

Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions

Inas Al Khatib , Abdulrahim Shamayleh  and Malick Ndiaye 

Department of Industrial Engineering, American University of Sharjah, Sharjah 26666, United Arab Emirates; ashamayleh@aus.edu (A.S.); mndiaye@aus.edu (M.N.)

* Correspondence: g00091914@aus.edu

Abstract: In recent years, the Internet of medical things (IoMT) has become a significant technological advancement in the healthcare sector. This systematic review aims to identify and summarize the various applications, key challenges, and proposed technical solutions within this domain, based on a comprehensive analysis of the existing literature. This review highlights diverse applications of the IoMT, including mobile health (mHealth) applications, remote biomarker detection, hybrid RFID-IoT solutions for scrub distribution in operating rooms, IoT-based disease prediction using machine learning, and the efficient sharing of personal health records through searchable symmetric encryption, blockchain, and IPFS. Other notable applications include remote healthcare management systems, non-invasive real-time blood glucose measurement devices, distributed ledger technology (DLT) platforms, ultra-wideband (UWB) radar systems, IoT-based pulse oximeters, accident and emergency informatics (A&EI), and integrated wearable smart patches. The key challenges identified include privacy protection, sustainable power sources, sensor intelligence, human adaptation to sensors, data speed, device reliability, and storage efficiency. The proposed mitigations encompass network control, cryptography, edge-fog computing, and blockchain, alongside rigorous risk planning. The review also identifies trends and advancements in the IoMT architecture, remote monitoring innovations, the integration of machine learning and AI, and enhanced security measures. This review makes several novel contributions compared to the existing literature, including (1) a comprehensive categorization of IoMT applications, extending beyond the traditional use cases to include emerging technologies such as UWB radar systems and DLT platforms; (2) an in-depth analysis of the integration of machine learning and AI in IoMT, highlighting innovative approaches in disease prediction and remote monitoring; (3) a detailed examination of privacy and security measures, proposing advanced cryptographic solutions and blockchain implementations to enhance data protection; and (4) the identification of future research directions, providing a roadmap for addressing current limitations and advancing the scientific understanding of IoMT in healthcare. By addressing current limitations and suggesting future research directions, this work aims to advance scientific understanding of the IoMT in healthcare.

Keywords: healthcare; IoMT; edge-fog computing; blockchain; network controlling; encryption; cryptography; Internet of medical things; healthcare system



Citation: Al Khatib, I.; Shamayleh, A.; Ndiaye, M. Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions. *Informatics* **2024**, *11*, 47. <https://doi.org/10.3390/informatics11030047>

Academic Editor: Alessandro Pozzebon

Received: 4 June 2024

Revised: 27 June 2024

Accepted: 5 July 2024

Published: 16 July 2024

Correction Statement: This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The advancement of technology within medical systems is crucial for pioneering new approaches to illness prevention and treatment, while also enhancing resilience during public health emergencies. Technological innovations are anticipated to significantly improve the effectiveness and capacity of medical systems, thereby bolstering public health outcomes [1]. A particularly promising area of technological advancement in healthcare is the Internet of medical things (IoMT).

The Internet of medical things (IoMT) constitutes a network of interconnected systems and devices designed to collect, process, and disseminate health data [2]. This transforma-

tive technology revolutionizes healthcare delivery by enabling remote patient monitoring, diagnosis, and treatment. The IoMT applies the principles of the Internet of things (IoT) specifically within the medical domain, addressing the unique needs and challenges of the healthcare industry [3].

By leveraging the IoMT, medical systems can establish comprehensive information platforms that interconnect various smart devices, including hospital assets, medical examination tools, and wearable sensors. These devices serve as foundational nodes in the IoMT network, continuously gathering and generating health data, which are then transmitted to centralized servers for further processing and analysis. The insights derived from these data are pivotal in informing medical professionals' decision-making processes [4].

In recent years, the IoMT has garnered significant attention and adoption across diverse fields within healthcare, including illness detection, remote health monitoring, smart hospitals, and the tracking of infectious diseases. This widespread adoption underscores the transformative potential of the IoMT in revolutionizing healthcare delivery and improving patient outcomes [5].

Despite the growing interest in and adoption of the IoMT, there is a notable gap in the literature regarding how the IoMT specifically addresses the challenges and requirements of the healthcare industry. While existing studies provide a general overview of the IoMT and its various applications, they often lack a detailed exploration of how the IoMT meets specific healthcare needs. This paper aims to bridge this gap by focusing on the following aspects:

1. Specific challenges in healthcare systems: identifying the limitations and challenges within current healthcare systems that the IoMT aims to overcome, such as data privacy, power sustainability, sensor intelligence, and device reliability.
2. Unique features of IoMT: highlighting the unique capabilities of IoMT that make it well-suited for addressing these challenges, including its ability to provide continuous health monitoring, real-time data processing, and the integration of advanced technologies such as machine learning and AI.
3. Practical implementation and impact: providing concrete examples and case studies that illustrate the practical implementation and impact of IoMT in real-world healthcare settings. This includes detailed examinations of IoMT applications in remote health monitoring, smart hospitals, and disease tracking.

By elaborating on these aspects, this paper aims to provide a comprehensive understanding of the IoMT's significance and potential contributions to the healthcare sector, thereby addressing the existing gap in the literature. Through detailed analysis and case studies, we seek to demonstrate how the IoMT can effectively transform healthcare delivery and improve patient outcomes.

1.1. Research Aims and Objectives

The ensuing goals give this review article the necessary emphasis and direction by helping to define what is crucial in the process of achieving the research aim:

- Objective 1: to identify different IoMT applications in use within the healthcare industry.
- Objective 2: to identify the key challenges faced by end-users of IoMT applications in healthcare.
- Objective 3: to identify the proposed resolutions/mitigations to overcome the key challenges encountered when using IoMT applications.

Consequently, the main research area of this review paper is the IoMT and the recent applications of such technology in the healthcare industry, alongside the challenges encountered by end-users and the proposed mitigations to overcome such challenges. This paper aims to answer the following main research question through a systematic literature review: Has IoMT dependency increased within the healthcare technological domain?

1.2. Research Methodology

A systematic review approach will be used throughout this research review work to gather secondary research material and evaluate its content in relation to the goals. This technique will involve a critical examination of the existing literature and a qualitative synthesis of the findings to produce a comprehensive overview of the evidence that is currently available in relation to the research topic. In order to ensure validity and dependability throughout this research, the literature review portion that follows will only include papers published between 2004 and 2024. A targeted literature search of the Scopus database was conducted using a key search phrase, ‘internet of medical things applications and challenges’, which yielded 348 papers. Screening articles on the basis of title and abstract resulted in references to 291 articles, leading to the identification of 134 articles that met the inclusion criteria, as illustrated in Figure 1, which shows the different steps of the academic journal selection process. Furthermore, we adhered to the PRISMA guidelines in conducting our Systematic Literature Reviews (SLRs) and in synthesizing and presenting the results [6,7].

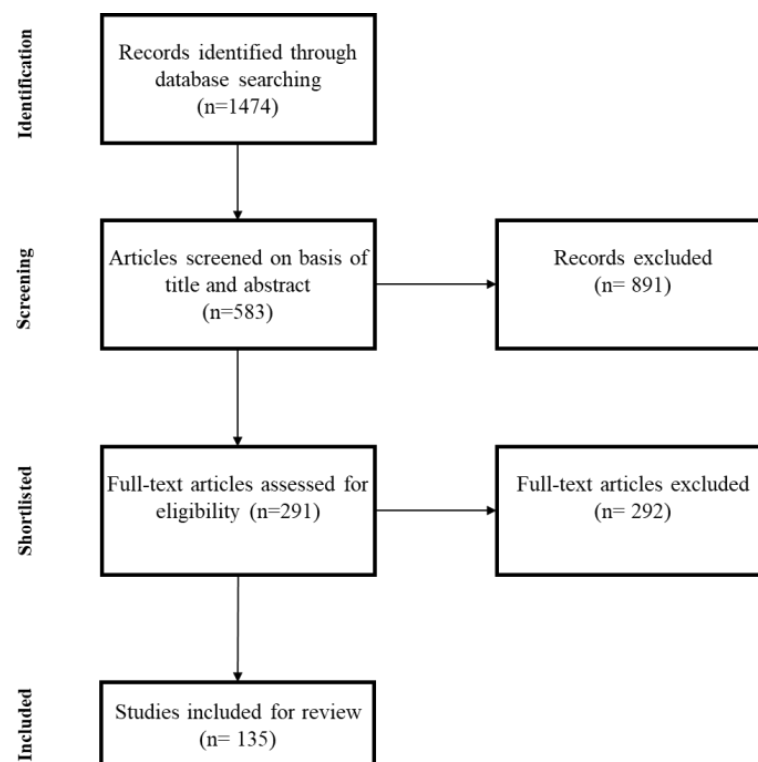


Figure 1. The systematic article selection process for this review.

After conducting a thorough bibliographic review, a suitable keyword search strategy, specifically “internet of medical things applications and challenges”, was adopted. Initially, the search was confined to the predetermined timeframe. Bibliometric networks were generated using VOSviewer software, utilizing data from the Scopus database, to construct various bibliometric maps for this study. The results of an advanced search, comprising 348 items, were exported to VOSViewer for network visualization, as depicted in Table 1, aiming to identify the leading countries in publications within this domain. Upon analysis of the 348 search results, the top five countries emerged were India, China, the United States, Saudi Arabia, and South Korea. These countries share common traits, such as a robust industrial landscapes, significant investments in the healthcare sector, and prowess in technology advancement.

The prominence of countries in the network visualization depicted in Figure 2 reflects the frequency of healthcare sectors in those nations publishing articles on the Internet of

medical things’ applications and challenges. This highlights India as the most invested country in researching this subject matter. Moreover, the interconnections between these circles illustrate the extent of co-citation relationships among the journals, indicating the influence of articles across different nations’ publications.

Table 1. Most countries with research on the subject of “internet of medical things applications and challenges”.

Country	Documents	Citations	Total Link Strength
India	105	1578	85
Saudi Arabia	47	718	81
China	73	1029	70
Pakistan	31	391	65
South Korea	32	533	52
United States	43	882	45
Australia	21	375	44
United Kingdom	17	319	42
France	15	337	33
Malaysia	14	171	33
Canada	20	325	31
Iraq	11	78	28
Taiwan	13	22	26
Italy	14	95	23
Iran	11	34	19
Spain	13	399	19
United Arab Emirates	8	7	17
Jordan	5	49	16
Oman	6	92	15
Sweden	7	125	15
India	105	1578	85
Saudi Arabia	47	718	81
China	73	1029	70
Pakistan	31	391	65
South Korea	32	533	52
United States	43	882	45
Australia	21	375	44
United Kingdom	17	319	42
France	15	337	33
Malaysia	14	171	33
Canada	20	325	31
Iraq	11	78	28
Taiwan	13	22	26
Italy	14	95	23
Iran	11	34	19
Spain	13	399	19
United Arab Emirates	8	7	17
Jordan	5	49	16
Oman	6	92	15
Sweden	7	125	15

Throughout this methodology, we critically examined the existing literature and synthesized their findings qualitatively to offer a comprehensive overview of the evidence pertaining to the research question or problem. Secondary research data were collected and analyzed in alignment with the objectives of this paper, involving a thorough search to identify all relevant articles, facilitating a systematic integration of data, and evaluating the evidence in the context of the specific research question. Forward and backward citations from studies were utilized.

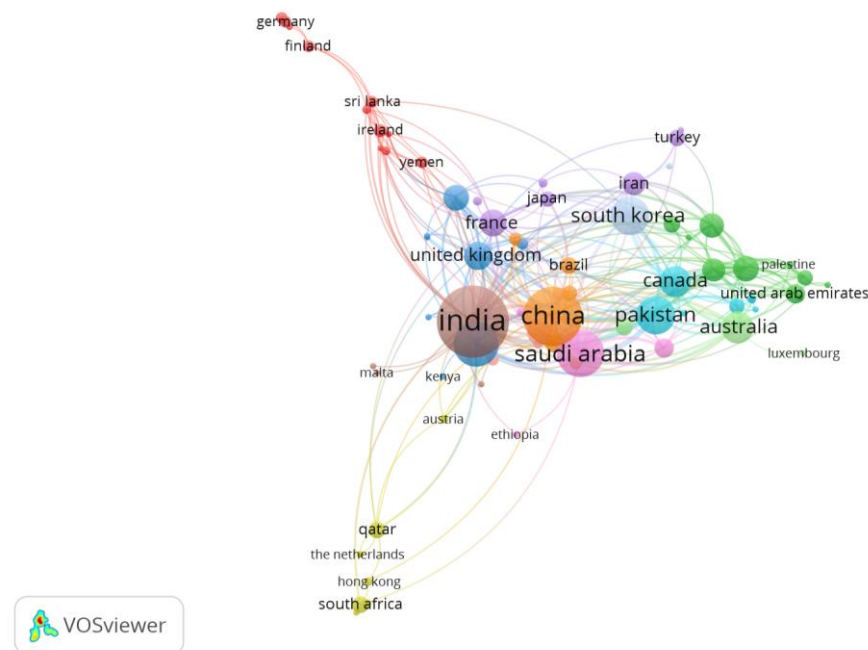


Figure 2. Network visualization.

1.3. Data Selection

The data collected from the 1474 references were arranged into a digital folder, with files in both Excel and Word formats, based on the compatibility features of the databases utilized. Studies that did not align entirely with the research objectives of this review and papers lacking empirical research or literature reviews were excluded. Criteria regarding the subjects, content of articles, and inclusion and exclusion were applied. Inclusion criteria represent the necessary qualities a data source must possess to be considered for inclusion in this study, while exclusion criteria outline the characteristics that disqualify a data source. These criteria were instrumental in identifying 135 relevant journals published between 2004 and 2024.

1.4. Data Thematic Analysis

In this systematic review, data extraction occurs post the selection of relevant studies and precedes data analysis. Apart from acquiring the information necessary for qualitative synthesis and meta-analysis, the primary objective of data extraction was to gain insights into the selected studies, including their demographics and characteristics. We adhered to proper procedures to ensure effective and error-free data gathering, thereby avoiding the production of a less useful systematic review and meta-analysis with shaky conclusions and inaccurate research findings. To achieve this, we followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) reporting standards, as recommended by [8]. The subsequent phase of Systematic Research (SR) involved extracting and analyzing relevant data from the selected publications using content and thematic analysis techniques. Content analysis, a standard approach for text analysis, typically yields a numerical breakdown of textual attributes or image collections. While theme analysis and content analysis share similarities, the former focuses more on the qualitative aspects of the material being studied [9].

As demonstrated in the Results/Bibliometrics section, we initially classified the chosen articles based on their publication characteristics, such as journal name, publication years, countries, and research methodologies. The literature mapping was conducted as the initial step, followed by an examination of the findings, categorized according to their respective themes and paper titles. For the data analysis, thematic analysis was employed to identify patterns in the meaning of the qualitative data extracted from the literature, thereby uncovering themes. An active reflexivity method based on subjective experience

was utilized to interpret the examined data. Additionally, Ref. [10] utilized content analysis as a research tool to validate the existence of these themes and establish connections among the data derived from the literature study. To extract and analyze patterns from the selected articles, we employed a multi-step approach. Initially, two independent reviewers used a standardized data extraction form to capture key information from each study, including study design, sample size, methods, and outcomes. This process ensured consistency and minimized bias. Subsequently, we conducted a thematic analysis to identify recurring themes and patterns across the studies. This involved coding the data and grouping similar concepts to uncover common trends. We also used statistical tools, such as meta-analysis, where applicable, to quantify patterns and relationships. Throughout the process, any discrepancies between reviewers were resolved through discussion or consultation with a third reviewer, ensuring the reliability and robustness of our findings.

2. Discussion and Results

2.1. IoMT Applications

In this section, multiple applications of the Internet of medical things, or IoMT, are explored.

2.1.1. Mobile Health (mHealth) Applications

It is becoming more and more important to deploy mobile health (mHealth) apps that can do things such as gather health data streams, interpret the data, trigger actions, and provide feedback. Three essential parts make up a standard mHealth system: a central cloud server, as well as individual interfaces for users and researchers/clinicians [11]. While guaranteeing the preservation of data integrity, security, and participant privacy, the cloud server serves as the basis for data storage, model construction, and action initiating directed towards the participants. Another essential element is the participant interface, which requires methods for both objective and subjective data collecting, in addition to real-time participant interaction capabilities [12]. Every component has a defined set of functions and functions inside a certain portion of the technological stack [13].

There are five levels in the IoMT architecture. The “perception layer”, at the bottom, is made up of various machines and sensing devices that have sensors incorporated in them. All of them allow for gateway-based internet connectivity. Various link layer technologies, such as Wi-Fi, 4G/5G mobile networks, ZigBee, and near-field communication (NFC), are used by these machines, equipment, and gadgets. This layer’s primary responsibility is to gather medical data and send them to the next level [14]. The IoMT places strict requirements on the accuracy and dependability of devices, media, and protocols because even a small discrepancy in the facts might be lethal. Work efficiency increases as a result of these efficient and quick connections [15]. Patients and physicians now have greater expectations as a result of these developments. They anticipate that medical records will be exchanged throughout several institutions in order to facilitate online diagnosis and improve the efficacy and accuracy of the outcomes. Making contact with the professionals at pertinent hospitals would also be helpful. To improve therapy, it may be possible to communicate information about illness conditions, electronic health records (EHR), personal information, and family medical history that is relevant to differential diagnosis. Since the IoMT is now being employed in several medical sectors, a large amount of data will be generated by it. The two primary things preventing IoMT development are its transmission and processing [16].

2.1.2. Remote Biomarker Detection

In customized medicine and health protection, timely and distant biomarker detection is greatly sought after [17]. A versatile, affordable, and self-sufficient sensing device based on galvanic cell structure may be used for H₂S biomarker detection in a variety of application situations. The change in electrode potential brought about by the chemical adsorption of gas molecules on the electrode surfaces is thought to be the sensing process.

Organohydrogels with intrinsic stretchability are utilized as solid-state electrolytes to allow devices to operate steadily and long-term in a variety of environments and stretching deformations. The end product is an open-circuit sensing device with excellent selectivity for H₂S, low detection limit, and high sensitivity. Its demonstrated use in the non-invasive diagnosis of halitosis and the detection of meat rotting has significant economic potential in the fields of food security and portable medical technology. Using cloud and Bluetooth technologies, a wireless sensory system for remote H₂S monitoring has also been created. By addressing the drawbacks of conventional chemiresistive sensors, this study provides guidance and a theoretical framework for the development of wearable sensors that meet various stimuli detection needs [18].

2.1.3. Hybrid RFID-IoT Scrub Distribution Solutions in Operating Rooms

An RFID/Internet-of-things uniform distribution system for medical staff to keep track of their scrubs in operation rooms has been implemented. The system lowers and regulates the amount of inventory in the operating rooms, stabilizes the demand for scrubs, enhances infection control, and prevents cross-contamination (by preventing scrub manipulation and hoarding). The hospital will be able to address two main challenges by using a hybrid simulation model to compare creative solutions for uniform distribution systems, such as “smart cabinets” powered by RFID and the Internet-of-things (IoT) technologies. The goal is to determine which design is best for the hospital and address the inefficiencies of the uniform replenishment-distribution system, as well as the distribution system’s contribution to noncompliance with infection control regulations [19].

2.1.4. IoT-Based Disease Prediction Using Machine Learning

In order to accurately and comprehensively predict the disease that patients are suffering from, the Internet of things (IoT) has the potential to play a significant role in telemedicine, teleconsultation, and virtual consultation. This can be achieved by creating a novel system that uses the most effective machine learning (ML) algorithm and gathers patient data, including symptoms, audio recordings, available medical reports, and past medical histories. A number of the symptoms, including fever and low blood oxygen, may also be monitored with sensors that use the ESP8266 and Arduino boards. Then, with its continuously updated database, which may be implemented as an application-based or website-based platform, it offers the proper diagnosis and treatment of the ailment [20].

2.1.5. Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS

One of the major issues in the healthcare ecosystem is the secure storing and sharing of personal health records (PHRs) on the Internet of medical things (IoMT). PHRs are one of the most sought-after targets for cybercriminals globally because of the significant value of personal health information. Numerous solutions rely on pre-existing plans, such as the creative PHR-sharing plan, which is useful, effective, and dynamic. In particular, this plan utilizes blockchain technology, searchable symmetric encryption, and the Inter-Planetary File System (IPFS) decentralized storage system to provide PHR confidentiality [21], search result verifiability, and forward security. Furthermore, it presents official security certifications for the plan [22].

2.1.6. Remote Healthcare Management Systems Built on IoT

The remote healthcare monitoring (RHM) system, which is built on the Internet of things, primarily uses deep learning (DL) [23] and artificial intelligence (AI) to analyze the data it gathers [24]. On the other hand, DL approaches are frequently used in CDSS and other types of healthcare services for the purpose of creating analytical representations. Clinical decision support systems provide patients with tailored suggestions for therapy, lifestyle modifications, and care plans, following a comprehensive analysis of each component. This technology supports healthcare applications by evaluating tasks, among other

things [25]. The term “big data” or “health data” describes the data that IoT devices and RHM networks collect. This volume of healthcare data requires powerful computational capabilities and a lot of data storage space [26]. Cloud computing and cloud storage provide the answer to the issue of managing health care data. Patient confidentiality, however, safeguards the majority of these data [27]. The security and privacy of data are the main issues with RHM. Individuals, groups, and companies should not misuse these data for personal gain. Data safety is influenced by a number of factors, including computer, network, storage, physical, and authentication security. The prevalence of genetic algorithms, data encryption, encipherment, and decipherment methods also plays a significant role [28]. The majority of security and privacy frameworks use unreliable third parties to deliver services [26].

2.1.7. Internet of Medical Things (IoMT)-Based Wearable Device for Non-Invasive and Real-Time Measurement of Blood Glucose

Due to the many drawbacks and difficulties associated with the current gold-standard invasive glucose-monitoring technologies, including concerns related to cost and comfort, non-invasive blood glucose estimation has been actively studied [29]. A user-worn photoplethysmography (PPG) device, a smart analytics cloud that deploys models for blood glucose estimation, and an end-to-end mobile/web application for diabetes patient monitoring comprise the diabetic health monitoring platform architecture. This allows for the non-invasive and real-time measurement of blood glucose using a wearable device based on the Internet of medical things (IoMT). A unique light-weight one-dimensional input-reinforced deep neural network architecture that we refer to as GlucoNet is used to compute blood glucose. This architecture extracts from the PPG signal both long and short temporal and spatial components [30].

2.1.8. Internet of Medical Things (IoMT)-Based Wearable Device for Non-Invasive and Real-Time Measurement of Blood Glucose

Using Magnetic Resonance Imaging (MRI) methods, it is possible to visually see the comprehensive morphological changes in fetal brain development during the whole pregnancy [31]. The Convolutional Neural Network (CNN) approach enables automated segmentation and classification in the process of investigating embryonic brain development. To stop brain abnormalities, it is essential to monitor prenatal brain development [32]. IoT technology’s automation and resource optimization in healthcare applications may reduce costs and raise the quality of care [33]. The CNN has made significant strides in image identification tasks by identifying intricate patterns in picture data. It investigates the optimal performance evaluation for quantitative assessment and confronts the key issues in studying the fetal brain development, using photos taken between 16 and 39 weeks of gestation. Information on brain growth may be accessed more easily by integrating the Internet of things and using contemporary medical detection techniques. In order to address the issue of brain malformations, the Detection of Fetal Brain Abnormalities (DFBA) utilizing data augmentation employing IoT technology makes it simple to identify the detection. The three steps of the DFBA method are picture pre-processing, model building, and performance assessment. After the data are retrieved, normalization and reshaping are used in the preprocessing steps to improve the outcome. Data augmentation is used after pre-processing to expand the amount of the dataset so that the CNN may be processed for classification. Evaluation criteria including recall, F1-score, accuracy, precision, confusion matrix, and support have been used to assess the effectiveness of the DFBA technique [34].

2.1.9. The Phonendo 1.0 Distributed Ledger Technology (DLT) IoT-Based Platform

The Phonendo 1.0 distributed ledger technology (DLT) Internet-of-things platform is intended to collect data streams from wearable devices and publish them on a distributed ledger architecture. Distributed ledger technology (DLT) provides ways to reduce single points of failure and strengthen resilience against information manipulation [35]. Wearable-based solutions with a greater variety of capabilities may be produced by utilizing DLT.

By enabling wearable device pairing, Phonendo helps to overcome prior vulnerabilities by recording and authenticating wearable device data streams and publishing them on a specialized DLT infrastructure, also known as DLTi [36]. Timestamped modification protection, resistance to identity spoofing, resistance to alteration and/or deletion of data, and resilience to single points of failure are all advantageous for any solution that employs data stored on a DLTi. The five components of Phonendo's microservice event-driven architecture are Reader, Manager, Storage, Verifier, and Publisher. The links between each component and their primary function. This architecture's scalability, versatility, and capacity to adapt to various applications were all taken into consideration during design [35].

2.1.10. Flexible Triboelectric Sensors for Intelligent Medical Internet of Things (IoMT)

A strong and clever IoMT system combines adaptable wearable triboelectric sensors with data analytics powered by deep learning [37]. A bracelet with four triboelectric sensors is designed to evaluate and identify limb motions in Parkinson's disease (PD) patients. An intelligent healthcare monitoring system, comprising identity identification, heart monitoring, location/trajectory tracking, and surveillance of Parkinson's disease patients, was realized through the integration of deep learning-assisted data analytics. With the help of this creative method, it was possible to precisely record and examine the fine motor skills and delicate movements of PD patients, resulting in insightful analysis and a thorough evaluation of the patients' circumstances. Because of its low cost, ease of fabrication, great sensitivity, and intelligence, this monitoring system highlights the enormous potential of human body sensing technologies in a Health 4.0 society [38].

2.1.11. Ultra-Wideband (UWB) Radar-Based Internet-of-Medical-Things (IoMT) System

A radar-based ultra-wideband (UWB) Internet-of-medical-things (IoMT) system has been created to remotely monitor the vital signs and falls of elderly people as they go about their everyday lives [39]. The system uses a hybrid cloud infrastructure for additional processing and storage and edge computing for prioritizing important operations. For senior citizens, this system provides telehealth services and monitoring. It correctly identifies aberrant behaviors including falls and sleep apnea, as well as high-risk situations. Its mean absolute error (MAE) $\pm$ standard deviation of absolute error (SDAE) for heart rate (HR) detection is 1.23 ± 1.16 bpm, and for respiratory rate (RR), it is 0.22 ± 0.27 bpm. These results demonstrate its excellent accuracy levels. In addition, the system shows a 90.60% identification accuracy for one daily activity, three different fall kinds (stand, bow, and squat to fall), and no activity background. The radar sensor's great precision makes it ideal for a range of remote monitoring uses [40], boosting the security and wellbeing of elderly individuals living in their homes [41].

2.1.12. Federated Learning (FL)-Based Safe Patient Monitoring System in Internet of Medical Things

One exciting use of the Internet of medical things (IoMT) that has the potential to transform clinical diagnosis is the monitoring of patient activities. An IoMT trains a model on the server using sensory input gathered from smart devices [42]. The patient's actions on smart gadgets are recognized by the trained model. A federated learning (FL)-based safe patient monitoring system trains on local devices and only sends weight matrices to the server for aggregation. Through this approach, the system avoids security lapses and protects user privacy, two main challenges [43]. Based on resource availability, the system automatically groups participants into clusters, trains appropriate models on each cluster, and improves performance through knowledge distillation (KD). In order to enhance the performance of small-size clusters, the high-performing cluster model applies knowledge distillation to the model. The suggested approach functions well even with uneven resources [44].

2.1.13. Emotion-Aware Internet-of-Things (WBAN) System

An edge AI system handles long-distance data transfers and data processing for an emotion-aware Internet-of-things (WBAN) system in the healthcare context. This system predicts patients' spoken emotions in real time and records how patients' emotions change before and after therapy [45]. Utilizing a regularized CNN model in conjunction with a hybrid deep learning model that combines bidirectional long short-term memory (BiLSTM) and convolutional neural networks (CNNs). To increase prediction accuracy, decrease generalization error, and lower the computational complexity of neural networks in terms of computing time, power, and space, the models are coupled with various optimization strategies and regularization approaches [46].

2.1.14. IoT-Based Pulse Oximeter for Remote Health Assessment

Globally, cardiovascular diseases (CVDs) are among the leading causes of mortality. The human heart, the strongest muscle in the body, is continuously monitored by intrusive sensors to aid in early identification and timely administration of essential therapy [47]. It was essential to have an IoT-enabled pulse rate monitoring system in order to better assist patients at all times and from any location, using any kind of device. Raspberry Pi is used to run the gadget, which makes use of a simple pulse sensor. The device's efficacy is evaluated in comparison to a leading brand fingertip pulse oximeter, which is recommended for use in both home and clinical settings. Additionally, the non-invasive architecture of the pulse oximeter uses sensors for photoplethysmography (PPG) and electrocardiography (ECG) to measure blood pressure (BP) [48].

2.1.15. Accident and Emergency Informatics (A&EI)

The COVID-19 pandemic highlighted the need for the continued development of digital health paradigms, including telemedicine, m-health, and the Internet of medical things (IoMT), to prepare for future emergencies [49]. The frequency with which varying degrees of quarantine were encountered suggests the urgent need to create smart medical homes so that patients may be continuously monitored. Accident and emergency informatics (A&EI) focuses on the long-term health prediction and prevention of an individual and immediately identifies accidents and crises for additional procedures that link to rescue and hospital services to lessen the damage. The concept of One Digital Health (ODH) takes into account the health of people, animals, and the environment at large [50].

2.1.16. Integrated Wearable Smart Patch-Based Sensor System with Kirigami-Inspired Strain-Free Deformable Structures

Recent years have seen a significant increase in interest in epidermal and wearable electronic sensor technologies, since they may provide real-time healthcare information to a tailored smartphone. A fully functional wearable smart patch-based sensor system that includes a commercial acceleration sensor, temperature and humidity sensors, and strain-free deformable structures has been designed, inspired by origami. In order to help with emergencies resulting from "unpredictable" deviations and to support medical examinations for vulnerable patients, this fully integrated wearable sensor system attaches to the skin with ease and accurately measures bodily information. It also has an integrated circuit with a read-out circuit and wireless communication to transfer medical information (temperature, humidity, and motion) to a mobile phone. With the introduction of a well-equipped, breathable, biocompatible, and conformable smart patch that provides excellent adhesion to the skin, the system overcomes the challenge of all-day continuous monitoring of human biological signals. This allows users to continuously monitor the early detection of diagnosis. Additionally, the patch-based medical device, which is outfitted with a low-power Bluetooth module, a signal processing integrated circuit installed on a flexible printed circuit board, and a unique circuit design, allows wireless sensing capabilities in response to fast variation. As a result, a special platform is created for multipurpose sensors

to communicate with hard electronics, opening up new possibilities for Internet of things and biomedical applications [51].

2.2. Case Studies of Healthcare IoMT Implementations

This section of the paper outlines case studies of actual hospitals and healthcare providers that have successfully implemented IoMT solutions to support their operational effectiveness and the real-world impact, as illustrated in Table 2.

Table 2. IoMT implementation case studies in healthcare.

Case Study	Healthcare Facility	Details	Outcome
Remote Patient Monitoring for Chronic Disease Management	Partners HealthCare (part of Mass General Brigham)	Partners HealthCare deployed a remote patient monitoring system for patients with chronic heart disease. The system included wearable devices that continuously monitored vital signs, such as heart rate, blood pressure, and oxygen saturation. Data were transmitted in real-time to a cloud-based platform accessible by healthcare professionals [52].	• Reduction in Hospital Readmissions: a reduction in hospital readmissions for heart disease patients using RPM systems [53]. • Improved Patient Compliance: a higher compliance rate with medication and lifestyle recommendations due to regular monitoring and feedback [54]. • Cost Savings: significant cost savings were achieved due to reduced hospitalizations and emergency room visits [55].
Smart Inhalers for Asthma Management	Cleveland Clinic	Cleveland Clinic implemented smart inhalers equipped with sensors that tracked usage patterns and environmental conditions for asthma patients. Data were sent to a mobile app that provided patients with reminders, usage feedback, and alerts about environmental triggers [56].	• Enhanced Medication Adherence: the hospital reported that there was a significant increase in medication adherence among patients using the smart inhaler [57]. • Reduction in Asthma Attacks: the hospital reported that the frequency of asthma attacks decreased [58]. • Patient Satisfaction: higher patient satisfaction levels due to the personalized feedback and reminders provided by the application [59].
IoMT in Post-Surgical Care	Johns Hopkins Hospital	Johns Hopkins Hospital implemented an IoMT solution to monitor patients after surgery. Wearable sensors tracked vital signs, such as temperature, heart rate, and blood pressure, which were crucial for detecting early signs of infection or complications. Data were analyzed in real-time, and alerts were sent to healthcare providers if any abnormalities were detected [60].	• Early Detection of Complications: the system enabled early detection of post-surgical complications, allowing for timely intervention and reducing the severity of potential issues [61]. • Shorter Hospital Stays: ability to discharge patients earlier with continuous monitoring at home, leading to shorter hospital stays and reduced healthcare costs [62]. • Patient Empowerment: patients felt more secure and involved in their recovery process, knowing that their health was being monitored continuously [63].

Table 2. Cont.

Case Study	Healthcare Facility	Details	Outcome
Diabetes Management with Continuous Glucose Monitors (CGMs)	Mayo Clinic	Mayo Clinic implemented an IoMT solution using continuous glucose monitors (CGMs) for diabetes patients. The CGMs provided real-time blood glucose readings and transmitted data to a mobile app. The app analyzed the data and provided personalized recommendations and alerts [64].	- Improved Glycemic Control: patients using CGMs achieved better glycemic control, with a significant reduction in HbA1c levels [65]. - Reduction in Hypoglycemic Events: notable decrease in hypoglycemic events, enhancing patient safety [66]. - Enhanced Patient Engagement: patients felt more engaged and proactive in managing their diabetes due to the real-time feedback and data visualization [67].
Telehealth and Remote Monitoring for Elderly Care	Kaiser Permanente	Kaiser Permanente introduced a telehealth and remote monitoring system for elderly patients living in assisted living facilities. The system included various IoMT devices such as fall detectors, heart rate monitors, and smart medication dispensers. Data were transmitted to a central monitoring hub where healthcare providers could track patients' health status [68].	- Improved Health Outcomes: an overall improvement in health outcomes due to continuous monitoring and timely interventions [69]. - Increased Independence: elderly patients experienced increased independence and a higher quality of life, as they could manage their health more effectively at home [70]. - Reduced Caregiver Burden: the system helped reduce the burden on caregivers by providing automated alerts and reducing the need for constant supervision [71].

2.3. Critical Factors for a Successful IoMT Implementation

Factors such as infrastructure requirements, cost implications, maintenance, and scalability strategies provide a realistic and actionable framework for healthcare providers considering IoMT implementation. Starting with infrastructure, requirements encompass not only the physical hardware but also the necessary network capabilities to support a large number of connected devices. This includes considerations for bandwidth, data storage, and security measures to protect sensitive patient information [72]. Secondly, cost implications involve both initial investments and ongoing expenses, such as software updates, device replacements, and potential training for healthcare staff to effectively use and maintain IoMT systems [73]. Maintenance is another crucial factor, as IoMT devices and systems must be regularly updated and checked to ensure they are functioning correctly and securely. This includes addressing potential technical issues promptly to avoid disruptions in patient care [2]. Lastly, scalability strategies should outline how healthcare providers can expand their IoMT implementations as their needs grow, which might involve phased rollouts, pilot programs, and iterative improvements based on feedback and performance data [74].

2.4. Key Challenges of Healthcare IoMT Implementation and Proposed Resolutions

2.4.1. Challenge and Resolution 1: Lack of Sustainable Power Source, Sensor Intelligence, and Human Adaption in Sensors

The IoMT confronts a number of difficulties, such as the need for a sustainable power source, human adaptation in sensors, and sensor intelligence [35]. Because several kinds of sensors are being used, the data that are gathered may be erroneous and inconsistent. Wireless sensors are preferable because wearable sensors, particularly those intended for

children, have the potential to irritate. Safeguarding confidential patient data from cyberattacks is of utmost importance. One difficulty with IoT-based healthcare systems is fraud. Chronic patients benefit more from smart medical systems than from standard healthcare treatments. The electricity needed to power Internet-of-things devices is unavailable in remote regions. Because real-time monitoring requires a fast and stable network connection, it is more difficult in remote locations and with low-powered equipment. Stated differently, these limitations are independent of the advancement of novel technologies and are potentially surmountable [75]. A resolution to this challenge is interoperable modules that are generally required for the functioning of IoT applications in the healthcare industry [76]. These applications provide a number of security concerns at the network edge, despite their obvious advantages. For these applications to effectively and safely exploit the resources at hand, cutting-edge artificial intelligence (AI) techniques may be applied at the network edges. The term “cloud computing” describes the common pool of dynamic, widely available, and adjustable computer resources that provide on-demand access to resources such as servers, network infrastructures, storage, apps, and so forth. It facilitates a scalable, logical, and well-coordinated business model that works with mobile devices. A resolution to overcome the identified challenges [77], in addition to network controlling, includes cryptography, edge-fog computing and blockchain [75].

2.4.2. Challenge and Resolution 2: Lack of Privacy Protection in IoMT Healthcare Applications

Concerns over the security and privacy of vital health data have grown as a result of the Internet of things’ (IoT) rapid development and the expanding use of healthcare software in this field [78]. A resolution to this challenge is blockchain technology in conjunction with homomorphic encryption approaches to improve privacy protection in Internet-of-medical-things-based healthcare applications. Homomorphic encryption protects the privacy of the data during the computation process by making it easier to execute computations on encrypted data without the need for decryption. Patient privacy is preserved because authorized parties can process and evaluate the encrypted data without disclosing its true contents. Additionally, this method uses blockchain-based smart contracts to set data-sharing guidelines and impose access restriction. By offering fine-grained permission settings, these smart contracts make sure that only authorized parties are able to access and use the encrypted data [78,79].

2.4.3. Challenge and Resolution 3: Reduced Data Speed and Device Reliability

The device reliability and data speed are amongst the main challenges encountered when using IoMT despite most literature focusing on privacy issues. A resolution to this challenge is that data speeds and device reliability for Industry 4.0 applications might be greatly enhanced by implementing 5G standards. The computational expenses of Industry 4.0 and 5G-enabled intelligent healthcare systems have decreased thanks to a completely new design, making them a more effective option for practical uses [80].

2.4.4. Challenge and Resolution 4: Redundant Healthcare Data Decreasing Storage Efficiency

The IoT medical devices are producing an exponential amount of redundant healthcare data, decreasing storage efficiency [81]. Storage efficiency may be increased by running a deduplication algorithm, spotting redundant data, and preventing them from being stored onto cloud servers. Enhancing storage efficiency may be achieved by deduplicating data and preventing redundant data from being sent to the cloud. Nevertheless, there is a significant communication cost in the current methods. Both encryption and deduplication are carried out using the full hash values of the data chunks in conventional hash-based and convergent key-based deduplication techniques. As a result, the deduplication technology becomes susceptible to confirmation of file assaults (CFAs). Furthermore, current methods encounter a significant false-positive error on the hash table when performing deduplication [82]. A fog-centric strategy is proposed to tackle several issues and improve the

performance of the deduplication algorithm. Instead of sending full hash values to cloud storage, fog nodes share partial hash values (Pαvs) with neighboring fog nodes. These partial hash values are stored in a Scalable Bloom Hash Table (SBHT) maintained by each fog node, facilitating inline deduplication. The SBHT generates and stores the P\ν hash bits needed for inline deduplication. Before uploading non-redundant data chunks to cloud storage, the edge node encrypts them with an asymmetric Cramer–Shoup (CS) cryptosystem. This approach reduces communication overhead by 65–70%, enhances security against CFA, decreases false-positive errors, and improves storage efficiency. These advantages make the proposed technique viable for real-time IoT healthcare applications [83].

2.4.5. IoMT Influence on Healthcare Risk Management

The network of linked medical equipment and healthcare systems that gather, transfer, and share medical data is known as the Internet of medical things (IoMT) [84]. The IoMT has the potential to have a big influence on healthcare risk management in a number of ways, starting with enhanced data vulnerability. As connected devices proliferate, there is a greater chance that data may be compromised. IoMT devices might be the target of hackers looking to obtain private patient data [85], followed by patient privacy concerns, as sensitive patient data are frequently collected and sent by IoMT devices. It becomes imperative to protect the privacy of this information, and risk management strategies must take into account any breaches and illegal access [86]. Risks of malfunction in the form of cyberattacks, software errors, and malfunctions might affect IoMT equipment. Strategies to lessen the impact of device malfunctions on patient safety should be part of risk planning [87].

One important factor to take into account is how well-integrated IoMT devices are with the current healthcare infrastructure. Systems that are incompatible may cause problems with data integration, which may have an effect on patient care. Risk management should take these issues into account and guarantee a smooth integration [88]. The laws and regulations governing medical technology are always changing. In order to ensure compliance with new standards and requirements, risk planning must incorporate methods for adapting to changes in legislation and the regulatory environment [89]. Since IoMT devices depend on network access, they are vulnerable to attacks by cybercriminals. Risk planning must include the implementation of strong cybersecurity measures, as well as ongoing monitoring and upgrading of these procedures in order to guard against any breaches. Ensuring the security of network risks is essential [90].

A significant amount of data are generated by IoMT devices. Ensuring the precision and soundness of these data is crucial in order to arrive at well-informed healthcare decisions. Planning for risks should take into account any problems with data quality [91]. It is critical to inform patients and healthcare professionals alike about the dangers of the IoMT. Initiatives to raise awareness, provide training, and implement best practices should all be a part of risk planning in order to reduce human error and promote cybersecurity hygiene in general [15]. In conclusion, the new risk aspects brought about by the integration of the IoMT into healthcare must be properly taken into account when developing risk management methods. In order to reduce the dangers associated with IoMT, it is imperative that cybersecurity, data privacy, device dependability, and regulatory compliance be addressed.

2.5. Comparative Analysis

When comparing the results of the present study with previous studies and analyzing their results comprehensively, several trends and advancements in the field of the Internet of medical things (IoMT) applications were identified. Firstly, regarding the advancements in the IoMT architecture, previous studies have focused on developing and refining the architecture of IoMT systems. For instance, Ref. [15] highlighted the importance of the perception layer in IoMT architecture, emphasizing the need for accurate and reliable data collection from various devices. This aligns with the findings of our study, which also emphasize the critical role of data accuracy and connectivity in IoMT applications.

Secondly, regarding innovations in remote monitoring, several studies have explored the potential of the IoMT for remote monitoring of biomarkers, patient health, and vital signs. For example, Ref. [18] developed a wireless sensory system for remote H2S monitoring, while [92] introduced a radar-based IoMT system for monitoring vital signs and falls in elderly individuals. These findings demonstrate the diverse applications of IoMT in improving healthcare outcomes, especially in remote or home settings. Thirdly, regarding the integration of machine learning and AI, many studies have incorporated machine learning (ML) and artificial intelligence (AI) algorithms into IoMT systems for disease prediction, patient monitoring, and data analysis. Ref. [20] proposed an IoMT system for disease prediction using ML algorithms, while [93] discussed the use of deep learning (DL) and AI in remote healthcare management systems. These findings underscore the growing importance of data analytics and predictive modeling in IoMT applications [94].

Fourthly, regarding the enhanced security and privacy measures, as IoMT systems handle sensitive health data, ensuring security and privacy is paramount. It is necessary to fulfill the requirement for a more comprehensive understanding of blockchain and encryption methods in protecting sensitive health data in the IoMT (Internet of medical things) systems. As IoMT systems handle sensitive health data, ensuring security and privacy is paramount. Various studies have proposed solutions leveraging blockchain and encryption technologies to enhance data protection. For instance, Ref. [95] proposed a secure sharing method for personal health records using blockchain combined with traditional encryption techniques. This approach ensures data integrity and immutability, making unauthorized alterations virtually impossible.

To practically implement these technologies in IoMT systems, several key components must be considered. The first component is the blockchain technology. Blockchain's decentralized nature offers a robust framework for secure data transactions. It ensures transparency and traceability, with each data entry verified by consensus mechanisms [95]. Implementing blockchain in IoMT involves creating a distributed ledger where health data transactions are recorded and validated by multiple nodes, reducing the risk of single points of failure [96]. Second, the encryption methods, such as homomorphic encryption, as studied by [97], allow computations on encrypted data without decryption, preserving data privacy during processing. Implementing homomorphic encryption in IoMT systems requires adapting existing algorithms to handle the specific requirements of medical data, such as real-time processing and minimal computational overhead [98].

To provide a comprehensive understanding, it is essential to examine existing practices and their efficacy. These practices start with data anonymization, which is a fundamental privacy practice ensuring that patient data cannot be traced back to individuals [99]. Methods such as pseudonymization and de-identification are commonly used, though they must be carefully managed to prevent re-identification through data correlation [100]. The second practice is access controls, which involve implementing robust access control mechanisms to ensure that only authorized personnel can access sensitive health data [101]. Role-based access control (RBAC) and attribute-based access control (ABAC) are widely adopted frameworks [102]. The third practice is secure communication protocols, whereby the encryption of data in transit using protocols such as TLS (Transport Layer Security) ensures that data transmitted between IoMT devices and servers are secure from interception and tampering [103].

Analyzing real-world implementations as case studies, such as Estonia's e-Health System, which utilizes blockchain technology to secure its national health records system, provides valuable insights. The system ensures data integrity and provides patients with control over their data, exemplifying how blockchain can enhance data security and transparency [104]. Furthermore, MediBloc, a decentralized healthcare information ecosystem, uses blockchain to empower patients with data ownership and secure sharing capabilities. The system highlights the practical application of blockchain in ensuring data privacy and security [105].

Fifthly, regarding challenges and resolutions, previous studies have identified key challenges in IoMT implementation, such as power source sustainability, privacy protection, data speed, and storage efficiency. Various resolutions have been proposed, including the use of interoperable modules, blockchain technology, 5G standards, and data deduplication algorithms. This revision not only delves deeper into the technologies and their practical implementations but also provides an examination of current practices, case studies for context, and actionable recommendations, thus fulfilling the requirement for a comprehensive discussion on enhancing data protection in the IoMT systems. These findings emphasize the importance of addressing technical and regulatory challenges to realize the full potential of the IoMT in healthcare. Overall, the comparison of present and previous studies highlights the evolving landscape of IoMT applications, with advancements in architecture, remote monitoring, data analytics, security measures, and resolution of challenges. By addressing these challenges and leveraging emerging technologies, the IoMT has the potential to revolutionize healthcare delivery and improve patient outcomes.

2.6. User Experience and Acceptance of IoMT Technologies

Understanding the perspectives and concerns of end-users, including both healthcare professionals and patients, is crucial for the successful adoption of the Internet-of-medical-things (IoMT) technologies [106]. This section explores the usability, accessibility, and potential resistance to IoMT systems, supported by user feedback and relevant case studies. Additionally, we discuss user-centric design principles and strategies to enhance user engagement.

2.6.1. Usability and Accessibility

Usability refers to how effectively, efficiently, and satisfactorily users can interact with a technology. For the IoMT systems, usability is paramount to ensure that healthcare professionals can integrate these technologies into their workflows without excessive training or disruption. Similarly, patients must find these devices easy to use and non-intrusive in their daily lives [107].

Accessibility is another critical aspect, ensuring that IoMT technologies are usable by individuals with varying abilities and in different environments. This includes considerations for patients with physical disabilities, older adults, and those with limited technical proficiency [108].

A case study on remote patient monitoring systems reveals several key insights into usability and accessibility. For example, a trial involving elderly patients with chronic conditions showed that devices with simple interfaces and clear instructions significantly improved adherence and satisfaction. Healthcare professionals noted that systems that integrated seamlessly with electronic health records (EHRs) and provided real-time alerts enhanced their ability to deliver timely care [109].

2.6.2. Potential Resistance and Concerns

Despite the benefits, there is potential resistance to adopting IoMT technologies. *Privacy and security* is the first concern, as both patients and healthcare professionals express concerns about data privacy and the security of medical information. Ensuring robust encryption and compliance with health regulations (e.g., HIPAA) is essential to alleviate these fears [110]. Secondly, there is the issue of technical reliability. Concerns about the reliability and accuracy of IoMT devices can hinder acceptance. Demonstrating high levels of accuracy and providing reliable technical support can mitigate these issues [84]. Thirdly, change management, resistance to change, particularly among healthcare professionals accustomed to traditional practices, can pose a barrier. Providing comprehensive training and demonstrating the long-term benefits of the IoMT can facilitate smoother transitions [111].

A study involving wearable health devices found initial resistance among healthcare professionals, primarily due to concerns about data accuracy and the additional workload of monitoring device-generated data. However, after a pilot phase with extensive training and

support, the acceptance levels increased, highlighting the importance of proper onboarding and continuous support [112].

2.6.3. User-Centric Design Principles

To address these challenges, IoMT technologies should be developed using user-centric design principles. This approach involves engaging end-users in the design process. Involving healthcare professionals and patients in the design and testing phases ensures that the final product meets their needs and preferences [113]. Iterative testing and feedback by regularly testing prototypes with the end-users and incorporating their feedback leads to more refined and user-friendly designs [114]. Third, simplified user interfaces involves designing intuitive and easy-to-navigate interfaces that help reduce the learning curve and enhance user satisfaction [115]. The fourth principle is employing comprehensive training programs. Providing detailed training and resources for both healthcare professionals and patients ensures that they are confident in using the technology. Lastly, ongoing support and updates, which involve offering continuous technical support and updates based on user feedback, help maintain trust and satisfaction [116].

An IoMT project aimed at managing diabetes involved extensive user engagement throughout the design process. Focus groups with patients and healthcare providers identified key features and usability improvements, resulting in a highly accepted and effective management tool [117].

In conclusion to this section, the successful adoption of IoMT technologies hinges on understanding and addressing the user experience and acceptance among healthcare professionals and patients. By focusing on usability, accessibility, and potential resistance and incorporating user feedback and case studies, developers can create more effective and widely accepted IoMT solutions. Embracing user-centric design principles and strategies to enhance user engagement will not only improve the adoption rates but also ensure that these technologies deliver maximum benefit to their users.

3. Practical Implications

For healthcare providers, these recommendations could focus on implementing the latest IoMT technologies to enhance patient care and streamline operations. For technology developers, insights from this review could guide the development of more robust and user-friendly IoMT solutions that address current gaps and challenges. Policymakers could use the findings to formulate regulations and standards that ensure the safe and effective deployment of IoMT systems, promoting innovation while safeguarding public health. Providing such practical recommendations would not only strengthen the paper but also facilitate the real-world application of its findings.

4. Research Limitation and Future Areas of Research

Technology evolves rapidly, which limits the years of research to the past 3 years, as earlier publications would be deemed outdated in terms of technical content. Moreover, the identified literature scope of coverage was vast and not focused on certain technical aspects of IoMT, which is an area of potential exploration for future research.

A prominent area of future research is the applications that focus on OHS for corporate or industrial white-collar or blue-collar workers who must anticipate and track their health state in order to maintain future employment [42]. Another area of research could be to explore the effectiveness of such applications in mobile patients, such as those transferred from one geographical area to another for treatment and requiring medical assistance (MEDA). In other words, will their operational effectiveness be impacted when away from the conventional setting of care?

Moreover, focused scopes around the technical aspects of IoMT implementation in healthcare are required, as the current literature covers a vast range of topics, including e-health industrial applications in IoMT, layer management in IoMT, data acquisition in IoMT, software-defined IoMT and edge computing implementation, wearable sensor network,

e-health cloud for medical things, machine learning in IoMT, multimodality in IoMT data, and explainable AI for IoMT.

There is also a pressing need to address cybersecurity concerns within IoMT systems. Ensuring the privacy and security of patient data is paramount, given the sensitive nature of health information and the increasing frequency of cyber-attacks. Developing robust encryption methods and secure communication protocols for IoMT devices and networks is essential.

Furthermore, interoperability standards for IoMT devices and systems must be established to ensure seamless integration and communication between different healthcare technologies. This would facilitate a more cohesive and efficient healthcare delivery system, improving patient outcomes and operational efficiency [118]. Interoperability is a critical factor in the successful implementation of the Internet-of-medical-things (IoMT) systems, as it ensures seamless integration and communication among diverse medical devices and systems. The primary challenges in achieving interoperability include standardization, compatibility, and data exchange protocols [119]. To address these issues, the adoption of universally accepted standards is essential, enabling devices from different manufacturers to work together harmoniously. Compatibility can be enhanced through the development of middleware solutions that bridge the gaps between disparate systems, facilitating smooth data flow [120]. Robust data exchange protocols, such as HL7 and FHIR, should be implemented to ensure the secure and efficient communication of medical data [121]. Furthermore, fostering collaboration among stakeholders, including device manufacturers, healthcare providers, and regulatory bodies, is crucial for establishing a cohesive framework that supports interoperability [122]. By focusing on these strategies, the deployment of IoMT technologies can be more effective, leading to improved patient outcomes and streamlined healthcare operations.

Additionally, research into the scalability of IoMT solutions is crucial. As the number of connected medical devices grows, it is important to ensure that IoMT systems can handle increased data volumes and maintain performance levels. Exploring advanced data processing and storage solutions, such as cloud computing and edge computing, could provide valuable insights into managing the scalability of IoMT infrastructures.

Moreover, the impact of IoMT on healthcare policy and regulation warrants further investigation. Understanding how emerging technologies influence healthcare laws, ethical considerations, and regulatory frameworks will be vital in shaping the future landscape of IoMT in healthcare. By addressing these multifaceted challenges, future research can pave the way for more effective and sustainable IoMT implementations, ultimately enhancing patient care and health outcomes.

Finally, incorporating quantitative data, such as adoption rates, effectiveness, and cost-benefit analysis would substantiate claims and enhance empirical evidence. This will not only bolster the credibility of findings but also provide a more precise understanding of the impact and feasibility of IoMT solutions in healthcare settings.

5. Conclusions

It is anticipated that by 2025, there will be 75 billion IoT-connected devices. The Internet-of-things (IoT) paradigm blends the benefits of cloud computing, Wireless Body Area Networks (WBANs), edge, fog, and autonomic computing with the latest advancements in communication technologies and sensors to open up new possibilities and pathways across several industries, particularly healthcare [123]. Unfathomable changes in healthy lifestyles are being brought about by IoMT. Unlike the previous paradigm, everything is a networked smart device in the Internet-of-things era. Healthcare now faces a new problem as a result of the IoMT, which includes everything from smart clinical gadgets to digital records. The IoMT enhances people's well-being by lowering medical costs and improving the quality of life [42].

Amongst the various applications identified in the literature were mobile health (mHealth) applications, Remote Biomarker Detection, hybrid RFID-IoT scrub distribution

solutions in operating rooms, IoT-based disease prediction using machine learning, efficient sharing of personal health records on the Internet of medical things using searchable symmetric encryption, blockchain, and IPFS. Additionally, remote healthcare management systems built on the IoT include the Internet-of-medical-things (IoMT)-based wearable devices for non-invasive, real-time measurement of blood glucose, such as the Phonendo 1.0. The distributed ledger technology (DLT) IoT-based platform, the ultra-wideband (UWB) radar-based Internet-of-medical-things (IoMT) system, the IoT-based pulse oximeter for remote health assessment, the accident and emergency informatics (A&EI), and the integrated wearable smart patch-based sensor system with Kirigami-inspired strain-free deformable structures, all are indicative of the growing dependency on the IoMT within the healthcare technological domain.

Among the key challenges such IoMT healthcare applications face are the lack of privacy protection, lack of sustainable power source, sensor intelligence and human adaption to sensors, reduced data speed and device reliability, and redundant healthcare data decreasing storage efficiency. Adopting network control, cryptography, edge-fog computing, and blockchain are mitigations to such challenges. Lastly, by outlining the main limitations in this area of research and offering recommendations for future lines of inquiry, this work advances scientific understanding.

Author Contributions: Conceptualization, I.A.K. and A.S.; methodology, I.A.K.; software, I.A.K.; validation, I.A.K.; formal analysis, I.A.K.; investigation, I.A.K.; resources, I.A.K.; data curation, I.A.K.; writing—original draft preparation, I.A.K.; writing—review and editing, I.A.K., A.S., M.N.; visualization, I.A.K., A.S.; supervision, A.S.; project administration, I.A.K.; funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was financially supported by the American University of Sharjah (AUS).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors acknowledge the support of the American University of Sharjah under the Open Access Program. This paper represents the opinions of the authors and does not mean to represent the position or opinions of the American University of Sharjah.

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

References

1. Laal, M. Innovation in medicine; health information technology. In Proceedings of the 2nd World Conference on Innovation and Computer Sciences, Izmir, Turkey, 10–12 May 2017.
2. Ajagbe, S.A.; Awotunde, J.B.; Adesina, A.O.; Achimugu, P.; Kumar, T.A. Internet of Medical Things (IoMT): Applications, Challenges, and Prospects in a Data-Driven Technology. In *Intelligent Healthcare Infrastructure, Algorithms and Management*; Chakraborty, C.K.M., Ed.; Springer: Singapore, 2022; pp. 299–319.
3. Askar, N.A.; Habbal, A.; Mohammed, A.H.; Sajat, M.S.; Yusupov, Z.Y.Z.; Kodirov, D. Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT). *J. Commun.* **2022**, *17*, 900–918. [[CrossRef](#)]
4. Mishra, P.; Singh, G. Internet of Medical Things Healthcare for Sustainable Smart Cities: Current Status and Future Prospects. *Appl. Sci.* **2023**, *13*, 8869. [[CrossRef](#)]
5. Huang, C.; Wang, J.; Wang, S.; Zhang, Y. Internet of medical things: A systematic review. *Neurocomputing* **2023**, *557*, 126719. [[CrossRef](#)]
6. Page, M.; Moher, D.; Bossuyt, P.; Boutron, I.; Hoffmann, T.; Mulrow, C.; Shamseer, L.; Tetzlaff, J.; Akl, E.; Brennan, S.; et al. PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ* **2021**, *372*, n160. [[CrossRef](#)] [[PubMed](#)]
7. Page, M.; McKenzie, J.; Bossuyt, P.; Boutron, I.; Hoffmann, T.; Mulrow, C.; Shamseer, L.; Tetzlaff, J.; Akl, E.; Brennan, S.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Int. J. Surg.* **2021**, *372*, n71.
8. Taylor, K.S.; Mahtani, K.R.; Aronson, J.K. Summarising good practice guidelines for data extraction for systematic reviews and meta-analysis. *BMJ Evid.-Based Med.* **2021**, *26*, 88–90. [[CrossRef](#)] [[PubMed](#)]

9. Joffe, H.; Yardley, L. Content and thematic analysis. In *Content and Thematic Analysis*; Sage: London, UK, 2004; pp. 56–68.
10. Humble, N.; Mozelius, P. Content analysis or thematic analysis: Similarities, differences and applications in qualitative research. In Proceedings of the European Conference on Research Methodology for Business and Management Studies, Aveiro, Portugal, 2–3 June 2022.
11. Vaghefi, I.; Tulu, B. The Continued Use of Mobile Health Apps: Insights from a Longitudinal Study. *JMIR mHealth uHealth* **2019**, *7*, e12983. [[CrossRef](#)] [[PubMed](#)]
12. Lakhan, A.; Mohammed, M.A.; Rashid, A.N.; Kadry, S.; Abdulkareem, K.H.; Nedoma, J.; Martinek, R.; Razzak, I. Restricted Boltzmann Machine Assisted Secure Serverless Edge System for Internet of Medical Things. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 673–683. [[CrossRef](#)] [[PubMed](#)]
13. Labbaf, S.; Abbasian, M.; Azimi, I.; Dutt, N.; Rahmani, A.M. ZotCare: A flexible, personalizable, and affordable mhealth service provider. *Front. Digit. Health* **2023**, *5*, 1253087. [[CrossRef](#)]
14. Hernandez-Jaimes, M.L.; Martinez-Cruz, A.; Ramírez-Gutiérrez, K.A.; Feregrino-Urbe, C. Artificial intelligence for IoMT security: A review of intrusion. *Internet Things* **2023**, *23*, 100887. [[CrossRef](#)]
15. Yaacoub, J.A.; Noura, M.; Noura, H.; Chehab, A.; Salman, O.; Yaacoub, E.; Couturier, R. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [[CrossRef](#)]
16. Huang, W.; Ding, Q.; Wang, H.; Wu, Z.; Luo, Y.; Shi, W.; Yang, L.; Liang, Y.; Liu, C.; Wu, J. Design of stretchable and self-powered sensing device for portable and remote trace biomarkers detection. *Nat. Commun.* **2023**, *14*, 5221. [[CrossRef](#)] [[PubMed](#)]
17. National Academies of Sciences, Engineering, and Medicine. *Biomarker Tests for Molecularly Targeted Therapies: Key to Unlocking Precision Medicine*; National Academies Press: Washington, DC, USA, 2016.
18. Maizi, Y.; Bendavid, Y. Hybrid RFID-IoT simulation modeling approach for analyzing scrubs' distribution solutions in operating rooms. *Bus. Process Manag. J.* **2023**, *29*, 1734–1761. [[CrossRef](#)]
19. Siddiqui, S.A.; Ahmad, A.; Fatim, N. IoT-based disease prediction using machine learning. *Comput. Electr. Eng.* **2023**, *108*, 108675. [[CrossRef](#)] [[PubMed](#)]
20. Dhanda, S.S.; Singh, B.; Jindal, P.; Sharma, T.K.; Panwar, D. 6G-enabled internet of medical things. *Expert Syst.* **2023**, *41*, e13472. [[CrossRef](#)]
21. Kumar, M.; Chand, S. A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System with Public Verifiability. *IEEE Internet Things J.* **2020**, *7*, 10650–10659. [[CrossRef](#)]
22. Bisht, A.; Das, A.K.; Niyato, D.; Park, Y. Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS. *IEEE Open J. Commun. Soc.* **2023**, *4*, 2225–2244. [[CrossRef](#)]
23. Osman, R.A. Internet of Medical Things (IoMT) optimization for healthcare: A deep learning-based interference avoidance model. *Comput. Netw.* **2024**, *248*, 110491. [[CrossRef](#)]
24. Alshamrani, M. IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34 Pt A*, 4687–4701. [[CrossRef](#)]
25. Musen, M.A.; Middleton, B.; Greenes, R.A. Clinical Decision-Support Systems. In *Biomedical Informatics*; Shortliffe, E.C.J., Ed.; Springer: Cham, Switzerland, 2021; pp. 795–840.
26. Philip, J.; Gandhimathi, S.K.; Chalichalamala, S.; Karnam, B.; Chandanapalli, S.B.; Chennupalli, S. Smart Health Monitoring Using Deep Learning and Artificial Intelligence. *Rev. d'Intell. Artif.* **2023**, *37*, 451–464. [[CrossRef](#)]
27. Chenthar, S.; Ahmed, K.; Wang, H.; Whittaker, F. Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access* **2019**, *7*, 74361–74382. [[CrossRef](#)]
28. Upadrista, V.; Nazir, S.; Tianfield, H. Secure data sharing with blockchain for remote health monitoring applications: A review. *J. Reliab. Intell. Environ.* **2023**, *9*, 349–368. [[CrossRef](#)] [[PubMed](#)]
29. Bolla, A.S.; Priefer, R. Blood glucose monitoring- an overview of current and future non-invasive devices. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 739–751. [[CrossRef](#)]
30. Dahiya, R.; Arunkumar, B.; Dahiya, V.K.; Agarwal, N. Facilitating Healthcare Sector through IoT: Issues, Challenges, and Its Solutions. *EAI Endorsed Trans. Ind. Netw. Intell. Syst.* **2023**, *9*, e5. [[CrossRef](#)]
31. Saleem, S.N. Fetal Magnetic Resonance Imaging (MRI): A Tool for a Better Understanding of Normal and Abnormal Brain Development. *J. Child Neurol.* **2013**, *28*, 890–908. [[CrossRef](#)] [[PubMed](#)]
32. Attallah, O.; Sharkas, M.A.; Gadelkarim, H. Deep Learning Techniques for Automatic Detection of Embryonic Neurodevelopmental Disorders. *Diagnostics* **2020**, *10*, 27. [[CrossRef](#)] [[PubMed](#)]
33. Kumar, P.; Silambarasan, K. Enhancing the Performance of Healthcare Service in IoT and Cloud Using Optimized Techniques. *IETE J. Res.* **2022**, *68*, 1475–1484. [[CrossRef](#)]
34. Priya, M.; Nandhini, M. Detection of fetal brain abnormalities using data augmentation and convolutional neural network in internet of things. *Meas. Sensors* **2023**, *28*, 100808. [[CrossRef](#)]
35. Moya, F.; Quesada, F.J.; Martínez, L.; Estrella, F.J. Phonendo: A platform for publishing wearable data on distributed ledger technologies. *Wirel. Netw.* **2023**, 1–15. [[CrossRef](#)]
36. Moya, F.; Quesada, F.J.; Martínez, L.; Estrella, F.J. CertifIoT: An IoT and DLT-Based Solution for Enhancing Trust and Transparency in Data Certification. In Proceedings of the 15th International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2023), Riviera Maya, Mexico, 28–29 November 2023.

37. Rezaee, K.; Khosravi, M.R.; Neshat, N.; Moghimi, M.K. Deep Transfer Learning-Based Fall Detection Approach Using IoMT-Enabled Thermal Imaging-Assisted Pervasive Surveillance and Big Health Data. *J. Circuits Syst. Comput.* **2022**, *31*, 2240005. [\[CrossRef\]](#)
38. Mao, J.; Zhou, P.; Wang, X.; Yao, H.; Liang, L.; Zhao, Y.; Zhang, J.; Ban, D.; Zheng, H. A health monitoring system based on flexible triboelectric sensors for intelligence medical internet of things and its applications in virtual reality. *Nano Energy* **2023**, *118*, 108984. [\[CrossRef\]](#)
39. Li, Q.; Liu, J.; Gravina, R.; Zang, W.; Li, Y.; Fortino, G. A UWB-Radar-Based Adaptive Method for In-Home Monitoring of Elderly. *IEEE Internet Things J.* **2024**, *11*, 6241–6252. [\[CrossRef\]](#)
40. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofacial Res.* **2022**, *12*, 302–318. [\[CrossRef\]](#) [\[PubMed\]](#)
41. Hämäläinen, M.; Mucchi, L.; Caputo, S.; Biotti, L.; Ciani, L.; Marabissi, D.; Patrizi, G. Ultra-Wideband Radar-Based Indoor Activity Monitoring for Elderly Care. *Sensors* **2021**, *21*, 3158. [\[CrossRef\]](#) [\[PubMed\]](#)
42. Wagan, S.A.; Koo, J.; Siddiqui, I.F.; Attique, M.; Shin, D.R.; Qureshi, N.M.F. Internet of medical things and trending converged technologies: A comprehensive review on real-time applications. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 9228–9251. [\[CrossRef\]](#)
43. Garg, N.; Wazid, M.; Singh, J.; Singh, D.P.; Das, A.K. Security in IoMT-driven smart healthcare: A comprehensive review and open challenges. *Secur. Priv.* **2022**, *5*, e235. [\[CrossRef\]](#)
44. Singh, C.; Mishra, R.; Gupta, H.P.; Banga, G. A Federated Learning-Based Patient Monitoring System in Internet of Medical Things. *IEEE Trans. Comput. Soc. Syst.* **2023**, *10*, 1622–1628. [\[CrossRef\]](#)
45. Bhuiyan, M.N.; Rahman, M.M.; Billah, M.M.; Saha, D. Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities. *IEEE Internet Things J.* **2021**, *8*, 10474–10498. [\[CrossRef\]](#)
46. Olatinwo, D.D.; Abu-Mahfouz, A.; Hancke, G.; Myburgh, H. IoT-Enabled WBAN and Machine Learning for Speech Emotion Recognition in Patients. *Sensors* **2023**, *23*, 2948. [\[CrossRef\]](#)
47. McAloon, C.; Osman, F.; Glennon, P.; Lim, P.; Hayat, S. Chapter 4—Global Epidemiology and Incidence of Cardiovascular Disease. In *Cardiovascular Diseases Genetic Susceptibility, Environmental Factors and Their Interaction*; Academic Press: Cambridge, MA, USA, 2016; pp. 57–96.
48. Revathi, K.; Tamilselvi, T.; Gomathi, G.; Divya, R. IoT Based Pulse Oximeter for Remote Health Assessment: Design, Challenges and Futuristic Scope. *Int. J. Electr. Electron. Res.* **2022**, *10*, 557–563. [\[CrossRef\]](#)
49. Srivastava, M.; Siddiqui, A.T.; Srivastava, V. Application of Artificial Intelligence of Medical Things in Remote Healthcare Delivery. In *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2023; p. 22.
50. Haghi, M.; Benis, A.; Deserno, T.M. Accident & Emergency Informatics and One Digital Health. *Yearb. Med. Inform.* **2022**, *31*, 40–46. [\[PubMed\]](#)
51. Lee, S.; Gandla, S.; Naqi, M.; Jung, U.; Youn, H.; Pyun, D.; Rhee, Y.; Kang, S.; Kwon, H.-J.; Kim, H.; et al. All-Day Mobile Healthcare Monitoring System Based on Heterogeneous Stretchable Sensors for Medical Emergency. *IEEE Trans. Ind. Electron.* **2019**, *67*, 8808–8816. [\[CrossRef\]](#)
52. Broderick, A. *Partners HealthCare: Connecting Heart Failure Patients to Providers through Remote Monitoring*; The Commonwealth Fund: New York, NY, USA, 2013.
53. Harris, S.; Paynter, K.; Guinn, M.; Fox, J.; Moore, N.; Maddox, T.M.; Lyons, P.G. Post-hospitalization remote monitoring for patients with heart failure or chronic obstructive pulmonary disease in an accountable care organization. *BMC Health Serv. Res.* **2024**, *24*, 69. [\[CrossRef\]](#) [\[PubMed\]](#)
54. Hamine, S.; Gerth-Guyette, E.; Faulx, D.; Green, B.B.; Ginsburg, A.S. Impact of mHealth Chronic Disease Management on Treatment Adherence and Patient Outcomes: A Systematic Review. *J. Med. Internet Res.* **2015**, *17*, e52. [\[CrossRef\]](#) [\[PubMed\]](#)
55. Polisena, J.; Coyle, D.; Coyle, K.; McGill, S. Home telehealth for chronic disease management: A systematic review and an analysis of economic evaluations. *Int. J. Technol. Assess. Health Care* **2009**, *25*, 339–349. [\[CrossRef\]](#) [\[PubMed\]](#)
56. Patterson, H.; Nissenbaum, H. *Context-Dependent Expectations of Privacy in Self-Generated Mobile Health Data*; Privacy Law Scholars Conference (PLSC): Berkeley, CA, USA, 2013.
57. Attaway, A.H.; Alshabani, K.; Bender, B.; Hatipoğlu, U.S. The Utility of Electronic Inhaler Monitoring in COPD Management Promises and Challenges. *Chest* **2020**, *157*, 1466–1477. [\[CrossRef\]](#) [\[PubMed\]](#)
58. Thomas, M.; Bateman, E. Asthma attacks: How can we reduce the risks? *NPJ Prim. Care Respir. Med.* **2015**, *25*, 14105. [\[CrossRef\]](#) [\[PubMed\]](#)
59. van de Hei, S.J.; Stoker, N.; Blok, B.M.J.F.-D.; Poot, C.C.; Meijer, E.; Postma, M.J.; Chavannes, N.H.; Kocks, J.W.H.; van Boven, J.F.M. Anticipated barriers and facilitators for implementing smart inhalers in asthma medication adherence management. *NPJ Prim. Care Respir. Med.* **2023**, *33*, 22. [\[CrossRef\]](#) [\[PubMed\]](#)
60. D'Souza, R. Implementation of the Internet of Medical Things (IoMT): Clinical and Policy Implications. In *Efficient Data Handling for Massive Internet of Medical Things*; Springer: Cham, Switzerland, 2021; pp. 313–338.

61. Arthi, K.; Chidhambararajan, B.; Revathi, A.R. A Deep Investigation of Architectural Elements and Computing Technologies for Internet of Medical Things. In Proceedings of the 2022 6th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 1–3 December 2022; pp. 556–563.
62. Malik, H.; Anees, T.; Faheem, M.; Chaudhry, M.U.; Ali, A.; Asghar, M.N. Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions. *Internet Things* **2023**, *23*, 100860. [\[CrossRef\]](#)
63. Monteiro, A.C.B.; França, R.P.; Arthur, R.; Iano, Y. 5—An overview of the Internet of medical things (IoMT): Applications, benefits, and challenges. In *Security and Privacy Issues in Internet of Medical Things*; Academic Press: Cambridge, MA, USA, 2023; pp. 83–98.
64. Raj, K.; Raj, K. International Journal of Creative Research Thoughts (IJCRT). *AI Enabled Internet Med. Things* **2021**, *9*, d578–d602.
65. Rodríguez-Rodríguez, I.; Campo-Valera, M.; Rodríguez, J.-V.; Woo, W.L. IoMT innovations in diabetes management: Predictive models using wearable data. *Expert Syst. Appl.* **2024**, *238 Pt C*, 121994. [\[CrossRef\]](#)
66. Rodríguez-Rodríguez, I.; Campo-Valera, M.; Rodríguez, J.-V. Forecasting glycaemia for type 1 diabetes mellitus patients by means of IoMT devices. *Internet Things* **2023**, *24*, 100945. [\[CrossRef\]](#)
67. Prasad, S.J.S.; Devi, R.M.; Keerthika, P.; Suresh, P.; Arokiaaraj, A.R.M.; Sangeetha, M. From Remote Monitoring to Personalized Care: A Review of IoT-Based Patient Engagement Solutions in Healthcare. In *Convergence of Blockchain and Internet of Things in Healthcare*; Rana, A.K., Sharma, V., Rana, A., Alam, M., Tripathi, S.L., Eds.; CRC Press: Boca Raton, FL, USA, 2024; p. 26.
68. Wang, A.; Redington, L.; Steinmetz, V.; Lindeman, D. The ADOPT Model: Accelerating Diffusion of Proven Technologies for Older Adults. *Ageing Int.* **2011**, *36*, 29–45. [\[CrossRef\]](#)
69. Hicks, L.L.; Fleming, D.A.; Desaulnier, A. The Application of Remote Monitoring to Improve Health Outcomes to a Rural Area. *Telemed. e-Health* **2009**, *15*, 664–671. [\[CrossRef\]](#) [\[PubMed\]](#)
70. Botsis, T.; Demiris, G.; Pedersen, S.; Hartvigsen, G. Home telecare technologies for the elderly. *J. Telemed. Telecare* **2008**, *14*, 333–337. [\[CrossRef\]](#)
71. Chiang, L.-C.; Chen, W.-C.; Dai, Y.-T.; Ho, Y.-L. The effectiveness of telehealth care on caregiver burden, mastery of stress, and family function among family caregivers of heart failure patients: A quasi-experimental study. *Int. J. Nurs. Stud.* **2012**, *49*, 1230–1242. [\[CrossRef\]](#) [\[PubMed\]](#)
72. Jain, S.S.; Kothari, S.M.; Agrawal, S.K. The Role of IoMT Technologies in Revolutionizing Healthcare. In *WSN and IoT*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2024; p. 16.
73. Fuior, R.; Sălceanu, A.; Luca, C.; Corciovă, C. *Application of Internet of Things (IoT) in Biomedicine: Challenges and Future Directions*; IntechOpen: London, UK, 2023.
74. Jolfaei, A.A.; Aghili, S.F.; Singelee, D. A Survey on Blockchain-Based IoMT Systems: Towards Scalability. *IEEE Access* **2021**, *9*, 148948–148975. [\[CrossRef\]](#)
75. Firouzi, F.; Jiang, S.; Chakrabarty, K.; Farahani, B.; Daneshmand, M.; Song, J.S.; Mankodiya, K. Fusion of IoT, AI, Edge–Fog–Cloud, and Blockchain: Challenges, Solutions, and a Case Study in Healthcare and Medicine. *IEEE Internet Things J.* **2023**, *10*, 3686–3705. [\[CrossRef\]](#)
76. Kumar, M.; Chand, S. MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic. *J. Netw. Comput. Appl.* **2021**, *179*, 102975. [\[CrossRef\]](#)
77. Padmavilochanan, D.; Pathinarupothi, R.K.; Menon, K.U.; Kumar, H.; Guntha, R.; Ramesh, M.V.; Rangan, P.V. Personalized diabetes monitoring platform leveraging IoMT and AI for non-invasive estimation. *Smart Health* **2023**, *30*, 100428. [\[CrossRef\]](#)
78. Ali, A.; Al-rimy, B.A.S.; Alsubaei, F.S.; Almazroi, A.A.; Almazroi, A.A. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors* **2023**, *23*, 6762. [\[CrossRef\]](#) [\[PubMed\]](#)
79. Rafique, W.; Khan, M.; Khan, S.; Ally, J.S. SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things. *Wirel. Commun. Mob. Comput.* **2023**, *2023*, 2558469. [\[CrossRef\]](#)
80. Pradhan, B.; Das, S.; Roy, D.S.; Routray, S.; Benedetto, F.; Jhaveri, R.H. An AI-Assisted Smart Healthcare System Using 5G Communication. *IEEE Access* **2023**, *11*, 108339–108355. [\[CrossRef\]](#)
81. Tahir, A.; Chen, F.; Khan, H.U.; Ming, Z.; Ahmad, A.; Nazir, S.; Shafiq, M. A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. *Sensors* **2020**, *20*, 5392. [\[CrossRef\]](#)
82. Kaur, R.; Chana, I.; Bhattacharya, J. Data deduplication techniques for efficient cloud storage management: A systematic review. *J. Supercomput.* **2018**, *74*, 2035–2085. [\[CrossRef\]](#)
83. Yoosuf, M.S.; Anitha, R. Low Latency Fog-Centric Deduplication Approach to Reduce IoT Healthcare Data Redundancy. *Wirel. Pers. Commun.* **2022**, *126*, 421–443. [\[CrossRef\]](#)
84. Ahmed, S.F.; Alam, M.S.B.; Afrin, S.; Rafa, S.J.; Rafa, N.; Gando, A.H. Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Inf. Fusion* **2024**, *102*, 102060. [\[CrossRef\]](#)
85. Alzahrani, F.A.; Ahmad, M.; Ansari, T.J. Towards Design and Development of Security Assessment Framework for Internet of Medical Things. *Appl. Sci.* **2022**, *12*, 8148. [\[CrossRef\]](#)
86. Sun, Y.; Lo, F.P.-W.; Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access* **2019**, *7*, 183339–183355. [\[CrossRef\]](#)
87. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. *Sensors* **2022**, *22*, 5517. [\[CrossRef\]](#)
88. Blazeska-Tabakovska, N.; Bocevska, A.; Jolevski, I.; Ristevski, B.; Beredimas, N.; Kilintzis, V.; Maglaveras, N.; Savoska, S. Implementation of Cloud-Based Personal Health Record Integrated with IoMT. *UKLO Repos.* **2021**, *2933*, 178–188.

89. Magnusson, R.S. The Changing Legal and Conceptual Shape of Health Care Privacy. *J. Law Med. Ethics* **2004**, *32*, 680–691. [[CrossRef](#)] [[PubMed](#)]
90. Jegatheswaran, R.A.; Sakira, I.J.; Rahman, N.A.A. A Review on IoMT device Vulnerabilities and Countermeasures. *J. Phys. Conf. Ser.* **2020**, *1712*, 012020. [[CrossRef](#)]
91. Srivastava, J.; Routray, S.; Waris, M.M.; Ahmad, S. Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress. *Comput. Intell. Neurosci.* **2022**, *2022*, 7218113. [[CrossRef](#)] [[PubMed](#)]
92. Mika, H.; Pattama, P.; Khalid, A.; Niko, P.; Jack, R. Detecting depression in thai blog posts: A dataset and a baseline. In Proceedings of the Seventh Workshop on Noisy User-Generated Text (W-NUT 2021), Online, 11 November 2021.
93. Bury, T.M.; Sujith, R.I.; Pavithran, I.; Scheffer, M.; Lenton, T.M.; Anand, M.; Bauch, C.T. Deep learning for early warning signals of tipping points. *Proc. Natl. Acad. Sci. USA* **2021**, *118*, e2106140118. [[CrossRef](#)] [[PubMed](#)]
94. Baseer, K.; Sivakumar, K.; Veeraiah, D.; Chhabra, G.; Lakineni, P.K.; Pasha, M.J.; Gandikota, R.; Harikrishnan, G. Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease. *Biomed. Signal Process. Control* **2024**, *92*, 105988. [[CrossRef](#)]
95. Centobelli, P.; Cerchione, R.; Del Vecchio, P.; Oropallo, E.; Secundo, G. Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Inf. Manag.* **2022**, *59*, 103508. [[CrossRef](#)]
96. Kumari, K.A.; Padmashani, R.; Varsha, R.; Upadhayay, V. Securing Internet of Medical Things (IoMT) Using Private Blockchain Network. In *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*; Springer: Cham, Switzerland, 2019; pp. 305–326.
97. Ali, A.; Pasha, M.F.; Guerrieri, A.; Guzzo, A.; Sun, X.; Saeed, A.; Hussain, A.; Fortino, G. A Novel Homomorphic Encryption and Consortium Blockchain-Based Hybrid Deep Learning Model for Industrial Internet of Medical Things. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2402–24183. [[CrossRef](#)]
98. Rehman, A.; Saba, T.; Haseeb, K.; Marie-Sainte, S.L.; Lloret, J. Energy-Efficient IoT e-Health Using Artificial Intelligence Model with Homomorphic Secret Sharing. *Energies* **2021**, *14*, 6414. [[CrossRef](#)]
99. Vovk, O.; Pih, G.; Ross, P. Methods and tools for healthcare data anonymization: A literature review. *Int. J. Gen. Syst.* **2023**, *52*, 326–342. [[CrossRef](#)]
100. Oh, J.; Lee, K. Data De-identification Framework. *Comput. Mater. Contin.* **2023**, *74*, 3579–3606. [[CrossRef](#)]
101. Alhaqbani, B.; Fidge, C. Access Control Requirements for Processing Electronic Health Records. In Proceedings of the Business Process Management Workshops, BPM 2007, Brisbane, Australia, 24 September 2007; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 4928, pp. 371–382.
102. Khan, J.A. *Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)*; IGI Global: Hershey, PA, USA, 2024; p. 14.
103. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [[CrossRef](#)]
104. Saxena, D.; Verma, J.K. 4—Blockchain for public health: Technology, applications, and a case study. In *Computational Intelligence and Its Applications in Healthcare*; Academic Press: Cambridge, MA, USA, 2020; pp. 53–61.
105. Urkude, S.V.; Sharma, H.; Kumar, S.U.; Urkude, V.R. Anatomy of Blockchain Implementation in Healthcare. In *Blockchain Technology: Applications and Challenges*; Springer: Cham, Switzerland, 2021; Volume 203, pp. 51–76.
106. Kotronis, C.; Routis, I.; Politi, E.; Nikolaidou, M.; Dimitrakopoulos, G.; Anagnostopoulos, D.; Amira, A.; Bensaali, F.; Djelouat, H. Evaluating Internet of Medical Things (IoMT)-Based Systems from a Human-Centric Perspective. *Internet Things* **2019**, *8*, 100125. [[CrossRef](#)]
107. Roy, T.; Nahid, M.M. The IoMT and Cloud in Healthcare: Use, Impact and Efficiency of Contemporary Sensor Devices Used by Patients and Clinicians. In Proceedings of the ICCA'22: Proceedings of the 2nd International Conference on Computing Advancements, Dhaka, Bangladesh, 10–12 March 2022.
108. Indumathi, J.; Shankar, A.; Ghalib, M.R.; Gitanjali, J.; Hua, Q.; Wen, Z.; Qi, X. Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS). *IEEE Access* **2020**, *8*, 216856–216872. [[CrossRef](#)]
109. El-Rashidy, N.; El-Sappagh, S.; Islam, S.M.R.; El-Bakry, H.M.; Abdelrazek, S. Mobile Health in Remote Patient Monitoring for Chronic Diseases: Principles, Trends, and Challenges. *Diagnostics* **2021**, *11*, 607. [[CrossRef](#)] [[PubMed](#)]
110. Hatzivasilis, G.; Soutatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT). In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019.
111. Hajiheydari, N.; Delgosha, M.S.; Olya, H. Scepticism and resistance to IoMT in healthcare: Application of behavioural reasoning theory with configurational perspective. *Technol. Forecast. Soc. Chang.* **2021**, *169*, 120807. [[CrossRef](#)]
112. Tsai, T.-H.; Lin, W.-Y.; Chang, Y.-S.; Chang, P.-C.; Lee, M.-Y. Technology anxiety and resistance to change behavioral study of a wearable cardiac warming system using an extended TAM for older adults. *PLoS ONE* **2020**, *15*, e0227270. [[CrossRef](#)] [[PubMed](#)]
113. Falcone, F.; Astrain, J.J.; Aguirre, I.; Trigo, J.D.; Serrano, L. Future Wireless Communication Systems to Enable IoMT Services and Applications. In *Smart and Secure Internet of Healthcare Things*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2022; p. 22.
114. Abdulbaqi, A.S.; Obaid, A.J.; Alazawi, S.A.H. A Smart System for Health Caregiver Based on IoMT: Toward Tele-Health Caregiving. *Int. J. Online Biomed. Eng.* **2021**, *17*, 70–87. [[CrossRef](#)]
115. Razdan, S.; Sharma, S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [[CrossRef](#)]

116. Saha, J.; Sen, R. IoT vs IoMT—A comparative study based on knowledge among medical professionals. *Int. J. Multidiscip. Educ. Res.* **2024**, *13*, 99–109.
117. Adarsha, A.S.; Reader, K.; Erban, S. User Experience, IoMT, and Healthcare. *AIS Trans. Hum. Comput. Interact.* **2019**, *11*, 264–273.
118. Gorrepati, R.R.; Jonnala, P.; Guntur, S.R.; Kim, D.-H. Semantic Web of Things for Healthcare Interoperability using IoMT Technologies. In *Semantic Technologies for Intelligent Industry 4.0 Applications*, 1st ed.; Patel, A., Debnath, N.C., Eds.; River Publishers: New York, NY, USA, 2023; p. 34.
119. Pradyumna, G.R.; Hegde, R.B.; Bommegowda, K.B.; Jan, T.; Naik, G.R. Empowering Healthcare with IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges. *IEEE Access* **2024**, *12*, 20603–20623. [[CrossRef](#)]
120. Jaleel, A.; Mahmood, T.; Hassan, M.A.; Bano, G.; Khurshid, S.K. Towards Medical Data Interoperability Through Collaboration of Healthcare Devices. *IEEE Access* **2020**, *8*, 132302–132319. [[CrossRef](#)]
121. Abdelouahid, R.A.; Debauche, O.; Mahmoudi, S.; Marzak, A. Literature Review: Clinical Data Interoperability Models. *Information* **2023**, *14*, 364. [[CrossRef](#)]
122. Chiahhsu, Y.; Tzu-Chuan, C.; Yen-Hung, C. Bridging digital boundary in healthcare systems—An interoperability enactment perspective. *Comput. Stand. Interfaces* **2019**, *62*, 43–52.
123. Suryateja, P.S.; Reddi, S.; Murty, P.S.R.; Naresh, V.S. Internet of things in healthcare: Architecture, applications, challenges, and solutions. *Comput. Syst. Sci. Eng.* **2020**, *35*, 411–421.

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.