




# Risk Assessment of Heterogeneous IoMT Devices: A Review

Pritika <sup>1</sup>, Bharanidharan Shanmugam <sup>1,\*</sup> and Sami Azam <sup>2</sup>

<sup>1</sup> Energy and Resources Institute, Faculty of Science and Technology, Charles Darwin University, Darwin, NT 0810, Australia

<sup>2</sup> Faculty of Science and Technology, Charles Darwin University, Darwin, NT 0810, Australia

\* Correspondence: bharanidharan.shanmugam@cdu.edu.au

**Abstract:** The adaptation of the Internet of Medical Things (IoMT) has provided efficient and timely services and has transformed the healthcare industry to a great extent. Monitoring patients remotely and managing hospital records and data have become effortless with the advent of IoMT. However, security and privacy have become a significant concern with the growing number of threats in the cyber world, primarily for personal and sensitive user data. In terms of IoMT devices, risks appearing from them cannot easily fit into an existing risk assessment framework, and while research has been done on this topic, little attention has been paid to the methodologies used for the risk assessment of heterogeneous IoMT devices. This paper elucidates IoT, its applications with reference to in-demand sectors, and risks in terms of their types. By the same token, IoMT and its application area and architecture are explained. We have also discussed the common attacks on IoMT. Existing papers on IoT, IoMT, risk assessment, and frameworks are reviewed. Finally, the paper analyzes the available risk assessment frameworks such as NIST, ISO 27001, TARA, and the IEEE213-2019 (P2413) standard and highlights the need for new approaches to address the heterogeneity of the risks. In our study, we have decided to follow the functions of the NIST and ISO 270001 frameworks. The complete framework is anticipated to deliver a risk-free approach for the risk assessment of heterogeneous IoMT devices benefiting its users.

**Keywords:** Internet of Things; Internet of Medical Things; framework; risk assessment; privacy risk; security risk



**Citation:** Pritika; Shanmugam, B.; Azam, S. Risk Assessment of Heterogeneous IoMT Devices: A Review. *Technologies* **2023**, *11*, 31. <https://doi.org/10.3390/technologies11010031>

Academic Editor: Manoj Gupta

Received: 4 January 2023

Revised: 2 February 2023

Accepted: 7 February 2023

Published: 14 February 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

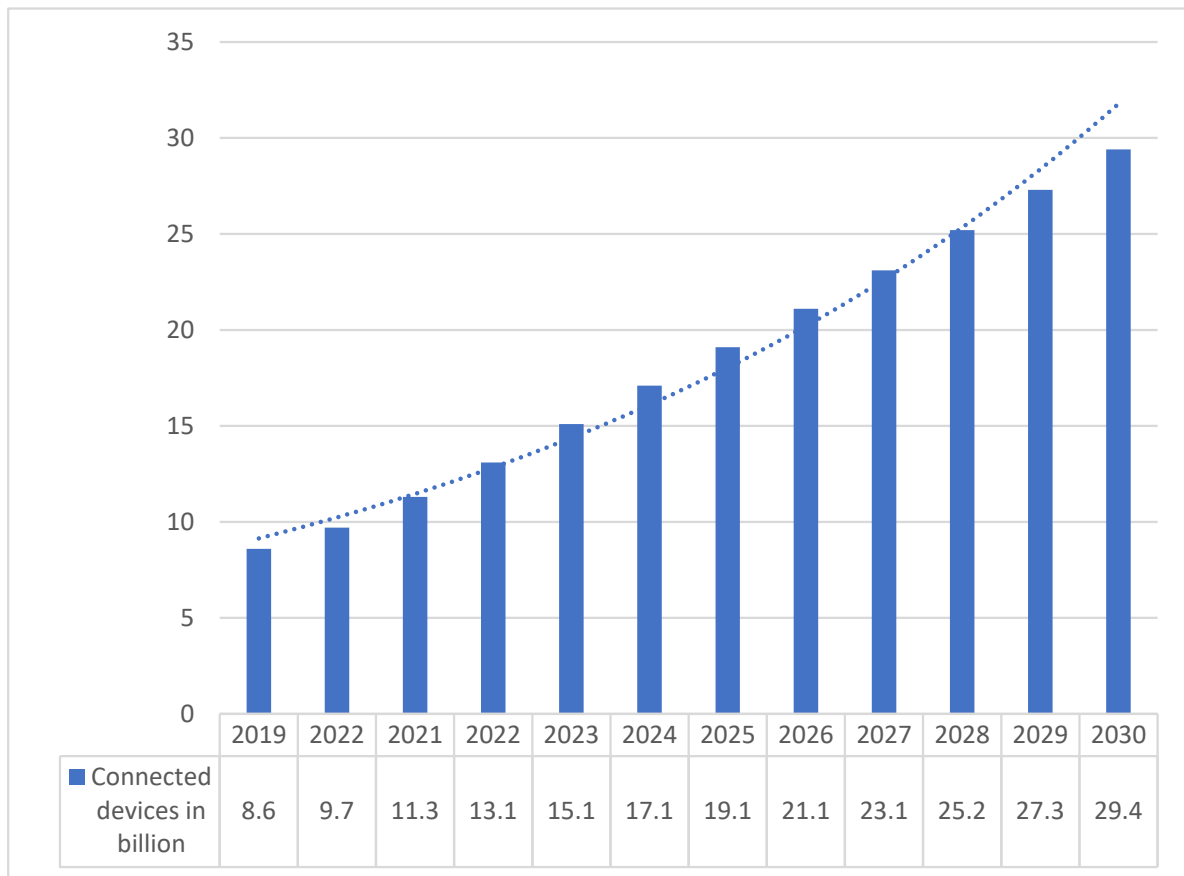
Kevin Ashton, a British technology pioneer, first introduced the term Internet of Things at Proctor & Gamble in 1999 in supply chain management. However, the definition has become more comprehensive in the past two decades, transforming various domains of our lives through agriculture, healthcare, transport, and the environment (smart buildings, energy-efficient cities, and infrastructure) [1,2]. In this section, the terms “Internet of Things” and “Internet of Medical Things” are defined along with a brief background. Statistics are provided to demonstrate their prevalence and level of integration in our lives. Furthermore, objectives, motivation, and contribution are outlined, and a quick overview of the structure of this paper is provided.

### 1.1. IoT (Internet of Things)

In general, the term refers to Internet-enabled objects like electronic devices and sensors interacting without human-to-human or human-to-computer interaction. These not only facilitate our life, but are also an integral part of it, providing services everywhere around the world [3].

Gartner’s global government IoT revenue for electronics and communication will reach USD 21.3 billion in 2022, an increase of 22% over the previous year [4], and USD 58 billion by 2025 [5]. There are currently 31 billion “things” connected, which is estimated to balloon to 75 billion by 2025 [6]. A report published in 2018 by PWC [7] for the Australian

Computer Society (ACS) states that IoT has the potential to bring about an annual benefit of AUD 194–308 billion in Australia alone over the period of eight to eighteen years. Out of the top five industries that account for 25% of Australia’s gross domestic product (GDP), the health industry alone contributes significantly. The number of IoT-connected devices globally from 2019 to 2030 is depicted in Figure 1.



**Figure 1.** Number of globally connected IoT devices [8].

However, despite several benefits and economic potential, it is widely acknowledged that security and privacy have become key concerns that will affect the future development of IoT [9]. A compound annual growth rate of 33.7 percent is anticipated for the worldwide IoT security market from 2018 to 2023 due to the proliferation of IoT device cyberattacks, growing IoT security mandates, and rising security concerns [10]. This rise uncovers many new and emerging threats; the Kronos and Colonial Pipeline ransomware attacks of 2021 are high-profile examples [11].

Based on our literature search, it has been found that security and privacy issues have received massive research attention but the focus on risk assessment has not been adequately explored [12]. This fact emphasizes the need for a risk assessment methodology, since creating a generic, universal approach for all the devices would be challenging.

### 1.2. IoMT (Internet of Medical Things)

IoMT is a cloud-connected network of medical devices used to transmit data [13]. IoMT has gained popularity by incorporating connected medical devices, computing, and clinical systems due to its efficiency and quality of services. It is considered as a breakthrough in the medical world having billions of Internet-connected medical devices. Heterogeneous IoMT devices refer to the diversity of these medical devices which are used to connect to the Internet. These devices are interconnected and are able to share and collect data which include a wide range of standards and technologies [14]. The global

IoMT market is projected to increase from USD 72.5 billion in 2020 to USD 188.2 billion by 2025, and the highest compound annual growth rate (CAGR) expected during the forecast period is APAC (Asia Pacific) due to its advancement over the previous decade, globalization-inspired government policies, and expansion of digitalization [15]. IoMT can potentially be a ‘Game-changer Technology’ if the concepts are applied tactfully [16].

It is believed to be a one-stop solution to the absence of medical resources and has helped minimize unnecessary hospital visits [17]. However, IoMT devices are more susceptible to cyberattacks than any other sector, as they are positioned in networks without considering risks. Medical device security has been a weak spot for healthcare firms. An article published by Cynerio in January 2022 reports that 53 percent of IoT and IoMT devices in hospitals are vulnerable to cyberattacks [18].

There are many reasons behind these risks, and to help the healthcare industry protect its patients, the National Institute of Standards and Technology (NIST) recently updated its cybersecurity guidance for the medical sector on July 21, 2022. The healthcare services will benefit from this update to preserve the confidentiality, integrity, and availability of electronically protected health information [19]. Asimily, a leading risk management platform for IoMT devices that provides safe and trusted care, has prioritized understanding the risks of IoT devices.

Because risk assessment and threats are not static targets [20], we constantly need to monitor the devices, detect irregular behavior, and alert the handlers to remediate any identified anomalies. Additionally, there is a constant need for a risk assessment model structured to address the security and privacy risks of IoMT devices. To address these needs, this paper presents a risk assessment framework that will identify potential risks and recommends specific risk assessment attributes, which are discussed in detail in Section 3.

### 1.3. Research Questions

In this section, research questions have been formed to better understand the available risk assessment approaches and frameworks. They will help us derive various IoMT research and implementation gaps.

**Research Question 1.** What are the approaches used in the existing literature for the risk assessment of IoMT devices? (Please refer to Section 2.5 for the approaches)

**Research Question 2.** Which of the available frameworks and standards can be applied for the risk assessment of IoMT devices? (Please refer to Section 2.7 for the approaches)

### 1.4. Research Objectives

Based on the above research questions, the following objectives have been formed.

**Objective 1.** The objective here is to provide an overview of the available risk assessment frameworks and standards employed for IoMT devices.

**Objective 2.** The objective here is to derive the standard criteria and limitations of these frameworks, and based on these criteria, how they can be modified or merged to provide a risk assessment for the IoMT devices.

### 1.5. Motivation

This research is motivated by the understanding that the assessment frameworks intended for use in various IoT scenarios may not directly address the need for IoMT-based devices. It aims to investigate the potential that existing assessment frameworks offer in addressing security and privacy concerns of IoMT-based devices by identifying their key functions. This research will share new knowledge with other researchers in the respective field and help those using the methodology for the risk assessment of IoMT-based devices.

### 1.6. Contribution

The contribution of this paper is highlighted by comparing several aspects of other papers such as techniques for security and privacy risks, risk assessment frameworks developed for various IoT- and IoMT-based scenarios, application areas, and architecture.

Between 2014 and 2022, several publications have been reviewed, but none of them have addressed all the necessary aspects including applications, architecture, risks, and common attacks for the risk assessment of IoMT devices, and only a small number of papers have discussed the need for a framework, which encourages us to further our research on the subject. Our primary contribution is the risk assessment of smartwatches, portable wireless vital monitors, and lung monitors. The heterogeneous properties of these devices have led us to propose a framework for risk assessment.

This framework classifies the methodology process into five steps so that it can be effectively understood and can also be applied by other researchers across the heterogeneous network.

### 1.7. How the Paper Is Organized

To discuss in detail, the paper is organized as follows: Section 2 presents the IoT applications and related risks. Furthermore, the focus is shifted towards the most prominent area of IoT, i.e., IoMT, also known as Healthcare IoT, and explains frequently used applications of IoMT. The architecture of IoMT devices and common attacks are also covered. Several papers on IoT, IoMT, risk assessment, and frameworks are also discussed in this section. Additionally, risk assessment and currently used frameworks are described. Section 3 anticipates the proposed methodology and the steps expected to be performed in the risk assessment of IoMT devices. Finally, a conclusion has been provided for this research paper, along with a recommendation for future research.

## 2. Literature Review

The overall literature review process is structured by first describing various IoT applications in detail and their associated risks. Furthermore, we limit our research to IoMT devices, their applications, architecture, and some of most common cyberattacks. The literature is then thoroughly evaluated, and the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) model is employed to illustrate the various stages of the review. It displays the number of identified, added, and removed records, and based on these identified records, related works are reviewed. Lastly, the study of some of the available frameworks and directions for using them in our research are provided.

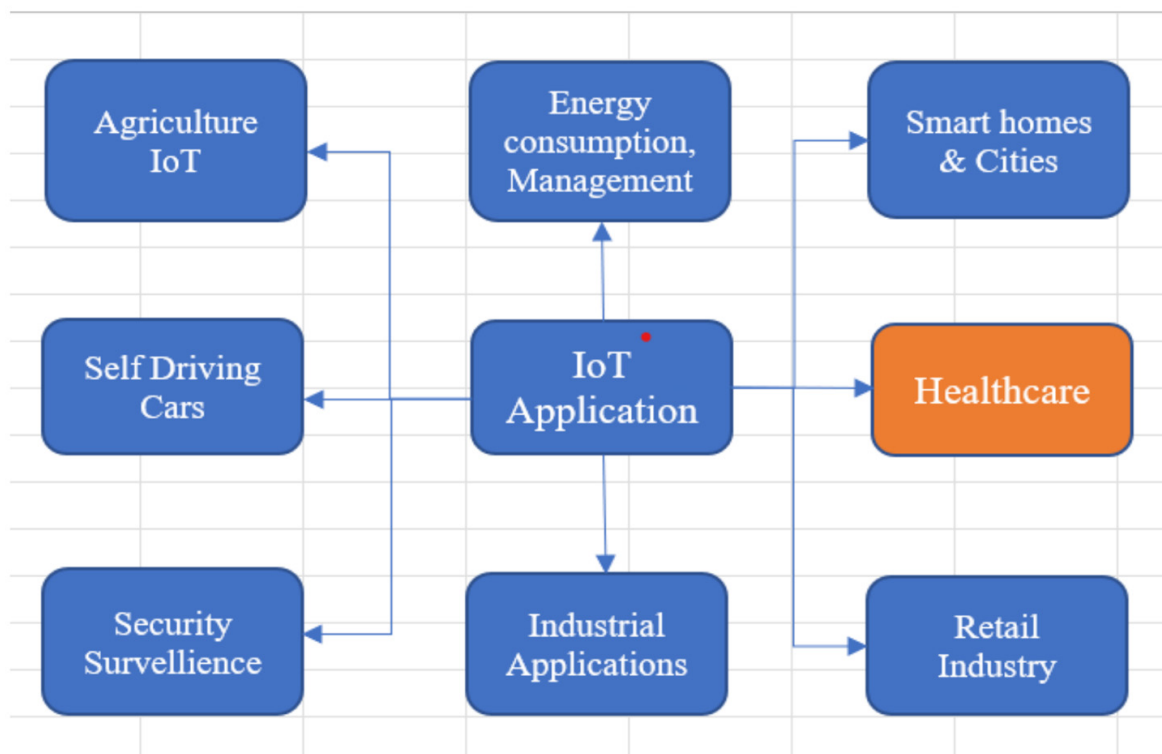
### 2.1. Applications of IoT and Its Associated Risks

Given the unique nature of cyber risks and vulnerabilities of the IoMT devices, coming out with a new risk assessment framework requires understanding both IoT applications and their associated risks, since IoMT is a subset of IoT and the risks can be similar to IoT risks as well.

#### 2.1.1. Applications

IoT's cosmic evolution has significantly contributed to advancing technology and assisting humanity in many ways. The potential application domains for IoT are depicted in Figure 2. In the agriculture domain, IoT helps farmers to earn profit, reduce labor costs, and increase their agricultural output, as well as improve the quality of products. Some IoT applications involved in agriculture are crop growth environment monitoring, water-saving irrigation, intelligent agricultural machinery, etc. In addition to these applications, China is using IoT in farmland planting, aquaculture, animal husbandry, and product safety traceability [21]. Limited energy has been a substantial issue for IoT devices, as they are expected to have a superior battery life to run smoothly for an extended time. Some of the energy management research perspectives in IoT are energy-efficient cognitive radio IoT, 5G IoT, and energy-efficient social network software IoT. With IoT, residential and

commercial buildings are undergoing a drastic change. Automation using IoT plays a vital role in smart buildings providing efficient, comfortable, and secure environments. The research in [22] presents all the potential applications of smart buildings. In the automotive industry, IoT is considered a blessing and is envisioned as shaping its future [23]. One of the core technologies is self-driving cars, which are being tested in some countries and will soon be available. There is a rapid growth in the next application of IoT, i.e., security and surveillance, to protect private organizations. Supply chain and logistics are the most common examples of industrial applications.



**Figure 2.** Applications of IoT.

While IoT focuses on multiple domains, in our research, we have concentrated on one of its subsets, IoMT. It incorporates small intelligent equipment and devices to support the healthcare system. These devices may access various health issues, fitness levels, and number of calories burnt in the fitness center. They are also used to monitor the critical health conditions of the patients in hospitals and trauma centers. Hence, IoMT has completely changed the structure of the medical domain by facilitating it with high technology and smart devices. Moreover, IoT developers are actively involved in elevating the lifestyle of the disabled and senior citizens and in making it accessible to the masses [24]. Despite IoMT's growth, there are still challenges with its implementation which need to be addressed. Hence, it is regarded as a critical area, because even the slightest error can be fatal [25].

All possible IoT application areas are discussed above, including agriculture, retail, security, the automotive industry, energy consumption, smart homes, smart cities, industries, and healthcare. As IoT continues to gain popularity in agriculture, we have included a few applications that have been widely used across several countries, including China. With the world moving towards less energy consumption, the energy sector also plays a significant role in our everyday lives. Self-driving cars are an example of IoT increasingly

becoming prominent in the automotive industry. In a similar manner, we have discussed IoT's growth in security and supply chains. Due to IoT's broader scope, it is important to know what other applications are available before moving on to IoMT, our primary focus.

### 2.1.2. Risks

Contrary to the dominance of IoT devices in our lives, its downsides cannot be overlooked. As the applications of IoT continue to escalate, it brings in significant security, privacy, and ethical challenges which introduce the need for a comprehensive overview covering all these challenges [26].

- **Privacy risks**—With the advancement of IoT and the diffusion of technology, privacy has become a prominent issue. IoT devices collect, analyze, and transmit a massive amount of confidential data that must be protected from adversaries [27]. The reason behind this privacy concern is the ubiquitous connectivity of IoT devices and the universal distribution of information [28]. For users of IoT medical devices, the concern grows wider due to the fear of sharing personal data such as dietary habits, exercise regimens, sleep patterns, and running routes. Hence, safeguarding them becomes more challenging when using medical devices such as smart monitors, smart test kits, and smart assistive technologies at home [29]. In October 2016, malware Mirai generated tens of millions of IP addresses on Dyn, resulting in parts of the Internet going down, including Twitter, Netflix, Cable News Network (CNN), Reddit, etc. [30].
- **Security risks**—A system is considered secure if it satisfies three primary objectives: confidentiality, integrity, and availability. It is commonly called the CIA Triad. Confidentiality signifies that private information is not accessed by unauthorized users. Integrity is keeping the message intact between the sender and receiver, meaning that IoT devices are not utilized or modified by unauthorized services, and availability is the continuation of computing resources, information, and services against disruption attacks. The security of IoT is essential, as most of the data collected in IoT devices are personal and need security. These sensitive data in IoT could be an open invitation to attackers to take and consume them in many ways [31].

In the context of security risks to IoMT devices, confidentiality pertains to safeguarding the medical information that a patient shares with doctors. This information must be protected from intrusion, eavesdropping, and organizations that could cause harm to the patient or use the patient's medical information against him. Integrity safeguards against unauthorized users alerting or destroying patient data, primarily ensuring that they reach their destination intact during wireless transmission. Availability is the efficiency of servers and medical devices to provide for users when required. The system needs to be modified to provide a suspect data storage or transmission channel in the event of a DoS attack [32].

- **Ethical risks**—In general terms, ethics means what is morally good or bad and ethically right or wrong. Ethical risks in the context of IoT devices are actions that are outside of a professional standard. Any new technology designed for the convenience of people will also have adverse effects on individuals and society. Thus, it is essential to define ethical rules and legal regulations to protect them. Since personal data will be in the system owner's hand, it may not be possible to control each data flow; thus, ethical manners and observing user rights are highly significant [33]. For example, Volkswagen, a vehicle manufacturing company, developed and installed software to elude diesel emissions tests. This action violated the USA's Clean Air Act, compromised organization and industry standards, and resulted in massive reputational and financial losses [34].

Given that the healthcare ecosystem is highly interconnected and generates a significant amount of data containing personal health information, some of the ethical risks associated with IoT, such as difficulty in identification, unpredictable behavior, life threats, and difficulty in controlling the data, may also exist in the IoMT environment.

An object needs to be identified to be connected, but data collected by these objects make it difficult to precisely identify the owner of the object. Therefore, collecting these data without the consent of the user makes it a significant issue, as most of the data collected on IoMT devices are personal. Similarly, a data breach in the IoMT network of connected devices can harm a patient's life directly, as collective information about their health is being shared [26].

Being a relatively new technology and an extension of IoT, all the risks associated with IoT are also associated with IoMT [34]. We are keen to investigate and see if these risks can be mitigated. In the above section, it is noted that security, privacy, and ethical risks are common to IoT devices and need to be addressed to protect them. The ubiquitous connectivity of IoT devices makes these risks omnipresent. We also discussed the triad that risk-free devices should meet: confidentiality, integrity, and availability. Furthermore, we have discussed how these risks apply to IoMT devices as well.

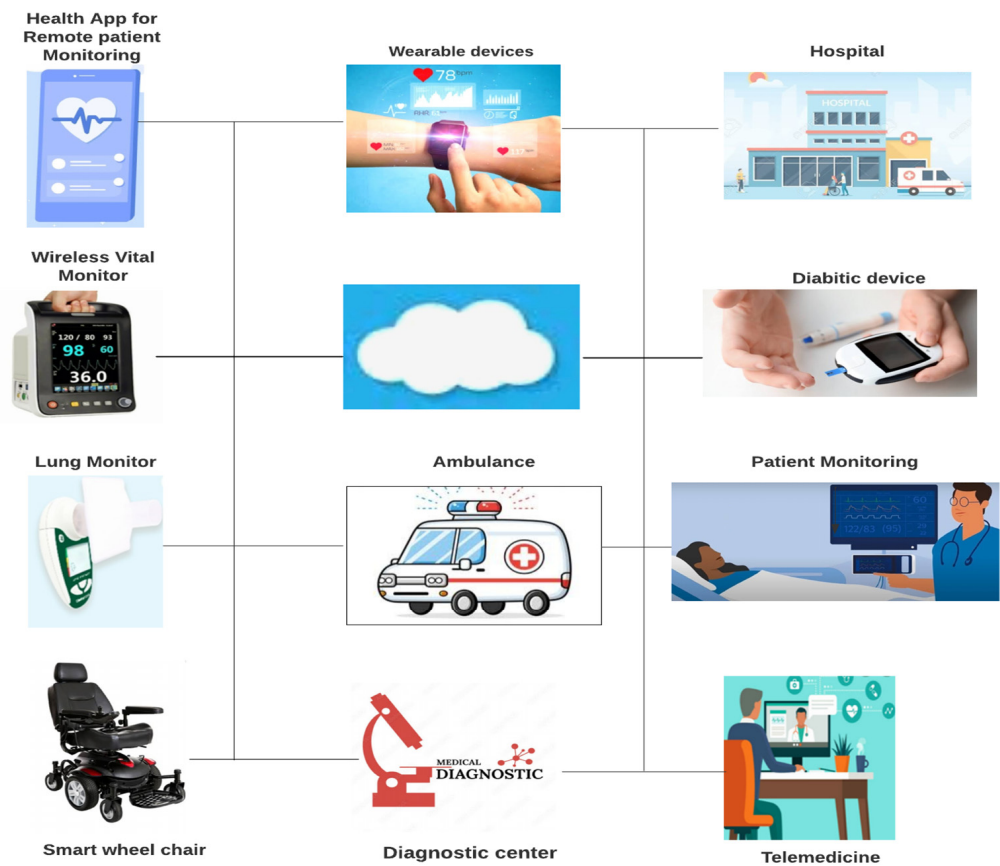
The tabular representation of the different types of risks is shown in Table 1 below.

**Table 1.** Types of IoT risks [26,31].

Type of Risks	Concerns	Concern for IoMT Devices
Privacy Risk	Ubiquitous connectivity Universal distribution of information	Sharing of personal data (dietary habits, sleep pattern, running routes, etc.)
Security Risk	Data breaching Data compromised during the wireless transmission	Attackers may gain access to and modify patient data
Ethical Risk	Ethical rules may be obstructed	Adverse effect on individual using the IoMT device

## 2.2. How IoMT Works

The healthcare industry has improvised from the time it was more doctor-centric, to patient-centric, now to technology-centric using IoT, cloud computing, fog computing, and tele healthcare technologies for sharing data [35]. The transformation of the healthcare sector has largely been improvised through the adaptation of IoMT by providing efficient and accurate services in a timely manner [36]. IoT is not a panacea, but if implemented wisely and strategically, it can change the healthcare industry for the better [37]. IoMT has the power to connect various devices, users, sensors, databases, etc., and is designed to facilitate medical services in a unified manner. Many of the medical tasks such as disease diagnosis and chronic disease monitoring can be performed remotely with more efficient and less costly healthcare services. IoMT is considered as networked communication between doctors and their patients through the sensors connected to the patient's body which can be used for monitoring, diagnosis, and further treatment [35]. The demand for IoMT devices has been soaring over the past few years, and in [38], it was forecasted that IoMT is ready to claim the most significant share of the IoT market after analyzing the trend and developments in the global industry. The changing face of the old healthcare system into a smart system is attributed to the arrival of newly developed devices revolving around IoMT technology. The sudden outbreak of COVID-19 in the past two years has forced people to take precautionary measures and prioritize their health [25]. To save and improve quality of life, IoMT has opened new opportunities in the healthcare sector and changed the way of doing things. Areas such as clinical decision making, patient record management, and data acquisition have become effortless [39]. A few of the familiar IoMT applications have been described below and are represented in Figure 3 along with the systems to which they are connected, such as hospitals, diagnostic centers, and ambulances.



**Figure 3.** Applications of IoMT.

### 2.2.1. Applications of IoMT

- Built-in sensors and wearable devices help to improve the healthcare industry and provide real-time health information, reducing the load on the medical staff. Assisting in the early detection of disease and infection symptoms enhances the efficiency of health monitoring. A common example is a glucose monitor linked to an insulin pump with an automatic suspension of insulin infusion, which is continuously monitored using these technologies [40]. Wearable smart devices are easy to use and are capable of monitoring heart rate, ECG (electrocardiogram patterns), blood glucose level, and cardiac pacemaker's activity in real-time and transmitting the data to the doctor [41]. It has greatly benefited patients, doctors, and healthcare professionals. The smart devices are connected to the user's smartphone and to the remote system to transmit data in a faster way.
- Telemedicine, commonly known as e-medicine or telehealth, is a new concept referring to the remote delivery of healthcare services, like consultations and tests [42]. Without physically seeing the patient, healthcare professionals can examine and treat patients. Similarly, patients can communicate with their doctors from the comfort of their homes by utilizing personal technologies. Blood sugar level, blood pressure, temperature, and other vital measures can be captured by the patients and can be provided to the doctors. Telemedicine systems are based on futuristic developing technologies and are used for efficient infection prevention [43].
- Remote patient monitoring helps in monitoring glucose levels and heart activities of the patients. Doctors can receive real-time updates if anything goes wrong [40]. It proved appropriate during the COVID-19 pandemic, as doctors were able to monitor patients remotely with fingertip medical data like blood pressure level, glucose level, ECG, temperature, pulse rate, heart rate, etc. [44]. Patients could monitor the status of



their disease and receive required medical needs on their phone without visiting the doctor [45].

- Diabetic devices are very commonly used, and most diabetic patients keep a glucose monitor and keep track of their glucose level, thus saving their time. IoMT devices also help insurers to view users' data more quickly, making the health insurance claim process faster.
- Smart wheelchair—The world today makes a massive difference in the life of people with restricted mobility. A smart wheelchair works depending upon the mood of the disabled person and helps effectively in different weather conditions, improving quality of life.
- A wireless vital monitor can be used both in hospitals to ease the load on a nurse and at home after the patient is discharged. It allows continuous recording of vital signs. It can measure heart rate, temperature, respiratory flow, ECG, etc., and these data are sent directly to an interactive monitoring device via Bluetooth for the doctor to check regularly [43,44].
- Lung monitors are mainly used by discharged patients to measure their vitals. They provide accurate and effective monitoring of lung function for respiratory conditions, including COPD, cystic fibrosis, and post-transplant patients.

There are a number of application areas for IoMT that we have discussed. Wearable devices with built-in sensors are becoming more popular, easing the workload of medical staff as they can also be used remotely. Another useful application is telemedicine, which allows patients to monitor their disease status and receive medication recommendations. Patients with diabetes are widespread users of the IoMT application. In addition, smart wheelchairs, lung monitors, and wireless vital monitors are all prevalent application fields [46].

However, the interconnectivity between numerous devices makes them vulnerable to security breaches in a way similar to how other networked computing systems are vulnerable, but the consequences can be pernicious, as they can be dangerous to users' lives [47]. It is a necessity to perform a risk assessment for these IoMT devices. In our study, we plan to perform a risk assessment for the wireless vital monitor, the smartwatch, and a lung monitor.

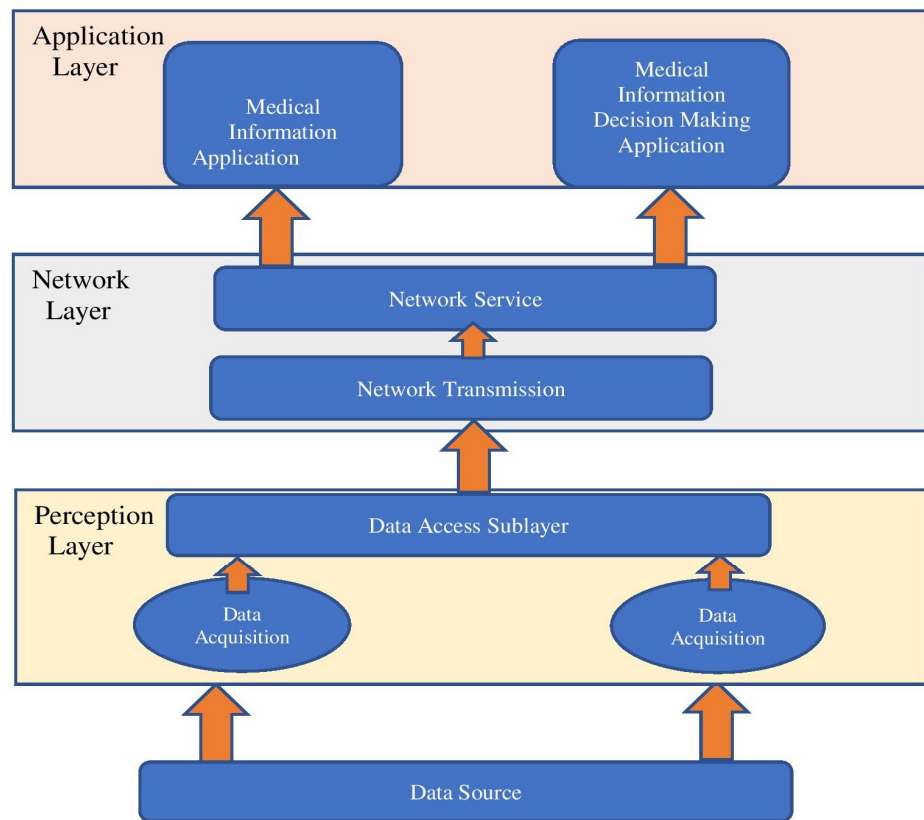
Different researchers have explained IoT, IoMT, and their components differently with respect to their own interests and aspects. In the next section, the criteria used to perform the literature review are explained. Firstly, the data sources are enumerated, and then the search and selection process is explained.

### 2.2.2. IoMT Architecture

A discussion on IoMT application and technology is not complete without reference to the architecture model, and not all applications use the same IoMT architecture. Most of the present IoMT systems are divided into three layers: the perception layer, the communication network layer, and the application layer.

- Sensor layer or perception layer—This is a foundational layer and deals with the collection of data from the source, providing the necessary viewpoint from the gathered data [48]. This layer ensures the precise sensing of the parameters related to health issues [32] and consists of hardware such as sensors, controllers, and actuators. The hardware presently in use includes the radio frequency identification (RFID) reader/tag, GPRS, facial recognition camera, fitness smartwatch, health-monitoring sensors, insulin pumps, and infrared temperature sensors. Wearable sensor devices, implanted sensor devices, and ambient sensor devices are three categories for the sensors [32]. As depicted in Figure 4, the perception layer comprises two sublayers, the data access sublayer and the data acquisition sublayer. The primary task carried out by the data acquisition sublayer is perception of the gathered data, for which it makes use of various medical perception equipment and signal acquisition equipment. Some of the major signal acquisition methods can be GPRS, RFID, graphic code, etc. [49]. Short-range data transfer technologies like Bluetooth, Wi-Fi, Zigbee, 4G, 5G [50,51],

etc., are then used to transfer this obtained data to the network layer via the data access sublayer.



**Figure 4.** IoMT architecture [49].

- **Network layer**—This is the subsequent layer, and it offers a wide range of platforms, interface-related services, and data transmission methods. This layer consists of two sublayers, which are the network transmission layer and the network service layer. The network transmission sublayer transmits the data it receives from the perception layer in real time and with accuracy using the Internet, mobile communication networks, wireless sensor networks, etc. The integration of various networks, information description formats, and data warehouses is accomplished via the service layer, which also offers a variety of platform-related services and open interface services for these integrations [49].
- **Application layer**—This is the topmost layer which utilizes the information taken from the network layer to manage medical records by means of various applications [32]. Like the previous two layers, this layer is also composed of two sublayers: the medical information decision-making application layer and the medical information application layer. The medical information application layer incorporates various healthcare equipment and other materials related to information for maintaining patient information, such as inpatient, outpatient, medical treatment, tracking system, fitness/ health system, remote diagnostic system, telemedicine, medical e-record, etc. [52]. On the other hand, the medical information decision-making application layer deals with the analysis of various pieces of information, such as patients, disease, medication, diagnosis, treatment, etc.

In [53], the researcher has adopted a three-tier architecture consisting of the sensor level, personal servers, and medical servers. As the name suggests, the sensor level contains sensors and medical devices, which form a local network known as the Body Sensor Network (BSN). For wireless communications at the sensors and personal server

level, low-power wireless technology protocols including RFID, Bluetooth Low Energy (BLE), and Near Field Communication (NFC) are employed. Data collected by the medical devices will be sent to personal servers, which could be either on-body devices or off-body devices. Prior to being transferred to the centralized medical servers, this layer will locally process and store patient data. It is needed when a network connection is lost or when a user needs access to the patient's data remotely. The last layer is the medical server layer which consists of an algorithm or program for early diagnosis, rehabilitation progress assessment, or continuous patient monitoring like MobiCare [54] or BSN-Care [55]. This architecture prioritizes usability and power consumption, but it does not cater to any security or privacy risks, leaving these considerations to future work.

In [56], the researcher here proposes an end-to-end architecture called the mHealth System, which is able to connect the IoT smart sensors directly with the Smart Healthcare System (SHS). This architecture consists of three layers: the data processing layer, the data collection layer, and the data storage layer. The data collection layer, which is the bottom layer, consists of IoT devices that can sense and collect medical parameters. The next layer, which is the data storage layer, stores medical data on wide-scale and high-speed storage racks. The topmost layer, the data processing layer, involves various techniques to analyze collected sensor data.

A foundational layer, which is called the perception layer, deals with data collection and making interpretations about gathered information. It facilitates the sensing of health parameters. The data are collected and transferred to the network layer where they are transmitted in real-time. The top layer is the application layer, where medical records are managed and information is gathered from the previous layer. Comparing the architectures, we can conclude that the bottom layer has sensors with direct contact with the human body. The middle layer is used for storage and processing of data, and the last layer is used for providing services to the users.

### 2.2.3. Most Common Cyberattacks on IoMT

- Denial-of-service attack—This type of attack occurs when an IoT system is prevented from uploading patients' health information onto the respective cloud-based services or medical database or when the medical professional is unable to retrieve patient information through the IoMT system. Frequent data backups would be essential for recovering historical data, but real-time services would be disrupted. Time stamping and strong authentication on IoMT devices may be taken into consideration to minimize these types of attacks [52].
- Injection attack—Data integrity is essential to ensure that the data received have not been altered or distorted in any way during communication channels. False data injection attacks, which cause false data to be transmitted to a hospital data center, are one example of such attacks. Another frequent attack is an SQL injection, which provides back doors for cyber criminals to access medical databases.
- Data leakage and privacy—Compilation and storing of an individual's health and movement records should conform to legal and ethical laws on privacy. Owing to the transparent and accessible nature of wireless messages, IoMT systems are also more likely to suffer from data leakage through sniffing attacks, and these include eavesdropping, traffic analysis, and brute force attacks (trial and error to guess login info) [52].

As IoMT devices increase in popularity, attacks and hacking opportunities also increase [57]. Insecure devices can put patients at risk and damage a healthcare organization's entire infrastructure. Above, we have discussed some common cyberattacks on IoMT devices.

Some of the most common attacks are presented in Figure 5 below.

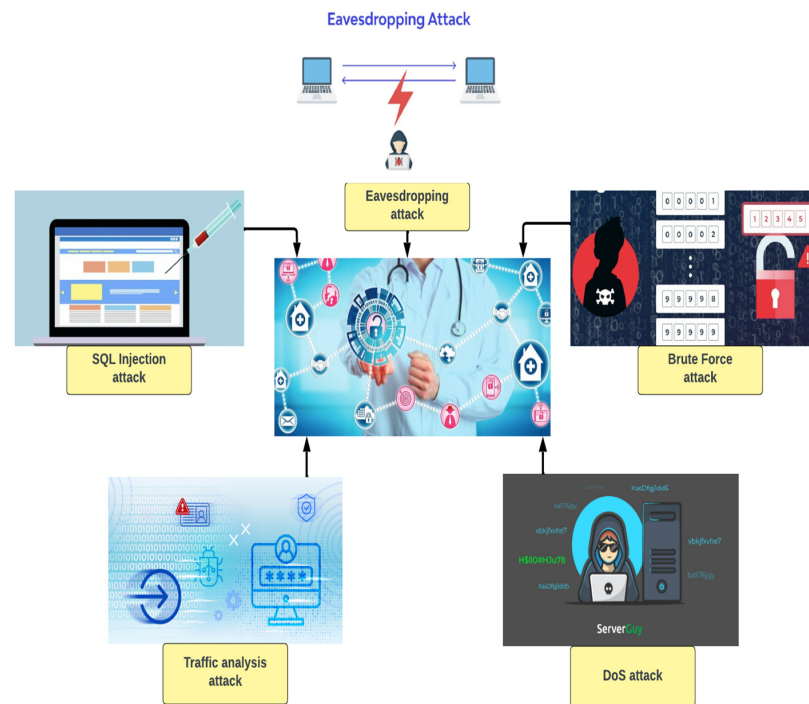
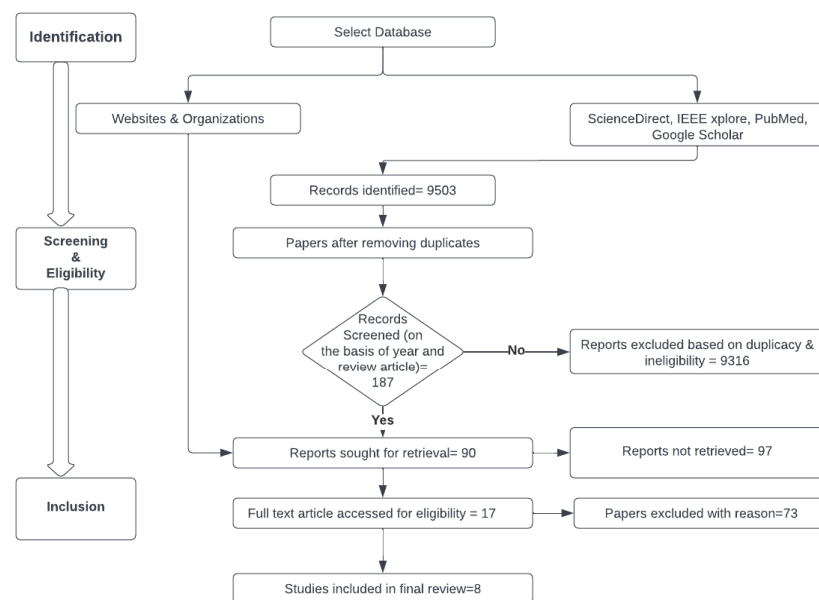


Figure 5. Common attacks of IoMT.

In the next section, the criteria used to perform the literature review are explained. Firstly, the data sources are enumerated, and then the search and selection process is explained.

### 2.3. Data Collection

To address the research objective, a systematic literature search was carried out on major indexing databases following PRISMA guidelines and is represented in Figure 6.



Flowchart of Literature review process

Figure 6. PRISMA.

The electronic search uses IEEE Xplore, ScienceDirect, MDPI, PubMed, Google Web browser, and Springer using the terminologies such as “Internet of Things”, “Risk Assessment in IoMT”, “Internet of Medical Things”, and “IoMT Frameworks”, as depicted in the Table 2. Academic review papers published between 2014 and 2022 were searched and were further studied based on their title/abstract. PubMed was particularly useful in gaining additional information about IoMT. In addition, some results have been removed to ensure that the paper contains only data from journals, top-quality review papers, and conferences. This step was performed by selecting studies published in journals and conference papers with competitive acceptance rates. Some studies were eliminated due to quality restrictions such as a slight increase from previous studies, technical issues, full-text unavailability, and were ruled out. It is worth noting that a keyword search of “IoT” returned maximum results on all the indexing databases, and the least number of papers were found on IoMT risk assessment and their framework.

**Table 2.** Keyword search of all indexing databases.

Source of Database	IoT	IoMT	Risk Assessment in IoMT	IoMT Framework
ScienceDirect	2599	79	45	63
IEEE Xplore	3551	82	3	18
PubMed	373	21	3	2
Springer	1923	55	13	42
MDPI	617	13	0	1
Total	9063	250	64	126

In the identification phase (phase 1), 9503 records were identified in the original and umbrella search, taken from the five aforementioned databases, websites, and organizations. Based on duplication and ineligibility, 9316 records from these studies were eliminated and 187 records remained. Phase 2 involved screening a total of 187 papers based on the year and review article. Out of those, 90 records were sought for retrieval so that they could be further examined based on the title and abstract, while 97 papers were not retrieved since they did not fit into the objective of this work. Out of the 90 full-text papers that were retrieved in the third phase, 73 papers were excluded because they met the exclusion criteria, which included papers that only discussed IoT devices but did not contain much information about IoMT-based devices or did not discuss risk assessment methodologies. The remaining 17 papers were sought for full-text review, out of which 8 papers were finally included in this systematic review, as they adhered to the aims/objectives of this study and met the inclusion criteria.

The pictorial representation of the selection of keywords from various databases is shown in Figure 7 below.

Figure 8 presents the search keyword “IoT” in all five databases, which brought about a total number of 9063 open-access review articles between 2014 and 2022.

Figure 9 presents the search keyword “IoMT” in all five databases, which brought about a total number of 250 review articles between 2014 and 2022.

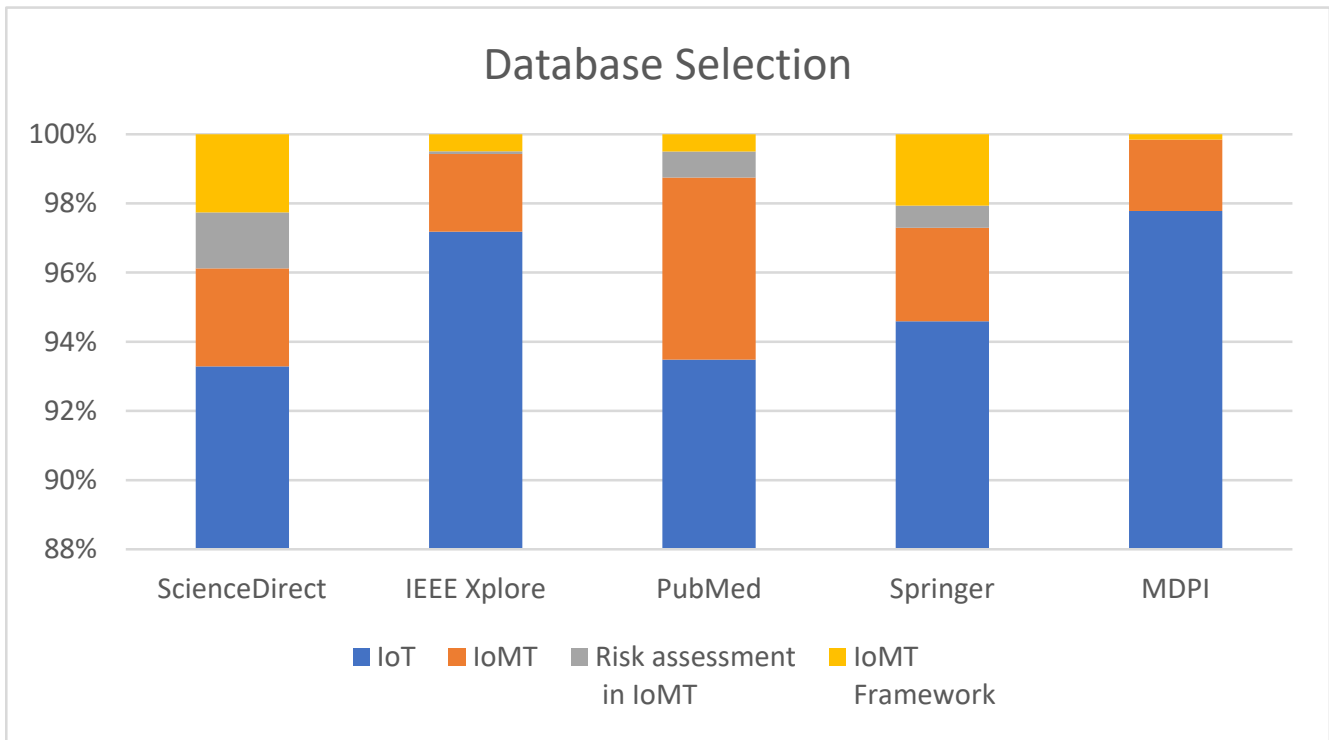
Figure 10 presents the search keyword “Risk assessment in IoMT” in all five databases, which brought about a total of 64 open-access review articles between 2014 and 2022.

Figure 11 presents the search keyword “IoMT Framework” in all the databases, which brought about a total of 126 open-access review articles between 2014 and 2022.

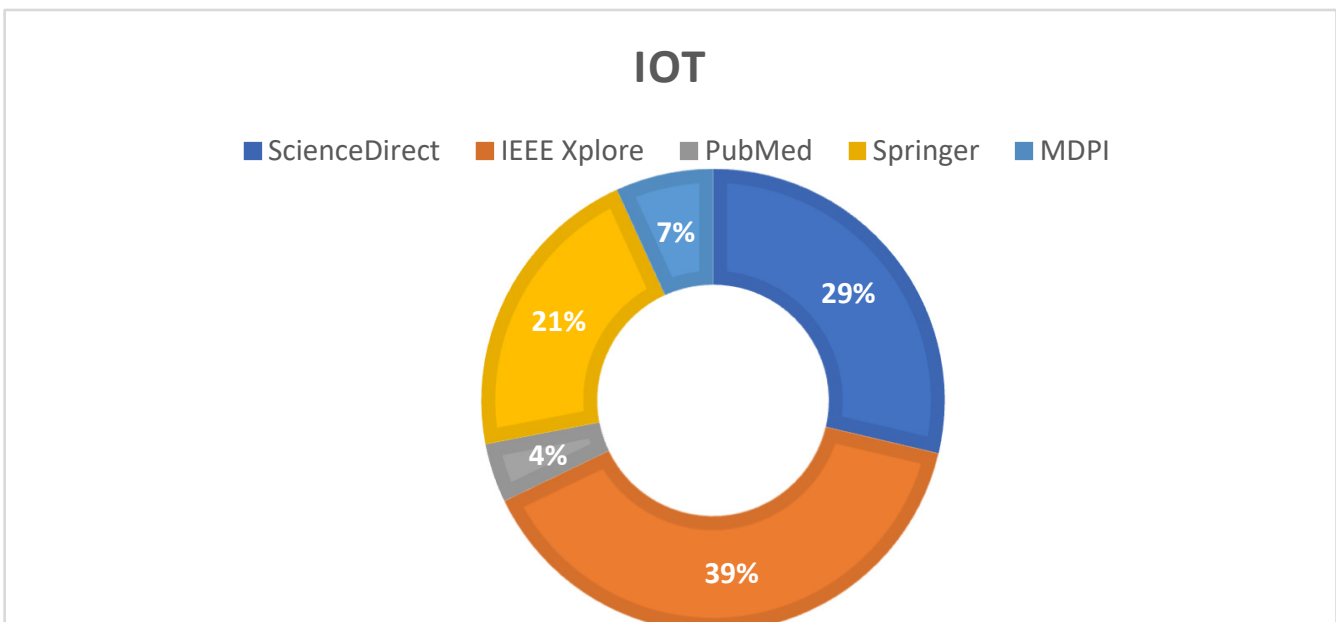
Applicable studies from the aforementioned data sources were carried out in three rounds.

- Round 1—An electronic search was conducted to identify and categorize the literature review related to primary studies. The title, abstract, and introduction were read to narrow down the selection of relevant papers, thereby removing the irrelevant studies.
- Round 2—The relevant papers selected in round 1 were carefully examined, and those found irrelevant were removed.

- Round 3—A snowball search using the reference list of papers from round 2 was applied to distinguish relevant papers and include them. If found applicable, they were read carefully and included.



**Figure 7.** Database search selection.



**Figure 8.** Search result for term IoT.

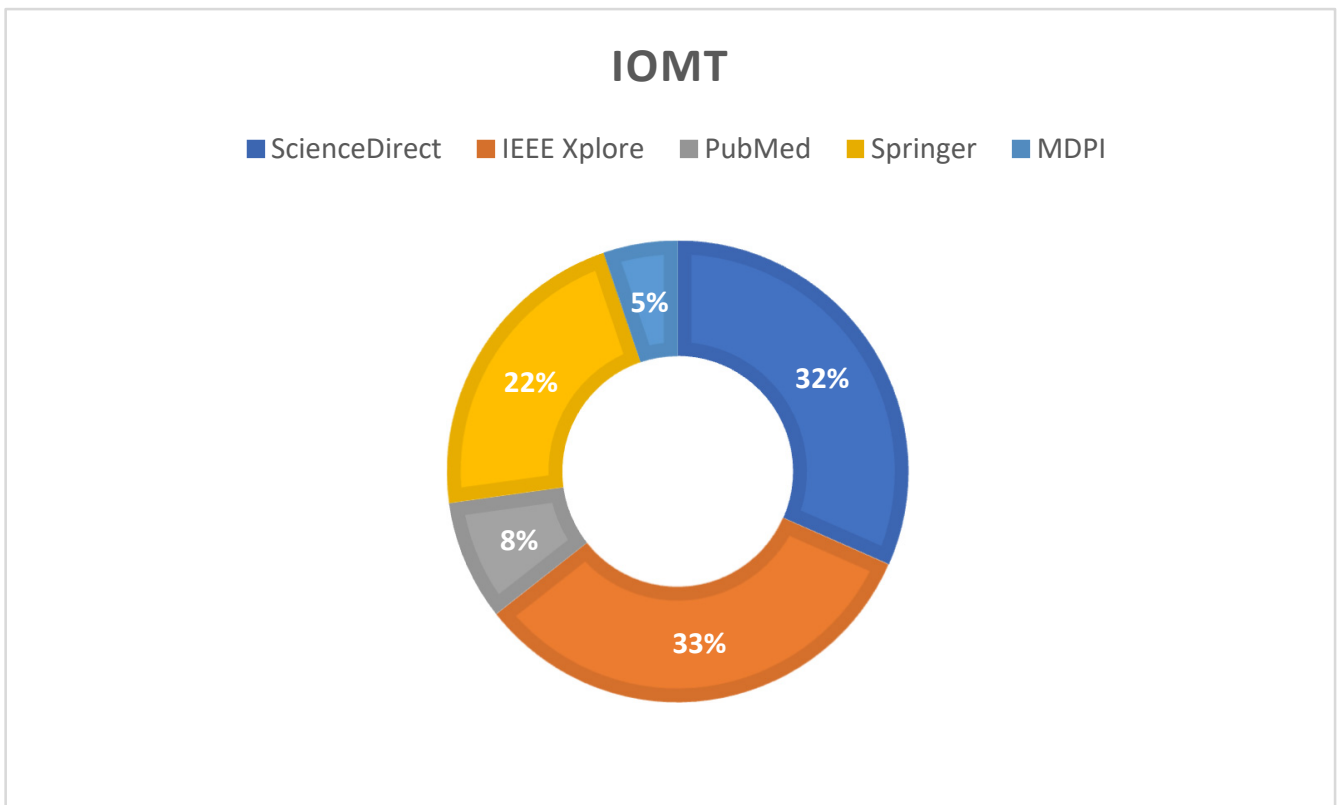


Figure 9. Search result for term IoMT.

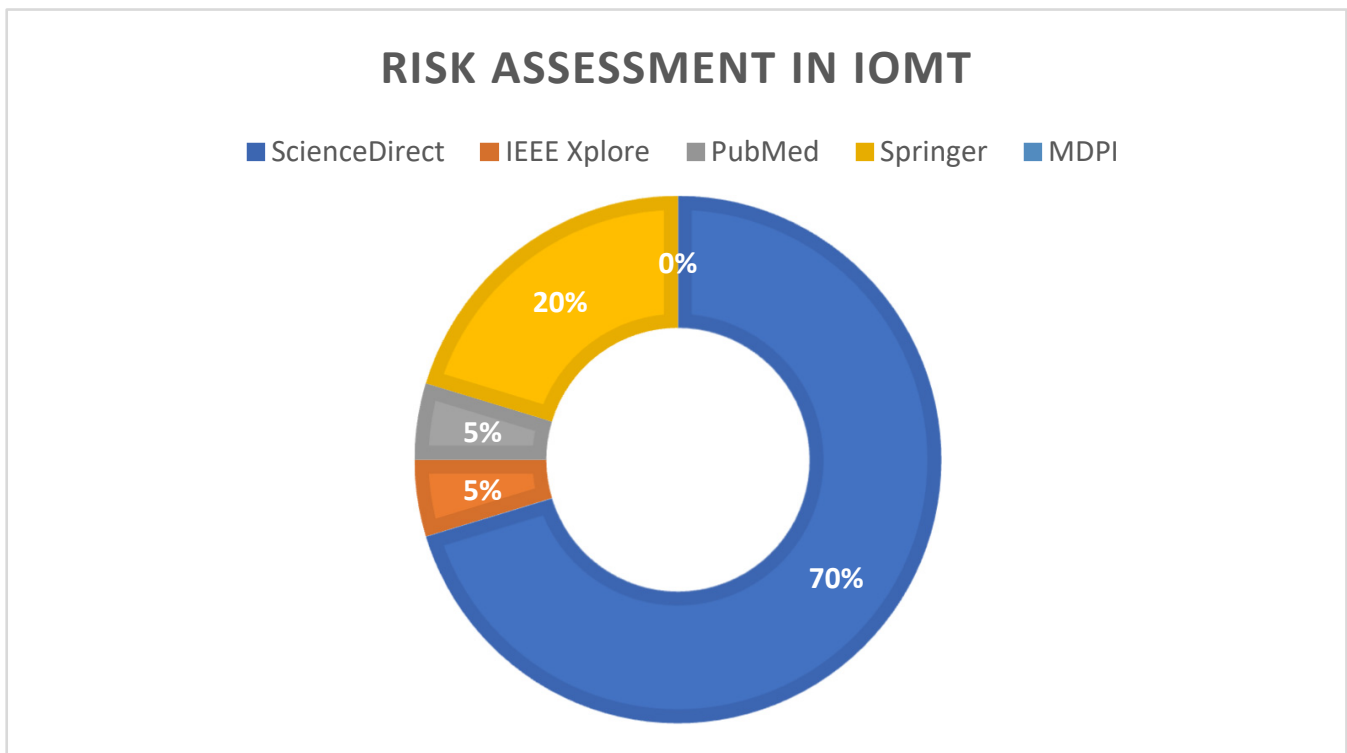
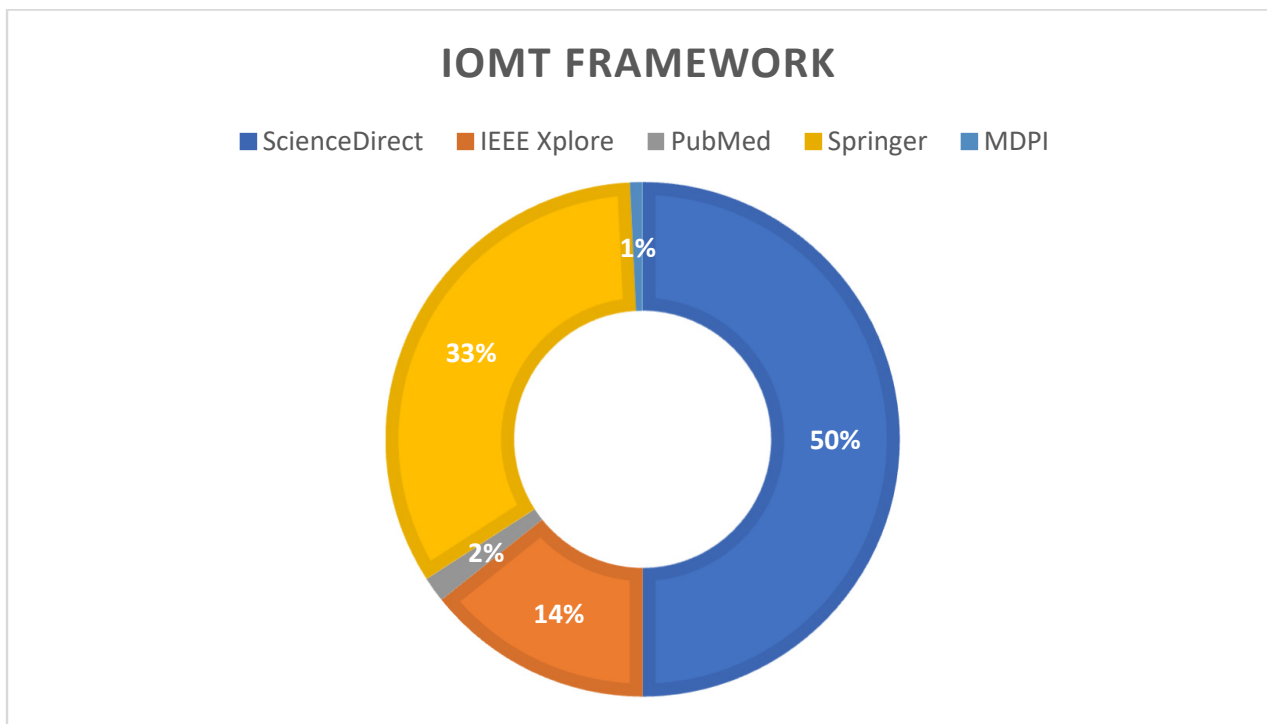


Figure 10. Search result for term Risk Assessment of IoMT devices.



**Figure 11.** Search result for term IoMT Framework.

#### 2.4. Quality of the Selected Papers

Different inclusion and exclusion approaches were applied to the remaining series of studies generated for the subsequent second and third rounds. In order to narrow down our search, we applied some exclusion criteria to the number of papers retrieved. In the selection process, an English-language criterion was first applied, while duplicates were removed based on keyword searches. All the papers were then reviewed for relevance based on their titles.

Our next step was to access the abstracts and introductions of the retrieved papers, which helped us decide whether or not to add a paper to our database for further research, following which an in-depth analysis of papers related to IoT, IoMT risk assessment, their frameworks, and countermeasures was conducted. Additionally, some papers were excluded during this step and were sorted based on the reason for exclusion. Retention was used only for the purpose of analyzing the literature review and answering the stated research questions.

#### 2.5. Review of the Existing Literature

In this section, papers based on the aforementioned keywords are explained along with their contribution. Various papers relevant to IoT applications, security, and architecture have gained considerable attention. Papers related to IoT frameworks and risk assessment have also been discussed. After the COVID-19 pandemic, special attention has been paid to IoMT applications and their security issues, but only a few papers discussed the risk assessment for IoMT devices. Below are the reviewed papers related to IoT, IoMT, risk assessment, and frameworks.

The author in [39] introduces the status of the healthcare sector, including applications and their research and development plans. The existing IoMT applications are classified into body-centric and object-centric applications. Data acquisition, communication gateways, and servers of IoMT architecture are discussed. Furthermore, the paper discusses the gaps, challenges, and open research issues. The main objective of this review paper is to offer a new research perception for the development and advancement of the IoMT ecosystem.

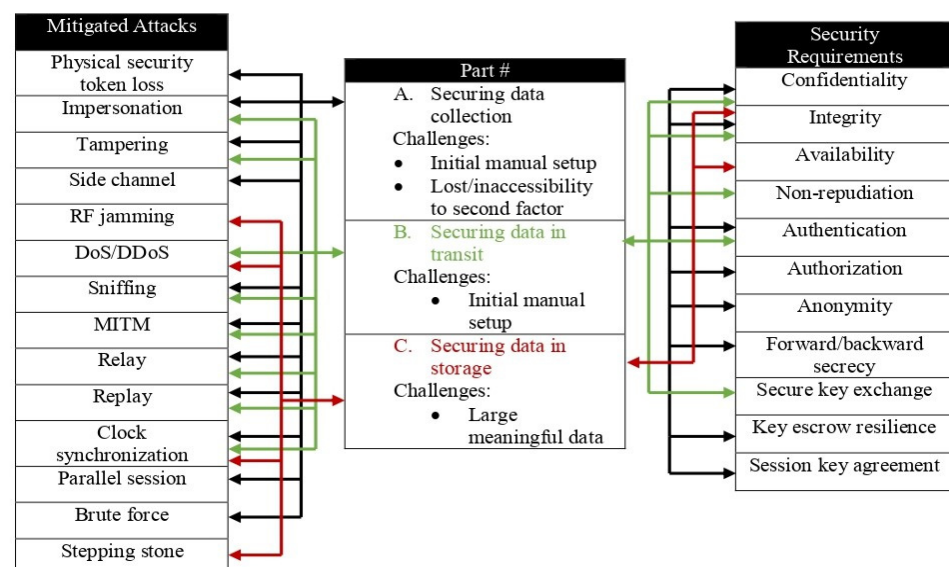


Even though both software and hardware aspects of IoMT are explained in detail, this paper does not come up with any assessment framework as a solution.

The author reviews the existing proposed security standards and assessment frameworks as well as those under development for assessing the security of IoT-based smart environments in [58]. They present the conclusion that most of the assessment frameworks and security standards do not directly address current needs but have the potential to be adapted to IoT-based smart environments. A taxonomy of challenges is proposed to address the current and future IoT security issues. A further study is necessary to enhance the quality of the research conducted and spark discussion about the development of new security standards and assessment frameworks for IoT-based smart environments.

The work in [59] performed a holistic analysis of the available technologies, system architecture, optimization factors, and challenges that emerge by incorporating IoT in a hospital environment. This article has come out as a bridge between business applications and sensors in the unified network, which will be successful in creating step-by-step interoperable smart hospital design, but the research work does not cover any privacy and security risks which may arise in creating the hospital design.

In [60], the researchers have reviewed the security requirements, security techniques, architecture, and various new attacks. Since the attacks are unique and none of the proposed frameworks can satisfy the systems, a framework is proposed covering all data and device security stages such as data collection, data storage, and data sharing. The aforementioned framework is only limited to fourteen mentioned attacks in the paper and faces certain challenges. Thus, there is a need to create a system that can sustain a remotely secure primary setup and an alternate access method. Moreover, the years covered by the selected papers are not specified. The proposed framework is presented in Figure 12.



**Figure 12.** Framework by Ghubais with security features [60].

The review paper [61] reflects an overview of IoT used in the healthcare industry along with the challenges faced by IoMT applications. It surveys the literature on the Internet of Things in healthcare. It suggests that even though there exist a plethora of studies, they are lacking in conceptual and theoretical approaches. In their examination, six major categories of healthcare are taken into consideration, and light is shed on the gap existing in the articles related to the field.

A novel key management framework is presented in [36], which provides point-to-point secure communication channels between devices of the IoMT platform. It is designed for continuous patient monitoring and general medical applications and claims that the framework will give the patients full control of their personal data.

The paper in [62] presents a comprehensive history of the growth of IoMT applications and the related machine-learning-based frameworks from 2010 to 2019, focusing primarily on monitoring health through mobile applications, controlling rural health, detecting stress in drivers, identifying e-health applications, recognizing other health-related human movements, etc. The paper also presents previous challenges which are still unresolved and discusses how the deployment of the discussed approaches has challenges ranging from leakage of patients' personal information to the unaffordable price range. The article is useful for the deployment of future healthcare units, but it does not provide much information about the mentioned frameworks and techniques.

In [63], an IoMT risk assessment framework is designed to indicate security and protection features in IoMT devices and other IoMT platforms. IoMT Security Assessment Framework (IoMT-SAF) enables users to make security decisions based on a quantitative assessment method that uses recommended scenario-based security assessment criteria. A case study has been considered to understand the potential security issues based on consumption scenarios. The paper presents a framework comprising two modules: the recommendation module and the assessment module. The recommendation module identifies IoMT security threats and recommends security measures needed to respond to these threats. In the assessment module, these threats are ranked based on their degree of security, and this hierarchy is used as assessment criteria. Furthermore, based on these criteria and additional user requirements, the solutions (device, service, and platform) are assessed. Finally, a detailed ranking result is generated to allow IoMT end users to choose a secure solution.

#### *2.6. Risk Assessment*

The security vulnerabilities of modern IoT systems are unique, mainly due to the complexity and heterogeneity of technology and data. From a security and trust management perspective, organizations need to invest effectively in IoT cybersecurity. However, the challenge for IoT is its existing risk assessment methods, which were established before its development and used in many locally deployed organizations. These methods may not be effective when trying to manage the complexity and pervasive nature of these automated systems. Extending the existing risk assessment methods to the IoT could lead us to overlook new risks in the ecosystem [64].

Risk assessment is a process of identifying and assessing the risks associated with an organization's assets. This process includes estimating the risks and ranking them based on their importance. Risk assessment is a necessary part of the risk management process as it constitutes an essential step towards addressing risks. The likelihood and impact of an attack are some of the features considered in the risk assessment process. Risk treatment includes (a) accepting the risk when it is under a harmless level, (b) mitigating the risk by applying security measures, (c) transferring the risk, or (d) avoiding the risk by removing the affected asset itself. Some of the core concepts in risk assessment include assets, vulnerabilities, threats, attacks, and their impact [65].

Assets are defined as the value of any enterprise, whether tangible or intangible. Vulnerabilities are the points of weakness in an asset that can be exploited by others. Threat is explained as a possible action that could exploit these vulnerabilities. These actions can be deliberately done or happen accidentally, therefore resulting in the likelihood of attack and harm to the assets [65].

#### *2.7. Risk Assessment Framework*

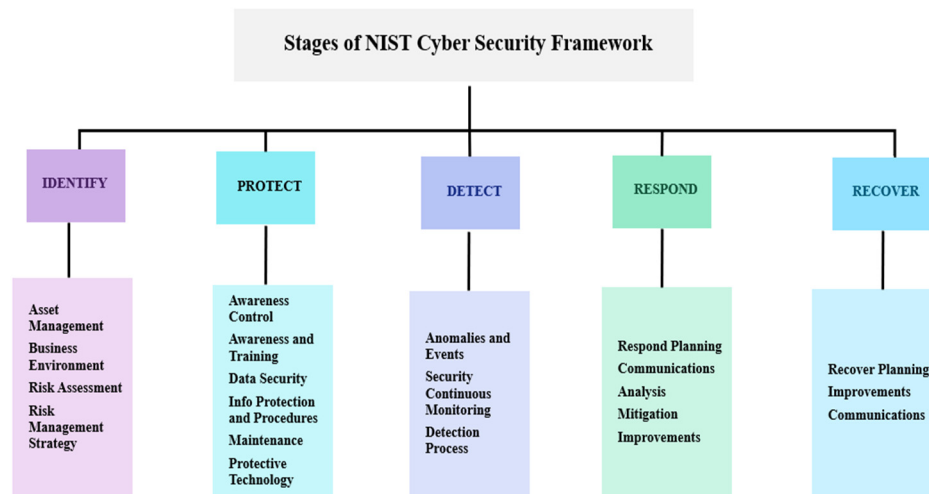
Although the required process for risk assessment is defined, we still need various methods, guides, and tools for undertaking a risk assessment. Therefore, there is a persistent need to implement an effective cybersecurity framework due to the heterogeneity of IoMT devices. Examples of the most popular and well-regarded approaches include NIST SP800-30, ISO/IEC 27001, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), the CCTA Risk Analysis and Management Method (CRAMM), and

the Expression of Needs and Identification of Security Objectives (EBIOS); their origins range from standard-setting bodies (such as NIST and ISO/IEC) to governments (CRAMM from the UK and EBIOS from France).

These approaches were by and large designed with specific application circumstances in mind; hence, they cannot be applied in the same way for the IoMT environment requirements because threats tend to be unique. As there is no standard framework available, these existing frameworks can be slightly modified for the risk assessment of IoMT devices in our research. Inferring from the aforementioned summarized research work, most of it does not provide risk assessment for IoMT devices and is only limited to a specific area; thus, it does not completely cater to the needs of IoMT-based devices. This section reviews the assessment frameworks suggested from the review literature and their limitations and forms the basis of the existing research.

### 2.7.1. NIST (National Institute of Standard and Technology) Framework

NIST's framework was created based on a set of organization standards to help them manage their cybersecurity requirements [58]. The framework's design aims to secure critical infrastructure but is used by private organizations to secure themselves from cyber threats [66]. It is suitable for organizations that are more technology-oriented and need to create a strong baseline strategy. NIST delivers regulatory and legal advantages that extend well for the organization which adopts it early [67]. It is not a one-size-fits-all approach to manage the threats to critical infrastructure because organizations will continue to have unique threats [68]. It has a structured and planned format, making it easier to execute at the enterprise level. The NIST framework is broken down into five functions: Identify, Protect, Detect, Respond, and Recover (as represented in Figure 13). These functions provide a systematic way to classify security risks, making it easier to implement controls [58].



**Figure 13.** NIST Cybersecurity Framework (based on NIST model) [68].

- Identify—Helps organizations to develop an understanding to manage cybersecurity risks to people, systems, data, assets, and capabilities. It also incorporates asset management, business environment, risk assessment, and governance [68].
- Protect—Assists organizations in developing and implementing adequate safeguards to ensure the delivery of critical services. This phase includes developing security controls to protect data and information systems, such as access control, data security, information protection procedures, and maintaining protective technologies [58].
- Detect—Supports organizations to develop and implement appropriate activities to identify the presence of a cybersecurity event. It also offers guidelines for detecting anomalies in security, monitoring systems, and networks to uncover security

incidences. It also incorporates access control, communication processes, detection processes, anomalies, and events [58].

- Respond—Once a cybersecurity incident is detected, it helps organizations to develop and implement appropriate activities to act. This includes planning response, security resilience, mitigation, and communication during a response [58]
- Recovery—Develops and implement steps needed to maintain plans for resilience and restore capabilities and services compromised during a cybersecurity incident [58].

Most of the categories and sub-categories of the NIST framework use reference to other frameworks such as ISO 27001, combining significant features of these frameworks. Below are the limitations of the NIST framework:

- Because of the voluntary nature of the NIST framework, it does not provide proper risk management. Therefore, it cannot be used as a long-term replacement for information security management frameworks.
- The NIST framework is not a one-size-fits-all approach to handle the breaches and threats, as the organizations are complex and threats are unique [66].

NIST is making a unique contribution to meet the interoperation capability. It is uniquely qualified to undertake this task because of its technical capability, industry knowledge, standards and testing expertise, and international influence. Ensuring interoperability requires the integration of technical expertise in numerous disciplines. NIST brings an understanding of various industries through its research in supporting technology and testing; expertise in advanced networking technology; expertise in controls and their interfaces; and expertise in technology, computer, and network security. It has a long track record of working closely with industry and standards development organizations to develop consensus standards for industry use and, where needed, for regulatory agencies. NIST has extensive experience establishing testing and certification programs in critical areas, including cybersecurity. Finally, it has a strong presence and leadership in key international standards organizations. Moreover, NIST Special Publication 800-53 provides the foundation for security controls and a method for tailoring security controls to an organization.

### 2.7.2. ISO 27001 Cybersecurity Framework

ISO 27001 is a globally recognized standard developed in 2005 by the International Organization for Standardization (ISO). It takes a broader approach, and its methodology is based on Plan-Do-Check-Act (PDCA) cycle, which means that it builds the management system that not only plans and implements cybersecurity but also maintains and improves the complete system. This framework provides a series of requirements for an information security management system (ISMS) that an organization must follow to secure their data and is best suited for commercial companies. One of the most significant advantages of ISO 27001 is that companies can become certified against it and gain client confidence in providing a safe and effective risk management framework. One more advantage of ISO 27001 is that its documentation, such as incident management, change management, BYOD policy, password policy, etc., is structured and streamlined [66]. Below are the limitations of the ISO 27001 cybersecurity framework:

- It does not provide any specific risk management method.
- Organizations are expected to define their own method for risk management depending on their own requirements [10].

The ISO 27001 standard defines the requirements for establishing, implementing, maintaining, and improving an ISMS. Through risk management, ISMS assures confidentiality, integrity, and availability of information and provides confidence to interested parties. ISO/IEC 27001 (2013) specifies a total of 114 security controls across the following areas: A.5 Security policy, A.6 Organization of information security, A.7 Asset management, A.8 Human resources security, A.9 Physical and environmental security, A.10 Communications and operations management, A.11 Access control, A.12 Information systems acquisition, development and maintenance, A.13 Information security incident management, A.14

Business continuity management, A.15 Compliance. It also provides guidelines for organizations to address common cybersecurity risks such as social engineering attacks, hacking, malicious software, spyware, or other potentially unwanted software. Moreover, it provides a framework for sharing information, coordinating efforts, and controlling incidents [69]. Every device has its own risks; therefore, even though the standards might not apply to all of them, the number of controls used to address these risks will depend on each device's risks. While interoperability is a concern, the controls can be chosen according to the risks [70–72].

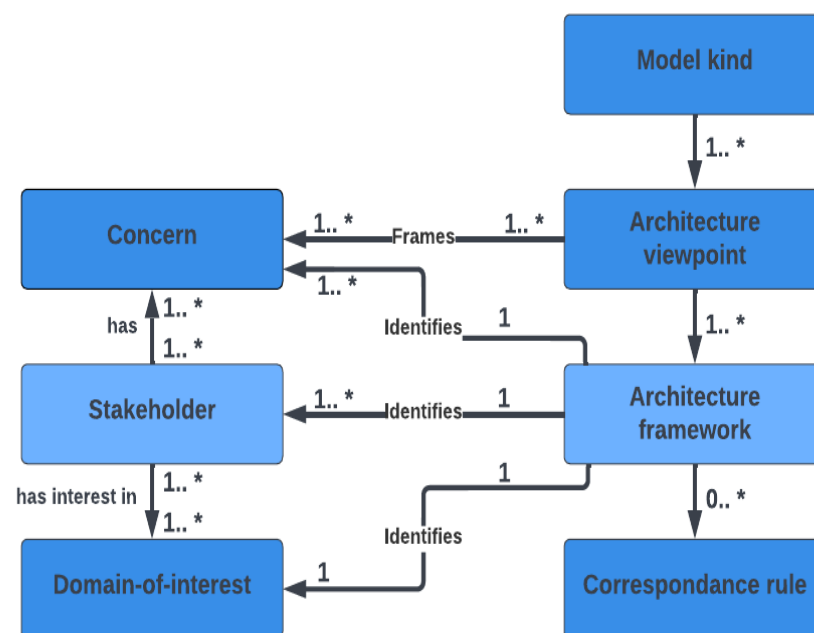
### 2.7.3. TARA Cybersecurity Framework

TARA (Threat Analysis and Risk Remediation) is a predictive framework initially developed within Intel to address complicated security risks. It is a qualitative approach to risk assessment that lists the expected attacks, communicates risks to the organizations, reduces the effort of risk analysis, and produces a better decision. TARA is mostly used alongside the NIST framework, applying IoT considerations of the NIST framework [34].

### 2.7.4. IEEE 2413-2019 (P2413) Standard

It is a standard that defines an architectural framework for IoT and conforms to the international standard ISO/IEC/IEEE 42010:2011. This framework is motivated by the concerns shared by stakeholders across several domains such as home, health, energy, transport, etc., and identifies intersection points between various domains. It does not define a specific standard for the IoMT platform but briefly outlines a domain of interest focused on health. The architectural framework in Figure 14 identifies sections like information, kind of model and viewpoints, architecture development, the rationale for key decisions, stakeholders' concerns, and viewpoint catalogue, where the last section serves as a reference for the adaptation of the standard to IoMT systems [72]. The standard focuses on two objectives: a) to deliver an interoperable and secure IoT systems framework for diverse application disciplines; b) to present a framework for the assessment and comparison between available IoT systems that will help in accelerating operations, design, and deployment of IoT systems [52]. Limitations of the framework include:

- It does not provide a specific standard for the IoMT platform.



**Figure 14.** Conceptual model of an architectural framework of P2413 standard (based on ISO/IEC/IEEE 42010:2011) [72].

Table 3 summarizes the focus area, strengths, limitations, and application area of these frameworks. Due to the heterogeneity of devices, none of the frameworks are universally accepted; therefore, they do not entirely address IoMT cybersecurity and its consequences.

**Table 3.** Summary of existing frameworks.

Name of the Framework	Owner	Focus Area	Strength	Limitation	Application Area
NIST Framework	National Institute of Standard and Technology	Standards, Technology, Publications, government adoption, market intelligence	Structured and planned format, easy to execute, good for disaster and recovery planning	Not suitable for long-term approach, need more work with other standards to address compliance	Healthcare, manufacturing, government and private firms, insurance, financial organizations
TARA	Intel	Threat analysis and risk remediation	Predictive for crucial threats, provides definition of a list of attacks	Risk impact quantification is not available	Manufacturing and healthcare, financial organizations
ISO 27001	International Standard Organization	Global standardization of risk assessment	Suitable for crucial risk, international experience	Expects organizations to develop their own method	Small business, private and government firms
IEEE 2413-2019 (P2413) Standard	IEEE	Cross-domain interaction, system interoperability, functional compatibility	Provides methodology for privacy and security	Does not provide standard for IoMT design	Energy, health, home, transport

By analyzing available frameworks and the applications of IoT and IoMT devices, we now have the understanding to use the methodology in the proposed framework. The papers which have been reviewed demonstrate that only a small number of studies discuss the risk assessment of internet of medical devices. In our research, for the risk assessment of IoMT devices, we will adopt the methodologies followed in NIST and ISO frameworks, which is covered in more detail in the following section. In Table 4 we have presented the statistical analysis of the papers reviewed.

**Table 4.** Statistical analysis of the papers [49].

No	Ref	Authors	Year	Type	Citation	Publisher	Journal Name	Impact Factor
1.	[1]	Vashi et al.	2017	Conference	245	IEEE	IEEEExplore	Q1
2.	[2]	Gulzar and Abbas	2019	Journal	30	IEEE	IEEEExplore	Q1
3.	[3]	Van Kranenburg and Bassi	2012	Journal	154	Springer	Communications in Mobile Computing	Q2
4.	[6]	Schiller et al.	2022	Journal	18	ScienceDirect	Computer Science Review	Q1
5.	[9]	Wang, Zhang and Taleb	2018	Journal	96	Springer	World wide web	Q1
6.	[10]	Lee	2020	Journal	74	MDPI	Future Internet	Q2
7.	[12]	Aven	2016	Journal	1313	ScienceDirect	European Journal of Operational Research	Q1
8.	[13]	Wang et al.	2020	Journal	58	IEEE	IEEE Access	Q2
9.	[14]	Rubi and Gondim	2020	Journal	37	SAGE	Distributed Sensor Networks	Q2

Table 4. Cont.

No	Ref	Authors	Year	Type	Citation	Publisher	Journal Name	Impact Factor
10.	[16]	Pratap Singh et al.	2020	Journal	165	ScienceDirect	Journal of Clinical Orthopedics and Trauma	Q3
11.	[17]	Li et al.	2020	Journal	51	ScienceDirect	Computer Communications	Q1
12.	[21]	Xu, Gu, and Tian	2022	Journal	33	ScienceDirect	Artificial Intelligence in Agriculture	Q1
13.	[22]	Lawal and Rafsanjani	2022	Journal	43	ScienceDirect	Energy and Built Environment	Q1
14.	[23]	Rahim et al.	2021	Journal	69	ScienceDirect	Vehicular Communications	Q1
15.	[24]	Kumar, Tiwari and Zymbler	2019	Journal	432	Springer	Journal of Big Data	Q1
16.	[25]	Dwivedi, Mehrotra and Chandra	2022	Journal	40	ScienceDirect	Journal of Oral Biology and Craniofacial Research	Q2
17.	[26]	Karale	2021	Journal	45	ScienceDirect	Internet of Things	Q1
18.	[27]	Ogonji, Okeyo, and Wafula	2020	Journal	74	ScienceDirect	Computer Science Review	Q1
19.	[28]	Tawalbeh et al.	2020	Journal	286	MDPI	Applied Sciences	Q2
20.	[30]	Bertino and Islam	2017	Journal	639	IEEE	IEEEExplore	Q1
21.	[31]	Hameed	2019	Conference	59	IEEE	IEEEExplore	Q1
22.	[32]	Hireche, Mansouri and Pathan	2022	Journal	6	MDPI	Journal of Cybersecurity and Privacy	Q1
23.	[33]	Mercan et al.	2020	Conference	5	IEEE	IEEEExplore	Q1
24.	[34]	Kandasamy et al.	2020	Journal	65	Springer	EURASIP Journal on Information Security	Q2
25.	[35]	Kakhi et al.	2022	Journal	10	ScienceDirect	Biocybernetics and Biomedical Engineering	Q2
26.	[36]	Ree et al.	2021	Conference	-	IEEE	IEEEExplore	Q1
27.	[37]	Furtado et al.	2022	Journal	1	ScienceDirect	Digital Communications and Networks	Q1
28.	[39]	Al-Turjman, Hasan Nawaz and Deniz Ulusar	2020	Journal	175	ScienceDirect	Computer Communications	Q1
29.	[40]	Haleem et al.	2022	Journal	8	ScienceDirect	Internet of Things and Cyber-Physical Systems	Q2
30.	[42]	Chau and Hu	2002	Journal	1558	ScienceDirect	Information & Management	Q1
31.	[43]	Moazzami et al.	2020	Journal	391	ScienceDirect	Journal of Clinical Virology	Q1
32.	[44]	Swayamsiddha and Mohanty	2020	Journal	168	ScienceDirect	Diabetes & Metabolic Syndrome: Clinical Research & Reviews	Q1
33.	[45]	Yang et al.	2020	Journal	100	MDPI	Diagnostics	Q2
34.	[49]	Srivastava et al.	2022	Journal	5	Hindawi	Computational Intelligence and Neuroscience	Q2
35.	[51]	Sengupta, Ruj and Das Bit	2020	Journal	477	ScienceDirect	Journal of Network and Computer Applications	Q1
36.	[52]	Mohd Aman et al.	2021	Journal	120	ScienceDirect	Journal of Network and Computer Application	Q1
37.	[53]	Sun, Lo and Lo	2019	Journal	122	IEEE	IEEEExplore	Q1
38.	[56]	Algarni	2019	Journal	50	IEEE	IEEEExplore	Q1
39.	[58]	Karie et al.	2021	Journal	30	IEEE	IEEEExplore	Q1
40.	[59]	Çalış, Uslu and Dursun	2020	Journal	76	Springer	Journal of Cloud Computing	Q1
41.	[60]	Ghubais et al.	2020	Journal	80	IEEE	IEEEExplore	Q1

Table 4. Cont.

No	Ref	Authors	Year	Type	Citation	Publisher	Journal Name	Impact Factor
42.	[61]	Lederman, Ben-Assuli and Vo	2021	Journal	-	ScienceDirect	Health Policy and Technology	Q1
43.	[62]	Din et al.	2019	Journal	72	IEEE	IEEEExplore	Q1
44.	[63]	Alsubaei et al. Radoglou	2019	Journal	104	ScienceDirect	Internet of Things	Q1
45.	[64]	Grammatikis, Sarigiannidis and Moscholios	2019	Journal	217	ScienceDirect	Internet of Things	Q1
46.	[65]	Nurse, Creese and De Roure	2017	Journal	182	IEEE	IEEEExplore	Q1
47.	[66]	Roy	2020	Conference	21	IEEE	IEEEExplore	Q1
48.	[72]	Talaminos-Barroso, Reina-Tosina and Roa	2022	Journal	-	ScienceDirect	Measurement: Sensors	Q3
49.	[73]	Kheirhahan et al.	2019	Journal	67	ScienceDirect	Journal of Biomedical Informatics	Q1

A list of the publications is presented in Table 4. The information contains reference, author's name, journal and publisher names, type of article, number of citations, and year of publication. The papers have all been published in peer-reviewed journals or at conferences. Overall, the research community is showing an increase in interest year after year. The worldwide pandemic probably contributed to a dip in research in 2021. Journal and peer-reviewed articles have been the focus of this review, followed by conference publications. There were 48 publications, five of which were conference proceedings, and the rest were journals. The referenced papers are compared according to their publication dates in Figure 15. It highlights the distribution of referenced papers based on the type of journal. Out of the total referenced papers, 45 originate from reputed journals, while 4 come from conferences. Figure 16 represents the frequency of papers concerning IoT and IoMT. Based on papers cited from 2016 to 2022, we found that numbers have increased yearly except for the decline in 2021 due to the global pandemic, and the PDF version of a few papers from 2018 cannot be found. We have reviewed only 2 papers that are published in or before the year 2016.

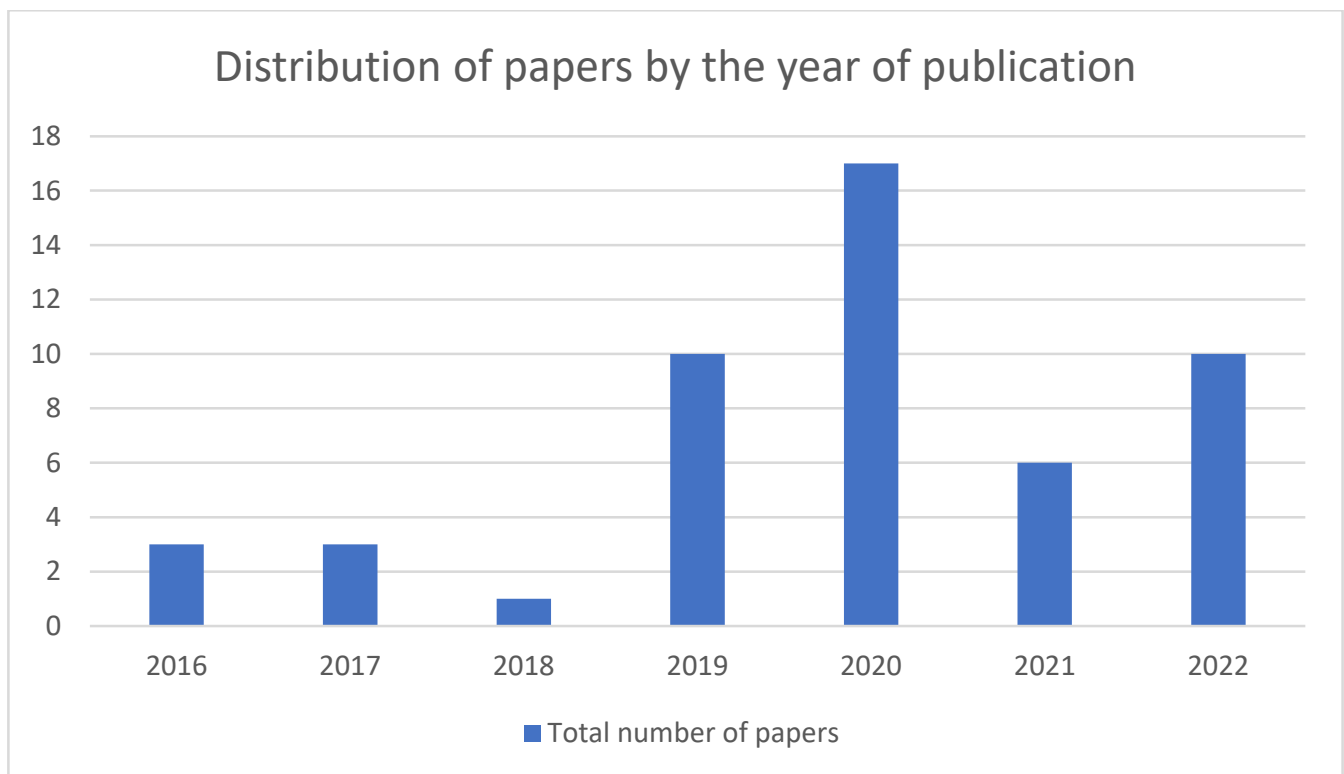


Figure 15. Distribution of papers by the publication year.



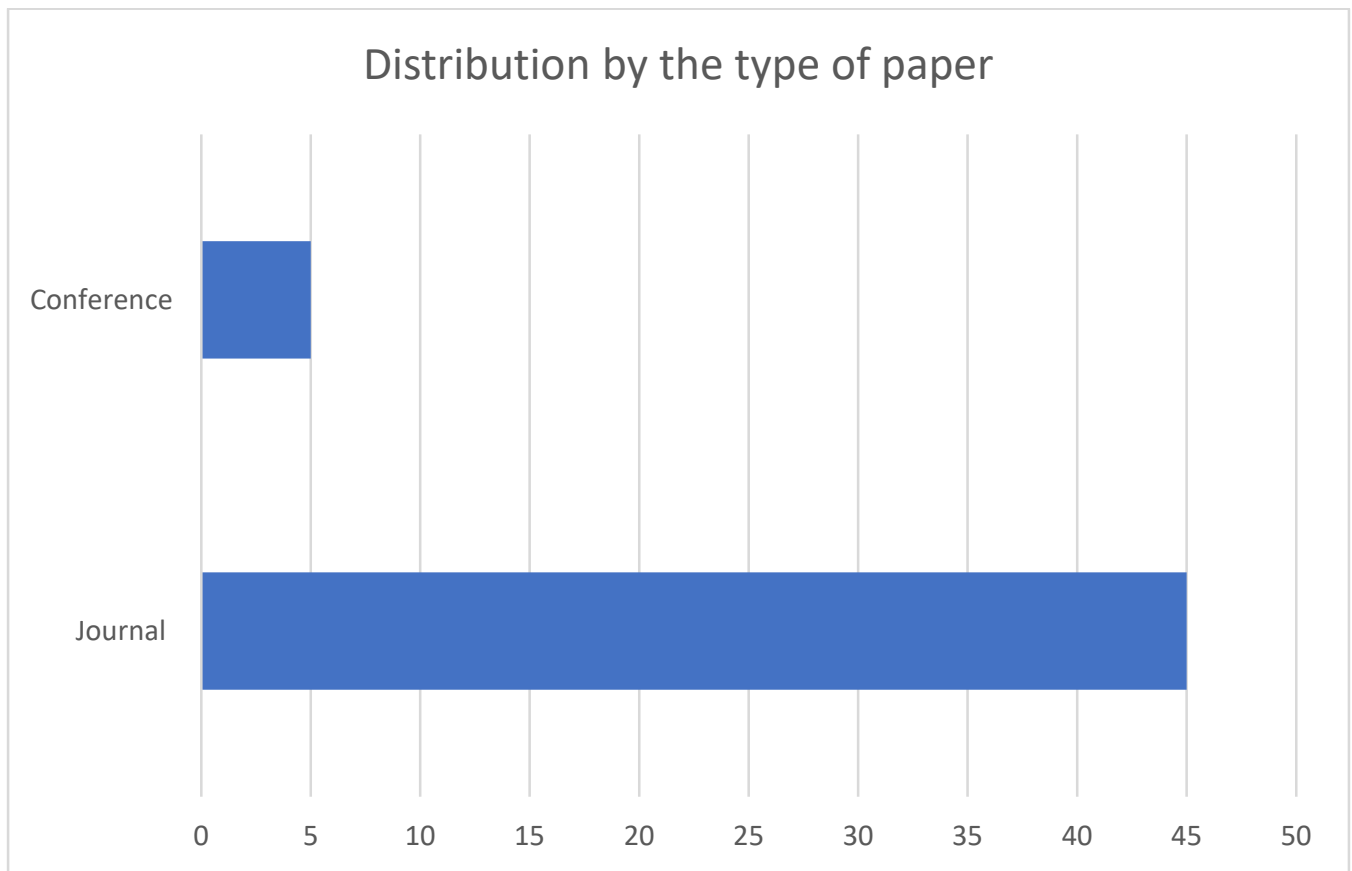


Figure 16. Distribution by the type of paper.

### 3. Methodology

The objective is to identify and predict a framework for evaluating the risk associated with IoMT devices because of their immunity to security measures and a large number of devices on the market that communicate private and sensitive information. Below is a flowchart in Figure 17 to represent the steps performed in the risk assessment.

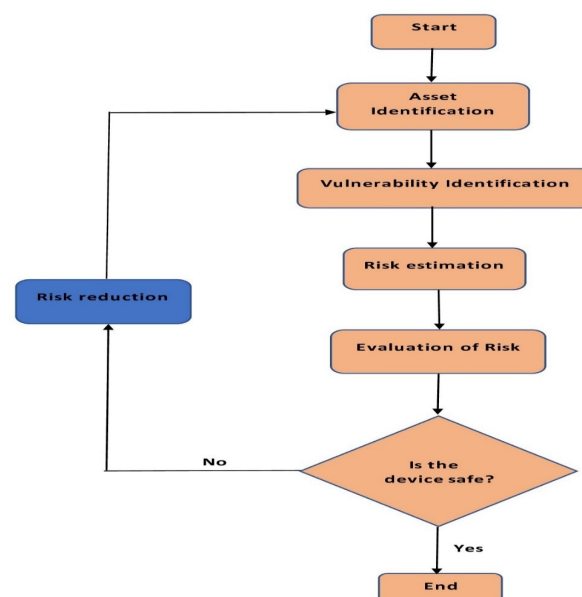
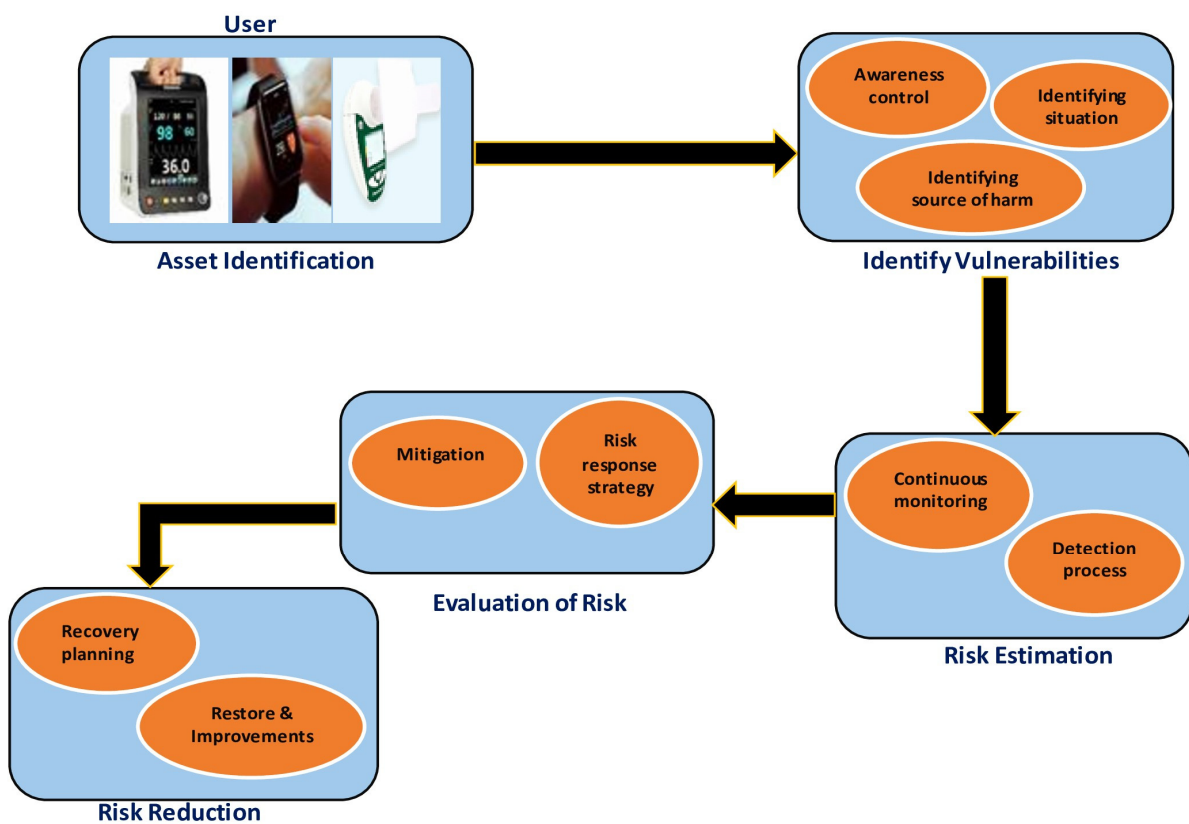


Figure 17. Risk assessment flowchart.

We will test the portable wireless vital monitor, smartwatches, and lung monitor. As the primary research methodology, this study will adopt a NIST- and ISO-based framework for the risk assessment. Since the NIST framework is threat-oriented, it can be tailored based on the requirement and will be appropriate to address the present threat landscape. The limitation of one size not fitting with all the approaches gives the flexibility to establish a strong baseline and augment compliance with new regulations.

ISO 27001, on the other hand, takes a more comprehensive approach. It bases its methodology on the PDCA cycle and creates a management system to plan, implement, maintain, and enhance the entire cybersecurity system. This framework provides a series of requirements that an organization must follow to secure its data. Its documentation is structured and streamlined. Based on both frameworks, we have proposed a framework, as shown in Figure 18, where we will create a checklist to perform the risk assessment. The methodology process entails the following steps: Asset identification, Identify vulnerabilities, Risk estimation, Evaluation of risk, and Risk reduction, which are described below.



**Figure 18.** Risk assessment flowchart.

### 3.1. Asset Identification

The first step is the identification of the asset, which focuses on monitoring and baselining, where an asset will be a device using the IoMT application. As explained in Section 2, there is a range of applications, and we anticipate testing a few, such as a wireless vital monitor, lung monitor, and wearable device, like a smartwatch. The first two are critical devices, but they are unapparent when it comes to performing risk assessment, and the third is chosen since it is a device with a high rate of user acceptance. This is why we selected them as assets. We classify these assets into two categories, where the value depends on the sensitivity of the data and their potential impact on the CIA.

- **High-Value Asset:** The wireless vital monitor and lung monitor will fall under this category, as the level of concern given to the asset will be high, because they need more security implementation. A wireless vital monitor is a portable device capable of

monitoring vital signs, including heart rate, electrocardiogram (ECG), blood pressure, temperature, and other vitals. It transmits the readings wirelessly through Bluetooth to an interactive monitoring device [44]. It is mainly used by patients who have been discharged but still need their vitals to be measured. For patients with respiratory issues, such as Chronic Obstructive Pulmonary Disease (COPD) or cystic fibrosis, and those who have undergone a lung transplant, a lung monitor provides accurate and effective monitoring of lung function [47]. Despite having a low asset value, they have high usability. Both the devices are used by patients with critical conditions, making them highly important.

- **Low-Value Asset:** Smartwatches will be considered low-value assets. Thus, concern will be low. They are convenient to wear and are equipped with several sensors suitable for gathering physical activity throughout the day [73].

Since the risk can come from both the use and misuse of the devices, in this step, we will set the limit of use, where a use statement will be created to get an exact idea of the precise data to be taken from these devices. This step will also help to identify the scenarios of predictable misuse. Next, the time limit will be determined. It is essential to describe estimates for how long each device component should endure because it may eventually wear out. In addition, we shall identify the safety characteristics of the device.

### 3.2. Identify Vulnerabilities

While baselining is the primary focus of asset identification, this is the step where the framework starts to take action and become proactive. Adequate safeguards are implemented to ensure device safety, and security controls are developed to protect sensitive data and information. In this step, we will identify all the potential risks and the harmful situations that may arise. It is necessary to describe all the dangerous situations in this step, since failing to do so increases the likelihood that we may overlook them in the following steps, where the risk must be eliminated or reduced. For identifying, we will go through each step required to operate the device and note the potential source of damage along the way. It is necessary since the threat is not only limited to one user, but also to everyone using the device. Based on this identification, we can generate an awareness control (gathering, understanding, and anticipating information) for the user.

### 3.3. Risk Estimation

The next step is to estimate the risk after it has been identified. As the risk assessment is an iterative process, risks can also be found in this step and may become apparent when previously found risks are estimated. The primary objective of the risk estimation process is to analyze the risk and determine the severity and probability of risk occurrence. A qualitative risk assessment will be employed in our study to understand this likelihood and severity. The amount of risk will be broken down into high, medium, and low categories to help assess whether the current safeguards and controls are adequate or if more needs to be done to recover from the impact. Various methods can be used to estimate risk, such as a risk matrix or a risk graph.

Estimation is a critical step because the faster a risk is estimated, the faster the repercussions can be mitigated in the next step. As the IoMT devices may contain personal information, we anticipate using the best among the methods to lower the risk.

### 3.4. Evaluation of Risk

As the name suggests, in this step, we determine the actions that need to be taken to reduce the identified risks. We will consider two objectives in evaluating the risk:

1. Determining whether a hazardous situation requires further risk reduction.
2. Determining whether risk reduction has introduced any new risk or has increased the level of other risks.

Based on these two objectives, we will determine the action that needs to be taken to reduce the risk while making sure that these actions do not introduce any new risks. If there is a high risk involved, this process will be performed repeatedly until the above two objectives are met. This will be our response strategy to the risks to ensure the device is in a state of continuous improvement. After the risk estimation, it is necessary to evaluate risk, and if risks are found, we will need to go back and repeat the estimation for those risks. Although this is the last step of risk assessment, we will highlight some of the relevant risk reduction information, as it is connected to the risk assessment process.

### 3.5. Risk Reduction

Risk reduction entails reducing the risks to an acceptable level, putting resilience strategies into practice, and regaining access to the skills and services that were lost during a cybersecurity event. To minimize the impact of a cybersecurity event, this function will support prompt recovery. This step is closely connected to the risk assessment process, as every time risk reduction is not achieved, we will go back and perform the complete risk assessment process. The recovery function is required to ensure that, if a breach does occur, the employed device can stay on the right path to achieve the appropriate goals and objectives.

### 3.6. Summary

Throughout the risk assessment process, the goal is to understand potential risks before attempting to prevent them. By performing all the steps mentioned above, we will be able to safeguard patients from potential risks, recognize and evaluate the magnitude of these risks, and implement and monitor efficient control measures to reduce and eliminate them. The complete risk assessment procedure has been divided into four parts, starting with identifying the device that needs to be tested and concluding with evaluating the risk. We have also emphasized the significance of risk mitigation as the fifth phase. For every risk, there are possible scenarios that can unfold at any step, so given that it has to do with human life, we must be very cautious.

While IoT has been a dominant field of study for more than a decade and has received many accolades, only recently has the Internet of medical devices been receiving significant attention. Our literature review in Table 5 is based on papers published between 2019 and 2022 covering both IoT and IoMT. Our review is based on their findings, risks, and whether they propose a framework for risk assessment as a solution to these risks. These papers discuss IoMT application areas, challenges, architecture, risks associated with devices, and risk assessment frameworks. Despite the fact that privacy and security risks are significant issues with IoMT devices, more than half of the existing literature has not taken them into account. A few papers that included risks and challenges in their survey failed to offer an assessment framework for addressing them. There is a paper that discusses framework and security risks, but it only covers fourteen attacks, which is inadequate, as there will be new attacks for which we need to be prepared.

**Table 5.** Summary of literature review.

References	Year	Proposed Framework	Findings	Limitations	Privacy Risk	Security Risk
[10]	2020	Yes	IoT architecture; qualitative and quantitative approach for risk management; four-layer IoT cyber risk management framework; risk identification	Framework proposed for IoT systems but it may not work with all the security requirements for IoMT applications	×	×

Table 5. Cont.

References	Year	Proposed Framework	Findings	Limitations	Privacy Risk	Security Risk
[16]	2020	No	IoMT solutions and treatments for health issues related to orthopedic patients; challenges faced during COVID-19; digital connectivity of IoMT devices to the hospital; expected applications in the future	Challenges and applications mentioned are only limited to orthopedic patients	×	×
[25]	2022	No	Role of IoMT applications for the improvement of healthcare industry; challenges faced by IoMT in developing smart healthcare system	There are no frameworks designed for challenges faced	×	×
[36]	2021	No	Presents ad hoc, point-to-point secure channels between devices and IoMT system	Provides complete key management solution for IoMT patient monitoring system but does not present a framework	×	✓
[39]	2020	No	Surveys existing IoMT technologies, sensors, and communication protocols; provides new research perception	The paper does not present any assessment framework for the challenges mentioned	✓	✓
[58]	2021	No	Reviews security standards and frameworks for IoT-based environments, potential solutions for identified challenges	Taxonomy of challenges based on various categories are mentioned but further study is required to enhance the quality of work conducted	✓	✓
[59]	2020	No	Analyzes different factors affecting IoT-based smart hospitals based on various architectural layers	Provides an architecture for interoperable smart hospital design but this architecture needs further research and experimentation	×	×
[60]	2021	Yes	Reviews security requirements, architecture, techniques, and new attacks and presents a framework covering all device and data security stages	Framework is limited to only fourteen attacks and faces challenges	×	✓

Table 5. Cont.

References	Year	Proposed Framework	Findings	Limitations	Privacy Risk	Security Risk
[62]	2019	No	Describes a comprehensive view of IoMT-based applications developed and deployed over the last decade	Paper presents the limitations and challenges of IoMT applications but does not provide a way to overcome the difficulties	✓	✓
[63]	2019	Yes	Recommends detailed list of assessment attributes covering security measures	Missing on some security features needed for IoMT device users	×	✓
Our Work	2023	Yes	Discusses recent advances, probable risks, IoMT application areas, and risk assessment frameworks	This paper provides IoT and IoMT application areas, probable risks, architecture, and frameworks for the risk assessment	✓	✓

Traditional risk assessment methodologies cannot always cater to the new risks generated by the integration of IoT in a critical sector like healthcare. Contrary to the existing papers, we provide a comprehensive approach towards a risk-free IoMT device, starting with the application, the architecture, and plausible risks, followed by a framework for risk assessment.

#### 4. Conclusions

IoMT is evolving rapidly, and it can potentially change the healthcare industry cost-effectively, focusing on treatment, early diagnosis, and prevention of spread. It is becoming more diverse, prevalent, and highly successful at identifying, predicting, and monitoring recently emerging infectious diseases. However, it is still in its early stages of growth, and heterogeneity and associated risk are still significant concerns. Due to the rapid advancement and breakthroughs, security measures must be considered; if these risks are disregarded, there will be more cyber breaches.

This study has initially focused on the broader IoT domain and narrowed it down to IoMT and its risk assessment. To fully comprehend the concept, the paper reviewed previous research publications, and it was discovered that the current risk assessment approaches do not always cater to the new threat landscape generated by the integration of IoT in the healthcare sector. Despite the recent surge in interest in the IoMT sector, a detailed review of risk assessment methodology and the security precautions for IoMT devices is still in its infancy. Therefore, the paper examines the currently available risk assessment frameworks, standards, and their limitations to provide a comparative analysis. Lastly, a framework is proposed for the risk assessment of the selected devices.

#### 5. Future Work

This study will give readers a thorough understanding of the subject and aid future researchers in creating new IoMT risk assessment methodologies or enhancing those that already exist. The suggested methodology will be put to the test and implemented.

As a future direction, we plan to test heterogeneous devices, including a lung monitor, smartwatch, and wireless vital monitor. We intend to apply the proposed methodology to these devices, and a risk assessment will be conducted, which will address every aspect of data and device security, from data collection to storage and sharing. Based on the risks

mentioned in our paper, we will assess the efficiency and efficacy of the performance, and we anticipate having risk-free heterogeneous IoMT devices. Given the security and privacy risks, we will also study how the current taxonomy can be adapted and integrated into different IoMT-based systems.

This finding has the potential to spark additional IoMT research and advance society's ability to function effectively. Additionally, it will benefit the stakeholders and policymakers in the healthcare industry. Although IoMT has gained attention in the past few years, the research is still fragmented, with increased heterogeneity in approaches and devices. However, we strongly believe that IoMT risk assessment is an ongoing hot research topic, and we expect a significant amount of related literature to be produced in the near future.

**Author Contributions:** Conceptualization, P. and B.S.; Methodology, P., B.S. and S.A.; Formal analysis, P. and B.S.; Data curation, P., B.S. and S.A.; Writing—original draft preparation, P.; Writing—review and editing, B.S. and S.A.; Visualization, P., B.S. and S.A.; Supervision, B.S. and S.A. All authors have read and agreed to the published version of the manuscript.

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

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## References

1. Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT) A Vision, Architectural Elements, and Security Issues. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017.
2. Gulzar, M.; Abbas, G. Internet of Things Security: A Survey and Taxonomy; In Proceedings of the 2019 International Conference on Engineering and Emerging Technologies (ICEET), Lahore, Pakistan, 21–22 February 2019.
3. Van Kranenburg, R.; Bassi, A. IoT Challenges. *Commun. Mob. Comput.* **2012**, *1*, 9. [[CrossRef](#)]
4. Global Government IoT Revenue for Endpoint Electronics and Communications to Total \$21 Billion in 2022. Available online: <https://www.gartner.com/en/newsroom/press-releases/2021-06-30-gartner-global-government-iot-revenue-for-endpoint-electronics-and-communications-to-total-us-dollars-21-billion-in-2022> (accessed on 11 July 2022).
5. Forecast: IT Services for IoT, Worldwide, 2019–2025. Available online: <https://www.gartner.com/en/documents/4004741> (accessed on 11 July 2022).
6. Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B. Landscape of IoT security. *Comput. Sci. Rev.* **2022**, *44*, 100467. [[CrossRef](#)]
7. Australia's IoT Opportunity-Driving Future Growth. Available online: <https://www.acs.org.au/insightsandpublications/reports-publications/iot-opportunity.html> (accessed on 2 February 2023).
8. • IoT Total Revenue Worldwide 2019–2030 | Statista. Available online: <https://www.statista.com/statistics/1194709/iot-revenue-worldwide/> (accessed on 17 July 2022).
9. Wang, H.; Zhang, Z.; Taleb, T. Special Issue on Security and Privacy of IoT. *World Wide Web* **2017**, *21*, 1–6. [[CrossRef](#)]
10. Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet* **2020**, *12*, 157. [[CrossRef](#)]
11. IoT Security in 2022: Defending Data during the Rise of Ransomware. Available online: <https://www.perle.com/articles/iot-security-in-2022-defending-data-during-the-rise-of-ransomware-40193618.shtml> (accessed on 24 July 2022).
12. Aven, T. Risk assessment and risk management: Review of recent advances on their foundation. *Eur. J. Oper. Res.* **2016**, *253*, 1–13. [[CrossRef](#)]
13. Wang, L.; Ali, Y.; Nazir, S.; Niazi, M. Special Section on Lightweight Security and Provenance for Internet of Health Things ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods. *IEEE Access* **2020**, *8*, 152316–152332. [[CrossRef](#)]
14. Rubí, J.N.S.; Gondim, P.R.D.L. Interoperable Internet of Medical Things platform for e-Health applications. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147719889591. [[CrossRef](#)]
15. 2025 Forecast: Global IoT Healthcare Market Looks Good—A \$188.2 Billion Opportunity | TechRepublic. Available online: <https://www.techrepublic.com/article/2025-forecast-global-iot-looks-good-a-188-2-billion-opportunity/> (accessed on 11 July 2022).

16. Pratap Singh, R.; Javaid, M.; Haleem, A.; Vaishya, R.; Ali, S. Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications. *J. Clin. Orthop. Trauma* **2020**, *11*, 713–717. [CrossRef]
17. Li, X.; Dai, H.-N.; Wang, Q.; Imran, M.; Li, D.; Imran, M.A. Securing Internet of Medical Things with Friendly-jamming schemes. *Comput. Commun.* **2020**, *160*, 431–442. [CrossRef]
18. 53% of Connected Medical Devices Contain Critical Vulnerabilities. Available online: <https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities> (accessed on 26 July 2022).
19. Marron, J.A. *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*; NIST Special Publication: Gaithersburg, MD, USA, 2022. [CrossRef]
20. Asimily: Healthcare & Medical Device Security (IoMT). Available online: <https://www.asimily.com/> (accessed on 24 July 2022).
21. Xu, J.; Gu, B.; Tian, G. Review of agricultural IoT technology. *Artif. Intell. Agric.* **2022**, *6*, 10–22. [CrossRef]
22. Lawal, K.; Rafsanjani, H.N. Trends, benefits, risks, and challenges of IoT implementation in residential and commercial buildings. *Energy Built Environ.* **2022**, *3*, 251–266. [CrossRef]
23. Rahim, M.A.; Rahman, M.A.; Rahman, M.M.; Asyhari, A.T.; Bhuiyan, M.Z.A.; Ramasamy, D. Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Veh. Commun.* **2021**, *27*, 100285. [CrossRef]
24. Kumar, S.; Tiwari, P.; Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: A review. *J. Big Data* **2019**, *6*, 1–21. [CrossRef]
25. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofac. Res.* **2021**, *12*, 302–318. [CrossRef]
26. Karale, A. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet Things* **2021**, *15*, 100420. [CrossRef]
27. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. *Comput. Sci. Rev.* **2020**, *38*, 100312. [CrossRef]
28. Tawalbeh, A.I.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
29. Kathryn Cormican, S.M.; Dhanapathi, C. Analysis of critical success factors to mitigate privacy risks in IoT Devices. *Procedia Comput. Sci.* **2022**, *196*, 191–198. [CrossRef]
30. Bertino, E.; Islam, N. Botnets and Internet of Things Security. *Computer* **2017**, *50*, 76–79. [CrossRef]
31. Hameed, A.; Alomary, A. Security Issues in IoT: A Survey. In Proceedings of the 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 22–23 September 2019.
32. Hireche, R.; Mansouri, H.; Pathan, A.-S.K. Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. *J. Cybersecur. Priv.* **2022**, *2*, 640–661. [CrossRef]
33. Mercan, S.; Akkaya, K.; Cain, L.; Thomas, J. Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain. In Proceedings of the 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Rhodes, Greece, 2–6 November 2020; pp. 198–203.
34. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
35. Kakhi, K.; Alizadehsani, R.; Kabir, H.M.D.; Khosravi, A.; Nahavandi, S.; Acharya, U.R. The internet of medical things and artificial intelligence: Trends, challenges, and opportunities. *Biocybern. Biomed. Eng.* **2022**, *42*, 749–771. [CrossRef]
36. De Ree, M.; Vizár, D.; Mantas, G.; Bastos, J.; Kassapoglou-Faist, C.; Rodriguez, J. A Key Management Framework to Secure IoMT-enabled Healthcare Systems. In Proceedings of the 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Porto, Portugal, 25–27 October 2021; pp. 1–6.
37. Furtado, D.; Gyax, A.F.; Chan, C.A.; Bush, A.I. Time to forge ahead: The Internet of Things for healthcare. *Digit. Commun. Netw.* **2022**. [CrossRef]
38. Internet of Medical Things (IoMT) Market: Global Industry Analysis, Trends, Market Size, and Forecasts up to 2026. Available online: <https://www.researchandmarkets.com/reports/5338262/internet-of-medical-things-iomt-market-global> (accessed on 20 June 2022).
39. Al-Turjman, F.; Hassan Nawaz, M.; Deniz Ulusar, U. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. *Comput. Commun.* **2020**, *150*, 644–660. [CrossRef]
40. Haleem, A.; Javaid, M.; Pratap Singh, R.; Suman, R. Medical 4.0 technologies for healthcare: Features, capabilities, and applications. *Internet Things Cyber-Phys. Syst.* **2022**, *2*, 12–30. [CrossRef]
41. Lu, L.; Zhang, J.; Xie, Y.; Gao, F.; Xu, S.; Wu, X.; Ye, Z. Wearable Health Devices in Health Care: Narrative Systematic Review. *JMIR mHealth uHealth* **2020**, *8*, e18907. [CrossRef]
42. Chau, P.Y.K.; Hu, P.J.H. Investigating healthcare professionals' decisions to accept telemedicine technology: An empirical test of competing theories. *Inf. Manag.* **2002**, *39*, 297–311. [CrossRef]
43. Moazzami, B.; Razavi-Khorasani, N.; Dooghaie Moghadam, A.; Farokhi, E.; Rezaei, N. COVID-19 and telemedicine: Immediate action required for maintaining healthcare providers well-being. *J. Clin. Virol.* **2020**, *126*, 104345. [CrossRef]
44. Swayamsiddha, S.; Mohanty, C. Application of cognitive Internet of Medical Things for COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 911–915. [CrossRef]



45. Yang, T.; Gentile, M.; Shen, C.-F.; Cheng, C.-M. Diagnostics Combining Point-of-Care Diagnostics and Internet of Medical Things (IoMT) to Combat the COVID-19 Pandemic. *Diagnostics* **2020**, *10*, 224. [CrossRef]
46. Kaputa, D.; Price, D.; Enderle, J.D. A portable, inexpensive, wireless vital signs monitoring system. *Biomed Instrum Technol.* **2010**, *44*, 350–353. [CrossRef] [PubMed]
47. Lung Monitor | Healthcare | Vitalograph. Available online: <https://vitalograph.com/intl/product/lung-monitor/> (accessed on 31 July 2022).
48. Williams, P.A.H.; Woodward, A.J. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Med. Devices (Auckl.)* **2015**, *8*, 305. [CrossRef]
49. Srivastava, J.; Routray, S.; Ahmad, S.; Waris, M.M.; Asghar, M.Z. Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress. *Comput. Intell. Neurosci.* **2022**, *2022*, 7218113. [CrossRef]
50. Ahad, A.; Tahir, M.; Kok-Lim, A.; Yau, A. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. *IEEE Access* **2019**, *7*, 100747–100762. [CrossRef]
51. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
52. Mohd Aman, A.H.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *J. Netw. Comput. Appl.* **2021**, *174*, 102886. [CrossRef] [PubMed]
53. Sun, Y.; Lo, P.-W.; Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
54. Chakravorty, R. A Programmable Service Architecture for Mobile Medical Care. In Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), Pisa, Italy, 13–17 March 2006. [CrossRef]
55. Yeh, K.H. A Secure IoT-Based Modern Healthcare System with Body Sensor Networks. *IEEE Access* **2022**, *4*, 10288–10299. [CrossRef]
56. Algarni, A. A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems. *IEEE Access* **2019**, *7*, 101879–101894. [CrossRef]
57. Increase in Health-Care Security Breach by Proliferation of IoMT Devices—dynamicCISO. Available online: <https://dynamicciso.com/increase-in-health-care-security-breach-by-proliferation-of-iomt-devices/> (accessed on 2 February 2023).
58. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access* **2021**, *9*, 121975–121995. [CrossRef]
59. Çalı ş, B.; Uslu, Ç.; Dursun, E. Analysis of factors affecting IoT-based smart hospital design. *J. Cloud Comput.* **2020**, *9*, 67. [CrossRef]
60. Ghubaish, A.; Salman, T.; Zolanvari, M.; Al-Ali, A.; Jain, R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security; Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet Things J.* **2021**, *8*, 8707–8718. [CrossRef]
61. Lederman, R.; Ben-Assuli, O.; Vo, T.H. The role of the Internet of Things in Healthcare in supporting clinicians and patients: A narrative review. *Health Policy Technol.* **2021**, *10*, 100552. [CrossRef]
62. Din, I.U.; Member, S.; Almogren, A.; Guizani, M.; Zuair, M. Special Section on Data Mining for Internet of Things A Decade of Internet of Things: Analysis in the Light of Healthcare Applications. *Ieee Access* **2019**, *7*, 89967–89979. [CrossRef]
63. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet Things* **2019**, *8*, 100123. [CrossRef]
64. Radoglou Grammatikis, P.I.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, threats and solutions. *Internet Things* **2019**, *5*, 41–70. [CrossRef]
65. Nurse, J.R.C.; Creese, S.; De Roure, D. Trusting the Internet of Things Security Risk Assessment in Internet of Things Systems. *IT Prof.* **2017**, *19*, 20–26. [CrossRef]
66. Roy, P.P. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 Natl. Conf. Emerg. Trends Sustain. Technol. Eng. Appl.* **2020**. [CrossRef]
67. Institute of Standards, N. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014. [CrossRef]
68. Strengthen Security of Your Data Center with the NIST Cybersecurity Framework | Dell Technologies United States. Available online: <https://www.dell.com/en-us/blog/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/> (accessed on 12 July 2022).
69. Lechner, N.H. An Overview of Cybersecurity Regulations and Standards for Medical Device Software. *Cent. Eur. Conf. Inf. Intell. Syst.* **2017**, 237–249. Available online: <https://cve.mitre.org> (accessed on 15 July 2022).
70. Moreira, A.; Guimarães, T.; Duarte, R.; Salazar, M.M.; Santos, M. Interoperability and Security Issues on Multichannel Interaction In Healthcare Services. *Procedia Comput. Sci.* **2022**, *201*, 714–719. [CrossRef]
71. Barata, J.; Cardoso, A.; Haenisch, J.; Chaure, M. Interoperability standards for circular manufacturing in cyber-physical ecosystems: A survey. *Procedia Comput. Sci.* **2022**, *207*, 3320–3329. [CrossRef]

72. Talaminos-Barroso, A.; Reina-Tosina, J.; Roa, L.M. Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems. *Meas. Sensors* **2022**, *22*, 100375. [[CrossRef](#)]
73. Kheirkhahan, M.; Nair, S.; Davoudi, A.; Rashidi, P.; Wanigatunga, A.A.; Corbett, D.B.; Mendoza, T.; Manini, T.M.; Ranka, S. A smartwatch-based framework for real-time and online assessment and mobility monitoring. *J. Biomed. Inform.* **2019**, *89*, 29–40. [[CrossRef](#)] [[PubMed](#)]

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