

Review

Not peer-reviewed version

---

# Wireless Communication Protocols for Internet of Medical Things Applications: An Exploration of Practical Use-Case Scenarios

---

[Idris Balarabe Aljyu](#)\*, [Caroline Omonatse Alenoghena](#), [Suleiman Zubair](#), Nathaniel Salawu

Posted Date: 28 October 2025

doi: 10.20944/preprints202510.2120.v1

Keywords: architecture; communication protocol; interoperability; telemedicine



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Review

# Wireless Communication Protocols for Internet of Medical Things Applications: An Exploration of Practical Use-Case Scenarios

Idris Balarabe Aliyu\*, Caroline Omonatse Alenoghena, Suleiman Zubair and Nathaniel Salawu

Department of Telecommunication Engineering, Federal University of Technology, PMB 65, Minna, Niger State, Nigeria

\* Correspondence: aliyuidris.pg2114873@st.futminna.edu.ng

## Abstract

The implementation of the Internet of Medical Things (IoMT) in telemedicine necessitates the deployment of various medical devices, including wearable and implantable sensors, in a network to collect diverse categories of medical data, resulting in the accumulation of large data volumes. The interoperability of these IoMT devices and networks determines to what extent the devices and networks can exchange and interpret medical data. The lack of standardised communication protocols for sharing medical data between individual devices and networks remains a serious challenge that needs to be addressed to unravel the potential of healthcare information sharing using IoMT. This article presents an exploration of practicable IoMT communication protocols to identify possible means of enabling cross-platform interoperability between devices and networks. Taxonomy of IoMT-based telemedicine communication protocols with use-case examples leveraging a large number of existing works of literature, have been examined. The use of open API, gateways and microservices for effective cross-platform medical data sharing is common due to the lack of standard communication protocols. Standardisation of IoMT communication protocols is possible by adopting the most effective open-source communication protocol such as the Message Queuing Telemetry Transport (MQTT) Protocol.

**Keywords:** architecture; communication protocol; interoperability; telemedicine

## 1. Introduction

Internet of Medical Things (IoMT) is an extension of IoT for specific applications in healthcare delivery aimed at creating medical platforms for online medication [1]. IoMT has transformed healthcare delivery services in several dimensions, particularly in the area of remote medication [2]. It is the basis of smart healthcare, also referred to as the Internet of Health Things (IoHT), which consists of a group of medical devices and applications that connect to healthcare networks through the Internet [3,4]

While attempting to come up with standardised communication protocols, LoRaWAN and SIGFOX have been proposed [5]. The LoRaWAN protocol was developed by LoRa for long-range transmission, while the SIGFOX protocol was used for flexible universal networks considering low-powered smart health applications. The need for flexible and cohesive models was also suggested by [5] To enable data integration and communication to attain full interoperability.

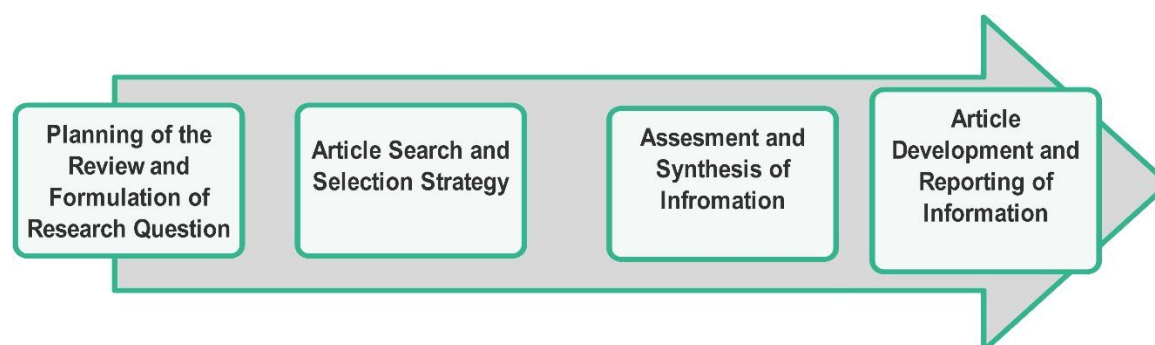
Despite several efforts by researchers to address the peculiar IoMT telemedicine challenges, a standardised communication protocol for the IoMT-based telemedicine network is still lacking. There is a need to assess functional IoMT-based telemedicine communication protocols aimed at finding out the most effective means of sharing medical data across all platforms using a unified communication protocol.

The focus of this survey is to explore available IoMT communication protocols used in Telemedicine designs. Specifically, the study explores the IoMT communication protocols implementation based on layered architectures, protocol standardisation approaches for cross-platform interoperability and open issues regarding implementations. In this context, the contributions to knowledge of this work are highlighted.

- We present a taxonomy of IoMT architectures and communication protocols, indicating practical use-case scenarios of the protocols to enable cross-platform interoperability between devices and networks.
- We provide examples of use-case scenarios of IoMT protocols and architectures that have addressed some standardisation issues for the rapid deployment of IoMT in telemedicine.
- We also provide a list of open research issues limiting the implementation of IoMT-based telemedicine with a specific focus on standardisation of various technologies that do not compromise data integrity, safety and Quality of Service (QoS).

## 2. Research Methodology

The methodology for this survey is shown in Figure 1. The procedure comprises four stages, which involve planning the review and formulation of research questions (RQs), searching for articles, strategy selection, assessment, synthesis and classification of information, and finally, developing the article and writing the report from the information gathered.



**Figure 1.** Research Methodology for the Survey In planning the review for this study, we adopted the approach employed by [6]. This involves formulating research questions (RQs) and searching for relevant articles and a selection strategy. Several considerations were taken into account from relevant literature, for instance, research issues in the IoMT, with particular preference to communication protocol deployments, were examined. Several research challenges of practical use cases examined include medical data transmission [7], Security and privacy [8,9], power consumption [10], QoS [11], data accuracy [12] and interoperability [9,13–16]. Based on these considerations from the literature, the research questions listed below were formulated for this review.

**RQ1:** What are the most practical communication protocols for the transmission of medical data in an IoMT-based telemedicine framework?

**RQ2:** What are the challenges of communication protocols that impact the full implementation of IoMT in modern healthcare delivery?

**RQ3:** What are the possible solutions to varying protocol applications that could aid the rapid deployment of IoMT-based telemedicine?

## 3. Survey of Related Studies

This section reviews related articles that focused on the architectures, protocols, implementations and open issues with particular concern on practical IoMT in telemedicine. Major areas examined and the aspects not given adequate attention are identified and elaborated. Particular

emphasis is given to IoMT communication protocols in telemedicine from the relevant literature. To broadly categorise the use-case scenarios in literature, four key areas were given more attention, namely: IoMT standardisation, communication protocols, architectures and implementation challenges as shown in Figure 2.

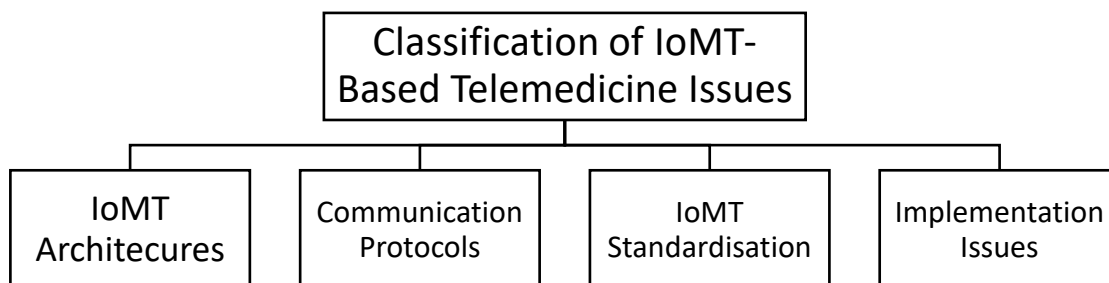


Figure 2. Focuses of IoMT-based Telemedicine.

### 3.1. IoMT Architectures

Several IoMT architectures adopted for telemedicine have been explored in the literature using different approaches and focuses. In [17], the Health Level Seven (HL7) architectures and the different layered architectures employed in the IoMT designs are presented in Figure 3. These layers consist of the following list.

- Three-layer architecture
- Four layers or Service-oriented Architecture (SoA-based architecture)
- Five layers or the Middleware-based architecture
- Seven layers (HL7) architecture

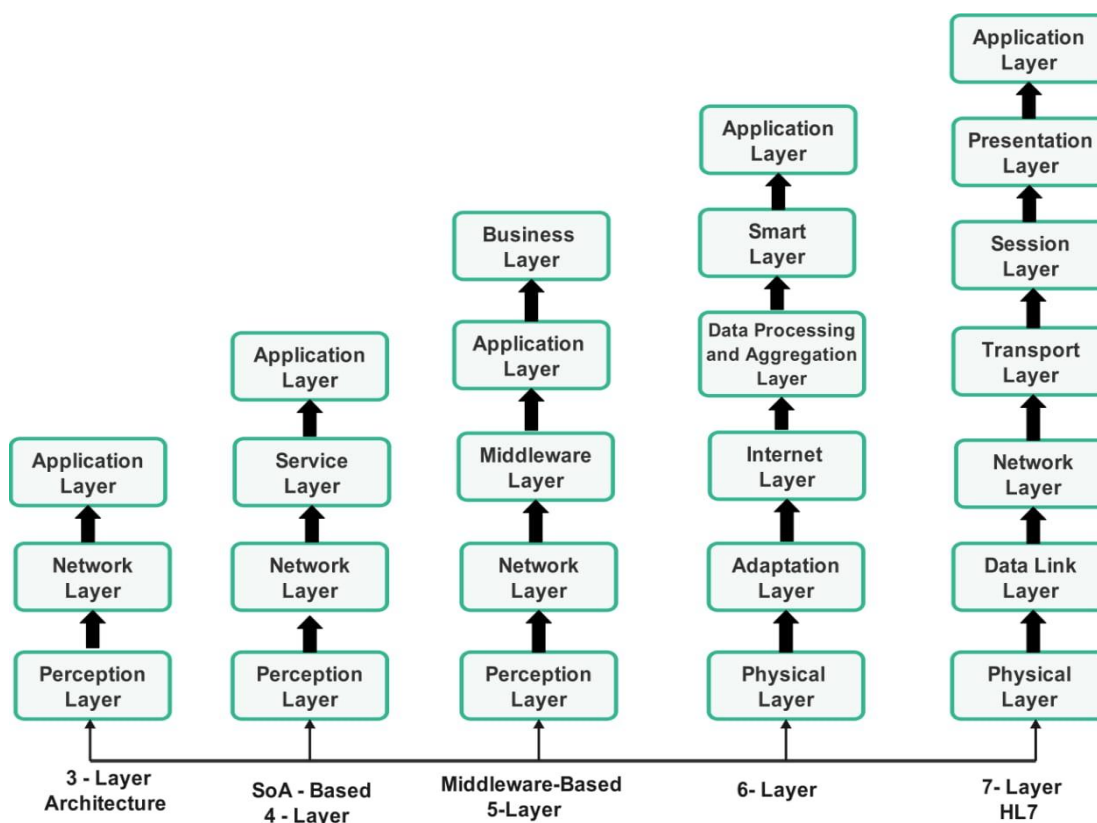


Figure 3. IoMT Layered Architectures.

### 3.1.1. Three-layer architecture

The three-layer architecture specifically for IoMT is made up of three sub-sections containing different communication stages between the devices, networks and users as shown in Figure 5. These sub-sections are:

- a. Perception layer
- b. Network layer
- c. Application layer

#### a. *IoMT Perception layer*

The perception layer is also called the device layer in the conventional IoT layers, responsible for the identification and collection of data through sensing devices [18]. It is the most important and difficult layer, comprising two sub-layers for data acquisition and access. In this layer, various medical perception tools are employed for gathering signals through General Packet Radio Service (GPRS), Radio frequency identification (RFID), graphic code, image recognition and different sensor nodes. In the data access sub-layer, short-range communications like Bluetooth and Bluetooth low energy (BT/BLE), ZigBee and WiFi are used to connect the acquired data to the network layer using a gateway [19].

#### b. *Network layer*

The IoMT network layer is made up of the internet, wireless communication and other private networks for IoMT medical data transmission for further processing. Depending on the network requirements, the data could be transmitted using wired or wireless communication in this layer [18]. This layer mainly takes care of communication, networking and transmission of medical data between devices within the IoMT framework [20].

#### c. *Application Layer*

In the OSI (open systems interconnection) layers architecture, the application layer matches the session and the application layers responsible for data control and applications [20]. IoMT implementations take place at this layer as an example application of smart health [18].

### 3.1.2. SoA-Based Architecture (Four-Layer)

This four-layer IoMT architecture has a service layer between the network and application layers. It is component-model based, designed to connect various functional elements of the applications through interfaces and communication protocols [17]. It manages services and allows the reuse of software and hardware components. It is also responsible for service management connected to the database for data processing or data storage.

### 3.1.3. Middleware-based Architecture (Five Layers)

In an attempt to address several issues such as interoperability, scalability, reliability and QoS by researchers in the IoT, the five-layer architecture with the addition of the business layer was introduced to contribute to building more efficient applications [20]. This middleware-based architecture serves as a connection between the data, applications and operators. The business layer serves as an additional top layer that manages the entire system as well as the applications and services by constructing business models, charts, flow diagrams, etc. It is a very significant layer in the prospects of the entire technology regarding future implementations [18].

### 3.1.4. HL7 Architecture (Seven Layers)

Health Level Seven or HL7 is a set of international standards for medical and organisational data exchange. It is a seven-layer architecture which consists of an application protocol for Electronic Medical Record (EMR) exchange in the healthcare domain. It is an ANSI-accredited, non-profit organisation established in 1987 by the HL7 international [21]. A summary of significant features of the layered IoMT architectures, indicating their merits and drawbacks, is shown in Table 1.

**Table 1.** Comparison of IoMT Layered Architectures.

Architecture	Unique features	Advantages	Disadvantages
<b>3-Layer</b>	It is Conventional and widely utilised	Serves as the basis for all the layered architectures	Interoperability and scalability are not addressed
<b>SoA-based (4-Layer)</b>	It consists of an additional service layer	Allows the reuse of software and hardware components and service management through the database	Operation is dependent on the database.
<b>Middleware-based (5-Layer)</b>	Introduction of the business layer for building more efficient applications	Addresses interoperability by providing a connection between data, applications and operators	The addition of more layers requires hardware modifications.
<b>6-Layer</b>	Data processing and aggregation layer	Enables data processing between the physical layer and the application layer	Data processing and aggregation take time.
<b>7-Layer (HL7)</b>	It is an International standard for medical and organisational data exchange.	It is the only accredited architecture that contains an application protocol for electronic medical record exchange in the IoMT context.	It requires data formatting to operate efficiently.

### 3.2. IoMT Communication Protocols

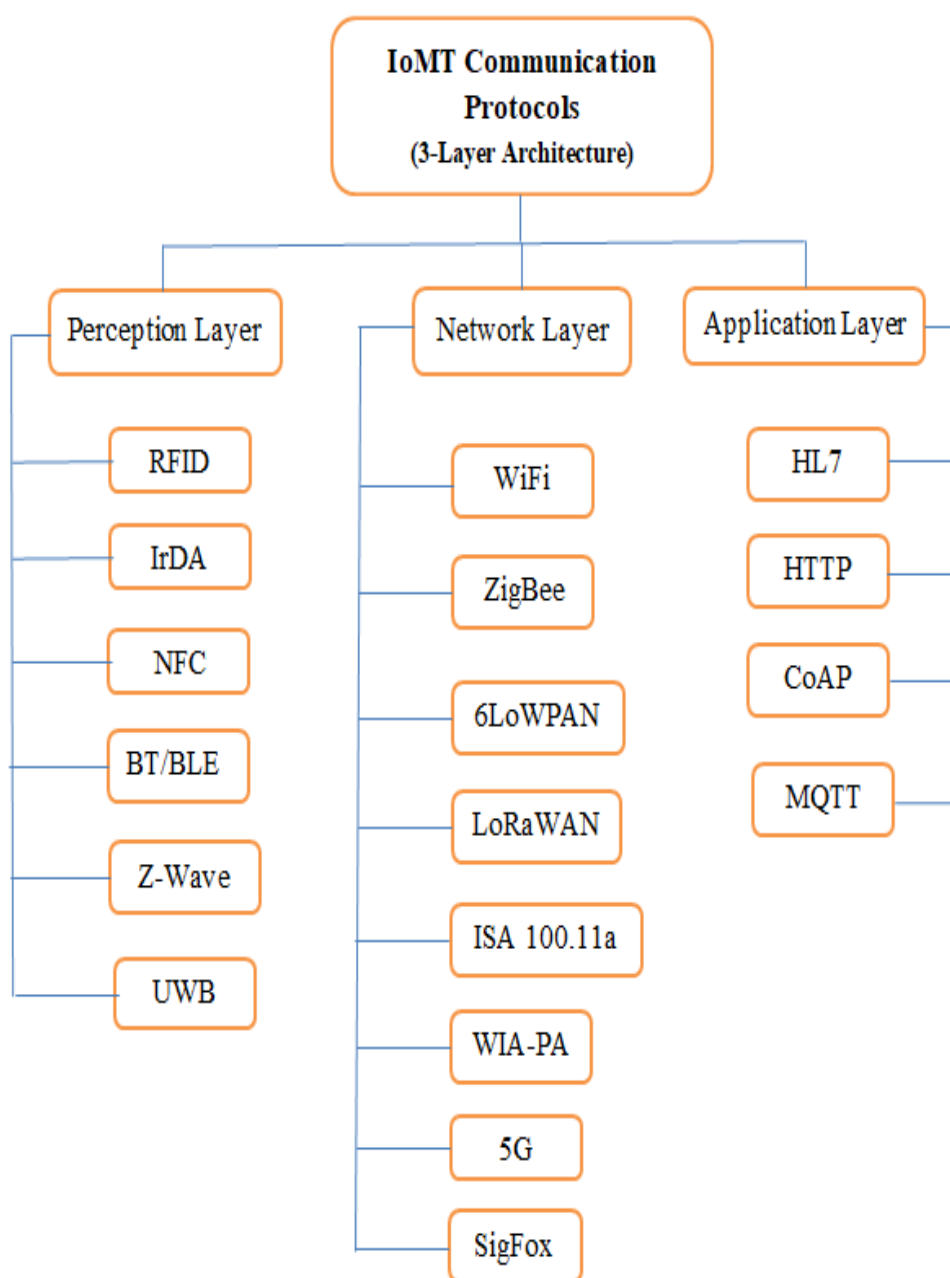
IoMT used for remote patient monitoring by healthcare providers contributes largely to telemedicine. Data generated from IoMT devices is multi-dimensional due to heterogeneous devices in the network [22]. Interoperability is significant for the exchange of medical data between the nodes and the back-end servers [23]. Efficient sharing of medical data, which could be achieved through interoperability, reduces errors and mortality in emergency cases [24].

Since IoMT networks are complex and diverse, a single communication protocol cannot be adopted as a perfect standard for all possible applications [25]. Data analysis, transmission and connectivity of device requirements vary for different medical situations [20]. For wearable sensors on ad-hoc networks, improved nodes, flexible operation, and optimised power consumption are some of the major requirements. Whereas, improved total security and collective data outlines are the common requirements for network technologies in large infrastructures like hospitals. In an attempt to address interoperability, for example, the IoMT architecture in [19] combined IoMT Communication protocol, machine learning (ML), mobile edge computing (MEC), fog computing and blockchain technology in a single design. This combination of technologies was conceived largely due to a lack of standard protocol as a result of the complex and diverse nature of medical data, as stated above.

Another instance in addressing the lack of interoperability in communicating medical data from wearable devices to back-end servers was the work of [16,26]. The study attempted to develop a standard protocol that addresses IoT interoperability challenges in wearable health devices for accurate remote health monitoring. Despite the success recorded in using a single protocol, no sufficient work was done to check the security for authentication and authorisation of access for the

architecture. Implementation of non-standardised devices and network interfaces that are heterogeneous makes interoperability difficult in most cloud-based IoT healthcare services [15,27].

IoMT wireless communication protocols are a set of rules for exchanging medical data between devices and networks [13]. These technologies support the interface of D2D communication for the patient with other medical devices on the network [20]. IoMT gadgets use sensing devices and actuators for wireless monitoring, diagnosis and patient treatment in real-time. These devices form part of the IoMT network, and their communication depends on the specific IoT protocols. Secure connection for IoMT devices across all the layers is highly important because any alteration, leak or inaccessibility of important information threatens the user's life. To adequately characterise these IoMT communication protocols as conceived in [20]. The three-layer architecture previously discussed is used as shown in Figure 4.



**Figure 4.** Taxonomy of Communication Protocols for Three-layer IoMT.

### 3.2.1. Protocols for Perception Layer

Communication protocols used in this layer are short-range, ultra-low energy, complexity and cost. Devices on this layer operate on the IEEE 802.15.4 protocol. Compatible IoMT protocols in this layer include UWB (Ultra-Wide Band), RFID, infrared (IrDA), NFC (Near Field Communication), Bluetooth and Bluetooth low energy (BT/BLE) and Z-wave. These protocols offer low power consumption and high security using the Advanced Encryption Standard (AES), but they have a low data rate [25].

### 3.2.2. Protocols for Network Layer

The layer consists of open-source IoT network protocols that correspond to the MAC layer in the OSI. Some of the communication technologies in this layer are non-standard proprietary protocols. These protocols include Wireless Fidelity (WiFi), ZigBee, 6LoWPAN (IPv6 over Low Power Wireless Personal Area Network), LoRaWAN (long-range wireless area network), ISA 100.11 and WIA-PA, which have been used for implementing IoMT-based telemedicine.

### 3.2.3. Protocols for Application Layer

Message Queue Telemetry Transport (MQTT), Firebase Cloud Messaging (FCM), CoAP, HTTP (Hypertext Transfer Protocol), HL7 (Health Level Seven) and XML (extensible markup language) are the common protocols used in the application layer in the 3-layered IoMT architecture. A typical example of XML is the XMPP (Extensible Messaging and Presence Protocol), which is scalable and secured with addressing capabilities employed for shared conversation, audio and video streaming, and remote presence [28]. Table 1 shows the application scenarios of IoMT communication protocols for telemedicine implementations.

### 3.3. Communication Protocols Standardisation

In an attempt to come up with a standardised communication protocol, LoRaWAN and SIGFOX were proposed in [5]. The LoRaWAN protocol was developed by LoRa for long-range transmission, while the SIGFOX provides a flexible universal network taking into account low-powered smart health implementation. The author also suggested the need for flexible and cohesive models for integration and transmission, such as the IP and CoAP (Constrained Application Protocol), as a means to attaining interoperability. To standardise the communication protocols across the IoMT devices and networks for easy interoperability, there is a need to focus on relevant literature that has dwelt on several architectures and protocols to figure out the most suitable designs for use-case scenarios towards achieving a standardised protocol.

## 4. Summary of IoMT Communication Protocols Use-Case Scenarios

To identify the best approach for implementing IoMT architectures using standardised communication protocols across devices and networks for easy interoperability, the study focused on relevant literature that has worked on the available communication protocols to determine the most suitable designs for use-case scenarios. These protocols are highlighted in Table 2

**Table 2.** Application Scenarios of IoMT Communication Protocols.

Layer	Protocol	Features	Use-case scenario	Barriers to Adoption	Reference
Perception layer	UWB	<ul style="list-style-type: none"> <li>Based on the IEEE 802.15.3</li> </ul>	<ul style="list-style-type: none"> <li>For data transmission between the sensor and the</li> </ul>	<ul style="list-style-type: none"> <li>Suitable for indoor use only</li> </ul>	[20,29]
		<ul style="list-style-type: none"> <li>High data rate</li> </ul>	<ul style="list-style-type: none"> <li>the sensor and the</li> </ul>	<ul style="list-style-type: none"> <li>Requires an external</li> </ul>	
		<ul style="list-style-type: none"> <li>Short-ranged</li> </ul>			

---

	<ul style="list-style-type: none"> <li>Wireless communication for indoor use</li> </ul>	<ul style="list-style-type: none"> <li>Microcontroller</li> <li>Short-distance communication of medical data</li> <li>Wearable antenna with a safe Specific Absorption Rate (SAR)</li> </ul>	<ul style="list-style-type: none"> <li>gateway to connect to the internet</li> </ul>	
RFID	<ul style="list-style-type: none"> <li>Protocol for devices without a battery</li> </ul>	<ul style="list-style-type: none"> <li>For patient identification, tracking, monitoring and medication compliance</li> </ul>	<ul style="list-style-type: none"> <li>High cost of implementation</li> <li>Patient safety issues</li> <li>Security and privacy</li> <li>Data management</li> </ul>	[30–32]
IrDA	<ul style="list-style-type: none"> <li>High-level data link control (HDLC) standard</li> <li>uses infrared light</li> <li>Short-range transmission</li> </ul>	<ul style="list-style-type: none"> <li>For wearable blood glucose monitoring</li> <li>For wearable patient monitoring and position tracking</li> </ul>	<ul style="list-style-type: none"> <li>Requires line-of-sight (LOS)</li> </ul>	[2,33]
Li-Fi	<ul style="list-style-type: none"> <li>Based on light</li> </ul>	<ul style="list-style-type: none"> <li>Uses Light Fidelity (Li-Fi) for vital sign monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Short-range design for indoor applications</li> </ul>	[33]
NFC	<ul style="list-style-type: none"> <li>A subset of RFIDs</li> <li>Uses IoT network protocols</li> </ul>	<ul style="list-style-type: none"> <li>Used to manage and transmit medical data instead</li> </ul>	<ul style="list-style-type: none"> <li>Uses Wireless Access Point (WAP) to</li> </ul>	[34,35]

---

---

	<ul style="list-style-type: none"> <li>• Very close communication</li> <li>• 0-10cm distance at Range 13.56 MHz</li> <li>• Compatible with BT and WiFi</li> <li>• Fast setup time over BT</li> <li>• 2-way communication compared to RFID</li> <li>• Consists of a Secured element</li> <li>• Do not require a battery</li> </ul>	<ul style="list-style-type: none"> <li>• of using paper documentation by employing a smartphone with NFC</li> <li>• NFC technology can be applied to existing frameworks for network integration in existing electronic health records (EMR)</li> <li>• Used in indigestible or implantable devices</li> <li>• Utilised for point-of-care (POC) H-IoT security</li> </ul>	<ul style="list-style-type: none"> <li>• connect to the internet</li> <li>• Relies on a smartphone as a gateway</li> <li>• Biocompatibility issues</li> </ul>
BT/BLE	<ul style="list-style-type: none"> <li>• 2.4 GHz PAN</li> <li>• Short-range</li> <li>• D2D file transfers</li> <li>• Lower-powered</li> <li>• Uses less data</li> </ul>	<ul style="list-style-type: none"> <li>• Ideal for wearable devices</li> <li>• Smart wearable HBR connected to a smartphone using a BR-LE 4.0-S3A module with a BLE chipset</li> </ul>	<ul style="list-style-type: none"> <li>• The accuracy depends on the sensors [36–38]</li> <li>• Short-ranged</li> </ul>

---

---

Z-Wave	<ul style="list-style-type: none"> <li>• 2-way MAC communication protocol</li> <li>• It can accommodate a large number of devices (232 physical devices)</li> <li>• High degree of interoperability</li> <li>• Mesh networking</li> <li>• High Security</li> </ul>	<ul style="list-style-type: none"> <li>• Used for smart wearable devices</li> <li>• It could also be used in the network layer</li> </ul>	<ul style="list-style-type: none"> <li>• Open source implementation relies on reverse-engineered Z-Wave protocol</li> <li>• Not suitable for data streaming</li> </ul>	[20,39]
NB-IoT	<ul style="list-style-type: none"> <li>• Narrowband IoT</li> <li>• Longer than BLE and WiFi</li> <li>• For M2M communication</li> </ul>	<ul style="list-style-type: none"> <li>• For wearable data transmission</li> <li>• Highly universal</li> <li>• Used for LwM2M data transmission</li> </ul>	<ul style="list-style-type: none"> <li>• Requires an application programming interface (API) to connect to the cloud</li> </ul>	[40]
AKA	<ul style="list-style-type: none"> <li>• New protocol based on ECC (cryptography)</li> </ul>	<ul style="list-style-type: none"> <li>• Implemented in the device layer between the sensing node and the base transceiver station (BTS)</li> </ul>	<ul style="list-style-type: none"> <li>• Not suitable for interoperability</li> </ul>	[41]
THREAD	<ul style="list-style-type: none"> <li>• Open protocol based on 802.15.4</li> </ul>	<ul style="list-style-type: none"> <li>• Applied in UAVs to improve interoperability in</li> </ul>	<ul style="list-style-type: none"> <li>• Connects to the internet through the user datagram</li> </ul>	[42]

---

		<ul style="list-style-type: none"> <li>Built on IPv6 and 6LoWPAN</li> <li>Flexible and seamless integration with large networks</li> <li>Unique interoperability</li> <li>804.15.4 MAC and PHY layer</li> <li>250kbps at 2.4GHz</li> <li>250 nodes with High-level encryption</li> </ul>	<ul style="list-style-type: none"> <li>remote locations for patient monitoring</li> <li>Used as an IP-based network for the addition of more layers</li> </ul>	<ul style="list-style-type: none"> <li>protocol (UDP) and CoAP</li> <li>Implementation is complex</li> </ul>	
<b>Network Layer</b>	WiFi/WLAN	<ul style="list-style-type: none"> <li>IEEE 802.11 standard</li> </ul>	<ul style="list-style-type: none"> <li>Used for Secure transmission of physiological data in an Ethereum blockchain</li> <li>Used for creating an access point through a WLAN in the perception layer for sensor nodes in remote health monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Prone to attacks</li> <li>Highly Vulnerable</li> </ul>	[43,44]
	ZigBee	<ul style="list-style-type: none"> <li>2.4 GHz mesh LAN protocol</li> </ul>	<ul style="list-style-type: none"> <li>For vital sign data collection</li> </ul>	<ul style="list-style-type: none"> <li>Short-ranged</li> </ul>	[45]

6LoWPAN	<ul style="list-style-type: none"> <li>• Open IoT network protocol</li> <li>• Lightweight IP-based communication</li> <li>• Open IoT network protocol</li> </ul>	<ul style="list-style-type: none"> <li>• Used by devices to join IP networks</li> </ul>	<ul style="list-style-type: none"> <li>• Affected by environmental factors</li> <li>• Routing protocols are not defined</li> <li>• Limited packet size</li> </ul>	[20,42]
LoRa	<ul style="list-style-type: none"> <li>• PHY layer protocol</li> <li>• Bidirectional communication</li> <li>• Non-standard proprietary protocol</li> </ul>	<ul style="list-style-type: none"> <li>• Used for communication between smart devices</li> </ul>	<ul style="list-style-type: none"> <li>• Routing protocols not defined</li> <li>• Low data rate compared to similar protocols in the layer</li> <li>• Battery operated</li> </ul>	[46,47]
LoRaWAN	<ul style="list-style-type: none"> <li>• MAC layer protocol</li> <li>• Cloud-based</li> <li>• Large-scale public protocol</li> <li>• Based on the ISM band</li> </ul>	<ul style="list-style-type: none"> <li>• Used for critical health data transmission in a disaster situation</li> </ul>	<ul style="list-style-type: none"> <li>• Uses a single operator</li> </ul>	[47,48]
SIGFOX	<ul style="list-style-type: none"> <li>• Non-standard proprietary protocol</li> <li>• Like a cell tower company</li> <li>• Uses DBPSK and GFSK</li> </ul>	<ul style="list-style-type: none"> <li>• Used as a base station for transmitting medical data</li> </ul>	<ul style="list-style-type: none"> <li>• Operates as a private network provider</li> </ul>	[46,48]
LTE-M	<ul style="list-style-type: none"> <li>• Broadband wireless access (BWA) 802.16</li> <li>• Robust infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>• For transmitting clinical data through portable devices</li> </ul>	<ul style="list-style-type: none"> <li>• Application depends on commercial network providers</li> </ul>	[49–51]

---

	5G	<ul style="list-style-type: none"> <li>Built-in security</li> <li>Very fast transmission rate</li> <li>Simple integration with other protocols using smart devices</li> <li>High data transmission capabilities</li> </ul>	<ul style="list-style-type: none"> <li>Used for disease observation and prediction</li> </ul>	<ul style="list-style-type: none"> <li>Roll-out is slow in some locations</li> </ul>	[48,52,53]
	ISA 100.11	<ul style="list-style-type: none"> <li>Compatible with IEEE 802.15.4 Standard</li> <li>Utilises TDMA protocols</li> </ul>	<ul style="list-style-type: none"> <li>Used for patient tracking</li> </ul>	<ul style="list-style-type: none"> <li>Not compatible with similar protocols</li> <li>Implementation is complex</li> <li>Lacks energy efficiency</li> </ul>	[50,54]
	WIA-PA	<ul style="list-style-type: none"> <li>Industrial standard for the MAC and PHY layer</li> <li>Based on 802.15.4</li> </ul>	<ul style="list-style-type: none"> <li>Used for remote health monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Not compatible with similar protocols</li> <li>Lacks energy efficiency</li> </ul>	[20,54,55]
<b>Applicati on layer</b>	MQTT	<ul style="list-style-type: none"> <li>It works on the principle of the publish/subscribe paradigm</li> </ul>	<ul style="list-style-type: none"> <li>Used to send data from devices (user) to the server (cloud) via a 3G/4G/5G smartphone</li> </ul>	<ul style="list-style-type: none"> <li>High data transmission time</li> <li>Bandwidth and range limitations</li> </ul>	[37,48,52,53,56]
	FCM	<ul style="list-style-type: none"> <li>Works as a transceiver</li> </ul>	<ul style="list-style-type: none"> <li>Notification from the server (cloud) to</li> </ul>	<ul style="list-style-type: none"> <li>High data transmission time</li> </ul>	[37]

---

---

			the user (device)	
CoAP	<ul style="list-style-type: none"> <li>• It uses Representational State Transfer (REST)</li> <li>• Network-oriented protocol</li> </ul>	<ul style="list-style-type: none"> <li>• It is used as a web transfer protocol</li> <li>• Used for transmitting data to the cloud</li> </ul>	<ul style="list-style-type: none"> <li>• It follows the UDP protocol format</li> </ul>	[42]
HTTP	<ul style="list-style-type: none"> <li>• Lightweight and versatile</li> <li>• Interoperable across other platforms</li> </ul>	<ul style="list-style-type: none"> <li>• Used in conjunction with microservices architecture in the network layer</li> </ul>	<ul style="list-style-type: none"> <li>• Used for implementing FHIR-based microservices in a layered architecture for scalability</li> </ul>	[57]
HL7	<ul style="list-style-type: none"> <li>• Interoperable protocol, which resulted in the Continuity of Care Document (CCD) standard through XML Format in EHR</li> <li>• It is in alignment with other standardisation bodies</li> <li>• ANSI standard for clinical interoperability</li> <li>• HL7 Architecture</li> </ul>	<ul style="list-style-type: none"> <li>• Used to develop a standardised data-sharing model for Fast Health Interoperability Resources (FHIR)</li> <li>• Used for sharing, exchange and retrieval of data</li> <li>• Versatile application in healthcare services</li> </ul>	<ul style="list-style-type: none"> <li>• Requires data formatting using other standards</li> </ul>	[20,58,59]

---

LwM2M	<ul style="list-style-type: none"> <li>Defines logical operation, e.g. Write, Execute, Subscribe</li> </ul>	<ul style="list-style-type: none"> <li>Used in conjunction with BLE in an attempt to develop a standard protocol for interoperability</li> </ul>	<ul style="list-style-type: none"> <li>The protocol is not secure</li> </ul>	[40,60]
-------	---	--	--	---------

#### 4.1. Challenges of IoMT Telemedicine Deployment

IoMT is used to provide a medical platform database for government and healthcare service providers for effective disease management. [1]. As a network that consists of medical professionals, facilities, devices, software applications and services, IoMT is faced with security vulnerabilities due to a lack of standard regulations [50]. Also, IoMT networks and products are vulnerable to attacks due to a lack of standards, thus limiting their universal implementation [59]. Several attempts have been made by researchers to address standardisation and interoperability issues. However, due to the heterogeneity of IoMT devices, the medical data generated are usually multidimensional (extremely heterogeneous) because of variations in architectures, which do not follow a standard format [22]. Most researchers tend to adopt web-based interfaces, such as the API for cloud connection in the IoMT architectures [61].

The lack of a standard communication protocol for cross-platform interoperability is yet to be fully addressed in several research works and has seriously affected the implementation of telemedicine services, thereby limiting the deployment of telemedicine technology to remote areas [7]. The use of open API, gateways and microservices for effective cross-platform medical data sharing is common due to the non-existence of a standard communication protocol. This study, therefore, has highlighted all the major IoMT communication protocols with a specific focus on their applicability in real-world implementations, which, to the best of our knowledge, has not been considered in similar research articles examined. The comparison showing major highlights of this work with similar studies is shown in Table 3.

**Table 3.** Comparison of Related Studies on IoMT Communication Protocols and Devices.

Ref	Main Focus	Specific Focus	Open Identified	Issues	Approach	Communication Protocols Description	Practical Use-case Analysis
[62]	Performance Evaluation of CoAP and MQTT	Analysis of the most popular application layer protocols based on bandwidth and CPU	<ul style="list-style-type: none"> <li>Not specified</li> </ul>		Experimental	Yes	No

		utilisation in a realistic network condition				
[13]	Applications and Open Issues of Emerging IoMT Technologies	Analysis of IoMT protocols based on the three-layer architecture	<ul style="list-style-type: none"> <li>• Power consumption</li> <li>• Privacy and Security</li> <li>• Resource management</li> </ul>	Survey	Yes	No
[63]	Analysis of lightweight communication protocols in the application layer	Experimental Comparison of various IoT communication protocols, including the CoAP, MQTT & WebSocket protocols	<ul style="list-style-type: none"> <li>• Real-time analysis of IoT applications using case studies</li> </ul>	Survey	Yes	Yes
[64]	Taxonomies, Classification & Challenges of IoMT specific areas	Devices and sensor classification in the IoMT context	<ul style="list-style-type: none"> <li>• Security and Safety</li> <li>• Device flexibility</li> </ul>	Survey	No	No
[65]	Implementation of IoMT Healthcare using WSNs	Application of genetic algorithm on medical data collected from nano sensors in real time	<ul style="list-style-type: none"> <li>• Standardisation of communication protocols</li> <li>• Scalability</li> <li>• Energy efficiency</li> </ul>	Experimental	No	No
[8]	Security Techniques of IoMT Data	Modern techniques of securing IoMT	<ul style="list-style-type: none"> <li>• Lack of standard architecture, software</li> </ul>	Survey	Yes	No

	Transmission Designs	systems based on data transmission, collection, and storage		and protocols			
[9]	Security and Interoperability of IoMT using AI with emphasis on patient privacy	Optimisation of IoMT network performance, based on the throughput, power consumption, latency, packet drop rate, and network durability	<ul style="list-style-type: none"> <li>• Data immutability &amp; privacy</li> </ul>	Experimental	Yes	No	
[66]	IoMT Communication Protocols and Security	Devices Classification and associated communication protocols for medical data sensing devices	<ul style="list-style-type: none"> <li>• Data integration</li> <li>• Data preservation</li> </ul>	Survey	Yes	No	
[67]	Development of a Dataset for Multiprotocol Security Assessment in IoMT	Classification of cyber-attacks in IoMT devices and networks using the MQTT protocol	<ul style="list-style-type: none"> <li>• Real-world deployment</li> </ul>	Simulations	Yes	No	
[68]	AI-based Security protocols in IoMT, including MQTT	Security architecture of Wearable & implantable devices for	<ul style="list-style-type: none"> <li>• Data leakage</li> <li>• Cyber risk</li> </ul>	Survey	Yes	No	

		IoMT applications				
[69]	IoMT Technologies, Architectures and Challenges	Core technologies such as cloud computing, big data & AI for IoMT implementations	<ul style="list-style-type: none"> <li>• Cost-effectiveness</li> <li>• Security</li> <li>• Privacy</li> <li>• Accuracy</li> <li>• Power consumption</li> </ul>	Survey	Yes	No
[70]	Implementation of Benchmark Dataset for the Security of IoMT Devices	Use of representative IoMT scenarios to generate attacks and collect data for ML analysis	<ul style="list-style-type: none"> <li>• Data integrity</li> <li>• Data confidentiality</li> </ul>	Experimental	Yes	No
[71]	IoMT Security and Privacy Preventing malicious gateway attacks on the IoMT environment	Authentication protocol using the Elliptic curve cryptography (ECC) based on blind signature for data privacy	<ul style="list-style-type: none"> <li>• No further work suggested</li> </ul>	Experimental	Yes	No
<b>This Study</b>	IoMT communication protocols	Practical use-case description of twenty-five IoMT Communication protocols for a three-layer architecture	<ul style="list-style-type: none"> <li>• Vulnerability to attacks</li> <li>• Interoperability</li> <li>• Lack of standard communication protocol</li> </ul>	Overview of simulation, reported experiments and similar surveys	Yes	Yes

#### 4.2. Proposed Solutions for IoMT Protocols implementations and Standardisation

##### a. Real-Time Implementation of IoMT Protocols

Since IoMT applications send messages to multiple users simultaneously with high security requirements, the MQTT protocol is proven to outperform the others for reasons highlighted as follows. MQTT offers a reliable, bi-directional communication, ordered and lossless [62]. It employs the TCP communication protocol based on Client/Broker/ architecture and Publisher/Subscriber transmission model. It consists of a 2-byte minimum head size with three levels of QoS (QoS0, QoS1 and QoS2), with message size up to 256MB and TLS/SSL security. [63].

Also, the work of [72] proposed the use of intelligent reflective surfaces known as intelligent walls (IW) to employ Electromagnetic (EM) waves to act as gateways in heterogeneous network environments like the B5G. These IWs are planar and active surfaces equipped with machine learning (ML) algorithms and computation power to be utilised as key elements in the Beyond Fifth Generation (B5G) and Sixth Generation (6G) communication for IoMT healthcare applications. IW has also been employed for high data rate transmission and charging in IoMT applications to solve the problem of low data rate and power constraints of wearable sensing devices. Combination of the CoAP or MQTT protocols and intelligent walls (IW) in IoMT designs could be utilised to address chronic disease management focused on [73]emergency and daily healthcare management in hazardous area in [74] and for remote assisted living for the elderly [57].

##### b. Standardisation of Communication Protocols

A standardised communication protocol for IoMT-based telemedicine is still lacking. Presently, there is no best protocol for all scenarios. Applications of the protocols are based on best use-case scenarios, depending on the deployment requirement. This has affected full deployment due to the use of unregulated applications that have not been certified by any recognised medical and regulatory agencies [75]. There is a need to standardise communication protocols to optimally control the existing technologies, guaranteeing stability to emerging technologies for delivering effective healthcare solutions at reduced costs. Standardisation could lead to the provision of a universally accepted platform that is feasible and sustainable in the healthcare domain.

One of the solutions to standardisation issues is to adopt an open standard providing a framework specifying approved protocols that will be universally applied in the IoT-based healthcare industry [76]. Organisations such as the FDA (Food and Drug Administration) and the EU are currently working to regulate and amend IoMT protocols/standards to eliminate ambiguities in the IoMT ecosystem [59]. Standardisation requires more attention in the practical IoMT projects due to its benefits by means of improving and enabling the items highlighted in Figure 5. Achieving global standardisation of IoMT communication protocols could address most of the open issues identified in the studies examined by this work. This could enable cross-platform interoperability, easy access, seamless connectivity, highly secured privacy-preserved data and feasibility of IoMT designs.

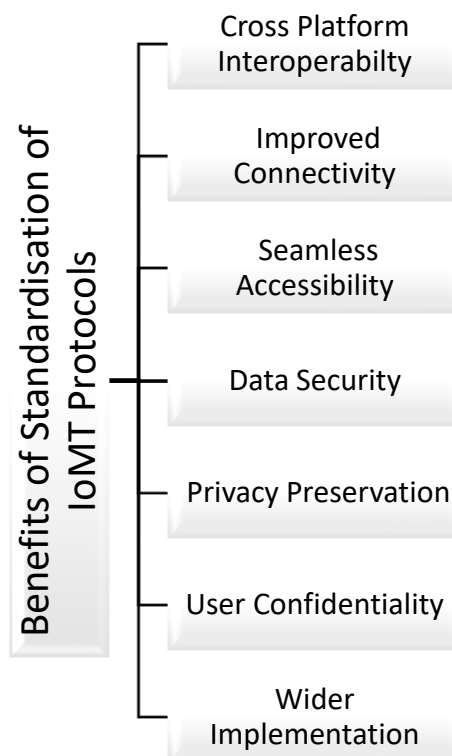


Figure 5. Benefits of IoMT Communication Protocols Standardisation.

## 5. Conclusions

This survey has provided an overview of various communication protocols suitable for IoMT in the telemedicine context based on practical applications. In the three-layered architecture, in particular, the NFC offers more flexible applications in the perception layer due to its various use-case scenarios reported in the literature. It could be used for an existing platform for network integration, ideal for wearable and ingestible devices and POC H-IoT. Similarly, the network layer could adopt 5G communication due to its high data transmission capabilities and simple integration with other protocols using smart devices. In the application layer, HL7 has been used to develop a standardised data-sharing model for Fast Health Interoperability Resources (FHIR) due to its versatile application. This makes it simple to share, exchange and retrieve medical data across different platforms operating on diverse communication protocols.

Some of the steps adopted towards the standardisation of protocols in the literature include the use of gateways, virtual networks, open APIs and open standards. Despite these tremendous efforts documented in the literature, a standardised communication protocol for IoMT-based telemedicine is still lacking. Presently, there is no best protocol for all scenarios. Applications of the protocols are based on best use-case scenarios, depending on the deployment requirement.

To aid the rapid practical deployment of IoMT for efficient healthcare delivery, there is a need to develop a standardised protocol for IoMT-based telemedicine. Collaboration between organisations such as the FDA, EU, OIC, AllSeen Alliance, oneM2M, OMA LWM2M, ETSI M2M, IPSO and other research industries is necessary to address the lack of standard protocol in IoMT for effective healthcare delivery.

## 6. Future Work and Recommendations

Considering the global economic prospects of IoMT in modern healthcare services, several telemedicine devices and network technologies are envisioned to emerge. Further research could look at the implementation of the e-regulation layer in the layered architecture paradigm to enforce the adoption of standards at the design stage. It will also be of great advantage to study the use of hybrid

technologies such as the combination of medical sensors, 5G cellular gateways and tracking systems in modular designs of IoMT-based telemedicine devices and networks. Presently, the proliferation of non-standardised IoMT communication technologies and gadgets is inevitable due to the market projection and rising demand for wireless healthcare services. Future studies could look at a universal means of checking the use of substandard and unapproved devices that may not meet basic technological and safety standards. Global standardisation of IoMT technologies utilised for telemedicine systems is highly recommended to guarantee universal cross-platform interoperability and, above all, continued human safety.

## References

1. T. Yang, M. Gentile, C. F. Shen, and C. M. Cheng, "Combining point-of-care diagnostics and internet of medical things (IOMT) to combat the Covid-19 pandemic," *Diagnostics*, vol. 10, no. 4, pp. 4–6, 2020, doi: 10.3390/diagnostics10040224.
2. A. M. Joshi, P. Jain, S. P. Mohanty, and N. Agrawal, "IGLU 2.0: A New Wearable for Accurate Non-Invasive Continuous Serum Glucose Measurement in IoMT Framework," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 4, pp. 327–335, 2020, doi: 10.1109/TCE.2020.3011966.
3. A. Mukhopadhyay, R. R. Hegde, and A. S. Thomas, "Handover mechanisms in wireless heterogeneous telemedicine networks," *Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019*, no. Iccmc, pp. 938–945, 2019, doi: 10.1109/ICCMC.2019.8819726.
4. M. A. Sayeed, S. P. Mohanty, E. Kougianos, and H. P. Zaveri, "Neuro-Detect: A Machine Learning-Based Fast and Accurate Seizure Detection System in the IoMT," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 359–368, 2019, doi: 10.1109/TCE.2019.2917895.
5. A. Ahad, M. Tahir, M. A. Sheikh, K. I. Ahmed, A. Mughees, and A. Numani, "Technologies trend towards 5g network for smart health-care using iot: A review," *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–22, 2020, doi: 10.3390/s20144047.
6. L. C. Schünke *et al.*, "A rapid review of machine learning approaches for telemedicine in the scope of COVID-19," *Artif Intell Med*, vol. 129, no. March 2021, 2022, doi: 10.1016/j.artmed.2022.102312.
7. G. Guo, G. Sun, S. Bin, and F. Shao, "Design and Analysis of Field Telemedicine Information Communication Protocol Based on Wireless Sensor Network," *IEEE Access*, vol. 7, pp. 50630–50635, 2019, doi: 10.1109/ACCESS.2019.2908932.
8. B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends," Apr. 01, 2023, *MDPI*. doi: 10.3390/su15076177.
9. E. V. D. Subramaniam, K. Srinivasan, S. M. Qaisar, and P. Pławiak, "Interoperable IoMT Approach for Remote Diagnosis with Privacy-Preservation Perspective in Edge Systems," *Sensors*, vol. 23, no. 17, Sep. 2023, doi: 10.3390/s23177474.
10. M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, and P. K. R. Maddikunta, "A Review on Security and Privacy of Internet of Medical Things," *Internet of Things*, pp. 171–187, 2022, doi: 10.1007/978-3-030-81473-1\_8.
11. D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligieris, "Security in iomt communications: A survey," *Sensors (Switzerland)*, vol. Koutras, D, no. 17, pp. 1–49, 2020, doi: 10.3390/s20174828.
12. K. A. I. Zhang, "Health Monitoring of Human Multiple Physiological Parameters Based on Wireless Remote Medical System," *IEEE Access*, vol. 8, pp. 71146–71159, 2020, doi: 10.1109/ACCESS.2020.2987058.
13. N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Yusupov, and D. Kodirov, "Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT)," *Journal of Communications*, vol. 17, no. 11, pp. 900–918, 2022, doi: 10.12720/jcm.17.11.900-918.
14. M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019, doi: 10.1007/s11036-018-1089-9.

15. S. Bhalla, S. Sachdeva, and S. Batra, "Semantic interoperability in electronic health record databases: Standards, architecture and e-health systems," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017. doi: 10.1007/978-3-319-72413-3\_16.
16. S. Roca, J. Sancho, J. García, and Á. Alesanco, "Microservice chatbot architecture for chronic patient support," *J Biomed Inform*, vol. 102, p. 103305, 2020, doi: 10.1016/j.jbi.2019.103305.
17. M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," *Information (Switzerland)*, vol. 12, no. 2, pp. 1–21, 2021, doi: 10.3390/info12020087.
18. C. O. Alenoghena *et al.*, "eHealth: A Survey of Architectures, Developments in mHealth, Security Concerns and Solutions," *Int J Environ Res Public Health*, vol. 19, no. 20, 2022, doi: 10.3390/ijerph192013071.
19. N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Yusupov, and D. Kodirov, "Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT)," *Journal of Communications*, vol. 17, no. 11, pp. 900–918, 2022, doi: 10.12720/jcm.17.11.900-918.
20. D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications: A survey," *Sensors (Switzerland)*, vol. 20, no. 17, pp. 1–49, 2020, doi: 10.3390/s20174828.
21. N. R. C. for E. Standards(NRCeS), "HL7."
22. S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, "Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems," *IEEE Trans Eng Manag*, vol. 67, no. 4, pp. 1363–1376, 2020, doi: 10.1109/TEM.2020.2989779.
23. M. Li, E. Moll, and C. M. Chituc, "IoT for healthcare: An architecture and prototype implementation for the remote e-health device management using Continua and LwM2M protocols," *Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 2920–2926, 2018, doi: 10.1109/IECON.2018.8591635.
24. B. Ahire, "Health Record Sharing with Secure NFC," no. August, 2022, doi: 10.13140/RG.2.2.36677.73449.
25. S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "ICIT 2017 : the 8th International Conference on Information Technology : Internet of Things IoT : conference proceedings : May 17th - 18th, 2017, Amman, Jordan.," *International Conference on Information Technology (ICIT) Internet*, pp. 697–702, 2017.
26. Z. Safdar, S. Farid, M. Qadir, K. Asghar, J. Iqbal, and F. K. Hamdani, "A Novel Architecture for Internet of Things Based E-Health Systems," *J Med Imaging Health Inform*, vol. 10, no. 10, pp. 2378–2388, 2020, doi: 10.1166/jmih.2020.3184.
27. A. Darwish, A. E. Hassanien, M. Elhoseny, A. Kumar, and S. Khan, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems : opportunities , challenges , and open problems," *J Ambient Intell Humaniz Comput*, vol. 0, no. 0, p. 0, 2017, doi: 10.1007/s12652-017-0659-1.
28. M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," *Information (Switzerland)*, vol. 12, no. 2, pp. 1–21, 2021, doi: 10.3390/info12020087.
29. A. Yadav, V. K. Singh, A. K. Bhoi, G. Marques, B. Garcia-Zapirain, and I. de la T. Díez, "Wireless body area networks: UWB wearable textile antenna for telemedicine and mobile health systems," *Micromachines (Basel)*, vol. 11, no. 6, 2020, doi: 10.3390/MII1060558.
30. M. Almulhim, N. Islam, and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications," vol. 19, no. 1, pp. 107–120, 2019.
31. I. de la Torre Díez, S. G. Alonso, S. Hamrioui, M. López-Coronado, and E. M. Cruz, "Systematic Review about QoS and QoE in Telemedicine and eHealth Services and Applications," *J Med Syst*, vol. 42, no. 10, 2018, doi: 10.1007/s10916-018-1040-4.
32. M. Haddara and A. Staaby, "RFID applications and adoptions in healthcare: A review on patient safety," *Procedia Comput Sci*, vol. 138, pp. 80–88, 2018, doi: 10.1016/j.procs.2018.10.012.
33. A. Thaljaoui, S. El khediri, S. Zeadally, and A. Alourani, "Remote monitoring system using Light Fidelity and InfraRed technologies," *Computers and Electrical Engineering*, vol. 101, p. 108073, Jul. 2022, doi: 10.1016/J.COMPELECENG.2022.108073.
34. B. Ahire, "Health Record Sharing with Secure NFC," no. August, 2022, doi: 10.13140/RG.2.2.36677.73449.

35. E. Raso, G. M. Bianco, L. Bracciale, G. Marrocco, C. Occhiuzzi, and P. Loreti, "Privacy-Aware Architectures for NFC and RFID Sensors in Healthcare Applications," *Sensors (Basel)*, vol. 22, no. 24, pp. 1–21, 2022, doi: 10.3390/s22249692.
36. M. Donati, A. Celli, A. Ruiu, S. Saponara, and L. Fanucci, "A Telemedicine Service System Exploiting BT/BLE Wireless Sensors for Remote Management of Chronic Patients," *Technologies (Basel)*, vol. 7, no. 1, p. 13, 2019, doi: 10.3390/technologies7010013.
37. A. F. Santamaria, F. De Rango, A. Serianni, and P. Raimondo, "A real IoT device deployment for e-Health applications under lightweight communication protocols , activity classi fi er and edge data fi ltering," *Comput Commun*, vol. 128, no. July, pp. 60–73, 2018, doi: 10.1016/j.comcom.2018.06.010.
38. Y. N. Teja, L. Vooha, A. R. Priya, and N. V. K. Ramesh, "IOT based smart health care," *International Journal of Engineering and Technology(UAE)*, vol. 7, no. 11, pp. 470–472, 2018, doi: 10.14419/ijet.v7i2.7.10865.
39. C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, "The Z-Wave routing protocol and its security implications," *Comput Secur*, vol. 68, pp. 112–129, 2017, doi: 10.1016/j.cose.2017.04.004.
40. J. Chu, Y. Wang, X. Li, and X. Yun, "NB-IoT-based health monitoring system for COVID-19," *Wearable Technology*, vol. 2, no. 1, p. 24, 2022, doi: 10.54517/wt.v2i1.1644.
41. M. Almulhim, N. Islam, and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications," vol. 19, no. 1, pp. 107–120, 2019.
42. S. R. Vangimalla and M. El-Sharkawy, "Interoperability enhancement in health care at remote locations using thread protocol in UAVs," *Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, vol. 1, pp. 2821–2826, 2018, doi: 10.1109/IECON.2018.8592759.
43. L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 1, pp. 20–29, 2021, doi: 10.1109/TCE.2020.3043683.
44. P. Yadav, R. Agrawal, and K. Kashish, "Performance Evaluation of ad hoc Wireless Local Area Network in Telemedicine Applications," *Procedia Comput Sci*, vol. 125, pp. 267–274, 2018, doi: 10.1016/j.procs.2017.12.036.
45. G. Guo, G. Sun, S. Bin, and F. Shao, "Design and Analysis of Field Telemedicine Information Communication Protocol Based on Wireless Sensor Network," *IEEE Access*, vol. 7, pp. 50630–50635, 2019, doi: 10.1109/ACCESS.2019.2908932.
46. M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019, doi: 10.1007/s11036-018-1089-9.
47. M. T. Buyukkaskar, M. A. Erturk, M. A. Aydin, and L. Vollero, "LoRaWAN as an e-Health Communication Technology," *Proceedings - International Computer Software and Applications Conference*, vol. 2, pp. 310–313, 2017, doi: 10.1109/COMPSAC.2017.162.
48. A. Ahad, M. Tahir, M. A. Sheikh, K. I. Ahmed, A. Mughees, and A. Numani, "Technologies trend towards 5g network for smart health-care using iot: A review," *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–22, 2020, doi: 10.3390/s20144047.
49. I. Chorbev and M. Mihajlov, "Wireless telemedicine services as part of an integrated system for e-medicine," *Proceedings of the Mediterranean Electrotechnical Conference - MELECON*, pp. 264–269, 2008, doi: 10.1109/MELCON.2008.4618445.
50. R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 640–661, 2022, doi: 10.3390/jcp2030033.
51. M. Sultan Ahammad and A. Rahman Lecturer, "A Framework for M-Health Services Using 4G (LTE) Technology," *International Journal of Innovative Science and Research Technology Mobile Health*, vol. 5, no. 3, 2020.
52. W. Duan, Y. Ji, Y. Zhang, G. Zhang, V. Frascolla, and X. Li, "5G Technologies Based Remote E-Health: Architecture, Applications, and Solutions," pp. 1–16, 2020.

53. K. Hameed, I. S. Bajwa, N. Sarwar, W. Anwar, Z. Mushtaq, and T. Rashid, "Integration of 5G and block-chain technologies in smart telemedicine using IoT," *J Healthc Eng*, vol. 2021, 2021, doi: 10.1155/2021/8814364.
54. S. Raza, M. Faheem, and M. Guenes, "Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey," *International Journal of Communication Systems*, vol. 32, no. 15, pp. 1–32, 2019, doi: 10.1002/dac.4074.
55. D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications: A survey," *Sensors (Switzerland)*, vol. 20, no. 17, pp. 1–49, 2020, doi: 10.3390/s20174828.
56. M. Subramanian, K. Shanmuga Vadivel, W. A. Hatamleh, A. A. Alnuaim, M. Abdelhady, and V. E. Sathishkumar, "The role of contemporary digital tools and technologies in COVID-19 crisis: An exploratory analysis," *Expert Syst*, vol. 39, no. 6, pp. 1–18, 2022, doi: 10.1111/exsy.12834.
57. H. Calderon-Gomez *et al.*, "Telemonitoring System for Infectious Disease Prediction in Elderly People Based on a Novel Microservice Architecture," *IEEE Access*, vol. 8, pp. 118340–118354, 2020, doi: 10.1109/ACCESS.2020.3005638.
58. S. Roca, J. Sancho, J. García, and Á. Alesanco, "Microservice chatbot architecture for chronic patient support," *J Biomed Inform*, vol. 102, p. 103305, 2020, doi: 10.1016/j.jbi.2019.103305.
59. P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions," *Sensors*, vol. 22, no. 15, pp. 1–31, 2022, doi: 10.3390/s22155517.
60. C. Kugean, S. M. Krishnan, O. Chutatape, S. Swaminathan, N. Srinivasan, and P. Wang, "Design of a mobile telemedicine system with wireless LAN," *IEEE Asia-Pacific Conference on Circuits and Systems, Proceedings, APCCAS*, vol. 1, pp. 313–316, 2002, doi: 10.1109/APCCAS.2002.1114960.
61. A. Darwish, A. E. Hassanien, M. Elhoseny, A. Kumar, and S. Khan, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems," *J Ambient Intell Humaniz Comput*, vol. 0, no. 0, p. 0, 2017, doi: 10.1007/s12652-017-0659-1.
62. V. Seoane, C. Garcia-Rubio, F. Almenares, and C. Campo, "Performance evaluation of CoAP and MQTT with security support for IoT environments," *Computer Networks*, vol. 197, Oct. 2021, doi: 10.1016/j.comnet.2021.108338.
63. C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things," *Digital Communications and Networks*, vol. 8, no. 6, pp. 1094–1104, Dec. 2022, doi: 10.1016/j.dcan.2022.03.013.
64. A. E. Khaled, "Internet of Medical Things (IoMT): Overview, Taxonomies, and Classifications," *Journal of Computer and Communications*, vol. 10, no. 08, pp. 64–89, 2022, doi: 10.4236/jcc.2022.108005.
65. T. Harshita, "Healthcare Using Wireless Sensor Networks in IoT," 2023. [Online]. Available: www.ijrpr.com
66. D. Riyadh Ibrahim and M. Younis Thanoun, "IoMT Survey: Device, Architecture, Communication Protocols, Application and Security," *International Journal of Wireless and Microwave Technologies*, vol. 14, no. 6, pp. 68–80, Dec. 2024, doi: 10.5815/ijwmt.2024.06.05.
67. S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Internet of Things (Netherlands)*, vol. 28, Dec. 2024, doi: 10.1016/j.iot.2024.101351.
68. Swetha Singiri, Naga santhosh reddy vootukuri, and Siri Chandana Katari, "Security protocols in healthcare: A comprehensive study of AI-Enabled IoMT," *Magna Scientia Advanced Biology and Pharmacy*, vol. 12, no. 1, pp. 032–037, May 2024, doi: 10.30574/msabp.2024.12.1.0030.
69. Q. Niu *et al.*, "Toward the Internet of Medical Things: Architecture, trends and challenges," *Mathematical Biosciences and Engineering*, vol. 21, no. 1, pp. 650–678, 2024, doi: 10.3934/mbe.2024028.
70. J. Areia, I. Bispo, L. Santos, R. Luís, and D. C. Costa, "Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. IoMT-TrafficData: Dataset and Tools for Benchmarking Intrusion Detection in Internet of Medical Things", doi: 10.1109/ACCESS.2023.1120000.

71. K. Samal, S. K. Sunanda, D. Jena, and S. Patnaik, "A lightweight privacy preservation authentication protocol for IoMT using ECC based blind signature," *International Journal of Engineering Business Management*, vol. 17, Jan. 2025, doi: 10.1177/18479790251318538.
72. R. Kazim, T. J. Cui, A. Zoha, L. Li, and S. A. Shah, "Wireless on Walls," pp. 2–8, 2021.
73. S. Vishnu, S. R. Jino Ramson, and R. Jegan, "Internet of Medical Things (IoMT)-An overview," *ICDCS 2020 - 2020 5th International Conference on Devices, Circuits and Systems*, pp. 101–104, 2020, doi: 10.1109/ICDCS48716.2020.243558.
74. S. A. Wagan, J. Koo, I. F. Siddiqui, M. Attique, D. R. Shin, and N. M. F. Qureshi, "Internet of medical things and trending converged technologies: A comprehensive review on real-time applications," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 9228–9251, 2022, doi: 10.1016/j.jksuci.2022.09.005.
75. S. O. Ajakwe, C. I. Nwakanma, D. S. Kim, and J. M. Lee, "Key Wearable Device Technologies Parameters for Innovative Healthcare Delivery in B5G Network: A Review," *IEEE Access*, vol. 10, pp. 49956–49974, 2022, doi: 10.1109/ACCESS.2022.3173643.
76. M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019, doi: 10.1007/s11036-018-1089-9.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.