 doi:10.20944/preprints202405.1056.v1



IoMT is vulnerable to many security threats in distributed environments, including internal and external attacks. Therefore, an adaptive security context framework [61] It was proposed that 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 the various 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 [62] investigated the challenges during data collection. The framework employs secret sharing and sharing repairing (in case of data loss or compromise) to safeguard patients' data privacy. 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 [63]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 [64]. The study proposed a health data aggregation scheme as a privacy-preserving solution that securely collects health data from multiple sources and guarantees fair incentives for contributing patients. Specifically, 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.

**Table 2.** The techniques and tools used by existing research.

| Ref. | Performance measure | Evaluation Tools | Experimental evaluation | Strength |
|---|---|---|---|---|
| [59] | 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) | For designing fog computing systems that meet 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. | |
| [40] | 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 | 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. |

 doi:10.20944/preprints202405.1056.v1



| | | | | |
|---|---|---|---|---|
| | | the Python script. The applications support the Message Queuing Telemetry Transport (MQTT) | | |
| [41] | 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. |
| [42] | 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. |
| [44] | 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. |
| [40] | 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. |
| [46] | 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. |
| [47] | Latency + Bandwidth efficiency + Classification | The smartphone is equipped with Snapdragon 410 Quad-Core, which is | J48Graft displayed a high classification accuracy of 98.56% compared to other baseline techniques. It utilized fog computing as the intermediary layer, which | They effectively predicted the risky blood glucose levels in diabetic patients. |

 doi:10.20944/preprints202405.1056.v1



| | | | | |
|---|---|---|---|---|
| | accuracy of the Fog compared to cloud computing. | 450 MHz, has 2 GB memory, and a J48Graft classifier. | 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. | |
| [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. |

### *5.2. Limitations and Research Directions for Distributed Processing in IoMT*

Distributed computing makes the processing and analyzing a massive amount of data generated in the IoMT much easier. It divides the big data into smaller pieces, 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. Existing research on big data distributed analytics and predictive modeling cater 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.

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.

### *5.3. Centralized Processing*

In their paper, referenced as [65], the authors presented an architecture for integrating IoT-based healthcare systems in a cloud environment. The proposed platform uses Fog Computing to run the framework. 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, [66] 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

 doi:10.20944/preprints202405.1056.v1



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 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. This framework uses network-wide knowledge and historical information at the cloud center to guide edge computing units in achieving various performance requirements 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. It also identifies and describes potential key enablers for the proposed edge-cloud collaborative framework, associated key challenges, and interesting future research directions. However, coordinating between the edge and cloud incurs additional expenditure, which can lead to increased delay.

A cluster-based hierarchical approach [68] 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 various 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 [69] 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.

### 5.4. 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 various 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 pre-processing 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.

### *5.5. Analysis Techniques*

 doi:10.20944/preprints202405.1056.v1



An increased time delay for data transmission due to large data size and multiple hops counts between IoT devices and cloud servers renders healthcare data irrelevant and inadequate for end-users. Time-sensitive healthcare applications require genuine data. Traditional cloud servers cannot meet healthcare IoT devices and end-users' minimum latency requirements. Communication latency, computation latency, and network latency must 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 [70] 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 in 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 [71] was built to provide privacy protection for IoMT systems. The model adopts kHealth, a personalized digital healthcare information system for disease monitoring. Likewise, [72] 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. [73] 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 privacy-preserving analytics model was developed to protect the privacy of IoMT systems. The model uses kHealth, a personalized digital healthcare information system for disease monitoring. Another model researchers propose uses a Random Forest-based algorithm for real-time remote health monitoring of IoMT. The model was trained using data stored in the cloud. However, a one-time training approach is unsuitable for real-time applications with dynamic IoMT environments. Another study used Decision Tree, Random Forest, and Naive Bayes machine learning classifiers to diagnose Parkinson's disease based on IoMT sensors. The IoT-based node receives the data and provides a faster classification solution for decision-making. However, offloading the sensors' decision is an additional overhead that drains the sensor's memory, CPU, and battery.

In a study by [75], 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 utilizes a dataset containing body motion and vital signs recordings for ten volunteers with different profiles while performing 12 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 [76]. 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 [77]. Also, in [78], 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. The study provided two components only.

### *5.6. Limitations and Research Directions for Techniques in IoMT*

 doi:10.20944/preprints202405.1056.v1



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, the 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 secured 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 various 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 come from various sources, which could contain conflicting and inconsistent labels. Such inconsistency is problematic when dealing with supervised learning, which degrades the model's performance.

## 6. Conclusions

This survey explored the myriad techniques and models proposed for the Internet of Medical Things (IoMT), elucidating each method's inherent limitations. The defining characteristics of IoMT standards, protocols, and diverse manifestations were meticulously examined. Furthermore, an in-depth analysis of scholarly works on integrating fog and edge computing into IoMT ecosystems was presented, affording a nuanced understanding of these cutting-edge advancements. Each study's proposed method, technique, or model was meticulously delineated, accompanied by a candid appraisal of its limitations and pragmatic suggestions for further refinement. By engaging in a thorough discourse on research directions and identifying prevailing gaps within diverse IoMT approaches and technologies, this survey serves as a blueprint for future research endeavors to mitigate these challenges effectively. IoMT applications are poised to flourish by addressing these identified limitations head-on, instilling greater trust in automated healthcare services, and fostering a paradigm shift in patient care. The evolving trends in IoMT are poised to seamlessly facilitate interactions between patients and medical and computing devices within the healthcare ecosystem, promising tangible benefits such as reduced costs, improved quality of life, and timely medical interventions. As we navigate the ever-expanding landscape of IoMT, this survey provides a compass, guiding researchers toward innovative solutions that will redefine the future of healthcare delivery.

**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

 doi:10.20944/preprints202405.1056.v1



authors contributed to Writing—original draft, review & editing, and Funding acquisition. All authors have read and agreed to the published version of the manuscript.

**Competing interest**: The authors declare that they have no conflict of interest.

## References


1. Al Hamid, H.A., et al., A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access, 2017. 5: p. 22313-22328.
2. Zhang, Y., et al., Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Systems Journal, 2015. 11(1): p. 88-95.
3. Damar, S., Koksalmis, G.H. A bibliometric analysis of metaverse technologies in healthcare services. Serv Bus (2024). https://doi.org/10.1007/s11628-024-00553-3
4. Batra, P. and Dave, D.M., 2024. Revolutionizing Healthcare Platforms: The Impact of AI on Patient Engagement and Treatment Efficacy. International Journal of Science and Research (IJSR), 13(10.21275), pp.613-624.
5. A. Rauniyar et al., "Federated Learning for Medical Applications: A Taxonomy, Current Trends, Challenges, and Future Research Directions," in IEEE Internet of Things Journal, vol. 11, no. 5, pp. 7374-7398, 1 March 1, 2024, doi: 10.1109/JIOT.2023.3329061.
6. Azizan, A., Ahmed, W. & Razak, A.H.A. Sensing health: a bibliometric analysis of wearable sensors in healthcare. Health Technol. 14, 15–34 (2024). https://doi.org/10.1007/s12553-023-00801-y
7. Ali, O., Abdelbaki, W., Shrestha, A., Elbasi, E., Alryalat, M.A.A. and Dwivedi, Y.K., 2023. A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities. Journal of Innovation & Knowledge, 8(1), p.100333.
8. M. Khalil, Q. Abu Al-Haija, S.Ahmad, "Healthcare IoT networks using LPWAN", Chapter in: Low-Power Wide Area Network for Large Scale Internet of Things, 1st Edition, CRC Press, eBook ISBN9781003426974, 2024.
9. Pergolizzi Jr. J, LeQuang J K, Vasiliu-Feltes I, et al. (October 04, 2023) Brave New Healthcare: A Narrative Review of Digital Healthcare in American Medicine. Cureus 15(10): e46489. DOI 10.7759/cureus.46489
10. Osama, M., Ateya, A.A., Sayed, M.S., Hammad, M., Pławiak, P., Abd El-Latif, A.A. and Elsayed, R.A., 2023. Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions. Sensors, 23(17), p.7435.
11. Ahmed, S.F., Alam, M.S.B., Afrin, S., Rafa, S.J., Rafa, N. and Gandomi, A.H., 2024. Insights into the Internet of Medical Things (IoMT): Data fusion, security issues, and potential solutions. Information Fusion, 102, p.102060.
12. Aski, V.J., Dhaka, V.S., Parashar, A. and Rida, I., 2023. Internet of Things in Healthcare: A survey on protocol standards, enabling technologies, WBAN architectures, and open issues. Physical Communication, p.102103.
13. Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y. and Moussa, S., 2023. Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. Sustainability, 15(4), p.3317.
14. K. T. Putra et al., "A Review on the Application of Internet of Medical Things in Wearable Personal Health Monitoring: A Cloud-Edge Artificial Intelligence Approach," in IEEE Access, vol. 12, pp. 21437-21452, 2024, doi: 10.1109/ACCESS.2024.3358827.
15. Yu, X., et al., An adaptive method based on contextual anomaly detection in Internet of Things through wireless sensor networks. International Journal of Distributed Sensor Networks, 2020. 16(5): p. 1550147720920478.
16. Azimi, I., et al., Hich: Hierarchical fog-assisted computing architecture for healthcare IoT. ACM Transactions on Embedded Computing Systems (TECS), 2017. 16(5s): p. 1-20.
17. Rahmani, A.M., et al., Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 2018. 78: p. 641-658.
18. Alabdulatif, A., et al., Secure Edge of Things for Smart Healthcare Surveillance Framework. IEEE Access, 2019. 7: p. 31010-31021.
19. Pace, P., et al., An Edge-Based Architecture to Support Efficient Applications for Healthcare Industry 4.0. IEEE Transactions on Industrial Informatics, 2019. 15(1): p. 481-489.
20. Wang, X. and S. Cai, Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. Future Generation Computer Systems, 2020. 112: p. 320-329.
21. Azimi, I., et al. Empowering healthcare IoT systems with hierarchical edge-based deep learning. In Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies. 2018.
22. Yu, J., et al. EdgeCNN: A Hybrid Architecture for Agile Learning of Healthcare Data from IoT Devices. in 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). 2018.
23. Li, J., et al., A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System. IEEE Access, 2020. 8: p. 135479-135490.
24. Abirami, S. and P. Chitra, Chapter Fourteen - Energy-efficient edge-based real-time healthcare support system, in Advances in Computers, P. Raj and P. Evangeline, Editors. 2020, Elsevier. p. 339-368.
25. Gia, T.N., et al. Low-cost fog-assisted health-care IoT system with energy-efficient sensor nodes. In 2017, the 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017. IEEE.

 doi:10.20944/preprints202405.1056.v1




26. Keramidas, G., N. Voros, and M. Hübner, Components and Services for IoT Platforms. 2016: Springer.
27. Dastjerdi, A.V., and R. Buyya, Fog computing: Helping the Internet of Things realize its potential. Computer, 2016. 49(8): p. 112-116.
28. Osanaiye, O., et al., From cloud to fog computing: A review and a conceptual live VM migration framework. IEEE Access, 2017. 5: p. 8284-8300.
29. Bonomi, F., et al., Fog computing: A platform for internet of things and analytics, in Big data and internet of things: A roadmap for smart environments. 2014, Springer. p. 169-186.
30. Kraemer, F.A., et al., Fog computing in healthcare–a review and discussion. IEEE Access, 2017. 5: p. 9206-9222.
31. Tahir, S., et al., Fog-based healthcare architecture for wearable body area network. Journal of Medical Imaging and Health Informatics, 2017. 7(6): p. 1409-1418.
32. Farahani, B. et al., Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 2018. 78: p. 659-676.
33. Rahmani, A.-M., et al. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In 2015, the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). 2015. IEEE.
34. Stantchev, V., et al., Smart items, fog and cloud computing as enablers of servitization in healthcare. Sensors & Transducers, 2015. 185(2): p. 121.
35. Andriopoulou, F., T. Dagiuklas, and T. Orphanoudakis, Integrating IoT and fog computing for healthcare service delivery, in Components and services for IoT platforms. 2017, Springer. p. 213-232.
36. Datta, S.K., C. Bonnet, and J. Haerri. Fog computing architecture to enable consumer-centric Internet of Things services. In 2015 International Symposium on Consumer Electronics (ISCE). 2015. IEEE.
37. Hou, X., et al., Vehicular fog computing: A viewpoint of vehicles as the infrastructures. IEEE Transactions on Vehicular Technology, 2016. 65(6): p. 3860-3873.
38. Yan, Y. and W. Su. A fog computing solution for advanced metering infrastructure. In 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). 2016. IEEE.
39. Li, J., et al. EHOPES: Data-centered Fog platform for smart living. In 2015 International Telecommunication Networks and Applications Conference (ITNAC). 2015. IEEE.
40. Vilela, P.H., et al., Performance evaluation of a Fog-assisted IoT solution for e-Health applications. Future Generation Computer Systems, 2019. 97: p. 379-386.
41. Aladwani, T., Scheduling IoT Healthcare Tasks in Fog Computing Based on their Importance. Procedia Computer Science, 2019. 163: p. 560-569.
42. Shukla, S., et al. A 3-Tier Architecture for Network Latency Reduction in Healthcare Internet-of-Things Using Fog Computing and Machine Learning. Proceedings of the 2019 8th International Conference on Software and Computer Applications. 2019.
43. Tahir, S., et al., An energy-efficient fog-to-cloud Internet of Medical Things architecture. International Journal of Distributed Sensor Networks, 2019. 15(5): p. 1550147719851977.
44. El Kafhali, S. and K. Salah, Performance modeling and analysis of Internet of Things enabled healthcare monitoring systems. IET Networks, 2019. 8(1): p. 48-58.
45. Badidi, E. and K. Moumane. We are enhancing the processing of healthcare data streams using fog computing at the 2019 IEEE Symposium on Computers and Communications (ISCC). 2019. IEEE.
46. Shrivastava, R. and M. Pandey, Real-time fall detection in fog computing scenario. Cluster Computing, 2020: p. 1-10.
47. Malathi, D., et al., Fog-assisted personalized healthcare-support system for remote patients with diabetes. J Ambient Intell Human Comput. 2019.
48. Tang, B., et al., A hierarchical distributed fog computing architecture for big data analysis in smart cities, in Proceedings of the ASE BigData & SocialInformatics 2015. 2015. p. 1-6.
49. Oueis, J., et al. Small cell clustering for efficient distributed fog computing: A multi-user case. in 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall). 2015. IEEE.
50. Agarwal, S., S. Yadav, and A.K. Yadav, An efficient architecture and algorithm for resource provisioning in fog computing. International Journal of Information Engineering and Electronic Business, 2016. 8(1): p. 48.
51. Gia, T.N., et al. Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction. in 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. 2015.
52. Verma, P. and S.K. Sood, Fog Assisted-IoT Enabled Patient Health Monitoring in Smart Homes. IEEE Internet of Things Journal, 2018. 5(3): p. 1789-1796.
53. Wang, K., et al., Adaptive and Fault-Tolerant Data Processing in Healthcare IoT Based on Fog Computing. IEEE Transactions on Network Science and Engineering, 2020. 7(1): p. 263-273.
54. Jia, X. et al., Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks, 2019. 25(8): p. 4737-4750.
55. Al-Khafajiy, M., et al., Intelligent Control and Security of Fog Resources in Healthcare Systems via a Cognitive Fog Model. ACM Transactions on Internet Technology, 2020.

 doi:10.20944/preprints202405.1056.v1




56. Saha, R. et al., Privacy Ensured ${e}$ -Healthcare for Fog-Enhanced IoT Based Applications. IEEE Access, 2019. 7: p. 44536-44543.
57. Devarajan, M., et al., Fog-assisted personalized healthcare-support system for remote patients with diabetes. Journal of Ambient Intelligence and Humanized Computing, 2019. 10(10): p. 3747-3760.
58. Awaisi, K.S. et al., Leveraging IoT and Fog Computing in Healthcare Systems. IEEE Internet of Things Magazine, 2020. 3(2): p. 52-56.
59. La, Q.D. et al., Enabling fog computing intelligence to reduce energy and latency. Digital Communications and Networks, 2019. 5(1): p. 3-9.
60. Muthanna, A., et al., Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. Journal of Sensor and Actuator Networks, 2019. 8(1): p. 15.
61. Sangpetch, O. and A. Sangpetch. Security context framework for distributed healthcare IoT platform. In International Conference on IoT Technologies for HealthCare. 2016. Springer.
62. Luo, E., et al., PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems. IEEE Communications Magazine, 2018. 56(2): p. 163-168.
63. Al Baqari, M.R., Sdhcare: Secured Distributed Healthcare System. 2020.
64. Tang, W., et al., Secure Data Aggregation of Lightweight E-Healthcare IoT Devices With Fair Incentives. IEEE Internet of Things Journal, 2019. 6(5): p. 8714-8726.
65. Thota, C., et al., Centralized fog computing security platform for IoT and cloud in the healthcare system, in Fog computing: Breakthroughs in research and practice. 2018, IGI Global. p. 365-378.
66. Gill, S.S., et al. Fog-based smart healthcare as a big data and cloud service for heart patients using IoT. in International Conference on Intelligent Data Communication Technologies and Internet of Things. 2018. Springer.
67. Sharma, S.K. and X. Wang, Live Data Analytics With Collaborative Edge and Cloud Processing in Wireless IoT Networks. IEEE Access, 2017. 5: p. 4621-4635.
68. Yang, G., et al., A Centralized Cluster-Based Hierarchical Approach for Green Communication in a Smart Healthcare System. IEEE Access, 2020. 8: p. 101464-101475.
69. Yuan, B., S. Ge, and W. Xing, A Federated Learning Framework for Healthcare IoT devices. arXiv preprint arXiv:2005.05083, 2020.
70. Shukla, S., et al., An analytical model to minimize the latency in healthcare internet-of-things in a fog computing environment. PloS one, 2019. 14(11): p. e0224934.
71. Sharma, S., K. Chen, and A. Sheth, Toward Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems. IEEE Internet Computing, 2018. 22(2): p. 42-51.
72. Kaur, P., R. Kumar, and M. Kumar, A healthcare monitoring system using random forest and internet of things (IoT). Multimedia Tools and Applications, 2019. 78(14): p. 19905-19916.
73. Panda, S. and G. Panda. Intelligent Classification of IoT Traffic in Healthcare Using Machine Learning Techniques. in 2020 6th International Conference on Control, Automation and Robotics (ICCAR). 2020. IEEE.
74. Patan, R., et al., Smart healthcare and quality of service in IoT using grey filter convolutional based cyber-physical system. Sustainable Cities and Society, 2020. 59: p. 102141.
75. Kumar, P.M., et al., Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. Future Generation Computer Systems, 2018. 86: p. 527-534.
76. Subasi, A., et al. IoT-based mobile healthcare system for human activity recognition. in 2018 15th Learning and Technology Conference (L&T). 2018. IEEE.
77. Farahani, B., M. Barzegari, and F.S. Aliee. Towards collaborative machine learning driven healthcare internet of things. In Proceedings of the International Conference on Omni-Layer Intelligent Systems. 2019.
78. Sharma, S., et al., DeTrAs deep learning-based healthcare framework for IoT-based assistance of Alzheimer patients. Neural Computing and Applications, 2020: p. 1-13.