

# A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations

Huda Hussein Mohamad Jawad <sup>1,\*</sup>, Zainuddin Bin Hassan <sup>1</sup>, Bilal Bahaa Zaidan <sup>2</sup>,  
Farah Hussein Mohammed Jawad <sup>3</sup>, Duha Husein Mohamed Jawad <sup>4</sup> and Wajdi Hamza Dawod Alredany <sup>5</sup>

<sup>1</sup> College of Information and Communications Technology, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, Kajang 43000, Malaysia

<sup>2</sup> Future Technology Research Center, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan

<sup>3</sup> Financial and Banking Sciences Department, Faculty of Administration and Economic, University of Babylon, Babylon 51001, Iraq

<sup>4</sup> Information Security Department, College of IT, University of Babylon, Babylon 51001, Iraq

<sup>5</sup> Department of Mathematics, Dhofar University, Salalah 211, Oman

\* Correspondence: [huda.hussein24@gmail.com](mailto:huda.hussein24@gmail.com)

**Abstract:** Internet of things (IoT) has revolutionized how we utilize technology over the past decade. IoT's rapid growth affects several fields, including the healthcare sector. As a result, the concept of smart healthcare or electronic healthcare (e-healthcare) has emerged. Smart healthcare promises to enhance people's lives and wellbeing by monitoring them, offering an efficient connection, improving mobility, gathering medical data, and decreasing hospital and patient costs. IoT in healthcare is still one of the hot and trendy topics that needs in-depth investigation. No recent review has been conducted to elucidate the extent of research in the area, features of published papers, motives, and challenges in enabling IoT in healthcare systems. This study presents a comprehensive systematic review of the screened articles published between 2015 and 2022 pertaining to enabling IoT in healthcare services and applications. A total of 106 papers fulfilled the final inclusion criteria and were analyzed using systematic literature review (SLR). Two procedures were used to review the final articles: First, publications are examined in terms of study designs, publishing journals, and topics/study objectives. In the second approach, motives, challenges, and recommendations for enabling IoT in healthcare systems are explored. This article summarizes published studies on IoT in healthcare systems and its usage in smart healthcare service delivery. Based on the reviewed studies, recommendations for future research to enable the effective application of IoT in healthcare and service delivery are proposed.



**Citation:** Mohamad Jawad, H.H.; Bin Hassan, Z.; Zaidan, B.B.; Mohammed Jawad, F.H.; Mohamed Jawad, D.H.; Alredany, W.H.D. A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations. *Electronics* **2022**, *11*, 3223. <https://doi.org/10.3390/electronics11193223>

Academic Editors:  
Francisco Luna-Perejón, Lourdes Miró Amarante and Francisco Gómez-Rodríguez

Received: 16 August 2022

Accepted: 2 October 2022

Published: 8 October 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 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/>).

**Keywords:** healthcare systems; Internet of Things (IoT); medical system; wellbeing; electronic healthcare; systematic literature review

## 1. Introduction

Smart healthcare is defined as the use of smart devices (such as mobile and electronic devices) to improve disease detection, medical management, and quality of life [1,2]. The concept of intelligent health care is presented when the IoT modules aid the basic roles of the health sector. The IoT has, over several years, been the focus of international interest. Still, the healthcare industry has only recently begun to see the huge opportunities and benefits that could come from using modern and technologically advanced tools, facilities, and relationships with other parts of the industry [2].

Nowadays, many countries consider healthcare services as one of the most significant socio-economic challenges facing both the private and public sectors [3]. Healthcare costs are expected to account for 20 to 30% of the GDP in some countries by 2050 [4]. In recent years, the IoT has become one of the most significant technologies of the 21st century.

Currently, a large population of people can connect with many objects linked to the internet through embedded devices. The importance of the IoT and its benefits can be seen in many fields, such as learning, governance environment, business, and management [5,6].

Given the significant role of IoT in the rapid development and revolutionization of technology, one of the most important disciplines that IoT has penetrated is human life and health. The IoT has paved the way for a variety of medical options: normal medical devices that capture useful additional data on the internet, provide additional information on symptoms and patterns, allow remote therapy to be provided, and typically monitor patients' recoveries and treatments [7,8]. In addition, IoT can easily be adopted by others. It provides access to the healthcare system and storage of data [7,8], while facilitating effective interaction between specialized doctors and medical staff, as well as easy access to patients' data [9], as well as interaction with doctors [7].

IoT has been integrated into healthcare systems mainly in the areas of remote patient monitoring, information collection and transfer in actual time, and end-to-end connectivity. These events allow the automation of patient flows on an organizational level, data and machine communication, interoperability, and essential information analysis [10,11]. In the case of medical diagnostics, IoT has been instrumental in transforming routine medical diagnosis into more patient- and home-centered approaches, compared to the hospital-centered approach [12]. IoT has therefore helped to redefine customary monitoring, diagnostics, treatments and decreasing expenses and detrimental errors [10,12]. However, cost-reduction is one of the significant benefits of IoT-healthcare innovation since the integration of devices and technology reduces operational costs and enhances service quality [5,13–15]. For instance, medical costs were significantly reduced while tenable solutions to minimize communication costs were provided by adopting cloud computing and the application of resource management [16,17]. On the other hand, the provision of IoT-healthcare reduced the number of people visiting clinics and hospitals, thereby reducing the cost burden to patients [7,18]. Given the adverse effects of rising costs on patients [3,19], researchers keep adopting new technologies to facilitate effective cost reduction [3,20] and provide a path to a healthy life with low cost [21].

Several topics have been studied in the context of IoT-healthcare, and issues related to the system and users have been raised. However, no recent review is available to elucidate the various investigations and integration of IoT in healthcare systems and service delivery, as well as the contemporary challenges and proposed solutions as presented in diverse publications. The purpose of this systematic review is to (A) provide an in-depth classification and distribution of articles published in the last few years, focusing on the application of IoT in healthcare systems and service delivery; and (B) to investigate the enabling of IoT in healthcare services with respect to motivations, challenges, and recommendations. This review aimed to achieve the mentioned objectives by using a systematic literature review (SLR) protocol.

The paper is organized as follows: An introduction about IoT technology in healthcare is discussed in Section 1. The used systematic review protocol is discussed with details in Section 2. Motivations, challenges, and recommendations are described with details in Section 3. Furthermore, limitation and conclusion are included in Section 4.

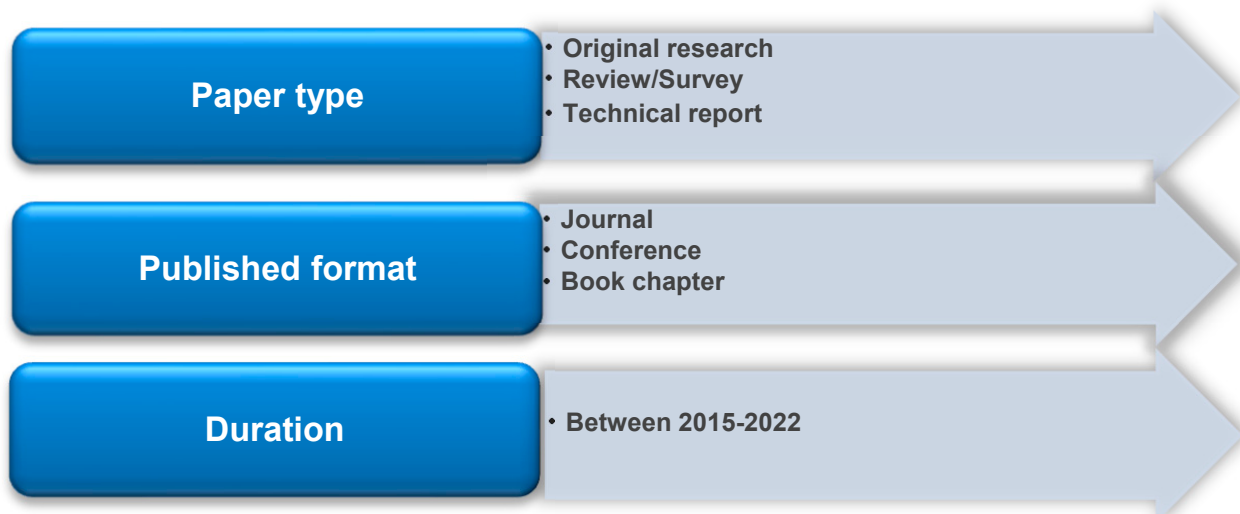
## 2. Systematic Review Protocol

The IoT is one of the new technologies that needs its own software and hardware. Therefore, the growth rate of this technology is not the same in different countries. Therefore, each community has tried to use this technology to the best of its ability. For this reason, this technology is used with varying degrees of quality and quantity in health services in different countries. Therefore, in this section, an attempt is made to show the authors' neutrality in the selection of articles, the breadth of the countries under study, and the authors' neutrality in introducing challenges by presenting a protocol for systematic review. For a more efficient and authentic review, this study followed a systematic review protocol that is commonly regarded as high-quality evidence [22].

This approach was adopted to fulfill the best method of answering the research questions developed in this study. The SLR Protocol entails scientific reasoning, the development of a hypothesis, and a systematic arrangement of techniques applied in the review article. Additionally, the SLR protocol was set up before the onset of the review and utilized as a guide in the review process. Its aim is to distinguish and synthesize all the scholarly research on a particular topic. The systematic review method is defined in an unbiased and reproducible manner to identify policies that can identify research gaps. To enable repeatability and prove a fair comparison, each review step is reported, including the search and article selection steps. Therefore, in this section, the criteria for selecting articles and journals as well as the diversity distribution of authors and countries are described.

### 2.1. Inclusion Criteria for Selecting Articles

The period of the search was specified between 2015 and 2022. This search period was selected because IoT is still relatively new, and its application can be traced back to 2009. In addition, only a few studies on IoT were published before 2015, and the selected period will provide recent and new achievements on the current trend in IoT and healthcare. The inclusion criteria were specified to be articles of all types (e.g., review, empirical, conceptual, conference proceedings etc.). The reviewed articles included various types of studies related to IoT healthcare services, comprising empirical studies which analyzed primary data using either quantitative, qualitative, or mixed methods to answer specific research questions. The second type was review studies, which are studies that explain and analyze the methodology and results of one or more previous studies as it shown in Figure 1.



**Figure 1.** Inclusion criteria for selecting articles.

### 2.2. Database Selection Process

The databases used for the systematic literature search were IEEE, Web of Science (WoS), and Science Direct. Briefly, the study selection procedure entailed the creation of a query using specific keywords into two parts. The first and second parts relate to healthcare and IoT terms, respectively. Both aspects were combined by using the term “AND” operator as shown in Figure 2. Upon retrieving the articles from the literature search, the titles and abstracts were used to filter them, followed by reading the full text before analysis.

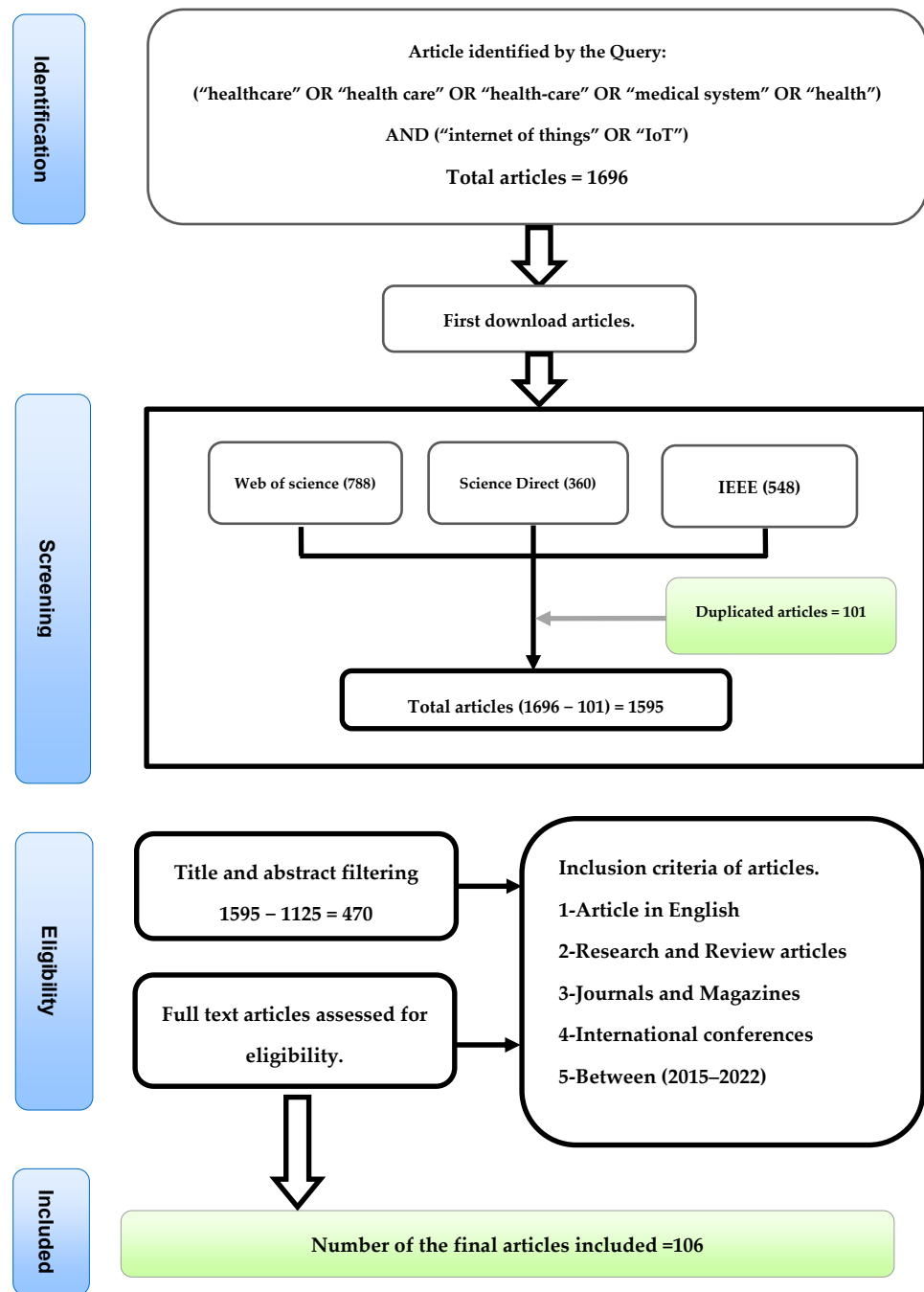


Figure 2. Selection of study, search query and inclusion criteria.

2.3. Search Results

In the identification process, 106 articles were retrieved from three databases: IEEE, Web of Science (WoS), and Science Direct. After eliminating duplicate records and articles with irrelevant topics and abstracts, 470 studies were retained for screening. Upon completing the screening, 207 articles were excluded because they were either irrelevant or full texts were unavailable; 263 relevant articles were retained. All the 263 articles were checked for eligibility and 106 were considered to fulfill the study objective, relevant to the topic, and mentioned either the motivations, challenges, and recommendations for enabling IoT in the healthcare system. It means that 106 studies met the inclusion measures and were selected to be included in this paper (Figure 2).

#### 2.4. Distribution of Research Articles

The distribution of research articles that were included in the final analysis is discussed in this sub-section. They are selected based on the following areas: (1) publication’s year, (2) countries, (3) study designs, (4) publishing journal, (5) publishers, and (6) main topics/research objectives. In order to provide detailed information about the distribution of the studies, some of the aspects, such as the year of publication and types of studies, were compared.

##### 2.4.1. Distribution of Papers in Terms of Publication’s Year

Figure 3 shows the number of studies published between 2015 and 2022 in terms of percentage. Of the studies included in this review, most of them were published in 2018 ( $n = 35$ ), followed by 2017 ( $n = 19$ ) and 2019 ( $n = 19$ ).

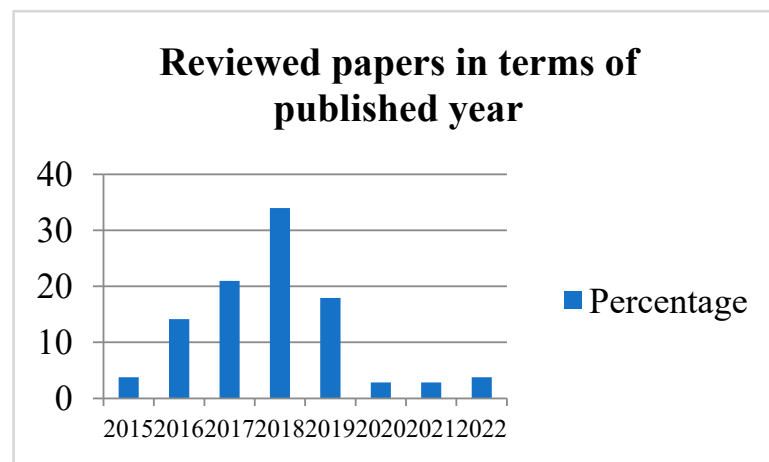


Figure 3. Distribution of articles in terms of the year of publication.

##### 2.4.2. Distribution of Papers in Terms of Study Designs/Methodologies

Figure 4 depicts the distribution of research articles in terms of methods or study types. Most of the studies were experimental ( $n = 77$ ), followed by review articles ( $n = 17$ ), empirical research ( $n = 7$ ) and surveys ( $n = 3$ ). Only one study was published as metadata. This distribution reflects the trend of research activities in the application of IoT in the healthcare system.

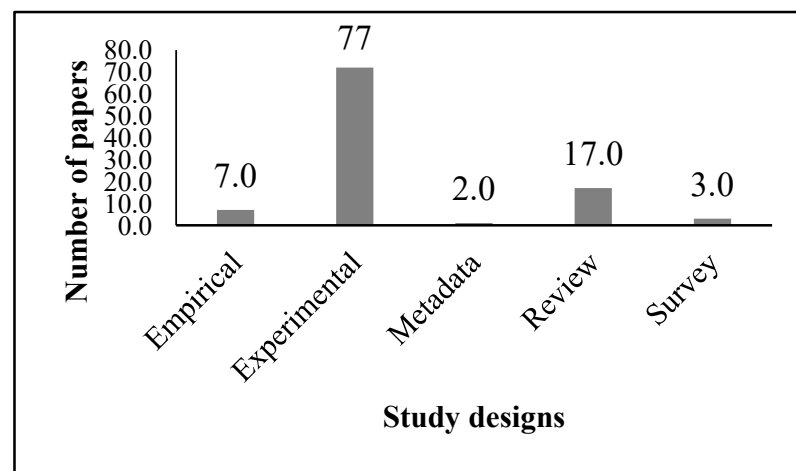
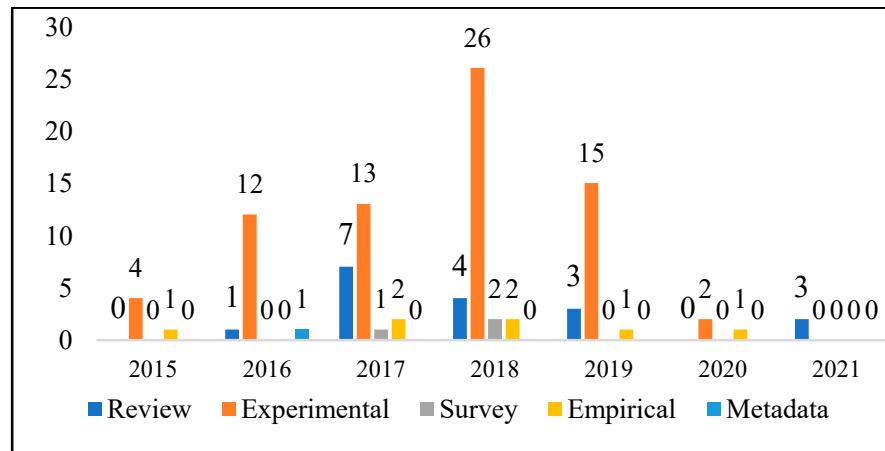


Figure 4. Distribution of articles according to study design/methodology.

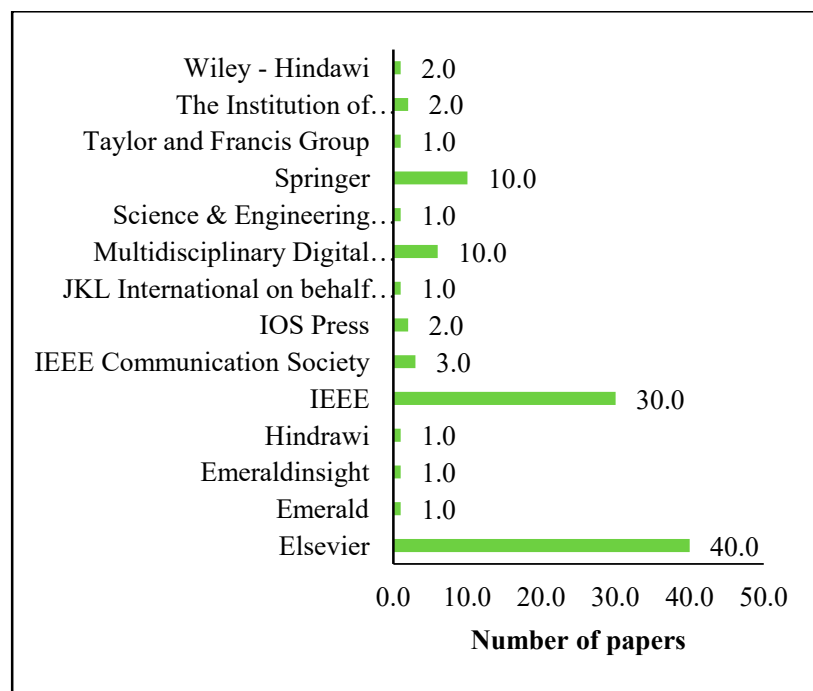
The majority of research articles published from 2016 to 2019 were experimental studies Figure 5, except in 2017, where seven review articles and 13 experimental studies

were published. The number of empirical studies was almost equally distributed across each year from 2015 to 2020.



**Figure 5.** Distribution of papers in terms of comparison between the year of publication and study designs.

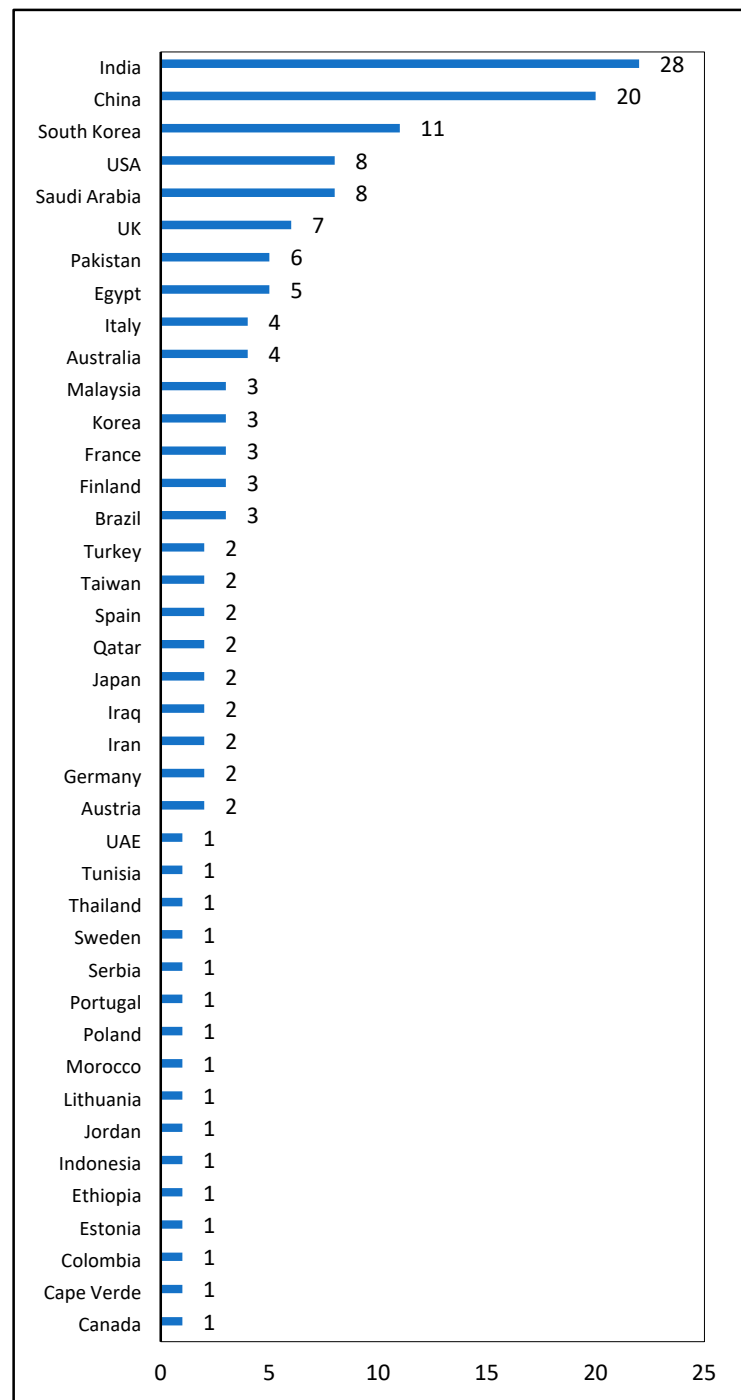
The various publishers of the articles that were considered for this review are outlined in detail in Figure 6 below. Most studies were published by Elsevier ( $n = 40$ ), followed by IEEE ( $n = 30$ ) and Springer ( $n = 10$ ). Less than 10 articles were published by MDPI, IEEE Communication Society, IOS Press, etc.



**Figure 6.** Distribution of articles according to Publishers.

### 2.4.3. Distribution of Papers in Terms of Countries of Origin

Figure 7 illustrates the distribution of articles depending on the countries in which the research was undertaken. Most of the papers originated from the following countries: India ( $n = 22$ ), China ( $n = 20$ ), South Korea ( $n = 11$ ), the United States ( $n = 8$ ) and the United Kingdom (6).



**Figure 7.** Distribution of studies based on country of origin.

#### 2.4.4. Distribution of Papers in Term of Publishing Sources

Table 1 shows the number of research articles in terms of published journal titles. In the last 7 years (2015–2022), the majority of relevant studies were published in IEEE Access ( $n = 17$ ), followed by Future Generation Computer Systems ( $n = 9$ ), IEEE Internet of Things Journal ( $n = 7$ ) and Procedia Computer Science ( $n = 4$ ). Other journals presented in Table 1 have published related articles between 2015 and 2021 with fewer than three cases.

**Table 1.** Distribution of papers in terms of publishing sources.

S/N	Journal Name	Number of Papers	Related References
1	IEEE Access	16	[3,5,7,8,16,23–34]
2	Future Generation Computer systems	9	[25,35–42]
3	IEEE Internet of things journal	7	[13,43–48]
4	Sensors	5	[49–53]
5	Procedia Computer Science	4	[11,19,54,55]
6	Computer Networks	3	[14,56,57]
7	IEEE communications magazine	3	[58–60]
8	Wireless communications and mobile computing	3	[10,61,62]
9	Journal of medical systems	3	[63,64]
10	Journal of Network and computer applications	2	[65,66]
11	Fundamental Informatics	2	[67,68]
12	Computer and Electrical Engineering	2	[69,70]
13	Big Data Research	2	[4,71]
14	Sustainability	2	[72,73]
15	IET networks	2	[74]
16	Computer Applications in Engineering Education	1	[75]
17	Smart and Sustainable Built	1	[2]
18	Ageing and Disease	1	[76]
19	Applied Sciences	1	[77]
20	Artificial Intelligence in Medicine	1	[78]
21	Cluster Computing	1	[79]
22	Computer Methods and Programs in Biomedicine	1	[80]
23	Computers in Human Behavior	1	[81]
24	Computers in Industry	1	[82]
25	Global Health Journal	1	[83]
26	Health Technology	1	[84]
27	IEEE Internet Computing	1	[85]
28	IEEE SYSTEMS JOURNAL	1	[86]
29	IEEE Transactions on Emerging Topics in Computational Intelligence	1	[87]
30	IEEE Transactions on Industrial Informatics	1	[88]
31	IEEE Transactions on Network Science and engineering	1	[89]
32	IEEE Transactions on Professional communication	1	[90]
33	IET Software	1	[91]
34	International Federation of Automatic Control	1	[20]
35	Security and communication networks	1	[92]
Conference Paper			
36	International Journal of Production Economics	1	[93]
37	International Journal of Security and Its	1	[94]

In the last 7 years (2015–2022), the majority of relevant studies were published in IEEE Access ( $n = 16$ ), Future Generation Computer Systems journal ( $n = 9$ ) and IEEE Internet of things ( $n = 7$ ).



#### 2.4.5. Distribution of Papers in Terms of Research Purpose/Objectives

Figure 8 shows the distribution of the articles according to the main topics and research objectives. The majority of the articles focused on remote health monitoring ( $n = 24$ ), followed by security and privacy ( $n = 17$ ), smart healthcare ( $n = 16$ ), technology acceptance ( $n = 8$ ), and fog computing ( $n = 7$ ). A total of five articles focused on the application of IoT for disease/medical diagnoses (diabetes, cardiac conditions, hypertension, etc.), whereas less than five articles were based on big data analytics and mobile healthcare. Research topics such as edge computing, living labs, and network layers were classified under “others,” while review articles and studies that were overly broad were classified as “non-specific.”

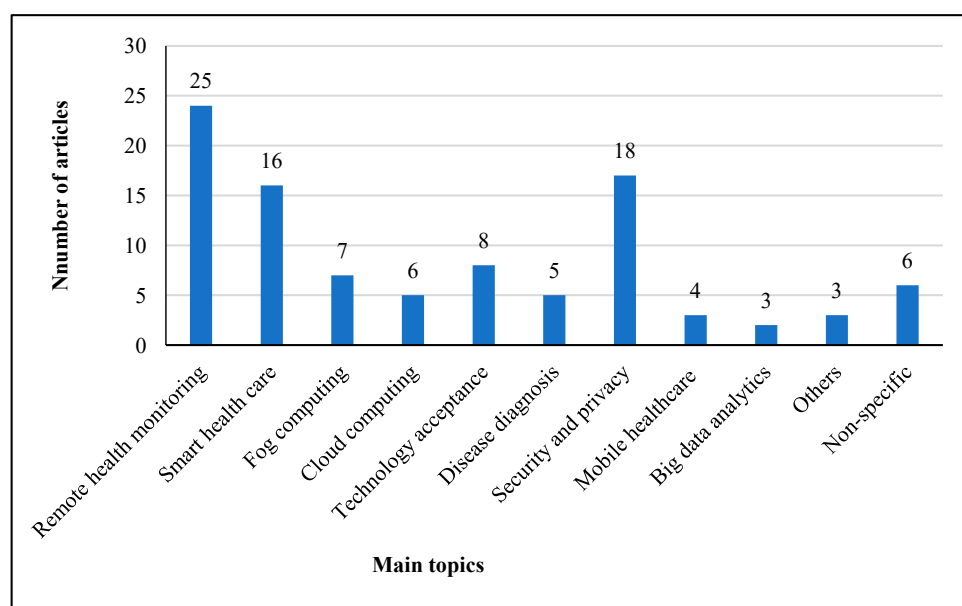


Figure 8. Distribution based on research purpose/objectives.

### 3. The Motivations, Challenges and Recommendations

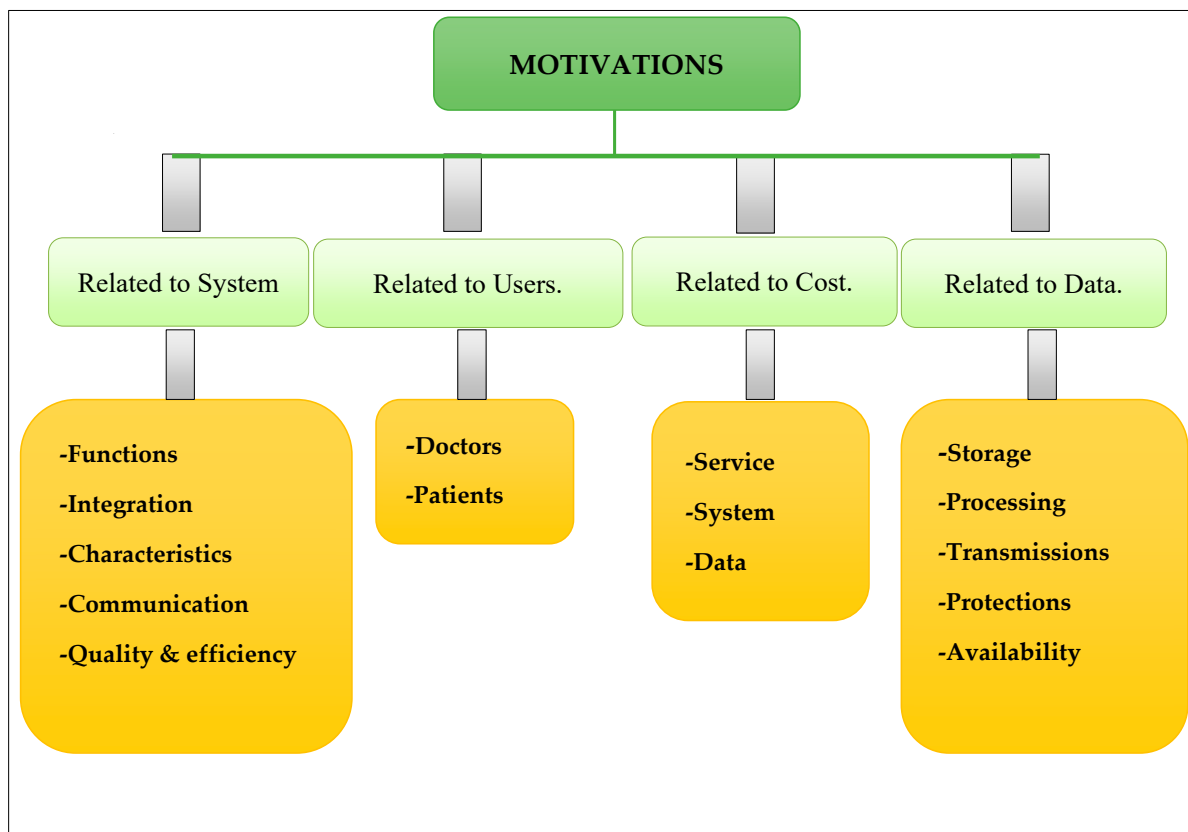
The concept of IoT is related to various technologies and sciences such as sensors, artificial intelligence, deep learning, machine learning, and decision-making, most of which are effectively integrated into the healthcare system. This systematic literature review presents the most relevant studies related to smart technology represented by the IoT. This review sheds light on how IoT imposes its control on the healthcare sector in all departments, and how the existence of such technology has made it easier for patient-doctor interaction and communication, as well as in terms of hospital management, diagnosis, and storage of huge amounts of data (about the patients, hospital staff, drugs, and equipment). Besides facilitating better diagnosis, IoT has a role in delivering appropriate treatment for each case and using devices or sensors for real-time weather monitoring. The remainder of the review is divided into three main aspects: (A) motivation, (B) challenges, and (C) recommendation, concerning the application of IoT in the healthcare system and service delivery. Each aspect is further classified into subgroups and the discussion is tailored towards assisting future researchers to have a clear view of the challenges in enabling IoT in healthcare systems, how the problems have been solved and those that remain unsolved, as well as the need to find better and more tenable solutions.

#### 3.1. Motivations

This section displays all the motivations for the research conducted in the present era. The reviewed articles are shown below in Figure 9, which are classified as follows:

1. Motivations related to the main components of healthcare system such as functions, process, integration, properties, resources, quality, and efficiency, communications;

2. Motivations related to users;
3. Motivations related to cost (system, data and maintenance);
4. Motivations related to data (storage, processing, transmissions, protection, and availability).



**Figure 9.** Categorized Motivations sections.

### 3.1.1.1. Motivations Related to System

This section focuses on system issues as an incentive. The first is related to functions such as monitoring, detection, computing, and protection, while the others are related to integration in terms of ease of use and the need for different devices and technologies. In addition, it includes system features that consist of different areas such as security, privacy, reliability, flexibility, accessibility, mobility, wireless, and wearability, followed by resources such as unlimited use and information sharing. On the other hand, accurate information communications focus on low latency, connectivity, and transmission at all times, as well as incentives to increase system quality and efficiency. In the following sections, each of the motivational factors related to the system is explained.

**1-Motives related to functions.** The potential of combining advanced technology has encouraged many researchers to develop internet of medical things (IoMT) platforms, including in the field of remote monitoring [26,64]. In addition, several reasons that increase the interest in remote monitoring include limited availability of specialist doctors, difficulty in navigating some remote areas, traffic jams, and patients' being unable to visit the hospital or doctors due to busy schedules [27,46]. For example, a voice pathology detection system on the mobile healthcare framework is proposed. In their proposed framework, sounds are first recorded using smart mobile devices, and the same audio signals are processed before being transmitted to a deep learning network [27]. The proposed remote healthcare system is shown in Figure 10.

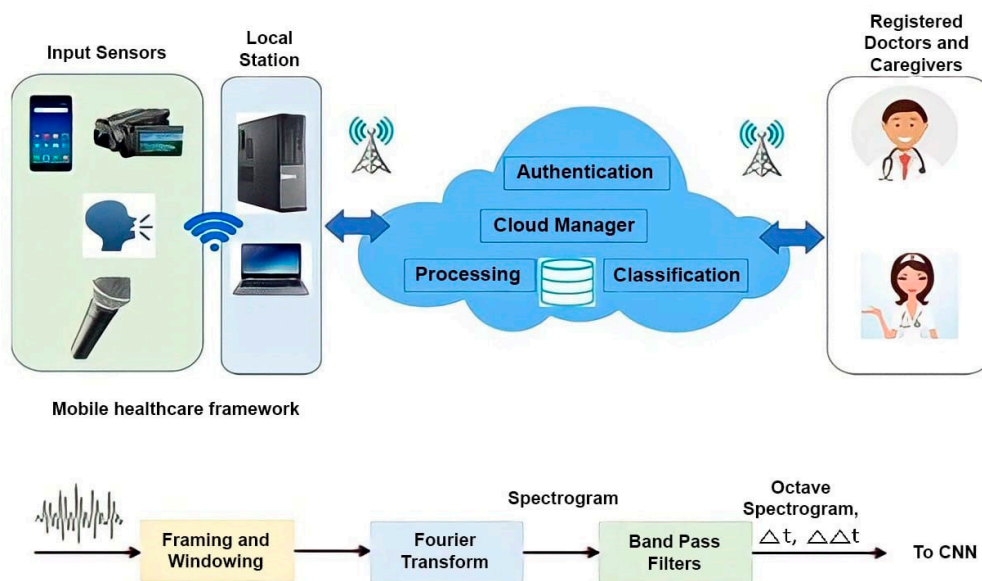


Figure 10. The proposed remote healthcare framework in.

Since the number of people over 60 will grow in the next few years [24], there is a need for better health care in remote areas with facilities for continuous monitoring. This has been specifically advocated to monitor food quality, diet, daily exercise, and physiological status and to enhance the well-being of the elderly population and others requiring such care [1,67]. Likewise, several researchers have demonstrated the urgent need to develop real-time monitoring due to the increase in the number of disabled people and those with chronic diseases [48,57].

Another point related to function is diagnosis. IoT in healthcare supports early diagnosis to help patients obtain better care [15,75], and the provision of real-time diagnosis helps to minimize the cost of visiting hospitals and save lives [34,44,63,95]. In addition, the early detection of some diseases prevents the spread of such outbreaks; thereby leading to improved life expectancy in the long term [85,96]. The third function in this review is computing. Computing is an advanced, flexible, and better way to collect and analyze personal health data [49,85]. Therefore, healthcare today depends on IT. The last function is protection, which entails how to protect information from unauthorized access. This is particularly important when information is shared online between the patient and the doctor [57,84].

**2-Motives related to integration.** This section aims to explain the role of integration in technologies or devices. Additionally, it aims to discuss how it would improve service delivery. For example, integration of IoTs with cloud and how it may facilitate the delivery [16]. The integration of different devices creates new opportunities to improve service in the fields of healthcare [13]. Because more devices can share information with other devices (IoT), this improves access to healthcare [11].

**3-Motives related to characteristics.** These motivations include several areas such as security, privacy, reliability, flexibility, accessibility, mobility, wireless, etc. When a new technology is used in the field of health, the security of devices and servers is a serious challenge for the user. Researchers generally consider security in areas such as the IoT secure system [16,70,97], secure connection [54], and information sharing to enhance system quality [86]. Besides providing privacy levels for users [34,88], the system should also ensure the reliability of IoT systems [19], flexibility, easy access, mobility, and wireless interconnection between sensors. It would also be helpful to have a smart device that can be worn on the body to make monitoring easier [45,54].

**4-Motives related to communications.** In relation to communications, IoT in healthcare emphasizes two vital aspects: traffic and latency. These two factors are directly

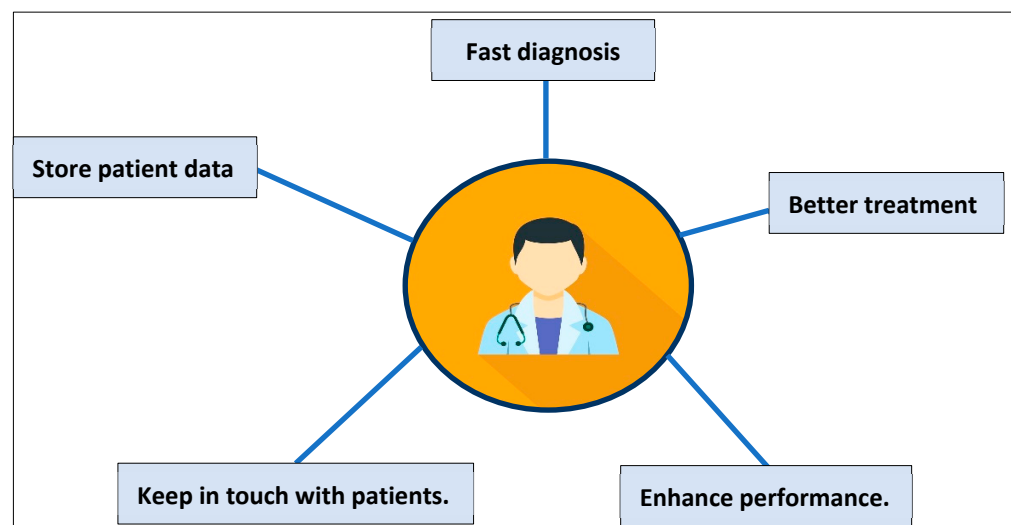
proportional and share a positive relationship. For instance, the reduction in traffic jams led to a proportional decrease in latency, which remains the main focus of most researchers, especially in emergencies. This is because any delay in communication or response time will have a detrimental effect on the patient [29,47,88]. Some researchers suggest using cloud-based systems or fog computing to reduce the delay [30,98]. These systems are available in each location and every time, so new healthcare paradigms and services are born.

**5-Motives Related to quality and efficiency.** In recent years, the average age of people in different societies has increased, so many researchers have tried to offer new approaches and technologies for long-term applications in smart healthcare systems [11,84,99]. This has revived the need for effective management of several aspects of providing high quality healthcare services, such as providing high levels of connectivity, ensuring users have access to services anywhere and anytime, and ensuring that the company has full control over its connections to prevent breakage or unwanted attack [60]. Other important functions are the provision of high-quality error correction capabilities to verify that the message sent is similar to the message received, as well as high availability to ensure that messages are delivered at the same time [4]. Some researchers focus on achieving efficiency, better tracking of patients and devices, prompt service, and increased safety [37,86]. Moreover, researchers have highlighted that despite the importance of safety, it has received less attention in research studies and is largely under-reported [91]. However, some studies attempted to use radio frequency identification (RFID) to address a variety of issues to improve the quality of healthcare systems [93] and provide a means of providing time-sensitive and efficient services [82]. In addition, some researchers have tried to offer technologies for patient-centered medical treatment at home instead of hospital treatment in order to reduce the cost of medical care and increase treatment outcomes [76], which has been projected to affect patients' lives positively in coming years [2].

### 3.1.2. Motivations Related to Users

This section is divided into doctors, and patients.

**1-Doctors.** As demonstrated in Figure 11, using IoT in healthcare systems offers several advantages and benefits to doctors in the performance of their duties. Among the advantages are the best-coordinated care and the storage of patients' sensitive data, to assist the understanding of their medical history and to deliver fast, accurate diagnosis and treatment [7,18,50,62]. The introduction of intelligent technology in the field of healthcare enables doctors to enhance their performance, improving efficiency and reliability in operations and allowing for subsequent remote monitoring [80,83]. It also promotes communication with patients through the use of specialized software [4,85].



**Figure 11.** The benefit of smart healthcare to doctors.

**2-Patients.** Due to the obvious rise in the elderly population and patients with chronic diseases, there is a need to develop new technologies and models to provide smart health-care services to patients over the long term [11,84]. This includes the provision of efficient treatment [14,23,26], making it easier to manage the treatment process of patients and the ability to provide instant, appropriate treatment to save the patient's life [7,23,37]. In addition, IoT-based health care systems aim to minimize hospital visits and facilitate access to patient data (regardless of location or time) [88]. It also provides constant monitoring of patients [77,99,100].

### 3.1.3. Motivations Related to Cost

Today, health services are one of the most significant social and economic concerns facing both the public and private sectors in many nations. This is due to a variety of factors, including rising medical care costs, steady population growth and aging, and increased health-care demands. Hence, these events highlight the need for new and more advanced scientific solutions [26]. Some statistics show that by 2050, health care spending will account for about 30% of some countries' GDP [4]. Thus, cost is considered as one of the main topics that motivates researchers to participate in research on IoT activation in health care systems and service delivery. The next subsection discusses various aspects of cost.

**1-cost related to service.** The purpose of this section is to examine the incentives for costing healthcare systems and data. From this perspective, in most studies, the two goals of reducing treatment costs and increasing the quality of services are pursued in parallel [7,60,90]. Given that rising costs have significant adverse effects on patients' lives [3,19], some researchers adopt new technologies to help in reducing costs, ensuring cost-effectiveness [3,20], and providing a path to a healthy life at a minimum cost [3].

**2-Cost related to System.** Various strategies have been reported in several studies to reduce healthcare system-related costs, such as the adoption of IT, using of cloud computing, and the application of resource management, which all led to a significant reduction in overall cost [16,93]. In addition, other researchers proposed solutions to reduce the cost of communications, data collection, processing, labeling, and data transmission [26,35,88,96,101].

### 3.1.4. Motivations Related to Data

One of the most widely discussed topics in healthcare data is dealing with the complexity and massive amounts of data that needs to be collected, processed, and analyzed while ensuring effective data security and management [102]. Several studies have been conducted in this area, while other research has focused on different aspects, such as improving the healthcare sector. This section discusses the data-related motivations in terms of data storage, processing, transmission, protection, and availability. Specifically, this involves the exploration of the most advanced technologies in this era, such as IoT and cloud computing, for the collection, storage, and analysis of personal healthcare data [68,85]. It also entails the adoption of new technologies over traditional techniques to meet the vast healthcare system's requirements. For instance, the adoption of fog computing systems reduces the load on cloud computing in terms of processing massive amounts of data [89].

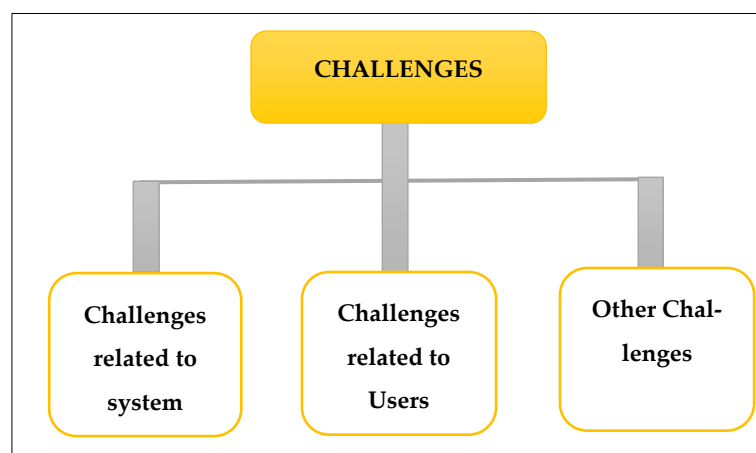
Enabling IoT in healthcare service delivery is addressing a lot of challenges related to data, such as ease of data transfer over the internet and the use of short-range wireless technologies [69]. These data need to be well protected at all stages, comprising collection, storage, communication, and transmission [7,60]. Numerous researchers have emphasized the importance of data privacy and security in healthcare applications [58]. Cloud computing helps in increasing the spectrum of healthcare services. It is associated with some privacy concerns that need to be addressed [101]. In addition, the system must be controlled and secured from unauthorized access while concurrently protecting medical data [42,55]. Furthermore, continuous rapid data growth is critical for improving methods of accessing health information and services [28,75]. The benefits that motivate researchers to examine this area are summarized in Table 2.

**Table 2.** Summary of common motivations.

Category	List of Benefits	References
Motivations Related to System	1- Develop internet of medical things (IoMT) platforms. 2- Improve service in the fields of healthcare. 3- Improve the characteristics of the system such as security, privacy, reliability, flexibility, accessibility, mobility, wireless, etc. 4- Reduce the delay time in communications or response time such as cloud computing and fog computing. 5- Provide new approaches and technologies for long-term applications in smart healthcare systems such as high levels of connectivity, achieving efficiency, better tracking of patients and devices, prompt service, and increased safety	[1–19,24,26,27,29,30,35,37,46,48,49,53,57,58,67,75,76,82,84–86,88,89,91,93,95,96,98,99]
Motivations Related to Users	1- Enable doctors to enhance their performance. 2- Improve efficiency and reliability in operations and allow subsequent remote monitoring 3- Promote communication with patients using specialized software. 4- Minimize hospital visits and facilitate access to patient data (regardless of location or time). 5- Provide constant monitoring of patients.	[3,4,7,11,14,18,23,37,62,77,85,88,99,100]
Motivations Related to Cost	1- Reduce treatment costs and increasing the quality of services in parallel. 2- Adopt new technologies to help in reducing costs and providing a way to a healthy life at a minimum cost. 3- Reduce the cost of communications, data collection, processing, labeling, and data transmission.	[3,4,7,16,19,20,26,35,60,90,93,96,101]
Motivations Related to Data	1- Reduce the load on cloud computing in terms of processing massive amounts of data. 2- Continuous rapid data growth is critical for improving methods of accessing health information and services	[28,68,69,75,85,89,102]

3.2. Challenges

In this section, the challenges of IoT healthcare systems are categorized as three classes as shown in Figure 12.



**Figure 12.** Challenges sections.

3.2.1. Challenges Related to System

The challenges related to the systems are summarized in this sub-section. The current sub-section follows main system challenges such as IoT, big data, cloud computing, security, sensors, real-time process, and requirements. Each of these challenges is discussed in the following subsections.

**1-Internet of Things.** The importance of the IoT is one of the technical factors emphasized by many researchers in their studies. For instance, the application of IoT in facilitating access to smart gadgets led to the identification of a patient's location, status, and tracking [42]. Other authors conducted a survey to investigate people's perceptions towards adopting and accepting IoT technology in healthcare and their attitudes towards adopting smart healthcare services [72,91]. In another study, the researchers discussed how IoT technology could be provided to individuals in their vehicles [79]. Accordingly, the technology is to be provided by the healthcare system and designed to enable patients to use a medical sensor in a vehicle equipped with IoT devices [79]. In some articles, researchers have focused on addressing stakeholder issues to improve the performance of the IoT healthcare system [55]. To this end, they focus on reducing processing time and identifying limitations for the wider use of the IoT that cover the entire hospital [25,86].

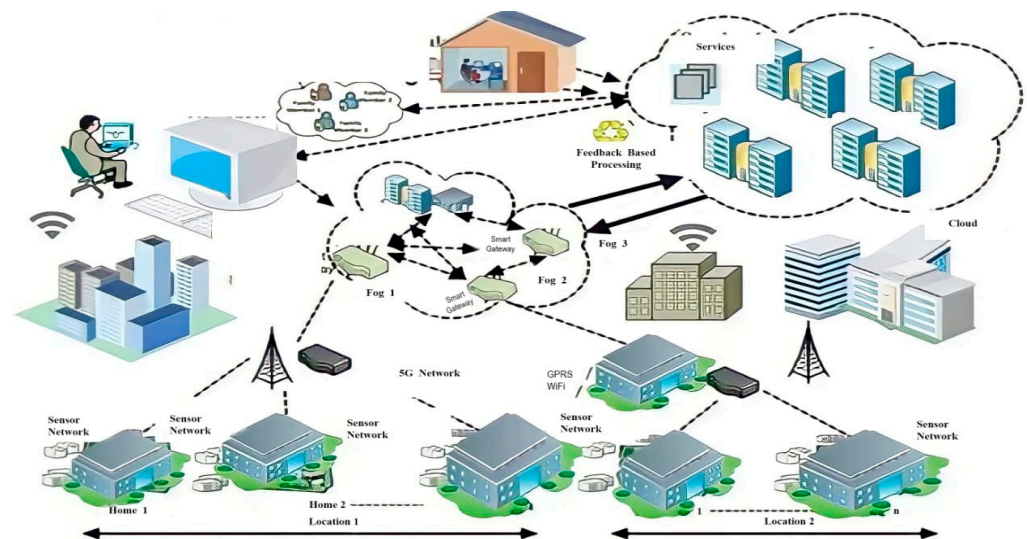
**2-Big data.** Some researchers have emphasized the analysis of big data in their research. The term "big data" refers to a large amount of data that can be easily stored and processed by the classical method [24]. This volume of data can be structured or unstructured. Therefore, some researchers in their papers have tried to use effective and efficient techniques to collect big data providers received by cameras, microphones, and other sensors [24]. In recent years, studies have been conducted on how to collect and store data in systems in a reliable and secure way [28,89] and how to maintain a high level of integrity [14,89]. Other researchers focused on how the system would efficiently deal with a large scale of healthcare data collected from many sensors [37]. Issues relating to speed and analysis of huge amounts of data [3,28,88] after data collection and processing [35,96], data management [8,23] and data monitoring were raised by several researchers. These potential issues need to be solved to ensure the availability, reliability, and accuracy of big data [89,103], as well as to assist the decision-makers in taking the right decision [94,96]. Nevertheless, a few studies highlighted the need to support the decision-making process by building a model on IoT-based platforms [26,100]. However, data sensing [44], data missing [26], data isolation [76], data transfer [90], and low capacity are still the current challenges that need to be addressed [7,25]. In a recent work, a decision support system was designed for data gathering from IoT-based healthcare systems [97]. Different sensors, such as heart pulse-rate, body temperature, blood oxygen level, etc., are extracted using sensor-based devices connected to patients. Additionally, different processes such as preprocessing, data analysis, and generating detailed information are performed. Experimental results show that combining data extracted by the IoT with methods of analysis in health care systems can be efficient [97].

**3-Cloud computing and fog computing.** In the last two decades, some researchers have proposed cloud computing in health IoT as a solution to different problems, such as estimating the number of required cloud and fog resources in a healthcare system [18], improving the flexibility of access to data, and preventing identity theft or clinical error by health care professionals [30,42,43,57]. In addition, cloud and fog computing make it possible to capture and analyze patient data at any time, any place, locally or remotely [10]. However, there are many studies that have concentrated on how the Cloud-of-Things (CoT) can handle large volumes of data received from billions of Internet-of-Things-connected objects [5,25]. With the recent rapid advancement in technology and widespread healthcare systems, cloud computing has been unable to meet all the needs of healthcare applications. However, these problems have been resolved with the emergence of fog computing systems, which are characterized by fast response times and low latency [12].

The latest research on fog computing in healthcare applications has been multidimensional [38]. Fog computing addresses important challenges related to system performance of IoT-based healthcare systems [12,89]. In addition, from an economic point of view, the fog computing system is considered more cost-effective because it tends to reduce costs, which is the goal of providers. In general, cloud computing and fog computing play an important role in health care systems. Therefore, researchers are constantly searching for solutions to the challenges related to applying fog computing in IoT-healthcare system.

**4-Security and Privacy.** Security and privacy have been reported in most previous articles on the application of IoT in healthcare systems. Generally, the terms “security” and “privacy” are interlinked, and both focus on how to secure data, although from different perspectives. Specifically, security pays more attention to unauthorized access to the system’s data or information, whereas privacy emphasizes how to secure individual or personal information. These phrases are more efficient in smart healthcare software to improve the security of patients’ records and related data [16,44,79].

Numerous studies have addressed potential security and privacy challenges such as security attacks, data leaks, device security, and wearability [8,20,70,90,101,104]. For a smart healthcare system to be sustainable over a long period of time, data security and patient privacy must be given considerable consideration [3,12,57]. This is especially important for sensitive medical data [36] because attacking the system can lead to vulnerable data leaks that can lead to more serious attacks. One of the most well-known types of attacks in this area is the Mirai attack, which can generate malicious and unusual traffic at several gigabits per second with the help of IoT devices [16,105]. Hence, authentication is the first step to ensure system security [32,74,101], while other studies have focused on the data security mechanism [84,94]. For example, the researcher Almaiah, proposed a creative hybrid model for authentication and reliable data retention in IoT-based healthcare software [52]. They proposed a lightweight authentication approach for IoT-based healthcare systems based on deep learning to facilitate decentralized authentication process in legal devices. Based on reported results, their proposed approach depreciated the validation latency among pairing devices and improved communication statistics. The proposed secure searchable encryption system in is shown in the Figure 13 [52]. Some researchers have sought to develop practical privacy practices in health care systems to provide better ways to protect such sensitive data [85], especially in terms of data collection and transmission [60,103]. Another challenge that researchers have addressed is the need to provide electronic health record (I) protection [39,87] and to examine the use of the Chinese block-chain to link patients’ electronic health records to a variety of healthcare services [65,78].



**Figure 13.** The Proposed secure searchable encryption system.

**5-Technical requirements.** Along with the core requirements that we mentioned above, there are some technical requirements we should consider [48,58] such as battery drain, leakage of energy storage devices [1,102], low-power operation [4,33], powering of IoT terminal nodes used in smart decisions and energy consumption [65,66,75,91,99,101,106] in order to enhance communications and store information effectively without any possible delay [39].



In fact, communication/connectivity is regarded as the foundational component in smart hospitals, as it allows all medical devices to connect to the internet, transfer data collected from patients, and provide rapid response (via sensors). That is why researchers focus on the reliability of network connections and data transmission [2,35,91], and they keep trying to find solutions to the challenges that face them, such as traffic problems [40]. Other researchers discuss how to enhance the quality and performance of the service [41,44,91].

**6-Enhance Quality of the system.** In the healthcare system, there are many significant aspects that the authors are interested in, to obtain a more efficient and accurate service [28,46], such as sparing awareness of using medical gadgets frequently [61], taking care of response time or latency [81,91], keeping fast and high quality of data transmission [39,107] and reducing the possibility of packet loss [107], determine the relationship between ICT and healthcare, as well as how ICT can help and improve the system [40]. This is in addition to providing a high level of software safety, reliability, device connectivity and giving attention to the network architecture topology to deliver the best healthcare application [1,2,66] to the patients. Some researchers pointed to providing early detection abilities with better monitoring system [30,73,103] such as diagnosis of hypertension and keep monitoring the blood pressure state [31], and explored a voice pathology detection system using deep learning to detect the fake primary users of the system [71,88]. Equitable access and delivery process of healthcare should be provided, especially in far rural-developing areas [26,28]. Keeping updating to the latest technologies made so far [97] and designing a course for smart healthcare engineering education to reduce the effort that could be made to get involved in this technology [98,108].

### 3.2.2. Challenges Related to Users

Some of the studies in the reviewed articles emphasized challenges relating to users as they remain a vital part of smart healthcare systems. Hence, one of the goals of IoT is to reduce patients' cost burden by minimizing the number of visits to hospitals or clinics while ensuring that accurate and efficient healthcare services and treatment are delivered [4]. These were the main challenges that most researchers attempted to address in their studies [71,73]. Nevertheless, a few others have attempted to develop strategies to reduce the cost of smart devices and communication technology to support remote monitoring systems [33,101]. Therefore, some researchers have used the concept of "smart stone" to reduce the system's interaction with the user and reduce the specific problems of the elderly in the use of mobile devices and tablets [20]. In a similar study, this concept was also used to identify the main factors affecting the increase in the acceptance rate of elderly people using smart devices to receive health care services [9]. However, one of the biggest challenges of IoT healthcare nowadays is the technology adoption by users. Researchers need to go in depth to figure out the most critical factors that affect user adoption of such a technology [11].

### 3.2.3. Other Challenges

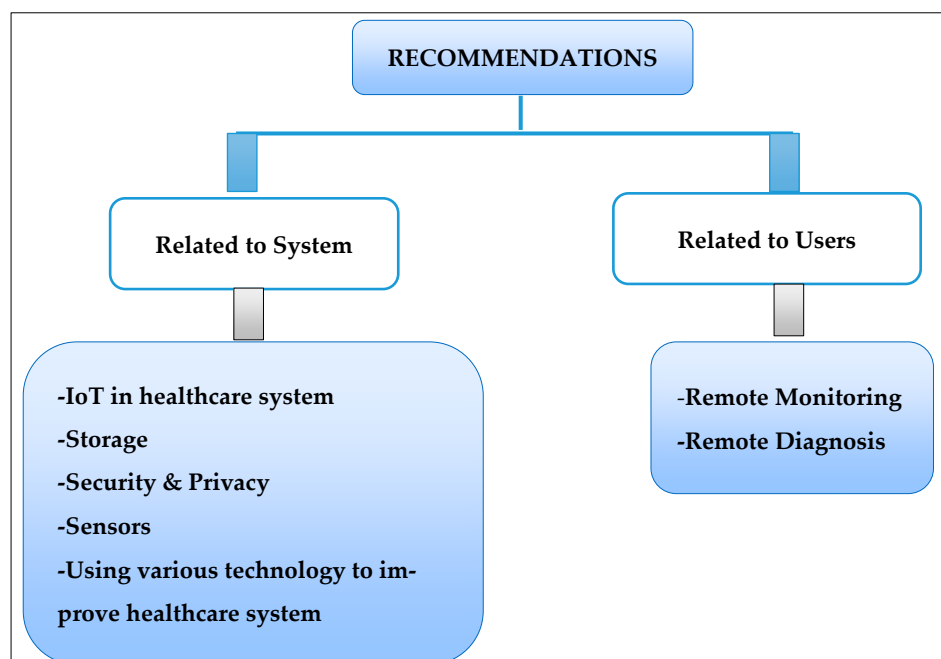
Despite all the challenges and problems discussed to this point, other issues have been reported by some researchers, especially in terms of environmental factors [7], culture, policies and regulations [76], platforms [26,103], embedded systems [105], adopting social media in healthcare systems and how it would be useful in spearheading healthcare information [101,109], and the advantage that comes from being in the healthcare sector for a long period [110]. The availability of improved healthcare systems is associated with an increase in the life expectancy of users; thereby resulting in a proportional increase in the older population. However, older people face special problems such as reduced physical fitness, chronic and long-term medical disorders, and digital migraines [11]. Table 3 summarizes the main challenges that researchers in this area encounter.

**Table 3.** Summary of common challenges.

Category	Identified Challenges	References
Challenges Related to System	1- IoT healthcare system performance needs to be improved 2- Finding effective and efficient techniques to collect big data in a reliable and secure way. 3- Data sensing, data missing, data isolation, data transfer, and low capacity, are significant challenges that need to be addressed. 4- Researchers are constantly searching for solutions to the challenges related to cloud computing and fog computing in IoT-healthcare systems. 5- Challenges related to privacy and security of IoT healthcare system are important because attacking the system can lead to vulnerable data leaks and traffic delays could affect patients' lives. 6- The need to provide electronic health record (EHR) protection. 7- Technical requirements should be considered such as battery drain, leakage of energy storage devices, low-power operation, powering of IoT terminal nodes, used in smart decisions and energy consumption, in order to enhance communications and store information effectively without any delay.	[7,24–26,41,43,44,76,90,102,106]
Challenges Related to Users	Challenges related to users include cost, number of visits to hospitals and identifying the main factors affecting the acceptance rate of people using smart devices to receive healthcare services.	[4,11,20,33,71,73,101]
Other Challenges	Other issues have been reported by some researchers, especially in terms of environmental factors, culture, policies and regulations, platforms, embedded systems, and adopting social media in healthcare systems.	[7,26,76,103,105,109]

### 3.3. Recommendation

This section comprises researchers' recommendations concerning the aspects to be considered in future work and gives an insight into the knowledge gaps that are yet to be investigated. The recommendations can be categorized into two main groups: healthcare system's recommendations (IoT, storage, security and privacy, sensors and improving healthcare systems) and users' recommendations (remote monitoring and remote diagnosis) as shown in Figure 14.



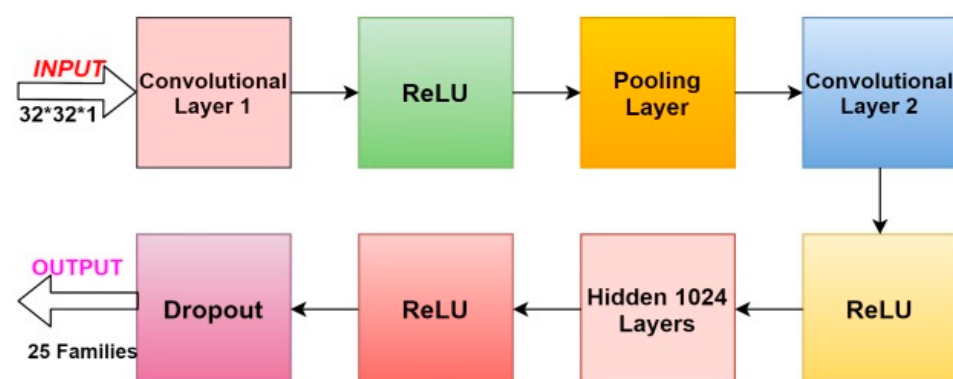
**Figure 14.** A summary of the recommendations from studies on enabling IoT in the healthcare system and service delivery.

### 3.3.1. Recommendations Related to System

**1-IoT in the healthcare system.** Some experimental results show that IoT in healthcare service delivery should be performed after proving its ability to reduce pressures on the systems [8], and it allows patients to constantly monitor and manage their health status [21]. Although the potential of the IoT has been identified for all, it is still in its infancy and more extensive studies and research are needed to discover the potential impact of the IoT on healthcare systems [15,62]. Other researchers recommended that extensive studies should be conducted to upgrade IoT in terms of health monitoring and management systems [107].

**2-Storage.** There is a fact here that cloud computing can be adapted in a simple way by others. In this respect, it is used to provide access to healthcare systems and storage of data [8]. Hence, a few studies recommended the need to improve storage capacity and the performance of the cloud by applying various enhancement infrastructures such as MapReduce. This will assist in reducing the main sources of delays, such as processing delays as well as integrating communication delays [96].

**3-Security and Privacy.** One of the widely discussed and investigated topics in IoT is security and privacy. Several authors recommended that future research should focus on how to enhance the healthcare system by improving the security and privacy aspects [10,62,65,84,86]. Other researchers were more specific by advocating the need to add some security protocols [98], secure communication in the wireless network, propose efficient trade-off between security issues and cost of the end-to-end security protocols in analysis [54], provides access control rules [8], and human-less autonomic control of programs [99]. Furthermore, there are suggestions to introduce protocols that enable a doctor to access records without authorization during emergencies [65] while others emphasized federal enforcement of data protection and security, privacy, as well as the confidentiality of data control and storage [8,48]. According to these authors, these strategies will promote the development and implementation of robust IoT-based healthcare policies and care models. For example, in [51], Anand et al. proposed a deep network based on convolutional neural network (CNN) to detect malware attacks in 5G-IoT healthcare applications. The network's structure of their proposed network is shown in Figure 15. As can be seen, different deep features are extracted from input data and finally 25 malware types are classified. Experimental results in show that the proposed approach improves the security of IoT healthcare systems, especially in 5G format [51].



**Figure 15.** The deep network to detect malware attacks in 5G-IoT healthcare systems.

**4-Sensors.** Another type of important recommendation that should be noted is sensor-related recommendations, such as smart stones, which are new types of sensors that can be used in healthcare IoT-based systems to improve operational performance [20]. Due to the increasing expansion of health care in most communities, the need to develop remote sensing devices in these systems is strongly felt [56]. Some researchers have said that future work should continue to investigate wireless sensors, while the authors of some studies have tried to make applications more scalable by obtaining more sensors.

**5-Using various technologies to improve healthcare systems.** To improve healthcare systems, some significant issues can be considered to propose future studies, such as using machine learning techniques, secure encryption theories for cloud storage [8], integrating mobile internet of things devices (MIoT), and facilitating fog and cloud computing as main solutions for typical healthcare monitoring systems [18]. A recent study [99] proposed an innovative security framework for healthcare systems. According to a study, secret data, like most systems, should be stored on cloud servers but first encrypted using block-based data encryption techniques [92]. In most attacks that occur on the Internet, information is the main damage. Patients' medical records are also part of the patient's personal information and identity and should not be accessible to anyone. A blockchain-based framework is used. The proposed framework has the ability to update any changes in the patient's health characteristics (such as allergies, new symptoms, side effects of medications, etc.) at any time and create a separate block in the chain [92]. Securing patient-sensitive information in health care systems builds trust between patients or users and health care providers. In this paper, the main goal of the authors was to secure information based on the development of a multi-layered block chain-based IoT data security approach. In another study, it suggested that combining theories is recommended to improve the performance of existing models [94]. Furthermore, several open research scopes that require efficient and innovative solutions include the communication network; complexity trade-off; data duplication; reducing fault detection rate [58] and using the real dataset to solve real problems more efficiently [65]. Another new idea is that some researchers attempt to use deep learning networks to enhance a system's performance, whereas others suggest using deep learning networks as efficient tools to improve next-generation IoT systems [13]. This includes shifting from the static nature to a dynamic status, enhancing the security, reliability, scalability, and privacy of network-based healthcare systems [16,105]. Overall, the use of new technology helps improve the quality of the system and lower costs [5].

### 3.3.2. Recommendations Related to Users

This section discusses researchers' recommendations on how medical services could be enhanced in the near future to deliver better service to users and achieve the highest usefulness of such technology for their health. Examples include embedding more sensors for tracking and monitoring services.

**1-Remote Monitoring.** In term of remote monitoring, some authors have made suggestions to increase the speed of tracking and remote monitoring [7]. In this research, advanced embedded sensors, destructive sensors in real world applications, increasing awareness of chronic diseases, and development of programmability features of technologies have been used [103]. However, other researchers seek to continuously increase the accuracy and credibility of dynamic adaptation monitoring and support systems to prevent potential problems in future technologies [88]. The concept of "combined real-time remote monitoring (HRRM)" was mentioned as one of the new monitoring approaches that can be used in monitoring various diseases in future work [37].

**2-Remote diagnosis.** For disease diagnosis, researchers have recommended the provision of intelligence and the provision of more versatile disease detection techniques via the use of IoT [92]. Others have recommended the improvement of detection rate and access time based on the development of real-time response systems [38]. Likewise, another study emphasized the need to consider the mobility power of medical sensors between smart e-health gateways of different types [92]. And the easy interoperability of different nodes using different policies and protocols [38]. The recommendations given by previous researchers are outlined in Table 4.

**Table 4.** Summary of common recommendations.

Category	Common Recommendations	References
Recommendations Related to System	1- To upgrade IoT in terms of health monitoring and management systems, in addition to more extensive studies and research are needed to discover the potential impact of the IoT on healthcare systems. 2- To improve storage capacity and the performance of the cloud. This will assist in reducing the main sources of delays, such as processing delays as well as integrating communication delays. 3- To enhance the security and privacy of healthcare system, such as the need to add some security protocols, secure communication in the wireless network. 4- To introduce protocols that enable a doctor to access records without authorization during emergencies. 5- To use new type of sensors in healthcare IoT-based systems to improve operational performance. 6- To improve healthcare systems, some significant issues can be considered in future studies, such as using machine learning techniques, secure encryption theories for cloud storage, integrating mobile internet of things devices (MIoT), facilitating fog and cloud computing as main solutions for typical healthcare monitoring systems...etc.	[10,15,20,62,65,84,86,96,98,107]
Recommendations Related to Users	1- To increase the speed of tracking and remote monitoring such as advanced embedded sensors. 2- To continuously increase the accuracy and credibility of dynamic adaptation monitoring and support systems to prevent potential problems in future technologies. 3- To provide more disease detection techniques via the use of IoT 4- To improve detection rate and access time based on the development of real-time response systems.	[7,38,88,92]

## 4. Conclusions and Limitation

### 4.1. Limitations

As stated, this is a systematic review, thus we attempted to be objective about all selection and research characteristics based on the suggested approach outlined at the beginning of the paper. Therefore, a brief explanation of the study's limitations follows. All of the conclusions discussed in this review are constrained by the examination of publications published within the specified time period (2015–2022). Moreover, the study used the terms “healthcare”, “health care”, “health-care”, “medical system”, and “health” in conjunction with “internet of things” and “IoT” as the primary keywords for locating the relevant literature, which may have led to the omission of some related articles from the specified databases. Therefore, it is suggested that future researchers who want to examine the literature include additional keywords such as “e-health”, “m-health”, and “electronic health” in their search queries.

Articles were also reviewed from the perspective of set goals. These findings in this review are limited by analyzing articles published within the investigated and targeted timeframe of the study to ensure that the relevant and recent articles were retrieved. This study selected keywords focusing on motivations for research published on enabling IoT in healthcare, challenges reported in the articles, and recommendations for future studies. Given the fact that these studies were conducted in different countries, some of the challenges may be specific to certain regions and not generalizable to other locations. Therefore, the issues raised in this article should be analyzed with caution.

Only articles written in English are reviewed in this article. Related articles written in other languages may therefore be ignored. This may be a minor limitation, but it is not a source of bias because most reputable magazines are published in English. Likewise, the challenges raised in this article might require empirical testing according to the respective location where IoT is to be implemented in the healthcare system. Review articles were also included in the literature search employed in this study. However, this was considered

given that only a few studies have been conducted worldwide on enabling IoT in the healthcare system and service delivery.

In this study, several researchers raised critical concerns about the urgent need to develop real-time monitoring systems due to the increasing number of people with disabilities and chronic diseases. This is also important in the healthcare system in Malaysia, as the aging population is projected to make up 7.2% of the total population by 2020 [23]. Hence, it is expected that the pressure on healthcare facilities will increase in line with the aging population and the number of those having chronic morbidities. Policymakers and IoT developers need to consider the contemporary aging population while planning to enable IoT in the Malaysian healthcare system. Presently, the area of smart healthcare service delivery to cater for chronically ill patients needs to be developed [84]. The development of embedded and disruptive sensors, as well as real-time remote tracking and monitoring, could be used to help people with chronic diseases all over the world receive better care.

#### 4.2. Discussion

Most researchers and authorities around the world are working to harness the potential of the IoT to improve health services and improve provision. Numerous articles on topics relating to IoT have been published in recent times. However, the application of IoT in the healthcare system and its impact on human lives has received extensive attention from researchers. Therefore, this article elucidates the main research focus in published studies regarding IoT in healthcare systems and how it has been used in a smart way in the delivery of healthcare services to achieve maximum benefits by serving patients, doctors and physicians, hospitals, governments, and providers.

An SLR of 106 articles is conducted, identified and analyzed through a specific procedure. This article gives a clear indication of the motivations that encourage researchers and providers to involve IoT in healthcare. In order to facilitate the explanation, the sections were broadly divided into four main groups: systems, users, cost, and data, with each comprising subgroups. Various challenges were also raised in most studies on IoT in healthcare, comprising the adoption and integration of IoT with smart gadgets and vehicles to facilitate patient monitoring, developing algorithms in the big data field due to the growing population of people with chronic diseases and demand on healthcare systems, and resources required to execute cloud and fog computing. Other important constraints include the technical requirements, enhancing the performance and quality of sensors, providing real-time monitoring and minimizing the cost burden to end-users. Based on the reviewed studies, recommendations for future research to enable the effective application of IoT in healthcare and service delivery should focus on improving storage capacity, security and privacy, sensors and other advanced technologies. Additionally, recommendations focusing on users entail the provision for remote monitoring and remote diagnosis of diseases.

**Author Contributions:** H.H.M.J. is responsible for the study design, drafting and writing the original manuscript, as well as reviewing and editing it; Z.B.H. is responsible for supervising the study, funding it, and providing the necessary resources; B.B.Z. is responsible for supervising the study, investigating and validating the outcomes of the research; F.H.M.J. is responsible for doing literature search and articles' filtration; D.H.M.J. is responsible for interpreting the gathered information and analyzing it; W.H.D.A. is responsible for providing the generating the statistical figures, validating the gathered information and the study outcomes. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Papa, A.; Mital, M.; Pisano, P.; Del Giudice, M. E-health and wellbeing monitoring using smart healthcare devices: An empirical investigation. *Technol. Forecast. Soc. Chang.* **2018**, *153*, 119226. [[CrossRef](#)]
2. Dritsa, D.; Bioria, N. Towards a multi-scalar framework for smart healthcare. *Smart Sustain. Built Environ.* **2018**, *7*, 33–52. [[CrossRef](#)]
3. Aceto, G.; Persico, V.; Pescapé, A. The role of Information and Communication Technologies in healthcare: Tax-onomies, perspectives, and challenges. *J. Netw. Comput. Appl.* **2018**, *107*, 125–154. [[CrossRef](#)]
4. Sakr, S.; Elgammal, A. Towards a Comprehensive Data Analytics Framework for Smart Healthcare Services. *Big Data Res.* **2016**, *4*, 44–58. [[CrossRef](#)]
5. Alabdulatif, A.; Khalil, I.; Yi, X.; Guizani, M. Secure Edge of Things for Smart Healthcare Surveillance Framework. *IEEE Access* **2019**, *7*, 31010–31021. [[CrossRef](#)]
6. Delgosha, M.S.; Hajiheydari, N.; Talafidaryani, M. Discovering IoT implications in business and management: A computational thematic analysis. *Technovation* **2021**, *in press*. [[CrossRef](#)]
7. Amin, S.U.; Hossain, M.S.; Muhammad, G.; Alhussein, M.; Rahman, M.A. Cognitive Smart Healthcare for Pathology Detection and Monitoring. *IEEE Access* **2019**, *7*, 10745–10753. [[CrossRef](#)]
8. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [[CrossRef](#)]
9. Pal, D.; Funilkul, S.; Charoenkitkarn, N.; Kanthamanon, P. Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective. *IEEE Access* **2018**, *6*, 10483–10496. [[CrossRef](#)]
10. Pasha, M.; Shah, S.M.W. Framework for E-Health Systems in IoT-Based Environments. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 6183732. [[CrossRef](#)]
11. Gkouskos, D.; Burgos, J. I'm in! Towards participatory healthcare of elderly through IOT. *Procedia Comput. Sci.* **2017**, *113*, 647–652. [[CrossRef](#)]
12. Saha, R.; Kumar, G.; Rai, M.K.; Thomas, R.; Lim, S.J. Privacy Ensured e-Healthcare for Fog-Enhanced IoT Based Applications. *IEEE Access* **2019**, *7*, 44536–44543. [[CrossRef](#)]
13. Asif-Ur-Rahman, M. Towards a Heterogeneous Mist, Fog, and Cloud-based Framework for the Internet of Healthcare Things. *IEEE Internet Things J.* **2018**, *6*, 4049–4062. [[CrossRef](#)]
14. Dhanvijay, M.M.; Patil, S.C. Internet of Things: A survey of enabling technologies in healthcare and its applications. *Comput. Netw.* **2019**, *153*, 113–131. [[CrossRef](#)]
15. Karahoca, A.; Karahoca, D.; Aksöz, M. Examining intention to adopt to internet of things in healthcare technology products. *Kybernetes* **2017**, *47*, 742–770. [[CrossRef](#)]
16. Muhammed, T.; Mehmood, R.; Albeshri, A.; Katib, I. UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities. *IEEE Access* **2018**, *6*, 32258–32285. [[CrossRef](#)]
17. Rodriguez, C.; Castro, D.M.; Coral, W.; Cabra, J.L.; Velasquez, N.; Colorado, J.; Mendez, D.; Trujillo, L.C. IoT system for Human Activity Recognition using BioHarness 3 and Smartphone. In Proceedings of the International Conference on Future Networks and Distributed Systems, New York, NY, USA, 19–20 July 2017; Volume 49, pp. 1–7.
18. Kafhali, S.E.; Salah, K. Architecture to manage internet of things data using blockchain and fog computing. In Proceedings of the 4th International Conference on Big Data and Internet of Things, Rabat, Morocco, 23–24 October 2019.
19. Moosavi, S.R. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **2015**, *52*, 452–459. [[CrossRef](#)]
20. Bellagente, P. The “Smartstone”: Using smartphones as a telehealth gateway for senior citizens. *IFAC-PapersOnLine* **2016**, *49*, 221–226. [[CrossRef](#)]
21. Verma, P.; Sood, S.K. Cloud-centric IoT based disease diagnosis healthcare framework. *J. Parallel Distrib. Comput.* **2018**, *116*, 27–38. [[CrossRef](#)]
22. Moher, D.; Shamseer, L.; Clarke, M.; Ghersi, D.; Liberati, A.; Petticrew, M.; Shekelle, P.; Stewart, L.A. Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015 statement. *Syst. Rev.* **2015**, *4*, 1. [[CrossRef](#)]
23. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Moullec, Y.L. A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* **2018**, *6*, 36611–36631. [[CrossRef](#)]
24. Alkhomsan, M.N.; Hossain, M.A.; Rahman, S.M.M.; Masud, M. Situation Awareness in Ambient Assisted Living for Smart Healthcare. *IEEE Access* **2017**, *5*, 20716–20725. [[CrossRef](#)]
25. Elhoseny, M.; Abdelaziz, A.; Salama, A.S.; Riad, A.; Muhammad, K.; Sangaiah, A.K. A hybrid model of Internet of Things and cloud computing to manage big data in health services applications. *Futur. Gener. Comput. Syst.* **2018**, *86*, 1383–1394. [[CrossRef](#)]
26. Qi, J.; Yang, P.; Min, G.; Amft, O.; Dong, F.; Xu, L. Advanced internet of things for personalised healthcare systems: A survey. *Pervasive Mob. Comput.* **2017**, *41*, 132–149. [[CrossRef](#)]
27. Alhussein, M.; Muhammad, G. Voice Pathology Detection Using Deep Learning on Mobile Healthcare Framework. *IEEE Access* **2018**, *6*, 41034–41041. [[CrossRef](#)]
28. Harerimana, G.; Jang, B.; Kim, J.W.; Park, H.K. Health Big Data Analytics: A Technology Survey. *IEEE Access* **2018**, *6*, 65661–65678. [[CrossRef](#)]
29. Vemishetty, N. Low power personalized ECG based system design methodology for remote cardiac health monitoring. *IEEE Access* **2016**, *4*, 8407–8417. [[CrossRef](#)]

30. Bellavista, P.; Berrocal, J.; Corradi, A.; Das, S.K.; Foschini, L.; Zanni, A. A survey on fog computing for the Internet of Things. *Pervasive Mob. Comput.* **2019**, *52*, 71–99. [\[CrossRef\]](#)
31. Rodrigues, J.J.P.C.; Segundo, D.B.D.R.; Junqueira, H.A.; Sabino, M.H.; Prince, R.M.; Al-Muhtadi, J.; De Albuquerque, V.H.C. Enabling Technologies for the Internet of Health Things. *IEEE Access* **2018**, *6*, 13129–13141. [\[CrossRef\]](#)
32. Li, X.; Huang, X.; Lia, C.; Yu, R.; Shu, L. EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems. *IEEE Access* **2019**, *7*, 22011–22025. [\[CrossRef\]](#)
33. Muzammal, S.M. Counter measuring conceivable security threats on smart healthcare devices. *IEEE Access* **2018**, *6*, 20722–20733. [\[CrossRef\]](#)
34. Zaman, S.; Khandakar, R.A.; Khan, R.T.; Tariq, F.; Wong, K.K. Thinking out of the blocks: Holochain for dis-tributed security in IoT healthcare. *IEEE Access* **2022**, *10*, 37064–37081. [\[CrossRef\]](#)
35. Din, S.; Paul, A. RETRACTED: Smart health monitoring and management system: Toward autonomous wearable sensing for Internet of Things using big data analytics. *Futur. Gener. Comput. Syst.* **2019**, *91*, 611–619. [\[CrossRef\]](#)
36. Guan, Z.; Lv, Z.; Du, X.; Wu, L.; Guizani, M. Achieving data utility-privacy tradeoff in Internet of Medical Things: A machine learning approach. *Futur. Gener. Comput. Syst.* **2019**, *98*, 60–68. [\[CrossRef\]](#)
37. Hassan, M.K.; El Desouky, A.I.; Elghamrawy, S.M.; Sarhan, A. A Hybrid Real-time remote monitoring framework with NB-WOA algorithm for patients with chronic diseases. *Futur. Gener. Comput. Syst.* **2018**, *93*, 77–95. [\[CrossRef\]](#)
38. Mutlag, A.A.; Ghani, M.K.A.; Arunkumar, N.; Mohammed, M.A.; Mohd, O. Enabling technologies for fog computing in healthcare IoT systems. *Futur. Gener. Comput. Syst.* **2018**, *90*, 62–78. [\[CrossRef\]](#)
39. Parah, S.A.; Sheikh, J.A.; Akhoun, J.A.; Loan, N.A. Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication. *Futur. Gener. Comput. Syst.* **2018**, *108*, 935–949. [\[CrossRef\]](#)
40. Manashty, A.; Light, J. Life Model: A novel representation of life-long temporal sequences in health predictive analytics. *Futur. Gener. Comput. Syst.* **2018**, *92*, 141–156. [\[CrossRef\]](#)
41. Vilela, P.H.; Rodrigues, J.J.; Solic, P.; Saleem, K.; Furtado, V. Performance evaluation of a Fog-assisted IoT solution for e-Health applications. *Futur. Gener. Comput. Syst.* **2019**, *97*, 379–386. [\[CrossRef\]](#)
42. Adame, T.; Bel, A.; Carreras, A.; Melià-Seguí, J.; Oliver, M.; Pous, R. CUIDATS: An RFID-WSN hybrid monitoring system for smart health care environments. *Futur. Gener. Comput. Syst.* **2018**, *78*, 602–615. [\[CrossRef\]](#)
43. Hahn, C.; Kwon, H.; Hur, J. Trustworthy Delegation toward Securing Mobile Healthcare Cyber-Physical Systems. *IEEE Internet Things J.* **2018**, *6*, 6301–6309. [\[CrossRef\]](#)
44. Abdellatif, A.A.; Khafagy, M.G.; Mohamed, A.; Chiasserini, C.F. EEG-based transceiver design with data de-composition for healthcare IoT applications. *IEEE Internet Things J.* **2018**, *5*, 3569–3579. [\[CrossRef\]](#)
45. Tokognon, C.A.; Gao, B.; Yun Tian, G.; Yan, Y. Structural Health Monitoring Framework Based on Internet of Things: A Survey. *IEEE Internet Things J.* **2017**, *4*, 619–635. [\[CrossRef\]](#)
46. Pathinarupothi, R.K.; Durga, P.; Rangan, E.S. IoT Based Smart Edge for Global Health: Remote Monitoring with Severity Detection and Alerts Transmission. *IEEE Internet Things J.* **2018**, *6*, 2449–2462. [\[CrossRef\]](#)
47. Habibzadeh, H.; Dinesh, K.; Shishvan, O.R.; Boggio-Dandry, A.; Sharma, G.; Soyata, T. A Survey of Healthcare Internet of things (HioT): A Clinical Perspective. *IEEE Internet Things J.* **2019**, *7*, 53–71. [\[CrossRef\]](#)
48. Sood, S.K.; Mahajan, I. IoT-Fog based Healthcare Framework to Identify and Control Hyperten-sion Attack. *IEEE Internet Things J.* **2018**, *6*, 1920–1927. [\[CrossRef\]](#)
49. Mora, H.; Gil, D.; Terol, R.M.; Azorin, J.; Szymanski, J. An IoT-based computational framework for healthcare monitoring in mobile environments. *Sensors* **2017**, *17*, 2302. [\[CrossRef\]](#) [\[PubMed\]](#)
50. Takabayashi, K.; Tanaka, H.; Sakakibara, K. Integrated Performance Evaluation of the Smart Body Area Net-works Physical Layer for Future Medical and Healthcare IoT. *Sensors* **2019**, *19*, 30. [\[CrossRef\]](#) [\[PubMed\]](#)
51. Anand, A.; Rani, S.; Anand, D.; Aljahdali, H.M.; Kerr, D. An Efficient CNN-Based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IoT Healthcare Applications. *Sensors* **2021**, *21*, 6346. [\[CrossRef\]](#)
52. Almaiah, M.A.; Hajje, F.; Ali, A.; Pasha, M.F.; Almomani, O. A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS. *Sensors* **2022**, *22*, 1448. [\[CrossRef\]](#)
53. Hussain, F.; Abbas, S.; Shah, G.; Pires, I.; Fayyaz, U.; Shahzad, F.; Garcia, N.; Zdravevski, E. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. *Sensors* **2021**, *21*, 3025. [\[CrossRef\]](#)
54. Moosavi, S.R.; Nigussie, E.; Levorato, M.; Virtanen, S.; Isoaho, J. Performance Analysis of End-to-End Security Schemes in Healthcare IoT. *Procedia Comput. Sci.* **2018**, *130*, 432–439. [\[CrossRef\]](#)
55. Nishdia, Y.; Kitamura, K.; Yamamoto, H.; Takahashi, Y.; Mizoguchi, H. Living Function Resilient Service Using a Mock Living Lab and Real Living Labs: Development of Balcony-IoT and Handrail-IoT for Healthcare. *Procedia Comput. Sci.* **2017**, *113*, 121–129. [\[CrossRef\]](#)
56. Khowaja, S.A.; Prabono, A.G.; Setiawan, F.; Yahya, B.N.; Lee, S.-L. Contextual activity based Healthcare Internet of Things, Services, and People (HIoTSP): An architectural framework for healthcare monitoring using wearable sensors. *Comput. Netw.* **2018**, *145*, 190–206. [\[CrossRef\]](#)
57. Hossain, M.S.; Muhammad, G. Cloud-assisted industrial internet of things (IioT)-enabled frame work for health monitoring. *Comput. Netw.* **2016**, *101*, 192–202. [\[CrossRef\]](#)



58. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Kumar, N.; Das, A.K.; Saxena, N. LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. *IEEE Commun. Mag.* **2018**, *56*, 24–32. [[CrossRef](#)]
59. Luo, E.; Bhuiyan, M.Z.A.; Wang, G.; Rahman, M.A.; Wu, J.; Atiquzzaman, M. Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun. Mag.* **2018**, *56*, 163–168. [[CrossRef](#)]
60. Alabdulatif, A.; Khalil, I.; Forkan, A.R.M.; Atiquzzaman, M. Real-time Secure Health Surveillance for Smarter Health Communities. *IEEE Commun. Mag.* **2018**, *57*, 122–129. [[CrossRef](#)]
61. Touati, F.; Mnaouer, A.B.; Erdene-Ochir, O.; Mehmood, W.; Hassan, A.; Gaabab, B. Feasibility and performance evaluation of a 6LoWPAN-enabled platform for ubiquitous healthcare monitoring. *Wirel. Commun. Mob. Comput.* **2016**, *16*, 1271–1281. [[CrossRef](#)]
62. Jabbar, S.; Ullah, F.; Khalid, S.; Khan, M.; Han, K. Semantic interoperability in heterogeneous IoT infrastructure for healthcare. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 9731806. [[CrossRef](#)]
63. Bhatia, M.; Sood, S.K. A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective. *Comput. Ind.* **2017**, *92*, 50–66. [[CrossRef](#)]
64. Sundarasekar, R.; Thanjaivadivel, M.; Manogaran, G.; Kumar, P.M.; Varatharajan, R.; Chilamkurti, N.; Hsu, C.-H. Internet of Things with Maximal Overlap Discrete Wavelet Transform for Remote Health Monitoring of Abnormal ECG Signals. *J. Med. Syst.* **2018**, *42*, 228. [[CrossRef](#)]
65. McGhin, T.; Choo, K.-K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [[CrossRef](#)]
66. Ge, M.; Hong, J.B.; Guttman, W.; Kim, D.S. A framework for automating security analysis of the internet of things. *J. Netw. Comput. Appl.* **2017**, *83*, 12–27. [[CrossRef](#)]
67. Chen, Y.; Sun, W.; Zhang, N.; Zheng, Q.; Lou, W.; Hou, Y.T. Towards Efficient Fine-Grained Access Control and Trustworthy Data Processing for Remote Monitoring Services in IoT. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1830–1842. [[CrossRef](#)]
68. Chen, Y.; Lei, M.; Ren, W.; Ren, Y.; Qu, Z. RoFa: A Robust and Flexible Fine-Grained Access Control Scheme for Mobile Cloud and IoT based Medical Monitoring. *Fundam. Inform.* **2018**, *157*, 167–184. [[CrossRef](#)]
69. Santos, D.F.; Almeida, H.O.; Perkusich, A. A personal connected health system for the Internet of Things based on the Constrained Application Protocol. *Comput. Electr. Eng.* **2015**, *44*, 122–136. [[CrossRef](#)]
70. Pirbhulal, S.; Shang, P.; Wu, W.; Sangaiah, A.K.; Samuel, O.W.; Li, G. Fuzzy vault-based biometric security method for tele-health monitoring systems. *Comput. Electr. Eng.* **2018**, *71*, 546–557. [[CrossRef](#)]
71. Hassan, M.K.; El Desouky, A.I.; Elghamrawy, S.M.; Sarhan, A.M. Intelligent hybrid remote patient-monitoring model with cloud-based framework for knowledge discovery. *Comput. Electr. Eng.* **2018**, *70*, 1034–1048. [[CrossRef](#)]
72. Liu, Y.; Yang, Y.; Liu, Y.; Tzeng, G.H. Improving Sustainable Mobile Health Care Promotion: A Novel Hybrid MCDM Method. *Sustainability* **2019**, *11*, 752. [[CrossRef](#)]
73. Bennett, J.; Rokas, O.; Chen, L. Healthcare in the smart home: A study of past, present and future. *Sustainability* **2017**, *9*, 840. [[CrossRef](#)]
74. Fan, K.; Zhu, S.; Zhang, K.; Li, H.; Yang, Y. A Lightweight Authentication Scheme for Cloud-Based RFID Healthcare Systems. *IEEE Netw.* **2019**, *33*, 44–49. [[CrossRef](#)]
75. Rodic, B. Usability of m-Health services: A health professional's perspective. *Management* **2017**, *21*, 45–54.
76. Sun, J.; Guo, Y.; Wang, X.; Zeng, Q. mHealth for ageing China: Opportunities and challenges. *Aging Dis.* **2016**, *7*, 53–67. [[CrossRef](#)]
77. Peng, Y.; Wang, X.; Guo, L.; Wang, Y.; Deng, Q. An Efficient Network Coding-Based Fault-Tolerant Mechanism in WBAN for Smart Healthcare Monitoring Systems. *Appl. Sci.* **2017**, *7*, 817. [[CrossRef](#)]
78. Da Costa, C.A.; Pasluosta, C.F.; Eskofier, B.; da Silva, D.B.; Righi, R.D.R. Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards. *Artif. Intell. Med.* **2018**, *89*, 61–69. [[CrossRef](#)]
79. Jeong, Y.-S.; Shin, S.-S. An IoT healthcare service model of a vehicle using implantable devices. *Clust. Comput.* **2016**, *21*, 1059–1068. [[CrossRef](#)]
80. Aghdam, Z.N.; Rahmani, A.M.; Hosseinzadeh, M. The Role of the Internet of Things in Healthcare: Future Trends and Challenges. *Comput. Methods Programs Biomed.* **2020**, *199*, 105903. [[CrossRef](#)]
81. Marakhimov, A.; Joo, J. Consumer adaptation and infusion of wearable devices for healthcare. *Comput. Hum. Behav.* **2017**, *76*, 135–148. [[CrossRef](#)]
82. Bhatia, M.; Sood, S.K. Temporal informative analysis in smart-ICU monitoring: M-HealthCare perspective. *J. Med. Syst.* **2016**, *40*, 190. [[CrossRef](#)]
83. Tian, S.; Yang, W.; Le Grange, J.M.; Wang, P.; Huang, W.; Ye, Z. Smart healthcare: Making medical care more intelligent. *Glob. Health J.* **2019**, *3*, 62–65. [[CrossRef](#)]
84. Javdani, H.; Kashanian, H. Internet of things in medical applications with a service-oriented and security ap-proach: A survey. *Health Technol.* **2018**, *8*, 39–50. [[CrossRef](#)]
85. Sharma, S.; Chen, K.; Sheth, A. Toward Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems. *IEEE Internet Comput.* **2018**, *22*, 42–51. [[CrossRef](#)]
86. Laplante, N.L.; Laplante, P.A.; Voas, J.M. Stakeholder identification and use case representation for Internet-of-Things applications in healthcare. *IEEE Syst. J.* **2016**, *12*, 1589–1597. [[CrossRef](#)] [[PubMed](#)]
87. Bian, J.; Yang, S.; Xiong, H.; Wang, L.; Fu, Y.; Sun, Z.; Guo, Z. CRLEDD: Regularized Causalities Learning for Early Detection of Diseases Using Electronic Health cord (I) Data. *IEEE Trans. Emerg. Top. Comput. Intell.* **2021**, *5*, 541–553. [[CrossRef](#)]

88. Pace, P.; Aloï, G.; Gravina, R.; Caliciuri, G.; Fortino, G.; Liotta, A. An Edge-Based Architecture to Support Efficient Applications for Healthcare Industry 4.0. *IEEE Trans. Ind. Inform.* **2018**, *15*, 481–489. [[CrossRef](#)]
89. Wang, J.; Fu, Y.; Yang, X. An integrated system for building structural health monitoring and early warning based on an Internet of things approach. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147716689101. [[CrossRef](#)]
90. Alaiad, A.; Zhou, L. Patients' adoption of WSN-based smart home healthcare systems: An integrated model of facilitators and barriers. *IEEE Trans. Prof. Commun.* **2017**, *60*, 4–23. [[CrossRef](#)]
91. Leotta, M. An acceptance testing approach for Internet of Things systems. *IET Digit. Libr.* **2017**, *12*, 430–436.
92. Jeet, R.; Kang, S.S.; Hoque, S.M.S.; Dugbakie, B.N. Secure Model for IoT Healthcare System under Encrypted Blockchain Framework. *Secur. Commun. Netw.* **2022**, *2022*, 3940849. [[CrossRef](#)]
93. Chong, A.Y.-L.; Liu, M.J.; Luo, J.; Keng-Boon, O. Predicting RFID adoption in healthcare supply chain from the perspectives of users. *Int. J. Prod. Econ.* **2014**, *159*, 66–75. [[CrossRef](#)]
94. Shi, K. Research on the Security Enhanced Smart Hardware Assisted Regression Analysis and Health Monitoring Technique based Expanded Training Exercise Effect Evaluation Model. *Int. J. Secur. Its Appl.* **2016**, *10*, 311–324. [[CrossRef](#)]
95. La, H.J. A conceptual framework for trajectory-based medical analytics with IoT contexts. *J. Comput. Syst. Sci.* **2016**, *82*, 610–626. [[CrossRef](#)]
96. Quwaider, M.; Jararweh, Y. A cloud supported model for efficient community health awareness. *Pervasive Mob. Comput.* **2016**, *28*, 35–50. [[CrossRef](#)]
97. Saroja, S.; Haseena, S.; Blessa, B.P.M. Data-driven decision making in IoT healthcare systems-COVID-19: A case study. In *Smart Healthcare System Design: Security and Privacy Aspects*; John Wiley & Sons: Hoboken, NJ, USA, 2022; Chapter 3; pp. 63–90.
98. Gupta, V.; Singh, H.; Gill, P.; Singh, R.K. An energy-efficient fog-cloud based architecture for healthcare. *J. Stat. Manag. Syst.* **2018**, *21*, 529–537. [[CrossRef](#)]
99. Ould-Yahia, Y.; Banerjee, S.; Bouzeffrane, S.; Boucheneb, H. *Exploring Formal Strategy Framework for the Security in IoT towards e-Health Context Using Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 63–90. [[CrossRef](#)]
100. Hussain, A.; Wenbi, R.; da Silva, A.L.; Nadher, M.; Mudhish, M. Health and emergency-care platform for the elderly and disabled people in the Smart City. *J. Syst. Softw.* **2015**, *110*, 253–263. [[CrossRef](#)]
101. Ahmad, M.; Amin, M.B.; Hussain, S.; Kang, B.H.; Cheong, T.; Lee, S. Health Fog: A novel framework for health and wellness applications. *J. Supercomput.* **2016**, *72*, 3677–3695. [[CrossRef](#)]
102. Babar, M.; Rahman, A.; Arif, F.; Jeon, G. Energy-harvesting based on internet of things and big data analytics for smart health monitoring. *Sustain. Comput. Inform. Syst.* **2018**, *20*, 155–164. [[CrossRef](#)]
103. Gahlot, S.; Reddy, S.R.N.; Kumar, D. Review of Smart Health Monitoring Approaches with Survey Analysis and Proposed Framework. *IEEE Internet Things J.* **2018**, *6*, 2116–2127. [[CrossRef](#)]
104. Sicari, S.; Rizzardi, A.; Grieco, L.; Piro, G.; Coen-Porisini, A. A policy enforcement framework for Internet of Things applications in the smart health. *Smart Health* **2017**, *3–4*, 39–74. [[CrossRef](#)]
105. Rekha, K.; Sreenivas, T.; Kulkarni, A. Remote Monitoring and Reconfiguration of Environment and Structural Health Using Wireless Sensor Networks. *Mater. Today Proc.* **2018**, *5*, 1169–1175. [[CrossRef](#)]
106. Venčkauskas, A.; Štūkys, V.; Toldinas, J.; Jusas, N. A model-driven framework to develop personalized health monitoring. *Symmetry* **2016**, *8*, 65. [[CrossRef](#)]
107. Aktas, F.; Ceken, C.; Erdemli, Y.E. IoT-based healthcare framework for biomedical applications. *J. Med. Biol. Eng.* **2018**, *38*, 966–979. [[CrossRef](#)]
108. Javaid, M.; Khan, I.H. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J. Oral Biol. Craniofacial Res.* **2021**, *11*, 209–214. [[CrossRef](#)]
109. Sharma, P.; Kaur, P.D. Effectiveness of web-based social sensing in health information dissemination—A review. *Telemat. Inform.* **2017**, *34*, 194–219. [[CrossRef](#)]
110. Lohachab, A.; Karambir. ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. *J. Inf. Secur. Appl.* **2019**, *46*, 1–12. [[CrossRef](#)]