applied sciences

MDPI

Article

Taxonomic Exploration of Healthcare IoT: Challenges, Solutions, and Future Frontiers

Lutifa Alashlam [1,2] and Ahmad Alzubi [1,*]

[1] Department of Management Information Systems, Institute of Graduate Research and Studies, University of Mediterranean Karpasia, TRNC, 33010 Mersin, Turkey; 220635014@std.akun.edu.tr
[2] Department of Computer Science, Higher Institute of Science and Technology, Institute of Graduate Research and Studies, Qasr Ben Ghashir 22131, Libya
* Correspondence: ahmad.alzaubi@akun.edu.tr

Abstract: An Internet of things (IoT) ecosystem is a fast-developing network in which users can connect a heterogeneity of physical and virtual devices, including customized healthcare areas. As medical resources are scarce, populations are aging with chronic diseases and require remote monitoring, medical expenses are rising, and telemedicine is being demanded in developing nations, the IoT is an attractive topic in healthcare. Through the IoT, people can enjoy better health and diminish pressure on sanitary systems. In this study, previously published studies in Healthcare IoT (HIoT) systems are detailed, analyzed, and taxonomically classified. By categorizing the articles according to the types of HIoT systems, we dispense a detailed taxonomical study. In addition, different evaluation methodologies, tools, and metrics are discussed, along with their advantages and disadvantages. The studies indicate that power management, trust, privacy, fog computing, and resource management are among the open issues. The future of the Internet includes tactile networks, social networks, big data analytics, software-defined networking, network function virtualization, the Internet of nano things (IoNT), and blockchain. It would be beneficial to study and research HioT systems further in terms of interoperability, the implementation of real-world test beds, scalability, and mobility.

Keywords: Internet of Things; e-healthcare; smart environment; security

Citation: Alashlam, L.; Alzubi, A. Taxonomic Exploration of Healthcare IoT: Challenges, Solutions, and Future Frontiers. *Appl. Sci.* **2023**, *13*, 12135. https://doi.org/10.3390/app132212135

Academic Editor: Yoshiyasu Takefuji

Received: 2 September 2023
Revised: 31 October 2023
Accepted: 7 November 2023
Published: 8 November 2023

1. Introduction

Today's world has faced numerous obstacles relating to chronic disease public health issues caused by hazardous viruses such as COVID-19 [1]. The increase in health-related issues coupled with rising healthcare expenditures has encouraged people, especially the elderly and disabled, to manage their health remotely. Many industries, such as remote and smart healthcare systems, have benefitted from the IoT in the past few years as a network of interconnected objects [2]. As part of the IoT, popular technologies like wireless body area networks (WBANs), wireless sensor networks (WSNs), and radio frequency identification (RFID) are used to transpose data to the cloud, which can then be analyzed and used for instantaneous decision-making [3,4].

It is possible to make health management systems more customized, provident, and cost-effective by using the IoT, including mental health services and the worldwide pandemic [5–7]. This strategy categorizes IoT implementation in healthcare into three categories: tracking people and other objects (staff, medical teams, and patients), person authentication and identity, and autonomous data sensing and gathering. IoT-based health monitoring, like WBAN, enables hospitals to prevent and manage hospital infections, manage emergencies, and dispense post-discharge care anywhere. As a result, the healthcare industry is completely redefined by the IoT in terms of its devices, applications, and users [8,9]. Therefore, healthcare environments can be dramatically

revolutionized by leveraging IoT technologies such as connected medical sensors or special medical devices [10–12].

Through the use of HIoT technology in healthcare systems, medical devices are connected to the Internet so that appropriate therapeutic strategies can be developed for patients. Eldercare supervision, telemonitoring, teleconsultations, and computer-assisted rehabilitation are just some telehealth services offered by this technology [13]. Internet of medical things and HIoT are abbreviations that are frequently used interchangeably to refer to the integration of medical applications and equipment that can be linked to systems of health care information technology [14,15]. Meanwhile, big data combined with IoT can be used to support sanitary systems that are more effective in managing healthcare operations. The analysis of healthcare practices can now be prescriptive, autonomous, and predictive thanks to big data analytics [16].

Diabetes, obstructive lung disease, cancer, arthritis, and heart disease are some chronic diseases that can be managed remotely by customized healthcare [17,18]. Rarely do systematic literature reviews (SLR) of HIoT research clarify the overall development and pinpoint particular research problems, patterns, and future directions [19,20]. Investigating an HIoT research plan is essential given the increased interest in the IoT in healthcare. Discovering, classifying, and synthesizing a comparative technique of inquiry through a systematic review may lead to the transposition of knowledge within research organizations [21,22].

1.1. Motivation

Numerous pieces of research have revealed that new criteria not typically addressed in traditional IoT systems are present in smart health products [10]. They have also shown how in order to fully utilize these technologies' capabilities, those needs must be met by a piece of infrastructure designed with them in mind. Significantly, data accessibility coupled with contemporary intelligent processing algorithms at previously unanticipated scales and temporal longitudes can (a) simplify a change in the medical profession from the current reactive method of post facto diagnosis and care to a practical system for illness prognosis at an early level, combined with the prevention, treatment, and general health rather than disease management; (b) enable customization of care; and (c) improve the quality of life of people with chronic illnesses [5]. As a result, adequate methods and strategies must be provided to ensure proper medical distribution, based on standards like authenticating and providing quick assistance. The articles that were looked into claim that there is not a thorough, organized document reviewing IoT-based medical management solutions. As a result, an effort has been made to close this gap. Therefore, the goal of this study was to perform an extensive literature assessment of contemporary IoT techniques in the medical industry. Additionally, difficulties are examined, and some directions for future research are offered.

1.2. Contributions

IoT-based medical management solutions are therefore studied in this study. In conclusion, past research has been thoroughly examined, and future work has been identified. The pros and cons of the various filters are outlined in the technique section before the IoT articles on health systems are chosen and analysed. Then, some solutions for future investigations are proposed based on their shortcomings and inadequacies. These have the following goals.

- Examining primary approaches to IoT-based medical management systems;
- Presenting an SLR and examining possible approaches to IoT-based medical management systems;
- Discussing important IoT challenges within the context of the methodologies under discussion;
- Offering the category of the methods investigated and highlighting their key characteristics.

1.3. Roadmap of the SLR

To this end, we intend to analyze previous studies in order to answer the following research questions:

- Why should IoT be incorporated into healthcare systems, practically speaking?
- What are the available research fields for IoT-based healthcare systems?
- What triumphs have been attained in this area?
- What current procedures and strategies are being used to integrate IoT into healthcare systems?
- What are the key challenges facing the IoT, its emerging trends, and open questions?
- What new HIoT system research areas should be developed?

We followed recommendations to conduct an SLR with the goal of identifying, categorizing, and systematically comparing current papers focusing on IoT in healthcare [23,24]. HIoT works are presented, systematically identified, and taxonomically classified in this study. As a result, we will be able to analyze the constraints and potentials of the current papers in a more comprehensive manner. This study offers a thorough analysis of recent studies on practical methodologies, tools, and approaches in HIoT. In order to assess the necessity of upgrading HIoT systems and to introduce unresolved issues and upcoming trends, prior research is therefore chosen, collocated, and contrasted.

This article examines the existing study approaches, methodology, best practices, and experiences in HIoT.

The articles selected for the SLR are based on an automated search in top databases such as Google Scholar, ScienceDirect, etc., based on relevant keywords such as healthcare IoT, medical diagnostic systems, smart healthcare, IoT in healthcare, etc. Further, inclusion–exclusion criteria are applied to the selected articles. The inclusion criteria are as follows:

- Studies that define the use of IoT in healthcare;
- Studies made by researchers and professionals;
- Peer-reviewed articles;
- Articles published in English.

Only one exclusion criterion is considered: studies published in journals. The rationale behind this exclusion criterion is that textbooks, white papers, dissertations, and editorial notes were omitted, as research scholars and professionals frequently collect information and publish new studies. The articles considered are from familiar publishers such as Elsevier, IEEE, Springer, MDPI, Taylor & Francis, Wiley, etc. This SLR also shows how quickly IoT research is developing, and how important it is for healthcare systems. In the examples listed below, the results of this SLR are impressive.

- IoT and contemporary healthcare researchers want to analyze the related investigations;
- Medical professionals are interested in applying modern methods, approaches, strategies, and technologies while working within the constraints of HIoT systems.

The remainder of this SLR is structured as follows: The background is presented in Section 2, and Section 3 provides an explanation of the pertinent literature reviews on HIoT. Section 4 discusses the research methodology in several ways. Section 5 presents the results and discussions. Section 6 also addresses unresolved issues and potential developments. Section 7 contains the conclusion and the scope for future research.

2. Background

IoT and healthcare are briefly defined in this section. An introduction to IoT and healthcare is given first. Then, a description of HIoT's layered architecture follows. Finally, the main metrics used in this study are described.

2.1. Internet of Things

Ashton et al. defined the phrase "Internet of Things" for the first time in the context of supply management [25]. Now, several IoT concepts are possible, including addressing

devices on a network and ensuring that they are uniquely identified. These devices communicate with computers to transpose data and extract critical information that allows them to dispense suitable services more effectively. In other words, the IoT is a collection of numerous hardware components, such as different types of sensors and actuators, that connect to and communicate with one another online.

A typical IoT ecosystem also contains cloud interfaces, complicated algorithms, sensors, communication interfaces, and privacy-protecting algorithms. Data collection from a range of devices is the responsibility of sensors. Network and communication infrastructures are also dispensed by RFID and WSN technologies, and sophisticated algorithms are used to process and handle data. Users can ingress various services at once thanks to the cloud environment's capacity for numerous client/server requests. Fog computing addresses these problems and enables instantaneous analysis and rapid decision-making near users by eliminating latency, dependability, resource constraints, and other problems associated with cloud computing.

Moreover, IoT ecosystems feature communication interfaces, sensors, sophisticated algorithms, and cloud interfaces [26,27]. Data collection from a range of devices is the responsibility of sensors. Network and communication infrastructures are also dispensed by RFID and WSN technologies, and sophisticated algorithms are used to process and handle data. Due to problems with latency, dependability, resource constraints, and other aspects of cloud computing, fog computing was created to circumvent these problems and execute the same applications anywhere near users with instantaneous analysis and swift decision-making capabilities [28].

Although IoT has advanced dramatically, it is still in its nascent stages. There are numerous study concerns such as standardisation, device heterogeneity, scalability, security, and privacy [29,30]. A unique issue in this industry is the interoperability of smart devices, which enables the integration of diverse devices and multi-vendor systems. Furthermore, a key element of IoT is the low-cost interoperability of smart objects, which will soon enable clients to continue working with numerous providers [31–33]. IoT can also help lessen construction costs, simplify organizational infrastructure challenges, and support diverse infrastructure.

Nowadays, the IoT paradigm encompasses a wide range of applications such as transportation, smart cities, monitoring, healthcare, and so on [34,35]. Despite the variety of IoT devices, it is simple to link, collect, and compare data in IoT applications like smart cities and smart homes in order to adjust to people's needs. The adoption of the IoT paradigm, for instance, has the potential to revolutionize sanitary systems in the healthcare sector [36]. It can be useful for telemonitoring in the hospital, as well as at home for elderly people with chronic conditions [37,38]. The application of this technology will help healthcare systems in the future to dispense high-quality care at low hospitalisation costs, with diminished response times in detecting anomalies and longer life spans.

2.2. Healthcare

As well as other factors related to the pandemic, such as high prices, long distances, and quarantine requirements, the world is currently shaped by epidemics and infectious diseases spreading more widely, including COVID-19. Many elderly and disabled people suffer from chronic diseases, so it is difficult, if not impossible, for them to go to medical centres [39]. A practical, comprehensive, computer-aided technology is therefore essential to offer patients long-term care and remote medical monitoring while minimizing financial burden.

Through the analysis of large amounts of data, IoT has revolutionized sanitary systems, turning them into intelligent and predictive systems. IoT devices have been connected to record patients' physiological data instantaneously, including blood glucose levels, temperature monitors, and other crucial information. Patients will benefit from novel medical services, including early diagnosis and continuous monitoring of serious diseases [40,41]. The IoT has several applications in the field of health care, including remote clinical monitor-

ing, assisted living, chronic disease management, and preventative treatment. In addition, there are a number of IoT applications in healthcare, including home healthcare, mobile health, and e-healthcare.

As a result, IoT technology has allowed healthcare processes to be managed smartly, and self-care is possible. To prevent pharmaceutical errors and human error, some events can be identified, such as seizures, falls due to Parkinson's disease, stroke rehabilitation, neurologic monitoring, and heart monitoring [42–44]. However, further hurdles remain to be overcome in order to produce successful and safe healthcare applications [45,46]. Numerous security protocols are available today to preserve data from assaults and threats.

The perception layer, networking layer, middleware layer, and application layer make up the HIoT system's prominent basic four-layered architecture. The following are the explanations of the layers.

1. Perception Layer: At the bottom of the hierarchy, we have this layer, which we may refer to as 'hardware' or 'physical'. By collecting and signalling data, this layer prepares data for transmission to the network layer.
2. Network Layer: In this layer, all smart devices are connected, and health data can be exchanged among them. The cutting-edge technologies used by this layer allow patients to securely transmit and receive health data from the base station.
3. Middleware Layer: In this layer, services are dispensed with names and addresses associated with requests. Non-homogeneous items can be used with HIoT applications without requiring peculiar equipment platforms. Health data are collected from the network layer and cached here.
4. Application Layer: Data from other layers are analyzed and combined in this layer to dispense healthcare services. Healthcare services can be dispensed at this layer to meet the needs of patients. In this layer, graphs, business models, and flowcharts that control all activities and healthcare services can be produced. HIoT systems cannot succeed without technological innovations, business models, and appropriate business models.

An IoT-based healthcare system known as HIoT also consists of three key phases of a workflow, namely data creation, data processing, and information consumption. The phases mentioned are described as follows.

(1) Data generation: The process of generating the required data involves using a variety of sensors, medical devices, and even direct data entry by patients or other involved healthcare teams. The perception layer is used for this phase, while the network layer is used to transpose the data collected.
(2) Data processing: In the data processing stage, collected data are analysed using well-known mechanisms including machine learning techniques and data analysis tools. Through the middleware layer, this stage is completed.
(3) Information consuming: In the information consumption phase, any decisions that medical teams must make on behalf of patients can be made utilizing the outputs and analytics from the data processing phase. This analytical information can even be used to activate the actuators. The application and business layers are used for this phase.

For greater understanding, the aforementioned processes are depicted in Figure 1 in a layered IoT architecture of a healthcare ecosystem. Wearable sensors are used to gather the user's vital signs, as seen in this picture. An infrared link is then used to transmit the data to the smartphone. Finally, the data are communicated from the mobile device to the server across a network, such as an advanced fifth-generation network. By pressing a button, the database server receives information from sensors or the patient's details in an instantaneous way [47].

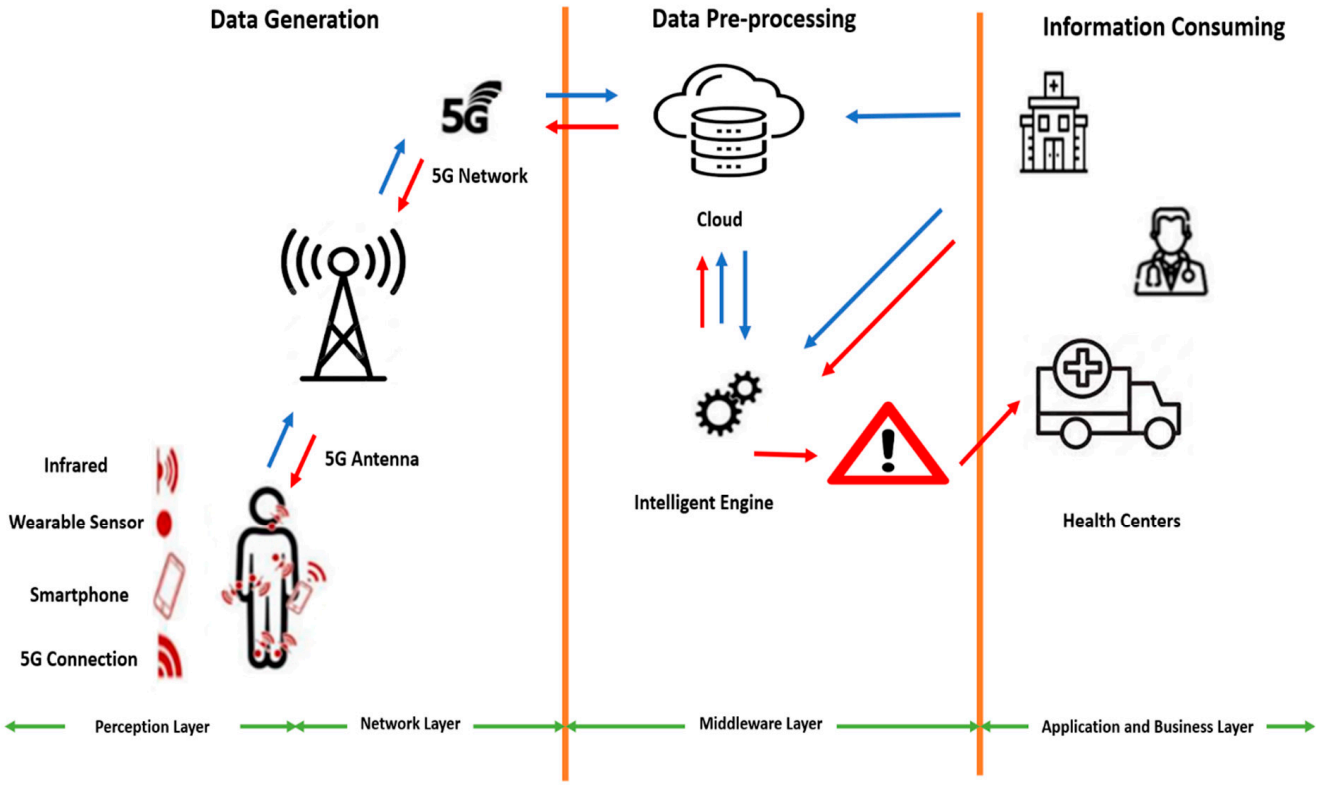

Figure 1. Layered architecture of IoT in healthcare.

Other information is gathered from healthcare facilities and stored in the database, such as physician opinions and medical analytics. The intuitive engine of the system then studies the data that have been stored in the database to determine whether any aberrant data have occurred. An alarm is transmitted to the patient or doctor when the system recognizes an abnormal situation, and the patient is admitted to the hospital if the alarm is accepted. As a consequence of recent improvements in healthcare systems and digital communications, it is now feasible to connect to remote healthcare services from any location, providing patients with the greatest options for personalized healthcare services.

2.3. Criteria for Evaluating HIoT Approaches

The criteria used to evaluate the suggested HIoT techniques are described in this section.

(1) Security and Privacy: Smart healthcare systems must prioritise security and privacy in order to protect health data against attacks such as side-channel attacks, physical attacks, and malicious attacks, as well as to maintain privacy and prevent unauthorised ingress to health data.
(2) Accuracy: Accuracy is essential for healthcare system carers. Depending on how the system is used, accuracy in healthcare IoT systems refers to how accurately the data collected reflect the patient's condition, how accurate the data used in the computation were, and how accurately the decision was made.
(3) Performance: Healthcare providers must perform well in order to obtain precise data, process the data, and offer services quickly. This parameter is a combination of efficiency, load balancing, resource utilization, overhead, and computing time, as well as network quality of service (QoS) factors including throughput, latency, delivery rate, mean time between failures, and bandwidth usage.
(4) Time: The time it takes for consumers to receive service after making a request is described by this parameter. The concept of time encompasses calculation time,

average response time, execution time (run-time), and latency (as the time lag in healthcare systems).

(5) Cost: This refers to the overall expense a patient who requests healthcare services may incur to receive the best care possible. The cost of computation, communication, data storage, and the upkeep of the desired service are all included.

(6) Energy: Energy conservation is crucial for device and network survival, since HIoT devices lack resources and are powered with meagre energy resources. Additionally, when there are more HIoT devices linked to the network, the network's energy usage grows as well. On the other hand, more energy use results in higher operating expenses, more carbon dioxide produced, and a shorter network lifetime.

(7) Interoperability: Interoperability refers to the capability of more than two HIoT systems to communicate and exchange information in a dependable, consistent, and efficient manner, use the information exchanged, and share resources. More than one medical informatics system, for example, may be necessary. The capacity to successfully grasp data across organizational or system boundaries is referred to as data interoperability. HIoT systems require the usage of standardized communication as well as a number of other interoperability-supporting technologies.

(8) Scalability: This refers to the capability of the system to extend and build an IoT-based healthcare methodology as service needs and expectations grow. These capabilities can be leveraged to create smart devices, new operations that act as user service nodes, and network infrastructures, while not adjusting the quality or effectiveness of healthcare services. Extending the system requires either the addition of new hardware or services or improvement of the operation of current hardware or services.

(9) Reliability: The capacity of a system to carry out its necessary functions under pre-determined circumstances and at a predetermined time. A healthcare system based on IoT is said to be reliable if it can provide requested services to patients in most conditions.

Research question 1 has been addressed in this section through our discussion of the layered architecture of healthcare IoT and steps to evaluate different HIoT approaches.

3. Related Works

IoT healthcare systems developed from clinic-based systems to customer-based systems were discussed by Farahani et al. [48]. A multi-layer IoT healthcare architecture with device, fog, and cloud layers has also been created to transform traditional healthcare systems into intuitive healthcare systems. Important products and services, on the other hand, were discussed, including mobile health, anomaly detection, early warning scores, ambient assisted living, and two real-world case studies involving smart eyewear for covert continuous heart rate monitoring and smart gloves in IoT for Parkinson's disease. Some of the difficulties and constraints of this market are data management, scalability, security, privacy, interoperability, and standardization. However, it should be highlighted that this study was not carried out methodically, and did not take into account the years covered by the evaluated publications, the taxonomy, the articles chosen, or future research.

Cloud IoT-health, a paradigm for cloud computing with the IoT, was introduced by Darwish et al. [49]. Before introducing the IoT and cloud computing as brand-new technologies for use in healthcare systems, the authors of this paper dispensed a full overview of their histories and current applications in healthcare systems. Then, particular challenges and issues within this spectrum were identified, including standardization, storage, scalability, and adaptability. Despite offering sufficient arguments, this evaluation was not systematic, the process for selecting the papers was murky, no taxonomy was supplied for the chosen studies, and the analyzed publications' covered years were not specified.

A study on advanced IoT that offers individualized healthcare solutions was presented by Qi et al. [50]. A four-layer design with levels for sensors, networks, data processing, and applications was developed for this inquiry, and the technology employed in each of

these tiers was fully explained. The authors also discussed the challenges of encouraging researchers to conduct fresh research. The structuring of this survey, however, was lacking, and it was not evident how the papers were picked. The papers under consideration did not cover any certain years, and no taxonomy of the publications under study was dispensed.

Qi et al. developed their idea into four layers using an IoT layer-based method and proposed a physical activity recognition and monitoring architecture. Emerging tendencies were also described for researchers [51]. However, this review was not carried out methodically, despite the article's title. Additionally, there was no special method of choosing the researched articles or any sort of classification to dispense readers with a clear picture. Additionally, articles published in 2019 and 2020 were not taken into account. Additionally, Dhanvijay and Patil dispensed a survey that examined the most significant recent technological advancements and how they may be used in IoT healthcare systems [52]. They focused particularly on WBAN and its security features.

In today's real-time applications, QoS and quality of experience (QoE) play a vital role. HIoT service systems are related to various types of quality indicators which can be qualitative/quantitative, discrete/continuous, etc. There are recent studies that propose an overall model normalization for the adequate prediction and presentation of QoS/QoE in telecommunication systems that are used for better quality estimation. The overall normalization of the quality models is an important step to adequately estimate the quality in use, which cannot be assessed due to the differences between the various software products [53–55]. Silva et al. proposed a QoE model for providing context-aware electronic healthcare services. This model improved the user experience by producing better quality in the provision of healthcare services [56]. Narralla et al. surveyed QoE in mobile healthcare. They explored the role of 6G technology in order to enhance both QoS and QoE. They concluded that not only is QoS sufficient in healthcare, but QoE is also needed in the modern healthcare environment [57].

Additionally, a classification based on technology was used to give researchers a clearer picture. Additionally, a few obstacles to developing this subject in future works have been addressed. However, this inquiry was not methodical, the selection of the papers was not precise, and no reference was made to the years that the papers were covered. Research question 2 has been addressed in this section. Table 1 tabulates the pros and cons of existing HIoT systems. In most of the works, security is a major issue.

Table 1. Pros and cons of existing HIoT systems.

References	Advantages	Disadvantages
[20]/2020	Efficient in terms of energy and battery	Lack of interoperability techniques and methods
[11]/2021	Fewer maintenance costs and duplicate patient entries	Failed to identify errors in a timely manner
[23]/2021	High efficiency	Lack of data collection and statistical analysis code
[24]/2021	Improved decision-making skills	Not suitable for real-time deployment
[8]/2022	Security solution for managing and tracking IoMT devices	Restriction imposed on execution in a real network
[26]/2022	High utilization of resources	Lack of service quality
[32]/2022	Scalable	Lack of data for model construction
[40]/2022	Reliable approach	Not resistant to future attacks
[57]/2023	High reliability and accuracy	Not tested for deployment in real time

4. Research Methodology

It is impossible to read through the pertinent reports on evidence-based practices. To support this practise, experts must assemble research. The purpose of the thorough review is to locate, assess, and evaluate all reports that are currently available for a specific research question or subject area. The SLR is performed based on the following phases:

- Planning and conducting

- Reviewing process
- Inclusion and exclusion
- Quality assessment

4.1. Plan and Conduct

The choice of the report was completed in three stages, including: Stage 1: automated search; Stage 2: article selection; and Stage 3: publication and related analysis.

Using specific keywords like healthcare IoT, medical IoT, smart healthcare, etc., in Stage 1, we used Emerald, Google Scholar, ABI/Inform Global ProQuest, and ScienceDirect as major search engines to find related papers. Thus, the search method is used to automatically find 72 papers from books, magazines, and conferences. In Stage 2, a quality evaluation checklist was created to evaluate only original publications published between 2015 and 2023 in peer-reviewed journals. In Stage 3, researchers examined the selected publications to determine their applicability.

4.2. Review Process

The review process is performed based on certain inquiries. The following inquiries are on the checklist:

- Will the study make the review procedure very clear?
- Is the analysis approach appropriate for the topic under consideration?
- Was the research evaluation carried out correctly?

'Yes' is entered if the analysis satisfies the assessment requirements.

The main search is performed using first-level keywords such as IoT, healthcare, smart health, IoMT, etc. Further, an extended search has been performed.

4.3. Inclusion and Exclusion Criteria

The publishing year, topic approach, and journal rating are the primary issues in each paper that need to be included or excluded. Table 2 lists the exclusion–inclusion criteria for the HIoT analysis.

Table 2. Review of the exclusion–inclusion standards.

Criterion	Rationale
Inclusion 1. Research that outlined the healthcare IoT explicitly	Articles that directly offered IoT-based medical management systems are sought, since this inquiry intends to determine how IoT affects those systems
Inclusion 2. Studies conducted by academics or professionals	This study has implications for both commercial and educational strategies
Inclusion 3. Published studies in the field of healthcare IoT	Healthcare IoT serves as the reference domain
Inclusion 4. A paper subjected to peer-review	A peer-reviewed article guarantees a particular level of consistency and has a reasonable amount of substance
Inclusion 5. A report written in English	For reasons of viability, articles published in languages other than English are excluded
Exclusion 1. Research that is exclusively published in journals	Since academics and professionals use journals more regularly to gather data and disseminate new research, conference articles, books, unpublished working papers, master's and doctorate dissertations, and editorial notes were excluded

4.4. Quality Assessment

Finally, the quality of the papers was assessed and included for review. The chosen papers were optimised using three criteria, viz., monitoring of HIoT system, patient infor-

mation analysis, and security architectures. After filters were applied, five well-known publishers and articles pertinent to healthcare IoT were chosen, leaving 36 papers out. Finally, 36 papers were collected and examined. The study's selection was one that has undoubtedly looked into the design and deployment of healthcare IoT systems; has clearly and concisely stated their suggested process; and has detailed some thought-out parameters. Figure 2 depicts the methodology used to categorize the papers. The scanning technique produced 36 related papers for additional investigation (30 research articles and 6 review articles).

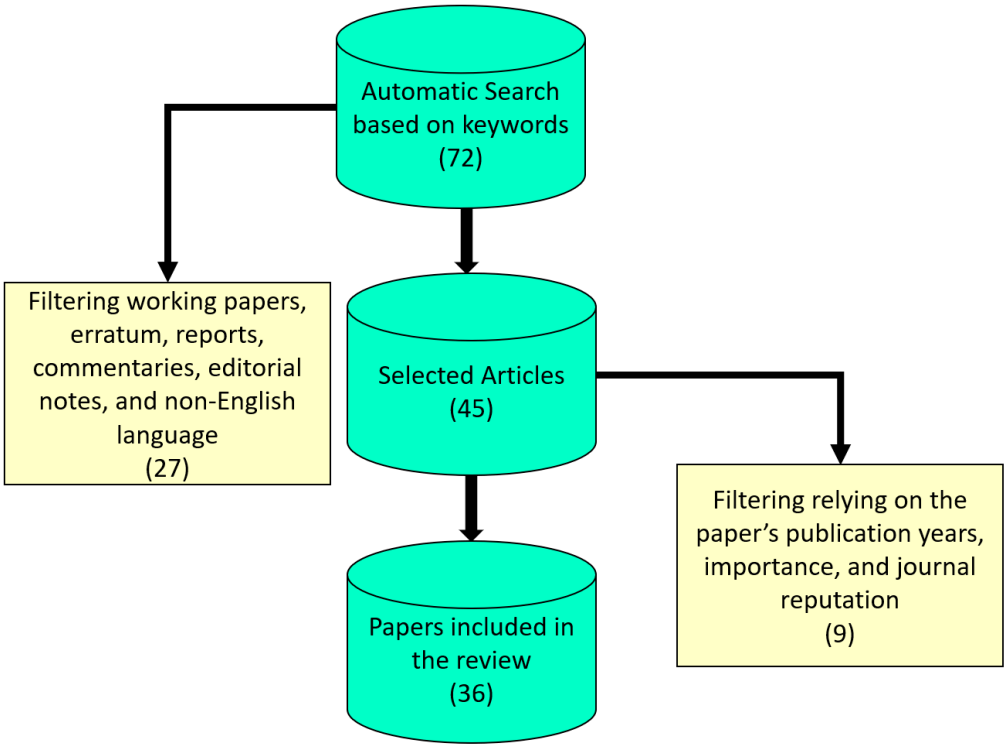

Figure 2. Overview of the paper selection procedure.

Research question 4 is addressed as follows. Sensor-based, resource-based, communication-based, application-based, and security-based techniques are the five divisions in the taxonomy of IoT-based healthcare technologies. The taxonomy of IoT-based healthcare strategies is shown in Figure 3.

4.5. Sensor-Based Approaches

A review of the publications revealed that some publications associated with HIoT focused on wearable sensors and environmental sensors, and could be categorized accordingly.

4.5.1. Wearable Sensors

According to Ray et al. [58], galvanic skin response data are amplified, gathered, and analysed in smart e-healthcare apps to identify an individual's level of human physiological activity. Furthermore, users' cell phones display the collected data with low power consumption. However, there was a lack of regard for security and privacy concerns. Bhatia and Sood proposed an intuitive healthcare system that can provide pervasive healthcare along with workouts by assessing instantaneous health conditions acquired from gyms across wristbands and anticipating health status deficiencies using artificial neural networks [59]. The test results confirmed the great performance and efficiency of the suggested system.

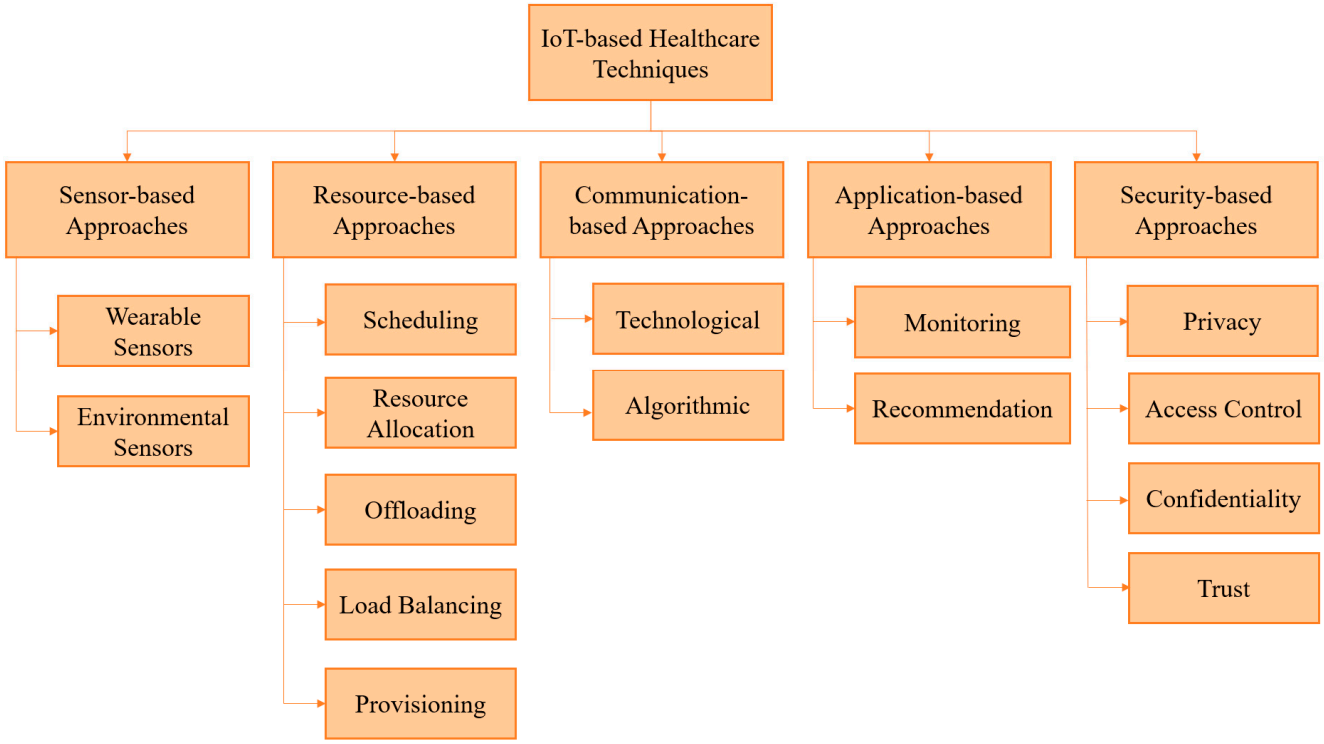

Figure 3. Taxonomy of IoT-based healthcare techniques.

4.5.2. Environmental Sensors

Vilela et al. proposed a fog-assisted health monitoring system for instantaneous applications, and they demonstrated the system's high performance and security using a hospital [60]. However, a major obstacle in this investigation was the interoperability of diverse devices. Ray et al. prototyped a non-invasive, low-power, and economically viable sensor system to detect intravenous fluid bag levels instantaneously for use in e-healthcare applications [61]. Carers may utilize this tool to monitor intravenous fluid bag status online, and estimate when bags will run out of fluid.

4.6. Resource-Based Approaches

As a consequence of the variability in available resources, resource limits, and the dynamic and unexpected character of the HIoT environment, resource management difficulties must be considered among the most difficult.

4.6.1. Scheduling

Ray et al. looked into three potential uses for IoT that could take advantage of instantaneous impacts [58]. The researchers also created a context-sensible fog computing-based architecture for time-critical applications, as well as a delay-tolerant technique for dynamically distributing different workloads to resources. In order to balance the load from healthcare systems to fog and cloud nodes, Abdelmoneem et al. proposed a dynamically distributed scheduling and allocation technique based on patient movement [4].

4.6.2. Resource Allocation

Asif et al. demonstrated an instantaneous HIoT framework with software-defined networks (SDN) and connection flexibility [62]. This paradigm also placed a heavy emphasis on allocating resources as efficiently as feasible. This system offers strong QoS, small packet loss and small end-to-end latency, according to the simulation. However, the system is overly complex and lacks proper security. Kavitha and Sharma demonstrated how ant colony optimisation (ACO) may effectively use cloud resources and speed up response times in life-critical healthcare applications by replacing ACO with a traditional

first-come first-served virtual machine allocation technique [63]. Stefanova et al. proposed a telehealth service that is modelled with generalized nets. This model was used to track the changes in the health status of patients. In this model, telecommunications and navigation technologies were used to monitor both active and mobile patients. The model used the current location of the patient as one of the vital variables [64].

4.6.3. Offloading

Using the reinforcement learning technique, Min et al. introduced a privacy-aware system to assist IoT healthcare equipment in protecting privacy [65]. In fact, this technique aids HIoT devices in choosing the offloading rate, boosts computing efficiency, lowers latency, safeguards user privacy, and conserves energy. Wang and Li used the in-network caching and request accumulation capabilities of fog computing to minimize the latency of retrieving patient data by approximately 28.5% [66].

4.6.4. Load Balancing

He et al. developed a provident hierarchical fog-cloud computing architecture for sophisticated event filtering to address the entanglement of tailored services in massive healthcare applications [67]. The load-balancing technique for fog computing was devised utilizing graph partitioning theory. The efficacy, instantaneous detection, minimum latency, and redundancy of this approach were all demonstrated. Bharathi et al. suggested an energy-efficient sensor clustering method for selecting cluster heads [68]. They made an effort to optimize factors including energy usage, sensitivity, specificity, accuracy, and F-score.

4.6.5. Provisioning

Kumar and Silambarasan presented artificial bee colony (ABC) optimization, cuckoo search optimization, and particle swarm optimization as three resource optimization strategies for scheduling resources for virtual machines in a cloud system [69]. The ABC was more effective than the other two approaches, according to the simulation data.

4.7. Communication-Based Approaches

The methods based on communication fall under the next classification category. This section discusses technological and algorithmic methods for managing communications through communication infrastructures.

4.7.1. Technological

A smart hospital system based on IoT, according to Caribinucci et al., provides automatic instantaneous observation of patients, workers, and biomedical devices in nursing institutions and hospitals for emergencies by merging several technologies such as smart mobile, RFID, and WSN [70]. Catherwood et al. introduced a LoRa/Bluetooth-enabled electronic reader and an IoT-based analyzer for customized monitoring with good coverage, mobility, and ease of installation [71].

4.7.2. Algorithmic

Qiu et al. [72] demonstrated a self-retrievable time synchronization system with a high level of balanced energy utilization and accuracy for IoT sensor networks. Almobaideen et al. [73] devised a method for choosing a route based on the proximity of medical facilities, as well as the quickest route for visitors with certain health issues and continuous monitoring in crises. To operate personal healthcare devices, Woo et al. use a fault-tolerant M2M-based IoT system with substitute copies [74].

4.8. Application-Based Approaches

Systems based on application-based approaches typically dispense one or more of the following services. A medical IoT-based system also encompasses resource management,

communication infrastructure, and sensors to dispense patient, caregiver, and user services. This segment of the application-based category includes two subcategories: monitoring systems and recommender systems.

4.8.1. Monitoring

Sood and Mahajan presented a healthcare monitoring technique based on IoT and fog for the treatment of hypertension. This healthcare monitoring technique was contrasted with cloud computing technology to demonstrate its high precision in reaction time, low latency, and good bandwidth efficiency [75]. Furthermore, an artificial neural network was used for predicting the severity of hypertension. As reported by Verma et al., their smart tracking student interactive healthcare system measures symptoms of aquatic illness for the purpose of identifying certain diseases using machine learning techniques based on k-cross validation [76]. Based on the simulation, it was shown that the suggested methodology performed better in terms of quick responses and accuracy.

4.8.2. Recommendation

Ullah et al. created a large data model with semantic interoperability for diverse IoT devices in order to collect users' sickness symptoms and propose medications with undesirable effects [77]. Ali et al. created a long-term care healthcare system based on IoT to collect patient risk indicators and diabetes drugs [78]. They also demonstrated a successful fuzzy ontology-based recommendation system which is based on a decision-making approach. Additionally, this system guards against unauthorized ingress to patient data. To validate this system, the performance, prediction accuracy, and suggestion precision were assessed.

4.9. Security-Based Approaches

The final category, security-based approaches, addresses aspects of a secure HIoT system such as privacy, access control, secrecy, and trust in order to provide QoS in HIoT.

4.9.1. Privacy

To ensure privacy, data integrity, and authentication, Boussada et al. proposed a privacy-preserving HIoT technique with a featherlight identity-based encryption algorithm [79]. The results of the experiments proved the technique's efficacy, privacy preservation, and diminished transmission time. Elmisery and colleagues created a seclusion-based fog middleware for HIoT that validated the proposed cloud-based healthcare service. Game theory, according to the authors, was essential for this model to have superior HIoT device groupings [80].

4.9.2. Access Control

Pal et al. developed a policy-based ingress control system to restrict unauthorized access to HIoT's limited resources [81]. Furthermore, to improve reaction time, the authors adopted a distributed architecture. Yang et al. demonstrated an HIoT-based system with self-flexible ingress control for authorized users in both normal and emergency situations. According to simulation data [82], the system surpassed the existing systems in terms of computational cost and efficiency.

4.9.3. Confidentiality

Kaw et al. designed a secure architecture that leverages information hiding in encrypted graphics in which the clients' data are protected and prevented from unauthorized access [83]. This project decreased computer costs as well as security concerns. A guided alternative quantum walk based on image encryption was introduced by El-Latif et al. to secure healthcare images in IoT from eavesdropping [84]. Simulation and numerical analysis were used to illustrate the system's effectiveness and security. To solve resource limits while still meeting storage, security, and privacy requirements, the authors developed a hybrid IoT-fog-cloud system that distributes fog between IoT

devices and the cloud [85]. Additionally, the system combined fine-grained ingress control with keyword-searchable encryption.

4.9.4. Trust

Manogaran et al. proposed the design of HIoT approaches within body-area sensor networks (BSN) to reserve, analyze, and assess huge amounts of data, with a focus on security [86]. Additionally, a map reduce-based prediction model was employed in this architecture to forecast heart disorders. The BSN-Care security and privacy framework was developed by Gope and Hwang to effectively meet the numerous security needs of BSN-based healthcare systems [87].

5. Results and Discussions

Research question 3 is addressed in this section. In total, 36 publications have been analyzed systematically to perform the review. The articles considered are from familiar publishers such as Elsevier, IEEE, Springer, MDPI, Taylor & Francis, Wiley, etc. Around 30% of the articles are from Elsevier, 24% are from Springer, 26% are from IEEE, and 20% are from other publishers such as MDPI, Taylor & Francis, Emerald, IOP, etc. Figure 4 depicts the percentage of publications from database sources. The publications demonstrate that IoT holds a lot of promise for clinical settings and healthcare. IoT may also be applied to medical applications that can save lives or enhance quality of life through monitoring habits, tracking health-related metrics, assisting with independent living, regulating drug use, etc. Internet-based patient systems have the potential to be helpful tools for public health organisations to maximise their efficacy, similar to IoT healthcare solutions.

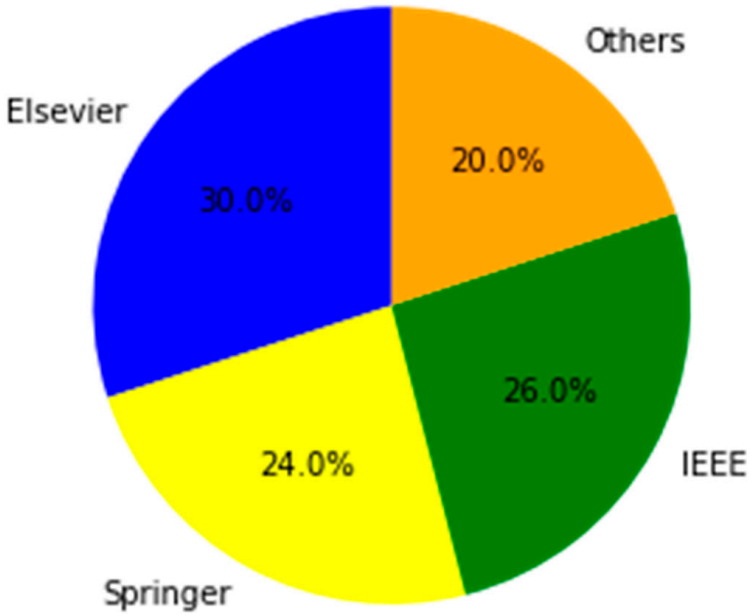

Figure 4. Percentage of publications relying on database sources.

Healthcare organisations supported by IoT operate with big data, which entails data-handling techniques like data gathering, mining, and analysis. Greater threat might result from attackers starting to alter data in order to give feedback to IoT devices. Risks linked with IoT devices used in healthcare management systems include the lack of a strong encryption strategy, a faultless access system, insufficient ability to protect personal privacy, and issues with mobile device security.

We looked at and analysed the factors that influence IoT-based medical systems. The attributes of IoT-based medical management systems are shown in Table 3. These factors' effects could be advantageous or harmful. Additionally, some of the mentioned properties

are reported indirectly. As a result, implicit qualities are identified and scored via a content analysis of the chosen articles that have been discussed with respect to these attributes.

Table 3. Attributes of IoT-based healthcare systems.

Attributes	Explanation
Response time	The reaction time of a task is the amount of time that passes between when a task is entered into the system and when it is completed.
Cost	The cost of running or maintaining the IoT at a particular time.
Flexibility	Flexibility is the ease with which IoT responds to unpredictability.
Scalability	The ability of an IoT system to handle a growing number of subscribers is referred to as scalability.
Security	Security prevents unauthorised access to or misdirection of the services provided by IoT devices' hardware, software, or data.
Efficiency	Efficiency is the ratio of productive labour to IoT resources, which translates to the output-to-input ratio for a fog device.
Real-time	The medical system requires quick action. Real-time data production, evaluation, and monitoring are crucial for tracking critical health issues, keeping tabs on outbreaks and pathogens, and hastening the adoption of remedies before the healthcare system becomes overburdened.
Overhead	In addition to the immediate costs of providing an item or service, overhead also refers to the ongoing costs of running a firm.

6. Open Concerns and Potential Developments

There are presently significant difficulties that must be solved in order to construct IoT-based healthcare systems, but they have received little attention according to recent research trends. After assessing the data acquired through this assessment as well as the expanding requirements for deploying efficient HIoT approaches in the tangible world, we discovered that open affairs, challenges, and upcoming directions in the HIoT sector may be split into separate groups. Another key impediment to the development of IoT systems is the shortfall of a real-world experimental set up environment for analysing their performance. Unresolved issues in the computing environments in which HIoT systems are designed and installed, such as fog computing, as well as some operational and technical issues, such as power and resource management affairs relating to fog node storage and computing capacity constraints, must be addressed. Multi-objective optimization and trust assurance are two further unresolved difficulties in HIoT systems. Given the increased demand for computer-aided approaches in the development of healthcare systems, a variety of HIoT techniques, including IoNT, blockchain, etc., could be regarded as upcoming trends in the healthcare field. The next section provides additional information on the aforementioned obstacles, challenges, and trends.

6.1. Issues

Smart healthcare management based on IoT faces the following issues:

(1) Trust and Privacy: Trust and privacy management is a significant open problem in IoT-based healthcare systems for data ingress and storage. Controlling access to credentials, protecting the privacy of patients and service providers, and preventing unauthorized access to any of these are all examples of trust. IoT-based systems for the healthcare industry are developed based on the data collected by IoT devices. As IoT devices are connected to the network, their susceptibility to data breaches rises [43]. However, the analyzed studies show that only a few papers have properly assessed this important parameter. As a result, trust and privacy are extremely difficult to sustain, as open concerns. Reducing the risk of critical data being hacked and improving data security is especially tough.

(2) Power Management: Reduced energy usage, according to the reviewed literature, is the key to minimizing high operational costs and large carbon emissions in HIoT systems. Furthermore, a typical HIoT network is made up of tiny devices with limited battery life. As a result, fundamental features such as data migration and systematic standby control are critical to minimizing energy consumption while maintaining the quality of smart healthcare services. As a result, low-power devices must be developed in order to extend the life of HIoT systems and limit the likelihood of patients being disconnected. As a result, another challenge for HIoT is power management [44].

(3) Fog Computing: Fog computing, which is location-aware and dependent on environment, context, and application needs, is an integral part of healthcare IoT. Furthermore, low and predictable latency is required to deliver services to end users in emergency situations, to save bandwidth, and save battery usage while essential data are delivered to the fog for processing and storing, and to diminish the volume of data transposed to the cloud. More activities are required to fulfil the aforementioned needs in HIoT systems, despite considerable advancements in this field. Fog computing is therefore exceedingly difficult for researchers.

(4) Resource Management: HIoT nodes' assignments are enormous despite their modest computational and storage capacity. Therefore, in the HIoT context, managing and effectively deploying smart healthcare equipment is essential. In general, resource management might result in greater research and analysis. Furthermore, resource management should successfully enact a wide range of services in order to make the most use of existing resources and deliver relevant services in HIoT. This is owing to smart gadgets' mobility and relocation capabilities. Therefore, resource management is another crucial unresolved topic in this study.

(5) Multi-objective Optimization: It is obvious that some QoS aspects of HIoT systems were taken into account, while others were not. For instance, some algorithms only take into account cost and delay, ignoring other considerations like reliability and electricity. Therefore, an ideal mechanism that takes into account various aims to make a tradeoff between various QoS parameters in HIoT systems may still be a work in progress.

6.2. Challenges

The following are the challenges faced in IoT-based smart healthcare management:

(1) Scalability: In the healthcare system, scalability is crucial. This implies a system's ability to meet shifting demands and adapt to developments that will become more significant in the future. According to the literature review, some of the suggested methods for HIoT systems can work on a limited scale, and only a few nodes or devices can vouch for their authenticity. Scalability is an important element. However, it appears to be a challenge because the offered ways were generally applied in confined contexts.

(2) Interoperability and Standardization: In the HIoT, interoperability is crucial for the transposition of information and resources between patients and smart objects. Open-source frameworks with reliable connections are the main obstacle to interoperability; standards must be established so that horizontal platforms can be operable, programmable, and communicable, regardless of the model or the manufacturer, among devices, operating systems, and applications. It is also important to acquire dynamic and flexible architectures that are interoperable with large-scale IoT applications, and to be able to interface with nonhomogeneous data centres and smart devices with scalable architecture. The interoperability and standardization of HIoT systems are the primary unresolved issues.

(3) Mobility: The literature has paid less attention to mobility as one of the biggest obstacles in HIoT. When it comes to IoT healthcare systems, mobility means providing patients with the ability to connect to the gateway whenever and wherever they want. A mobile network improves the quality of service, makes information accessible

no matter where users are, and makes the network fault-tolerant. It is essential in the healthcare industry that mobility protocols are dependable so that packet losses, network failures, and end-to-end delays are minimized. Therefore, mobility presents an intriguing research problem.

(4) Real Testbed Environment: Only 24% of the examined research was carried out in actual testbeds, while the rest was assessed using simulation tools. The HIoT methodologies suggested in these studies should be enacted in real situations. To be completely honest, all of the suggested methods need to be put to the test in actual settings in order to determine whether or not they can deliver a system of healthcare that is adequate. Real testbed implementation is difficult as a result.

6.3. Trends

The following are the trends in IoT-based smart healthcare management:

(1) Blockchain: Blockchain is a possible solution for the edge/IoT environment in the future. Health data can be securely managed and analyzed using blockchain technology. It is the greatest technology for the healthcare system because it cannot be altered or deleted from blocks [8]. It may be that the Internet of edge-blocks can be used to help the current edge-IoT environment handle decentralized end-user requests transparently and autonomously. Furthermore, it is a permanent, clear consensus system that relies on peer-to-peer and distributed communication rather than centralised authority; it is also an immutable, clear consensus protocol. Due to the fact that researchers have not given this issue much consideration, blockchain in HIoT may prove to be an important future development.

(2) Tactile Internet: The term Tactile Internet (TI) refers to the concept of sensory connectedness on the Internet [6]. In a digital environment, it develops perception skills by reproducing stimuli and senses using standardized communication among devices. Researchers are looking into TI-based applications in the areas of healthcare and robotics in particular as a result of the emergence of 5G communications technology. TI can be used in a variety of ways in healthcare, including Parkinson's disease tremor suppression, remote surgery, interactive medical training, trauma rehabilitation, and virtual and augmented reality. As a result, TI applications offer some HIoT possibilities that could present worthwhile research opportunities in the future.

(3) Software-Defined Networks/Network Function Virtualization: Support for software-defined networks (SDN) in IoT systems helps improve IoT administration due to resource constraints. The integration of IoT and network function virtualization (NFV) allows for the rapid creation, administration, and deployment of novel applicant-based services. Future research in this exciting area will aid in meeting the QoS needs of HIoT [44].

(4) Online Social Networks: In the digital era, online social networks can serve as a reliable platform link between healthcare providers and healthcare consumers at any time and in any place. Through this paradigm, remote healthcare providers can share health data with their patients through computationally and strongly resource-rich social networks. Social network nodes include friendship, employment, shared interests, knowledge, status, and other nodes that can be collocated to exchange information, knowledge, or financial assistance. This HIoT paradigm is a whole new arena for predicting a patient's health status, and it offers numerous research opportunities.

(5) Big Data Analytics: Modern smart healthcare solutions are built upon IoT big data analytics. Consequently, the development of contemporary medical telematics and informatics, including illness diagnosis, remote and instantaneous health monitoring, preventative systems, and emergency and alerting systems, is attributable to the convergence of big data analytics and the Internet of Things [46]. Combined with a complex background of other health-related information, data collected from diverse devices in IoT environments contains a great deal of long-term information about users' personal lives. In order to generate intelligence for the creation of policies and

more informed clinical decision making, it is important to investigate how to explore all of this huge data under IoT systems. However, this topic has not received much attention among all the investigations. In IoT-based healthcare systems, big data analytics are therefore needed for further research.

(6) Service Quality: Applications using instantaneous HIoT have recently been developed. QoS concerns revolve around HIoT data's quality and timeliness for supporting decisions. The timely collection, analysis, transposition, and use of data generated by healthcare sensors is essential; however, there are times when the pertinent data are not instantly accessible, which seems to be an issue for HIoT systems. The diversity, volume, and speed of the instantaneous data produced by IoT devices creates a significant barrier for data analysis. The immediate and life-critical nature of medical wearable systems necessitates a high standard of service quality. There are significant gaps in a variety of areas, including the instantaneous monitoring of patients, the collection of data, and decision-making support based on QoS. It goes without saying that the QoS must be the foundation for overcoming these difficulties [45].

(7) Internet of Nano Things: Nanorobots, precision medicine, minimally invasive surgery, nanosensors, and nanorobot swarms for inaccessible human body parts are some of the applications of the IoNT. Nanorobots can deliver medications to certain organs with extreme precision. Furthermore, as a possible future avenue in sensing and precision medicine, the IoNT is driving a nanoscale network revolution.

Table 4 is a reference mapping table for the issues, challenges, and trends of the current study. Research questions 5 and 6 have been addressed in this section.

Table 4. Mapping reference table.

Issues	Trust and privacy	[6,7,24,27,79]
	Power management	[44]
	Fog computing	[4,11,26,48]
	Resource management	[81]
	Multi-objective optimization	[24]
Challenges	Scalability	[67]
	Interoperability and standardization	[77]
	Mobility	[4]
	Real testbed environment	[58,61]
Trends	Blockchain	[6–8,19]
	Tactile internet	[6,31]
	Software-defined networks	[44]
	Online social networks	[10,22,56,71]
	Big data analytics	[23,27,52]
	Service quality	[45,66]
	Internet of Nano Things	[87]

7. Conclusions

Growing IoT adoption has the possibility to fundamentally alter how healthcare services are used in clinical settings as well as at home. The IoT can improve medical service maintenance, which will significantly improve the quality of medical equipment and increase equipment compatibility. The vital position, immense significance, and complex convergent nature of IoT also give medical organizations and sectors a substantial opportunity to grow their businesses and sales using comparatively novel strategies. New functional standards state that IoT requires a sophisticated safety infrastructure. The

adoption of contemporary IoT technology in healthcare has been encouraged by this research. As a result, the literature on IoT-based medical management system mechanisms has been thoroughly analyzed for this study. The authors have carried out their research with the selected papers, and all the six research questions have been addressed. The research revealed that a number of studies sought to improve security, cost, real-time, and efficiency. Additionally, the results showed that governments may benefit from IoT to improve commercial and societal ties and general wellness. As a result, the inventions in this research may be used to implement a landscape of IoT-based medical management systems and offer some strategies for the implementation of the next innovative generation of IoT-based health technologies.

The current paper did have some drawbacks. One was our exploration of Emerald, ABI/Inform Global ProQuest, Google Scholar, and Science Direct. Examples of related articles may be found in other scholarly magazines. Additionally, the publishers removed any works written in languages other than English. Even so, there might be a wealth of other research of a similar nature in different languages.

Future researchers interested in IoT technology in medical management procedures will benefit in certain ways from these results. This review aids in identifying the IoT requirements of healthcare and related industries. It is conceivable that carers and medical professionals may use it to provide pervasive and assistive healthcare. Therefore, there is a bright future for the development of IoT-based smart healthcare. This is a unique piece of research motivated by recent developments in IoT-based medical technologies.

Author Contributions: Conceptualization, L.A.; Methodology, L.A.; Project administration, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data supporting the results reported in this article are available within the article itself. No new data were created, and existing data utilized are covered under privacy or ethical restrictions, hence not publicly archived.

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

References

1. Nasajpour, M.; Pouriyeh, S.; Parizi, R.M.; Dorodchi, M.; Valero, M.; Arabnia, H.R. Internet of Things for current COVID-19 and future pandemics: An exploratory study. *J. Healthc. Inform. Res.* **2020**, *4*, 325–364. [CrossRef]
2. Huifeng, W.; Kadry, S.N.; Raj, E.D. Continuous health monitoring of sportsperson using IoT devices based wearable technology. *Comput. Commun.* **2020**, *160*, 588–595. [CrossRef]
3. Abdellatif, A.A.; Khafagy, M.G.; Mohamed, A.; Chiasserini, C.F. EEG-based transceiver design with data decomposition for healthcare IoT applications. *IEEE Internet Things J.* **2018**, *5*, 3569–3579. [CrossRef]
4. Abdelmoneem, R.M.; Benslimane, A.; Shaaban, E. Mobility-aware task scheduling in cloud-Fog IoT-based healthcare architectures. *Comput. Netw.* **2020**, *179*, 107348. [CrossRef]
5. AbdulGhaffar, A.; Mostafa, S.M.; Alsaleh, A.; Sheltami, T.; Shakshuki, E.M. Internet of things based multiple disease monitoring and health improvement system. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1021–1029. [CrossRef]
6. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.Y.; Bashir, A.K.; Abd El-Latif, A.A. DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access* **2020**, *8*, 111223–111238. [CrossRef]
7. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]
8. Alamri, B.; Crowley, K.; Richardson, I. Blockchain-based identity management systems in health IoT: A systematic review. *IEEE Access* **2022**, *10*, 59612–59629. [CrossRef]
9. Aghili, S.F.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Gener. Comput. Syst.* **2019**, *96*, 410–424. [CrossRef]
10. Ahmadi, H.; Arji, G.; Shahmoradi, L.; Safdari, R.; Nilashi, M.; Alizadeh, M. The application of internet of things in healthcare: A systematic literature review and classification. *Univers. Access Inf. Soc.* **2019**, *18*, 837–869. [CrossRef]
11. Ahmadi, Z.; Haghi Kashani, M.; Nikravan, M.; Mahdipour, E. Fog-based healthcare systems: A systematic review. *Multimed. Tools Appl.* **2021**, *80*, 36361–36400. [CrossRef] [PubMed]
12. Ahmed, A.; Latif, R.; Latif, S.; Abbas, H.; Khan, F.A. Malicious insiders attack in IoT based multi-cloud e-healthcare environment: A systematic literature review. *Multimed. Tools Appl.* **2018**, *77*, 21947–21965. [CrossRef]

13. 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]
14. Akhbarifar, S.; Javadi HH, S.; Rahmani, A.M.; Hosseinzadeh, M. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. *Pers. Ubiquitous Comput.* **2020**, *27*, 697–713. [CrossRef] [PubMed]
15. Aktas, F.; Ceken, C.; Erdemli, Y.E. IoT-based healthcare framework for biomedical applications. *J. Med. Biol. Eng.* **2018**, *38*, 966–979. [CrossRef]
16. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
17. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Le Moullec, Y. A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* **2018**, *6*, 36611–36631. [CrossRef]
18. Alhussein, M.; Muhammad, G.; Hossain, M.S.; Amin, S.U. Cognitive IoT-cloud integration for smart healthcare: Case study for epileptic seizure detection and monitoring. *Mob. Netw. Appl.* **2018**, *23*, 1624–1635. [CrossRef]
19. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1676–1717. [CrossRef]
20. Alladi, T.; Chamola, V. HARCI: A two-way authentication protocol for three entity healthcare IoT networks. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 361–369. [CrossRef]
21. Alzahrani, B.A. Secure and efficient cloud-based IoT authenticated key agreement scheme for e-health wireless sensor networks. *Arab. J. Sci. Eng.* **2021**, *46*, 3017–3032. [CrossRef]
22. Amin, M.; Shehwar, D.; Ullah, A.; Guarda, T.; Tanveer, T.A.; Anwar, S. A deep learning system for health care IoT and smartphone malware detection. *Neural Comput. Appl.* **2020**, *34*, 11283–11294. [CrossRef]
23. Karimi, Y.; Haghi Kashani, M.; Akbari, M.; Mahdipour, E. Leveraging big data in smart cities: A systematic review. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6379. [CrossRef]
24. Najafizadeh, A.; Salajegheh, A.; Rahmani, A.M.; Sahafi, A. Privacy-preserving for the internet of things in multi-objective task scheduling in cloud-fog computing using goal programming approach. *Peer-Peer Netw. Appl.* **2021**, *14*, 3865–3890. [CrossRef]
25. Ashton, K. That 'internet of things' thing. *RFID J.* **2009**, *22*, 97–114.
26. Sofla, M.S.; Kashani, M.H.; Mahdipour, E.; Mirzaee, R.F. Towards effective offloading mechanisms in fog computing. *Multimed. Tools Appl.* **2022**, *81*, 1997. [CrossRef]
27. Yang, Y.; Zheng, X.; Guo, W.; Liu, X.; Chang, V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Inf. Sci.* **2019**, *479*, 567–592. [CrossRef]
28. Gope, P.; Gheraibia, Y.; Kabir, S.; Sikdar, B. A secure IoT-based modern healthcare system with fault-tolerant decision making process. *IEEE J. Biomed. Health Inform.* **2020**, *25*, 862–873. [CrossRef]
29. Zhou, W.; Piramuthu, S. IoT security perspective of a flexible healthcare supply chain. *Inf. Technol. Manag.* **2018**, *19*, 141–153. [CrossRef]
30. Zou, N.; Liang, S.; He, D. Issues and challenges of user and data interaction in healthcare-related IoT: A systematic review. *Libr. Hi Tech.* **2020**, *38*, 769–782. [CrossRef]
31. 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]
32. Ali, M.; Naeem, F.; Tariq, M.; Kaddoum, G. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 778–789. [CrossRef] [PubMed]
33. Soni, G.; Kandasamy, S. Smart garbage bin systems—A comprehensive survey. In *Smart Secure Systems—IoT and Analytics Perspective: Second International Conference on Intelligent Information Technologies, ICIIT 2017, Chennai, India, 20–22 December 2017, Proceedings 2*; Springer: Singapore, 2018; pp. 194–206.
34. Xu, G. IoT-assisted ECG monitoring framework with secure data transmission for health care applications. *IEEE Access* **2020**, *8*, 74586–74594. [CrossRef]
35. Hassan, R.; Qamar, F.; Hasan, M.K.; Aman AH, M.; Ahmed, A.S. Internet of Things and its applications: A comprehensive survey. *Symmetry* **2020**, *12*, 1674. [CrossRef]
36. Sharma, A.; Kaur, S.; Singh, M. A comprehensive review on blockchain and Internet of Things in healthcare. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4333. [CrossRef]
37. Khanna, A.; Kaur, S. Internet of things (IoT), applications and challenges: A comprehensive review. *Wirel. Pers. Commun.* **2020**, *114*, 1687–1762. [CrossRef]
38. Salih KO, M.; Rashid, T.A.; Radovanovic, D.; Bacanin, N. A comprehensive survey on the Internet of Things with the industrial marketplace. *Sensors* **2022**, *22*, 730. [CrossRef]
39. Molaei, F.; Rahimi, E.; Siavoshi, H.; Afrouz, S.G.; Tenorio, V. A comprehensive review on internet of things (IoT) and its implications in the mining industry. *Am. J. Eng. Appl. Sci.* **2020**, *13*, 499–515. [CrossRef]
40. Boursianis, A.D.; Papadopoulou, M.S.; Diamantoulakis, P.; Liopa-Tsakalidi, A.; Barouchas, P.; Salahas, G.; Karagiannidis, G.; Wan, S.; Goudos, S.K. Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review. *Internet Things* **2022**, *18*, 100187. [CrossRef]
41. Malliga, S.; Kogilavani, S.V.; Nandhini, P.S. A comprehensive review of applications of Internet of Things for COVID-19 pandemic. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2021; Volume 1055, No. 1; p. 012083.

42. Ahmid, M.; Kazar, O. A comprehensive review of the internet of things security. *J. Appl. Secur. Res.* **2021**, *18*, 289–305. [CrossRef]
43. Latif, S.; Driss, M.; Boulila, W.; Huma, Z.E.; Jamal, S.S.; Idrees, Z.; Ahmad, J. Deep learning for the industrial internet of things (iiot): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions. *Sensors* **2021**, *21*, 7518. [CrossRef] [PubMed]
44. Song, Y.; Yu, F.R.; Zhou, L.; Yang, X.; He, Z. Applications of the Internet of Things (IoT) in smart logistics: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 4250–4274. [CrossRef]
45. Alhasnawi, B.N.; Jasim, B.H. Internet of Things (IoT) for smart grids: A comprehensive review. *J. Xi'an Univ. Arch.* **2020**, *63*, 1006–7930.
46. Heidari, A.; Jabraeil Jamali, M.A. Internet of Things intrusion detection systems: A comprehensive review and future directions. *Clust. Comput.* **2022**, *26*, 3753–3780. [CrossRef]
47. Kashani, M.H.; Madanipour, M.; Nikravan, M.; Asghari, P.; Mahdipour, E. A systematic review of IoT in healthcare: Applications, techniques, and trends. *J. Netw. Comput. Appl.* **2021**, *192*, 103164. [CrossRef]
48. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Gener. Comput. Syst.* **2018**, *78*, 659–676. [CrossRef]
49. Darwish, A.; Hassanien, A.E.; Elhoseny, M.; Sangaiah, A.K.; Muhammad, K. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 4151–4166. [CrossRef]
50. 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]
51. Qi, J.; Yang, P.; Waraich, A.; Deng, Z.; Zhao, Y.; Yang, Y. Examining sensor-based physical activity recognition and monitoring for healthcare using Internet of Things: A systematic review. *J. Biomed. Inform.* **2018**, *87*, 138–153. [CrossRef]
52. Dey, N.; Hassanien, A.E.; Bhatt, C.; Ashour, A.; Satapathy, S.C. (Eds.) *Internet of Things and Big Data Analytics toward Next-Generation Intelligence*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 35.
53. Quality of Experience Requirements. Available online: https://www.itu.int/pub/T-TUT-QOS-2022-1 (accessed on 19 September 2023).
54. Vocabulary for Performance, Quality of Service, and Quality of Experience. Available online: https://www.itu.int/rec/T-REC-P.10 (accessed on 19 September 2023).
55. Guidelines on Regulatory Aspects of Quality of Service. Available online: https://www.itu.int/rec/T-REC-E.800SerSup9/en (accessed on 19 September 2023).
56. da Silva, M.P.; Gonçalves, A.L.; Dantas, M.A.R. A conceptual model for quality of experience management to provide context-aware eHealth services. *Future Gener. Comput. Syst.* **2019**, *101*, 1041–1061. [CrossRef]
57. Nasralla, M.M.; Khattak SB, A.; Ur Rehman, I.; Iqbal, M. Exploring the Role of 6G Technology in Enhancing Quality of Experience for m-Health Multimedia Applications: A Comprehensive Survey. *Sensors* **2023**, *23*, 5882. [CrossRef] [PubMed]
58. Ray, P.P.; Dash, D.; De, D. Internet of things-based real-time model study on e-healthcare: Device, message service and dew computing. *Comput. Netw.* **2019**, *149*, 226–239. [CrossRef]
59. 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]
60. Vilela, P.H.; Rodrigues, J.J.; Solic, P.; Saleem, K.; Furtado, V. Performance evaluation of a Fog-assisted IoT solution for e-Health applications. *Future Gener. Comput. Syst.* **2019**, *97*, 379–386. [CrossRef]
61. Ray, P.P.; Thapa, N.; Dash, D.; De, D. Novel implementation of IoT based non-invasive sensor system for real-time monitoring of intravenous fluid level for assistive e-healthcare. *Circuit World* **2019**, *45*, 109–123. [CrossRef]
62. Asif-Ur-Rahman, M.; Afsana, F.; Mahmud, M.; Kaiser, M.S.; Ahmed, M.R.; Kaiwartya, O.; James-Taylor, A. Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things. *IEEE Internet Things J.* **2018**, *6*, 4049–4062. [CrossRef]
63. Kavitha, K.; Sharma, S.C. Performance analysis of ACO-based improved virtual machine allocation in cloud for IoT-enabled healthcare. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5613. [CrossRef]
64. Stefanova-Pavlova, M.; Andonov, V.; Stoyanov, T.; Angelova, M.; Cook, G.; Klein, B.; Vassilev, P.; Stefanova, E. Modeling telehealth services with generalized nets. *Recent Contrib. Intell. Syst.* **2017**, *657*, 279–290.
65. Min, M.; Wan, X.; Xiao, L.; Chen, Y.; Xia, M.; Wu, D.; Dai, H. Learning-based privacy-aware offloading for healthcare IoT with energy harvesting. *IEEE Internet Things J.* **2018**, *6*, 4307–4316. [CrossRef]
66. Wang, X.; Cai, S. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. *Future Gener. Comput. Syst.* **2020**, *112*, 320–329. [CrossRef]
67. He, S.; Cheng, B.; Wang, H.; Huang, Y.; Chen, J. Proactive personalized services through fog-cloud computing in large-scale IoT-based healthcare application. *China Commun.* **2017**, *14*, 1–16. [CrossRef]
68. Bharathi, R.; Abirami, T.; Dhanasekaran, S.; Gupta, D.; Khanna, A.; Elhoseny, M.; Shankar, K. Energy efficient clustering with disease diagnosis model for IoT based sustainable healthcare systems. *Sustain. Comput. Inform. Syst.* **2020**, *28*, 100453. [CrossRef]
69. 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]

70. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [CrossRef]
71. Catherwood, P.A.; Steele, D.; Little, M.; McComb, S.; McLaughlin, J. A community-based IoT personalized wireless healthcare solution trial. *IEEE J. Transl. Eng. Health Med.* **2018**, *6*, 2800313. [CrossRef]
72. Qiu, T.; Liu, X.; Han, M.; Li, M.; Zhang, Y. SRTS: A self-recoverable time synchronization for sensor networks of healthcare IoT. *Comput. Netw.* **2017**, *129*, 481–492. [CrossRef]
73. Almobaideen, W.; Krayshan, R.; Allan, M.; Saadeh, M. Internet of Things: Geographical Routing based on healthcare centers vicinity for mobile smart tourism destination. *Technol. Forecast. Soc. Chang.* **2017**, *123*, 342–350. [CrossRef]
74. Woo, M.W.; Lee, J.; Park, K. A reliable IoT system for personal healthcare devices. *Future Gener. Comput. Syst.* **2018**, *78*, 626–640. [CrossRef]
75. Sood, S.K.; Mahajan, I. IoT-fog-based healthcare framework to identify and control hypertension attack. *IEEE Internet Things J.* **2018**, *6*, 1920–1927. [CrossRef]
76. Verma, P.; Sood, S.K.; Kalra, S. Cloud-centric IoT based student healthcare monitoring framework. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 1293–1309. [CrossRef]
77. Ullah, F.; Habib, M.A.; Farhan, M.; Khalid, S.; Durrani, M.Y.; Jabbar, S. Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. *Sustain. Cities Soc.* **2017**, *34*, 90–96. [CrossRef]
78. Ali, F.; Islam, S.R.; Kwak, D.; Khan, P.; Ullah, N.; Yoo, S.J.; Kwak, K.S. Type-2 fuzzy ontology–aided recommendation systems for IoT–based healthcare. *Comput. Commun.* **2018**, *119*, 138–155. [CrossRef]
79. Boussada, R.; Hamdane, B.; Elhdhili, M.E.; Saidane, L.A. Privacy-preserving aware data transmission for IoT-based e-health. *Comput. Netw.* **2019**, *162*, 106866. [CrossRef]
80. Elmisery, A.M.; Rho, S.; Botvich, D. A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things. *IEEE Access* **2016**, *4*, 8418–8441. [CrossRef]
81. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. Policy-based access control for constrained healthcare resources in the context of the Internet of Things. *J. Netw. Comput. Appl.* **2019**, *139*, 57–74. [CrossRef]
82. Yang, Y.; Liu, X.; Deng, R.H. Lightweight break-glass access control system for healthcare Internet-of-Things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3610–3617. [CrossRef]
83. Kaw, J.A.; Loan, N.A.; Parah, S.A.; Muhammad, K.; Sheikh, J.A.; Bhat, G.M. A reversible and secure patient information hiding system for IoT driven e-health. *Int. J. Inf. Manag.* **2019**, *45*, 262–275. [CrossRef]
84. Abd EL-Latif, A.A.; Abd-El-Atty, B.; Abou-Nassar, E.M.; Venegas-Andraca, S.E. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Opt. Laser Technol.* **2020**, *124*, 105942. [CrossRef]
85. Li, H.; Jing, T. A lightweight fine-grained searchable encryption scheme in fog-based healthcare IoT networks. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1019767. [CrossRef]
86. Manogaran, G.; Varatharajan, R.; Lopez, D.; Kumar, P.M.; Sundarasekar, R.; Thota, C. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Gener. Comput. Syst.* **2018**, *82*, 375–387. [CrossRef]
87. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2015**, *16*, 1368–1376. [CrossRef]