future internet

MDPI

Review

Health IoT Threats: Survey of Risks and Vulnerabilities

Samaneh Madanian [1,*], Tserendorj Chinbat [1], Maduka Subasinghage [2], David Airehrour [3], Farkhondeh Hassandoust [4] and Sira Yongchareon [1]

[1] Department of Computer Science and Software Engineering, Auckland University of Technology (AUT), 6 St. Paul Street, Auckland 1010, New Zealand; tserendorjc9@gmail.com (T.C.); sira.yongchareon@aut.ac.nz (S.Y.)
[2] Business School, University of Western Australia, Perth 6009, Australia; maduka.subasinghage@uwa.edu.au
[3] Together Communications, 77 Cook Street, Auckland 1010, New Zealand; david@wearetogether.co.nz
[4] Department of Information Systems and Operation Management, University of Auckland, 12 Grafton Road, Auckland CBD, Auckland 1010, New Zealand; farkhondeh.hassandoust@auckland.ac.nz
* Correspondence: sam.madanian@aut.ac.nz

Abstract: The secure and efficient collection of patients' vital information is a challenge faced by the healthcare industry. Through the adoption and application of Internet of Things (IoT), the healthcare industry has seen an improvement in the quality of delivered services and patient safety. However, IoT utilization in healthcare is challenging due to the sensitive nature of patients' clinical information and communicating this across heterogeneous networks and among IoT devices. We conducted a semi-systematic literature review to provide an overview of IoT security and privacy challenges in the healthcare sector over time. We collected 279 studies from 5 scientific databases, of which 69 articles met the requirements for inclusion. We performed thematic and qualitative content analysis to extract trends and information. According to our analysis, the vulnerabilities in IoT in healthcare are classified into three main layers: perception, network, and application. We comprehensively reviewed IoT privacy and security threats on each layer. Different technological advancements were suggested to address the identified vulnerabilities in healthcare. This review has practical implications, emphasizing that healthcare organizations, software developers, and device manufacturers must prioritize healthcare IoT security and privacy. A comprehensive, multilayered security approach, security-by-design principles, and training for staff and end-users must be adopted. Regulators and policy makers must also establish and enforce standards and regulations that promote the security and privacy of healthcare IoT. Overall, this study underscores the importance of ensuring the security and privacy of healthcare IoT, with stakeholders' coordinated efforts to address the complex and evolving security and privacy threats in this field. This can enhance healthcare IoT trust and reliability, reduce the risks of security and privacy issues and attacks, and ultimately improve healthcare delivery quality and safety.

Keywords: internet of things; digital health; IoT; security; privacy; healthcare

Citation: Madanian, S.; Chinbat, T.; Subasinghage, M.; Airehrour, D.; Hassandoust, F.; Yongchareon, S. Health IoT Threats: Survey of Risks and Vulnerabilities. *Future Internet* **2024**, *16*, 389. https://doi.org/10.3390/fi16110389

Academic Editors: Nicholas Kolokotronis and Christos Tryfonopoulos

Received: 26 August 2024
Revised: 10 October 2024
Accepted: 21 October 2024
Published: 23 October 2024

1. Introduction

Collection of patient's vital information is a major challenge faced by the healthcare industry [1], particularly in real-time settings. To overcome this challenge, the adoption of Internet of Things (IoT) technologies has been substantially increased in mainstream healthcare [2] and disaster situations [3]. IoT refers to a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [4]. IoT embraces sensing devices and technologies such as sensors, RFID, GPS, and infrared sensors [5] to automatically gather various formats of data such as movements, sound, heat, moisture, light, and location. IoT has been applied in healthcare for various purposes, including remote patient monitoring [6], telemedicine [7], Electronic Healthcare

Record (EHR) management [8], and smart ambulance services [9]. The use of IoT devices has enabled medical practitioners to receive real-time information regarding patients' conditions, which facilitates health monitoring and treatment [10]. The integration of IoT in healthcare has also led to increased efficiency in the delivery of healthcare services [11] and improved patient outcomes [12].

IoT architecture is comprised of three main layers [5] (as shown in Figure 1):

The perception layer: Also referred to as the sensing layer [13], this layer integrates hardware for perception and data collection. Objects/human identification and environmental condition sensing are performed through various IoT devices in this layer [13,14]. With advancements in IoT technologies, this layer has become more sophisticated, including the use of sensors, cameras, and wearable devices to capture and transmit data [15,16].

The network layer: This layer is responsible for providing secure and dependable data transmission support and aggregating data from multiple sources [17,18]. Data transmission in this layer occurs through different networks, such as mobile communication [19], satellite [20], wireless [21], and the internet [21].

The application layer: This layer enables user interaction with IoT devices based on their needs and requirements [22]. This is crucial in the IoT architecture as it provides the platform for delivering IoT services and applications [23,24]. With the integration of artificial intelligence (AI) and machine learning algorithms, the application layer has become more intelligent, capable of providing personalized experiences to users and making real-time decisions [25].

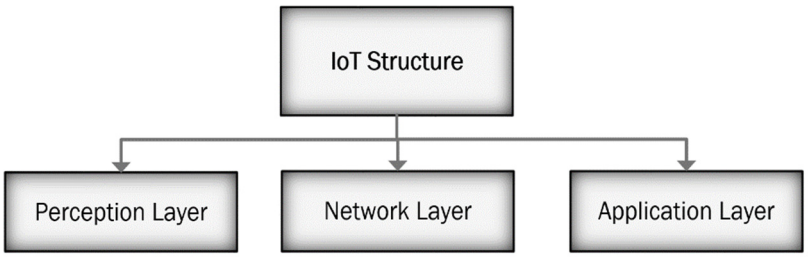

Figure 1. IoT structure.

The rise of IoT in healthcare has been a game changer for medical services, revolutionizing patient treatment with the deployment of online monitoring, usage of wearable devices, and remote access to medical consultations. Nevertheless, with the advancement of IoT technologies, safeguarding sensitive health information has become a major challenge and a concern [2,3,26,27]. As clinical data are being captured, transferred, and archived via these IoT medical devices, the volume of cyber incidents, data breaches, and infringements of privacy regarding such devices is also rising. This research is motivated by the lack of a grounded understanding of the specific risks, threats, and vulnerabilities posed by using IoT devices in the healthcare sector [16,28,29]. The use of IoT devices has made it easier for hackers to obtain access to sensitive patient information such as patient's email accounts, passwords, and medical records [29] and manipulate those records, which can lead to serious implications for patient's health [30]. Moreover, the leakage of patient's sensitive information can cause financial threats, mental anguish, medical identity theft, and possible social stigma or discrimination against people with a particular disease [31,32].

This study is further justified by the increase in the frequency and severity of hacking activities that have adversely impacted the healthcare industry [32–35]. Over the last decade, healthcare institutions have seen a dramatic rise in data breaches, which are underpinned by unauthorized access to millions of confidential patient information. Health-related data are probably the most sensitive and vulnerable to threats, as they not only include medical records and treatment protocols but personal information, including Social Security numbers, genetic data, and health insurance information as well. By accentuating the weakness of each layer, this research study lays the groundwork for further studies and

practical measures directed towards the improvement of the security and privacy of IoT healthcare devices for safe use and efficiency in enhancing patient care.

The remaining sections are structured as follows: A comprehensive introduction to the main concepts behind IoT in healthcare and the security and privacy concerns are provided in Section 2. This study's methodology, including the research strategy, data collection methods, and analytic procedures, is outlined in Section 3. The results of the analysis are presented in Section 4, with an emphasis on the vulnerabilities highlighted throughout the IoT architectural layers. The findings' consequences are covered in Section 5, while Section 6 presents the conclusion and suggestions for future research.

2. Background of the Research

Security and privacy are among the most important aspects of any system, and in healthcare, their importance cannot be overemphasized [30]. Clinical information, and in particular patient healthcare data, is considered sensitive information and mostly private as it may contain patient private information such as medical background, health conditions, and emergency contact details. This information becomes even more sensitive when it contains confidential medical data on sexual and physiological health or disease and drug misuse that patients generally refuse to share with anyone but their doctors. Moreover, over time patients' medical records become a rich repository of all types of information, including medical history, dietary and genetic data, and even family medical history.

Despite the significant IoT potential, security and privacy issues have limited the widespread deployment of IoT technologies in the healthcare domain [36]. Currently, healthcare information and data are exposed to more types of security and privacy breaches compared to the last 20 years, as reported by the Health Insurance Portability and Accountability Act (HIPAA) [37]. HIPAA is a US federal law that provides standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge [38].

The main issue of security and privacy breaches in healthcare is the lack of proper synchronization of security and privacy issues and technologies in the particular domain of healthcare [39]. This issue becomes further accentuated considering the new technologies such as mobile devices, cloud services, and remote applications being deployed in the healthcare system [40,41]. While these technologies have improved data accessibility in healthcare, they have also increased the risk of security and privacy breaches of health information.

The increasing dependence on technologies may result in increasing the vulnerability of population health data and makes citizens' healthcare information susceptible to different types of threats and misuse that may, in turn, have devastating impacts on both patients and healthcare organizations [42,43]. The lack of consideration for security and privacy in healthcare and IoT technologies is also a barrier to fully exploiting the potential of these technologies to address current challenges in healthcare. Therefore, it is crucial to clearly define and understand the concepts of security and privacy in healthcare. For this study, the following definitions were adopted from [44]:

Security: Protective measures that enable a healthcare organization to perform its critical functions despite risks posed by threats to its use of information systems.

Privacy: The restriction of access to healthcare information in accordance with laws and policies.

The significance of maintaining security and privacy in healthcare cannot be overstated, as evidence shows that security breaches in medical data can result in financial losses, medical identity theft, and discrimination [45,46]. Even the inappropriate disclosure of healthcare data can disrupt patients' privacy and expose them to further problems [47]. In some cases, people's health credentials can be stolen during medical treatments, leading to economic losses for healthcare providers and potential health consequences for patients due to the manipulation of their medical records [48].

Statistics show that breaches in healthcare records create financial concerns, psychological harm, medical identification fraud, and potential social stigma or prejudice against people with a specific condition [49]. Victims' health credentials are hijacked in some situations for medical treatment, which causes financial losses for healthcare institutions and could also have health effects for individuals owing to the alteration of their medical files [49]. Even inadvertently leaking healthcare data can affect patients' privacy [50,51] and expose them to additional issues like those described above.

Table 1 presents the number of healthcare data breaches from 2009 to 2022. Over the period of 2009 to 2022, the Health and Human Services (HHS) Office for Civil Rights has received reports of 5150 large-scale healthcare data breaches, affecting a total of 382 million healthcare records, equivalent to over 1.2 times the population of the United States. In 2018, one healthcare data breach of 500 or more records was reported daily. But five years later, the situation has worsened, with an average of 1.94 daily reports of such breaches in 2022.

Table 1. Healthcare Data Breaches Based on [37,52] Statistics.

Year	Number of Breaches (500+)	Healthcare Data Breaches (in Millions)
2022	707	50,000,000
2021	714	42,000,000
2020	642	34,000,000
2019	512	38,377,277
2018	368	12,069,868
2017	358	5,127,646
2016	329	16,657,540
2015	270	114,306,777
2014	307	12,901,859
2013	274	33,335,000
2012	209	23,335,000
2011	196	5,011,100
2010	198	1,151,000

To enhance security and address growing concerns over medical data privacy, various organizations have developed and established standards, policies, guidelines, protocols, and regulations for healthcare technology vendors and service providers. These regulations aim to protect healthcare systems and resources from intentional and unintentional risks while providing efficient and cost-effective clinical services to citizens [53]. Organizations such as HIPAA, the State Alliance for eHealth, and the National Governors Association Centre for Best Practices have provided rules and guidelines for using technology in healthcare that are widely recognized globally. Despite the potential benefits, IoT technologies offer to the healthcare system, the rapid advancements in technology have increased the vulnerability of population health data and exposed patients' information to various threats and misuses [54].

IoT Risks and Vulnerabilities in Healthcare

The use of IoT technology in the healthcare industry continues to grow. In 2022, the worldwide market for IoT in healthcare was estimated to be worth USD 99.58 billion. This market is predicted to increase to USD 486.34 billion by 2031, with a compound annual growth rate of 19.27% over the forecast period of 2023 to 2031 [55].

Studies have shown that the implementation of IoT in healthcare can improve patient outcomes and experience, increase the efficiency and productivity of healthcare organizations, and reduce costs [11,56]. For instance, wearable devices such as smartwatches and continuous monitoring systems can provide real-time monitoring of vital signs and early detection of potential health problems [57]. Therefore, this creates great opportunities for medical experts and the healthcare industry. However, security and privacy remain significant challenges in the implementation of IoT in healthcare. Health organizations reported security concerns as the main barrier to IoT adoption [58], while data privacy and data

protection ranked as the second largest concern among healthcare organizations [47]. Babar, et al. [59] claimed that having every 'thing' connected, new security and privacy problems arise, e.g., confidentiality, authenticity, and integrity of data sensed and exchanged by 'things'.

As most IoT devices and their applications are wireless in nature, security and privacy concerns are among the top areas of concern. A more highlighted issue with IoT in healthcare is the security of data transmitted from a patient's device through wireless media, which exposes the patient's data. In addition, this problem with IoT devices has been escalated due to the diversity of resources and the network heterogeneity [5]. The violations or privacy concerns discussed may restrict users from taking advantage of the full benefits IoT brings to the healthcare system [60].

Since IoT is a combination of heterogeneous networks of sensor network, mobile communication network, and the Internet, the same security and privacy threats of each of these networks directly pose security and privacy problems for IoT [5,61]. In addition, privacy protection problems, heterogeneous network authentication, and access control problems, information storage and management [5], confidentiality, and trustworthiness are other security areas for further consideration and investigation.

To address these security and privacy concerns, healthcare organizations are encouraged to implement robust security measures such as encryption, secure data storage, and access controls [62]. Additionally, there is a need for healthcare organizations to prioritize the development of industry-wide security and privacy standards for IoT devices and systems [54].

In 2020, a comprehensive survey of IoT in healthcare reported that the healthcare industry is one of the most promising fields for IoT applications due to its ability to transform healthcare services, reduce costs, and improve patient outcomes [26]. The survey also highlighted the importance of addressing the security and privacy challenges that arise with IoT systems in healthcare. Similarly, a 2020 study found that IoT technology can improve healthcare delivery by enhancing the quality of services, reducing healthcare costs, and improving patient outcomes. However, the study also cautioned that the risks associated with the use of IoT technology in healthcare, including cybersecurity concerns, must be managed appropriately [34].

While previous studies have explored the security and privacy concerns of IoT in general, there is however a notable research gap regarding the layered aspect of the IoT structure in the healthcare setting [28–30,35]. Each of the IoT layers, which includes perception, network, and application, has its security risks that when ignored stand to expose patient-sensitive information and the integrity of the data at stake. For example, the perception layer which collects data through sensors and wearable devices within the IoT infrastructure is highly prone to both physical attacks and data theft. The network layer where the data are encapsulated and sent from one point to another is faced with threats like eavesdropping, DDoS attacks, and man-in-the-middle strategies. The application layer which is a user interface and data storage system is vulnerable to weak authentication security, malware, and ransomware intrusions [32,34,35]. Reviewed studies always negate giving such distinct levels an inclusive scrutiny and treat them separately by concentrating on their security measures from the network scope [30,31]. It is therefore very important and timely to conduct such reviews along the IoT system layers for all IoT healthcare systems and deficiencies addressed. Table 2 compares our survey with other survey papers in the same area to demonstrate the gap in the literature this paper is trying to fill.

Table 2. Comparison Table: Survey Papers on IoT Security and Privacy in Healthcare.

Focus Area	IoT Layers	Recent Insight (2017–2023)	Limitation	Reference Paper
IoT security risks and threats to the healthcare sector	Network and application layers	No	Lacks updated solutions and real-time healthcare device security	[63]
Security and privacy issues in modern healthcare systems	Perception, network, and application layers	No	Does not provide practical solutions for recent IoT developments	[64]
Security and privacy in healthcare 4.0	Network, application, and cloud layers	No	Lacks focus on real-time healthcare IoT devices (perception layer)	[29]
IoMT edge network security issues	-	No	Lack of focus on IoT layers and structure	[65]
IoT security and privacy in healthcare-specific contexts	Perception, network, and application layers	updated to 2023		Our paper

Several studies have identified the security and privacy issues and attacks facing healthcare IoT systems. For example, a 2021 review of the existing literature on privacy and security in IoT-based healthcare systems identified the key challenges and potential solutions [27]. Another 2019 study reviewed the existing literature on IoT technologies and applications in healthcare and presented a case study of an IoT-based healthcare system [35]. Additionally, a 2018 study identified the security and privacy challenges in IoT-based healthcare systems and proposed potential solutions for addressing these challenges [66]. Some of the key security and privacy challenges identified in these studies include the vulnerability of IoT devices to attacks, data breaches, and unauthorized access to sensitive patient information.

Owing to the highlighted severity of the security and privacy concerns, a comprehensive review of the existing research studies is essential to provide a clear understanding of their types and prevalence. This review aims to identify the security and privacy issues and attacks facing healthcare IoT systems and how they manifest at the perception layer, the network layer, and the application layer. By doing so, this review will provide a foundation for future research and practical solutions to address the security and privacy challenges of IoT-based healthcare systems.

3. Research Methods

This research attempts to answer the following research question:

RQ: What are the security and privacy issues of each architectural layer of IoT technologies (i.e., the perception layer, the network layer, and the application layer) concerning their application in healthcare?

Our aim was to explore different types of security and privacy problems in each architectural layer of IoT in healthcare applications so that by addressing them, technology vendors and service providers can be informed to take them into consideration for their future technology/service development. To achieve our objective, we conducted a semi-systematic literature review as recommended by [67] to provide an overview of the research area over time.

3.1. Search Strategy and Selection Criteria

The search strategy for this review will involve a comprehensive search of various electronic databases, including Google Scholar, PubMed, IEEE, Scopus, and Science Direct. All potential variations in the keywords searching phrases in all databases were included in search engines: "Internet of Things" OR "IoT" AND "Healthcare" OR "Health Care" AND "Security" AND "Privacy". The search strategy will be designed to identify all relevant studies published between 2017 and 2023, to gather more up-to-date background information on this field.

The selection criteria will be based on predefined inclusion and exclusion criteria. Inclusion criteria will include studies that discuss security and privacy issues and attacks in healthcare IoT systems. Exclusion criteria will include studies not meeting the inclusion criteria and studies published before 2017.

In the first phase, 279 studies were obtained from various databases and placed into the dataset generated using Endnote software. A total of 13 duplicate papers were found and removed during the initial screening of the paper titles. Then, after skimming the abstracts, 112 research papers were removed based on the exclusion criteria (Table 3).

Table 3. Inclusion and Exclusion Criteria.

Inclusion Criteria	Exclusion Criteria
Studies in the English language	Articles not in the English language
Studies that discussed IoT security issues in healthcare	Studies with a pure technical focus
Conference proceedings and journal articles	Book chapters, company reports, letters, thesis, and abstracts
Studies after 2017	Studies with medical and healthcare focus only
	Studies on smart homes with no discussion of healthcare

After scanning the full text of 154 articles and applying the specified exclusion criteria, 85 articles were excluded. After this, 69 articles met the requirements for inclusion and were considered for a detailed search and analysis. Figure 2 illustrates the overall procedure and details of the research paper selection procedure.

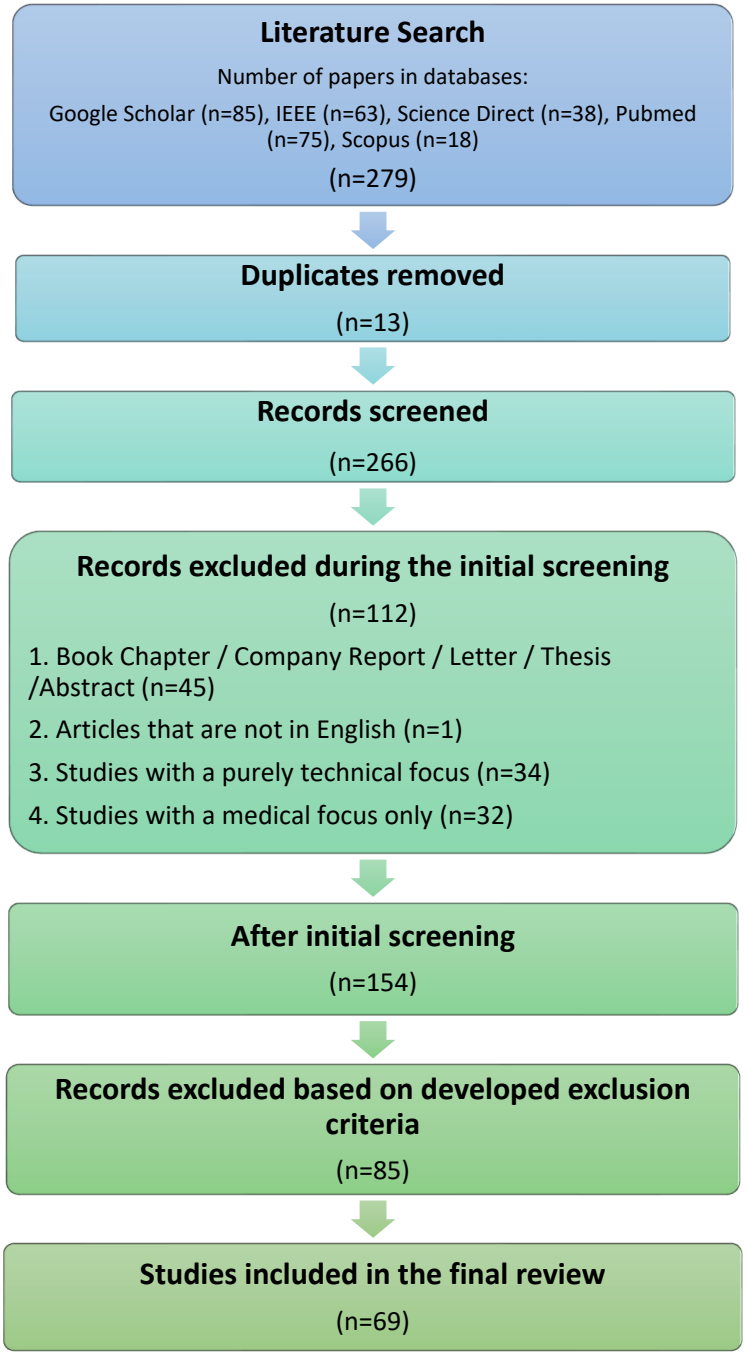

Figure 2. Literature review procedure.

3.2. Data Extraction and Analysis

The data extraction will involve systematically extracting relevant data from the selected studies using a predefined data extraction form. The extracted data will include study characteristics, such as the author, year of publication, study design, sample size, and study objectives. Additionally, the data extracted will include details about the security and privacy issues and attacks, such as the type of issue or attack, its prevalence, severity, and how it manifests at the perception, network, or application layers.

The analysis of the extracted data will involve a thematic analysis approach, where the data will be categorized into themes and sub-themes based on the research question and objectives. The analysis will be conducted using the appropriate software tool, NVivo, to manage and organize the data.

This phase collected data from selected articles and assigned them to predetermined groups. Several additional categories appeared at this step. Deductive and inductive coding is used in combination with this research method. Inductive coding is a non-predefined exploratory study, while deductive coding uses classifications as a guideline for the coding stage [68].

The pilot test outlined three essential security and privacy areas: the perception layer, the network layer, and the application layer of IoT devices in healthcare, used as a predeveloped dataset for deductive coding. In addition, new application areas were identified and introduced as new codes during the coding process. The combined coding method assisted in the coding phase using deductive and inductive coding to analyze the developing codes.

NVivo software (version 14) was used to organize the coding and data processing for data analysis. The review aimed to gather qualitative data for the investigation to comprehensively review existing and potential IoT security and privacy problems in healthcare. Due to the large amount of data, review analysis can be challenging. However, the process is manageable since a methodical approach is taken: Simply capture the main conclusions of all included articles by study type, and then evaluate the collection refers to results based on the frequency of data, to create a summary of results from multiple qualitative studies.

4. Results

The research results are depicted in both visual and narrative forms. The results of the data analysis from the records are included and showcased any correlations and patterns found in the collected data, which can help improve comprehension of the study outcomes and aid in addressing the research question.

IoT security and privacy threats can be categorized as physical, information and management [5], or system and information [60]. These threats can be passive or active. In the passive risks, attackers can capture information without impacting network behavior, while in the active ones, intruders can prevent or slow down administering the service [69]. As suggested by [5], IoT vulnerabilities can fall into the three layers of perception, network, and application (Figure 3).

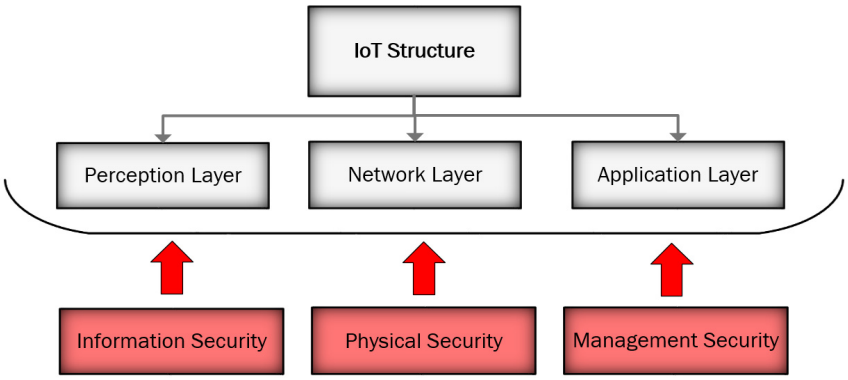

Figure 3. IoT structure and possible security threats.

4.1. Overview of IoT Security and Privacy in Healthcare

The integration of IoT in healthcare has the potential to benefit medical professionals and the healthcare industry greatly, but security remains a major barrier to its widespread adoption and implementation [58]. The primary concern is securing the data transmitted from patients' devices through wireless networks, which may result in unencrypted patient data being revealed [70]. The lack of security and privacy, especially with many IoT devices and applications being wireless, raises concerns among users regarding the full utilization of IoT capabilities in the healthcare system [43,71].

Networks and media are vulnerable to security and privacy threats, particularly in the healthcare industry, where personal and confidential information is involved [72]. The diversity of IoT devices and the heterogeneity of networks only exacerbate these security and privacy concerns [73]. To address these challenges, it is crucial to consider heterogeneous network authentication, privacy protection, access control, information management, confidentiality, and trustworthiness in the implementation of IoT in healthcare [72].

Users hesitate to adopt IoT-based healthcare services due to security and privacy concerns. Nevertheless, addressing these challenges is crucial for enhancing technology acceptance and reducing psychological and social barriers to IoT usage in healthcare [74].

Incorporating IoT in healthcare is not just about technological evolution but also involves the complex interplay of data privacy, security, and ethical considerations. The pervasive nature [75] IoT devices allow them to continuously gather and transmit sensitive health data, thus raising major concerns regarding data confidentiality and integrity. The nature of complexity mandates a multidisciplinary approach to security involving technical, ethical, and even legal expertise.

The threat landscape for IoT in healthcare has shown to be dynamic and multifaceted. IoT devices, by their very nature of always being interconnected and interdependent, create a vast attack surface [76] for cybercriminals. The risks are not just about data breaches but also the risk of manipulating the devices' functionalities, which creates grave security consequences for the health and safety of patients. The security of IoT in healthcare goes beyond the traditional cybersecurity challenges, thus requiring innovative solutions that address both data security and the physical safety of patients.

Enhancing security and privacy in IoT-based healthcare services can increase trust and adoption, thereby improving the overall healthcare system. Researchers have been exploring various security and privacy challenges in IoT applications in healthcare, and resolving these issues can guide technology suppliers and service providers to meet the requirements for potential advanced technology growth.

In this study, the design of IoT was used to investigate various issues. As a result, the vulnerabilities in IoT in healthcare were categorized into three layers, namely the perception, network, and application layers. The following subsections go over each of these categories.

4.1.1. The Perception Layer

The IoT perception layer is a vital element of healthcare IoT systems, enabling connected devices and sensors to capture and transmit data for analysis and decision-making purposes. Since IoT is an integration of multiple different networks, there are compatibility issues [61] that prone the overall IoT to various security risks. The security issues of this layer include those dealing with physical devices as well as data collection. The proliferation of these devices and sensors has led to significant security and privacy risks, as a variety of IoT devices [61,77], make implementing a single and unified security design burdensome. For example, there are two RFID-specific security vulnerabilities in this layer: uniform coding and conflict collision [61]. The variation in IoT devices may also cause a problem in data aggregation, which, in turn, jeopardizes data integration [61]. This issue is counted as one of the most critical security issues in healthcare [78].

As healthcare IoT systems continue to evolve and expand, it is vital to remain vigilant in addressing the security and privacy risks associated with the IoT perception layer. Collaboration among healthcare professionals, cybersecurity experts, and technology vendors is essential to mitigate these risks and ensure the safety and integrity of patient data and healthcare systems. It is crucial for healthcare organizations to implement security measures and stay informed of the latest security threats to ensure the safety of their patients and their systems.

Various types of security and privacy issues have been reported at the perception layer of healthcare IoT systems, including unauthorized access, data breaches, identity theft,

data manipulation, and denial-of-service (DoS) attacks [79]. These attacks can have serious consequences, including compromised patient data, system downtime, and financial loss.

One of the significant challenges of the IoT perception layer is the vulnerabilities that come with it. Several studies have investigated security and privacy issues and attacks at the IoT perception layer in healthcare IoT systems. A sniffing attack is a common example when an attacker intercepts data as they are transmitted between connected devices, allowing them to read and potentially modify the data. A replay attack involves the attacker intercepting and then resending a message, potentially leading to unintended consequences. A man-in-the-middle attack occurs when an attacker intercepts data between two parties and alters the data, leading to the parties unknowingly communicating with the attacker rather than each other. Finally, a buffer overflow attack occurs when an attacker sends more data than a system's memory can handle, potentially leading to a system crash or other unintended consequences [64].

One study found that some IoT medical devices have inadequate security controls in place, leaving them vulnerable to attack [80]. Therefore, in healthcare applications, probably the most crucial tasks to provide security are making IoT devices resistant to physical/device tampering and preventing physical/device manipulation, as they are the most common attack in this layer [81]. Since many IoT devices may be placed without extra security, attendance, or involvement in patients' environments, they are still subject to severe attacks. This also makes them susceptible to physical tampering, which could allow intruders to query the IoT devices and search the collection devices to exploit and steal data from patients [81]. Therefore, for the IoT healthcare system to maintain security, node authentication is the essential first step in identifying any malicious nodes because of physical attacks. Physical or device tampering can be serious in healthcare since IoT devices in healthcare are designed and programmed to capture, store, and protect patients' healthcare information.

Node authentication is the first critical step in identifying malicious nodes due to physical attacks for the IoT of healthcare systems to keep their safety. Physical or device exploitation in healthcare can be significant because many devices in healthcare have been designed and developed to record, store, and protect the health records of individuals [17]. In addition, data encryption requires protected distribution. Flexible encryption algorithms are suitable in cryptography because of hardware limitations. The resources of the IoT devices (battery power, memory, and CPU) are not drained rapidly. Moreover, some IoT medical devices have limited resources, such as memory and processing power, making it challenging to implement effective security controls. IoT sensors mostly have little external security features or protection, so they cannot handle complicated security and public key encryption techniques/algorithms or frequency hopping communication [5,82]. Also, most IoT devices just support short passwords [61] that compromise trust management in devices. These types of deficiencies result from memory, computational, and energy constraints; therefore, they make these devices prone to physical tampering and jamming attacks [61,69,77].

Additionally, the lack of industry standards for IoT devices can lead to inconsistencies in security protocols and make it difficult to ensure interoperability. The list of security and privacy issues of medical IoT in the perception layer is provided in Table 4.

Another study found that healthcare organizations are particularly vulnerable to phishing attacks, which can be used to steal sensitive patient information [83]. Such findings highlight the need for robust and proactive measures to address the security and privacy risks associated with the IoT perception layer, although the main reason of compromising security and privacy of IoT in this layer is hardware limitations [77].

Furthermore, some inherent challenges make securing the IoT perception layer in healthcare more difficult. For instance, the large number of connected devices and sensors in a typical healthcare IoT system makes it difficult to manage and secure them all.

To address these challenges, ongoing research is needed to identify vulnerabilities and develop effective security solutions for the IoT perception layer in healthcare. For instance,

researchers have proposed using machine learning algorithms to identify potential attacks and anomalies in data patterns, allowing for rapid detection and response to security threats [84]. Other researchers have suggested using blockchain technology to create a tamper-proof audit trail for medical data, ensuring its integrity and confidentiality [85].

It is also essential for healthcare organizations to stay informed of the latest security threats and implement best practices for securing their IoT systems. This includes using strong passwords, regularly updating software and firmware, and encrypting sensitive data in transit and at rest. Regular security audits and risk assessments can also help identify vulnerabilities and weaknesses in the system, allowing for proactive security measures to be implemented.

In conclusion, the IoT perception layer plays a crucial role in healthcare IoT systems, but it also poses significant security and privacy risks. Healthcare organizations must proactively secure their IoT systems and stay informed of the latest security threats and best practices. Ongoing research and collaboration among healthcare professionals, cybersecurity experts, and technology vendors are also necessary to develop effective security solutions and ensure the safety and integrity of patient data and healthcare systems. With proper security measures in place, the IoT perception layer can continue to enable the development of innovative healthcare technologies that improve patient outcomes and enhance the quality of care.

Table 4. Security and Privacy Challenges of the IoT Perception Layer.

Issue or Attack	Explanation and Highlight	Countermeasure
Man in the Middle	An attacker intercepts and manipulates the communication between an IoT device and the network, potentially stealing or altering sensitive information [86,87]. In 2019, a report found that almost 25% of attacks targeted the healthcare industry [88].	Implementing encryption for all communications between IoT devices and the network [86], using secure protocols [89], and implementing certificate-based authentication [90].
Denial of Service (DoS)	An attacker makes an IoT device unavailable by overwhelming it with traffic or by exploiting a vulnerability in the device, potentially compromising the security and privacy of patient information [91]. According to [92], 162 attacks targeted healthcare businesses, affecting 900 clinics, hospitals, and organizations.	Rate-limiting and filtering mechanisms [93] can be implemented to prevent traffic flooding. Network segmentation [54] can isolate IoT devices, and firewalls and intrusion detection systems [94], can prevent unauthorized access.
Distributed Denial of Service	An attacker floods an IoT device with a large amount of traffic, causing it to become unavailable and potentially leading to a failure of the device or the entire system [95,96]. In 2016, many IoT nodes were used in the DDoS attack known as "Mirai" [97].	Implementing a firewall [93], using intrusion detection and prevention systems [94], and using traffic filtering techniques [96,98] can help prevent DDoS attacks.
Malware and Virus	Malicious software infects an IoT device, potentially compromising the security and privacy of patient information [99].	Regularly updating and patching software [54], using antivirus and anti-malware software [100], and restricting the use of untrusted devices on the network [101].

Table 4. *Cont.*

Issue or Attack	Explanation and Highlight	Countermeasure
Phishing	This occurs when an attacker tricks individuals into revealing sensitive information or downloading malware onto an IoT device, potentially compromising the security and privacy of patient information [91].	Providing training to employees on how to recognize phishing attempts [102], implementing email filtering systems [13], and using multifactor authentication [101].
SQL Injection	This occurs when an attacker injects malicious code into a database, potentially compromising the security and privacy of patient information [103].	Implementing input validation [104] and regularly updating and patching database software [54].
Cross-Site Scripting	This occurs when an attacker injects malicious code into a database, potentially compromising the security and privacy of patient information [103].	Implementing input validation [104] and regularly updating and patching database software [54].
Insider Threats	An employee or contractor with access to sensitive information engages in malicious behavior, potentially compromising the security and privacy of patient information [105].	Employees and contractors should be trained on the importance of security and privacy in the healthcare sector [106]. Strict access control mechanisms, such as role-based access control [107].
Ransomware	An attacker encrypts sensitive patient information and demands a ransom in exchange for the decryption key, potentially compromising the security and privacy of patient information [74].	Regular backups of sensitive data can prevent data loss in the event of a ransomware attack [102]. Employees should also be trained on how to recognize and avoid phishing attacks, which are commonly used to deliver ransomware [102].
Jamming	This occurs when an attacker interferes with the communication between an IoT device and the network, potentially causing the device to fail and leading to security and privacy incidents [108]. In 2020, a hospital in Europe reported that its communication systems had been disrupted by a jamming attack, compromising patient information and care [53].	Encryption should be employed for communication between IoT devices and the network [109]. Secure communication protocols should be used.
Reply Attack	An attacker intercepts and reuses valid data transmission, potentially compromising the security and privacy of patient information [110].	Secure communication protocols that include message authentication codes [110], should be utilized. Encryption should also be employed for communication between IoT devices and the network.

Table 4. *Cont.*

Issue or Attack	Explanation and Highlight	Countermeasure
Side-Channel	This occurs when an attacker uses information obtained from the physical operation of an IoT device to exploit security vulnerabilities, potentially compromising the security and privacy of patient information [92]. In 2020, researchers disclosed a side-channel attack on a popular medical device, showing how an attacker could use information obtained from the physical operation of the device to compromise patient information [111].	Secure coding practices, such as constant-time coding [54], should be employed.
Eavesdropping	An attacker intercepts and listens to the communication between an IoT device and the network, potentially stealing sensitive information [87].	Encryption should be used for communication between IoT devices and the network [54]. Secure authentication methods like certificates or tokens can also be used to protect against eavesdropping [90].
Tampering Attacks	This occurs when an attacker modifies the data or configuration of an IoT device, potentially compromising the security and privacy of patient information [87].	Digital signatures can be used to verify the integrity of data [112]. Secure software update mechanisms [113] can also prevent tampering.
Insufficient Cryptographic Algorithms	The insufficient protection of sensitive data transmitted between IoT devices and networks due to the use of weak encryption protocols or lack of encryption altogether [114]. According to a report in 2019, almost 60% of all IoT devices in healthcare organizations were using outdated encryption technologies, posing a risk to patient privacy [92].	Secure encryption protocols should be used for communication between IoT devices and the network.

4.1.2. The Network Layer

The network layer, responsible for data transmission between devices, presents unique security challenges in healthcare IoT systems. The very flexibility and scalability of IoT networks [115] along with the mobility of devices complicate securing this layer [77].

The vast array of IoT devices often utilizes diverse network protocols for data transmission [92] This heterogeneity makes it challenging to implement a single, unified security protocol that caters to all network types (wired and wireless). Even existing security models have inherent flaws [77].

Establishing robust security standards across various networks, including cellular (4/5G), ad hoc, and Wi-Fi networks, is crucial [36]. It is important to note that security vulnerabilities in this layer can resemble conventional network security challenges. The network layer is susceptible to attacks like Trojan horses, viruses, spam, packet spoofing, route falsification, and flooding attacks, potentially leading to information disclosure [116].

The widespread use of wireless networks in healthcare IoT makes data inherently more vulnerable to eavesdropping due to the open nature of wireless communication [117].

Another significant security concern lies in the use of insecure communication protocols. Many healthcare IoT devices rely on unencrypted protocols like HTTP, which attackers can exploit to compromise patient data confidentiality and integrity [118]. Unencrypted data transmissions expose information to interception, modification, or deletion during transfer.

The network layer is also susceptible to various threats such as packet spoofing, route falsification, and flooding attacks [60]. A prevalent issue is the lack of encryption within the network layer [119]. Encryption is a crucial security measure that helps protect patient data as they are transmitted over the network [120]. Without encryption, sensitive patient data can be intercepted and read by cybercriminals, compromising patient privacy and confidentiality [114]. Encryption provides an additional layer of security that makes it more difficult for attackers to access and read the transmitted data.

Healthcare IoT devices are also susceptible to distributed denial of service (DDoS) attacks, which can overwhelm network resources and cause downtime for critical medical systems [121]. DDoS attacks can result in service disruptions, and in healthcare, such disruptions can be life-threatening. According to [36], DoS attacks can be a crucial problem for multidomain infrastructure and, therefore, for IoT medical applications. Healthcare IoT systems must have appropriate security controls in place to detect and mitigate DDoS attacks promptly.

Legacy devices and outdated software pose a significant security risk to healthcare IoT systems, as they often lack security patches and updates [54]. These devices and software can have known vulnerabilities that attackers can exploit to gain unauthorized access to sensitive patient data. Healthcare organizations must take appropriate measures to ensure that legacy devices and software are updated and protected against known vulnerabilities.

The use of mobile devices by healthcare providers to access IoT systems outside of the secure hospital network creates a significant security risk. Mobile devices can be infected with malware, targeted by phishing attacks, and can be vulnerable to network eavesdropping [122]. Healthcare organizations should ensure that mobile devices used to access IoT systems are appropriately secured and use secure communication protocols to communicate with IoT devices.

Several studies have identified vulnerabilities in the network layer of healthcare IoT systems that cybercriminals can exploit to launch various attacks. For example, a study by Obaidat et al. [101] identified vulnerabilities in the network layer that could be exploited to launch attacks, such as replay attacks, man-in-the-middle attacks, and message injection attacks. Similarly, another study by Islam et al. [123] reported on vulnerabilities in the ZigBee communication protocol, which is widely used in healthcare IoT systems. The researchers found that the lack of encryption and authentication mechanisms in ZigBee networks made them vulnerable to a range of attacks, including traffic sniffing, DoS, and spoofing attacks.

Some of the security and privacy issues of medical IoT in the network layer are presented and defined in Table 5.

To mitigate these risks, healthcare organizations must implement appropriate security controls such as encryption, authentication, and access control mechanisms [124]. Healthcare organizations should also use up-to-date software and security patches, conduct regular security assessments and testing, and ensure that legacy devices and software are updated and protected against known vulnerabilities. By remaining vigilant and proactive, healthcare organizations can prevent cyberattacks and safeguard the privacy and confidentiality of patient data.

Table 5. Security and Privacy Challenges of the IoT Network Layer.

Issue or Attack	Explanation and Highlight	Countermeasure
DOS Attacks	This type of attack involves overwhelming a network with a large amount of traffic, which can result in the disruption of critical services, such as electronic medical records systems or medical device networks [121].	Implementing network security solutions such as firewalls, intrusion prevention systems (IPS), and network behavior analysis systems to detect and block DDoS attacks [86,125].
IP Spoofing	This type of attack involves forging the source IP address of a network packet, which can be used to launch attacks or disrupt services, such as remote monitoring systems or telemedicine platforms [126].	Using strong authentication and encryption techniques, such as IPsec, to secure data transmission and prevent IP spoofing [127,128].
ARP Spoofing	This type of attack involves forging ARP (Address Resolution Protocol) messages on a network, which can be used to redirect network traffic and launch man-in-the-middle attacks, such as intercepting sensitive information transmitted between medical devices and servers [129].	Implementing ARP spoofing detection tools, such as ARPwatch or ARP poisoning detection tools, to detect and prevent ARP spoofing attacks [104].
DHCP Spoofing	This type of attack involves forging DHCP (Dynamic Host Configuration Protocol) messages on a network, which can be used to assign unauthorized IP addresses to IoT devices and launch man-in-the-middle attacks, such as intercepting sensitive information transmitted between medical devices and servers [130,131].	Implementing DHCP spoofing protection measures, such as static IP assignment, to prevent unauthorized IP assignments [130,131].
Sniffing Jamming	This type of attack involves intercepting and analyzing network traffic, which can be used to collect sensitive information, such as medical records or patient data, or launch attacks [104].	Using encryption techniques, such as SSL/TLS, to secure data transmission and prevent sniffing attacks [104,132].
Packet Injection	This type of attack involves injecting malicious packets into a network, which can be used to launch attacks or disrupt services, such as electronic medical records systems or medical device networks [104].	Implementing network security solutions, such as firewalls, intrusion detection systems (IDS), and network behavior analysis systems, to detect and prevent packet injection attacks [104].
Malware Attacks	This type of attack involves infecting devices with malicious software that can steal sensitive information or disrupt device operation [120]. In 2019, the malware known as Ryuk was found to be infecting hospital systems, leading to widespread disruption and ransom demands (A.).	Regular software updates and patches can prevent malware attacks. Implementing antivirus software and firewalls and using encrypted communication protocols can also help in preventing malware attacks [86,133].

Table 5. *Cont.*

Issue or Attack	Explanation and Highlight	Countermeasure
Man in the Middle	This type of attack involves intercepting and modifying network traffic, which can be used to steal sensitive information, alter device operation, or launch attacks [116]. In 2020, the malicious actor group known as APT10 was found to be using man-in-the-middle attacks to target healthcare organizations and steal sensitive information [134].	Encrypting all network traffic and using secure protocols such as SSL/TLS can prevent man-in-the-middle attacks. Implementing strong authentication mechanisms can also help in preventing these attacks [104].
Session Hijacking	This type of attack involves intercepting and taking over a user's network session, which can be used to steal sensitive information or launch attacks.	Implementing secure session management, using encrypted communication protocols, and implementing strong authentication mechanisms can help prevent session hijacking [54,135].
Forgery Attack	The use of forged or manipulated data to compromise the integrity of healthcare services and patient safety. An exploit leads an Internet browser to perform an inappropriate consumer application activity. A successful cyberattack can be catastrophic for both the patient and the healthcare organization [92].	Using digital signatures, access controls, encryption, network segmentation, blockchain technology, validating input data, and using intrusion detection and prevention systems to detect and prevent unauthorized access and modification of data in real time [65,133].
Hello Flood	A type of distributed denial-of-service (DDoS) attack that floods the target network with a large number of "hello" messages, overwhelming the network and causing it to crash or become unavailable [43,136]. "Hello" signals are defined in various routing protocols, allowing nodes to communicate with their neighbors [43].	Technical measures such as network segmentation, rate limiting, intrusion prevention systems, continuous network monitoring, and using content delivery networks, as well as organizational measures such as keeping IoT devices up to date and planning for disaster recovery [136].
Black Hole	A type of DDoS attack that exploits vulnerabilities in IoT devices to drop or discard legitimate network traffic, causing network congestion and disruption of healthcare services [137]. The attacker creates a fake node that accepts network traffic by claiming to have the quickest route. Network traffic could be forwarded to the fake node, which is used as a proxy server or ignored [138].	Using intrusion detection and prevention systems, implementing access controls, using network traffic analysis, rate limiting, keeping IoT devices up to date, deploying firewalls, and implementing network segmentation to isolate critical healthcare systems and data from less critical systems [137,139].

Table 5. *Cont.*

Issue or Attack	Explanation and Highlight	Countermeasure
Gray Hole	A type of attack where an IoT device selectively drops or modifies some network traffic, leading to degradation in service quality and potential data loss. This attack is similar to a black hole attack; instead of destroying all signals, it just removes a selection of those [140].	Using encryption, implementing access controls, network traffic analysis, intrusion detection and prevention systems, keeping IoT devices up to date, deploying firewalls, and implementing data redundancy [137,141].
Worm Hole	A type of attack where an attacker captures packets from one part of the network and tunnels them to another part of the network, bypassing network security measures [137]. By managing at least two network nodes or adding additional false nodes to the network, the attacker establishes a link between different parts of the network. The hacker gathers data from one point and replays it to the other after confirming the link [142].	Implementing secure communication protocols, using location-based authentication, network traffic analysis, intrusion detection, and prevention systems, implementing access controls, using digital signatures, and deploying firewalls [137].
Congestion Attack	A type of attack where an attacker floods the network with traffic, causing it to become congested and resulting in the degradation of service quality or even network failure [124]. This attack succeeds by flooding networks with unprocessed responses until their period runs out. Then, the lane is restricted to transactions whenever the highest number of unsolved requests (HTLCs) is achieved [143].	Using traffic shaping, implementing Quality of Service (QoS) policies, using rate limiting, implementing access controls, deploying intrusion detection and prevention systems, using network traffic analysis, and keeping IoT devices up to date with the latest security patches and firmware updates [65].

4.1.3. The Application Layer

This layer is responsible for data processing, storage, and presentation. It provides the interface through which users interact with IoT devices. As a result, healthcare IoT systems are vulnerable to a wide range of security and privacy issues and attacks at the application layer. The high number of IoT applications and their diversity and complexity could be considered the main cause of the security issues of the IoT caused by system integration [68,91].

One of the most common issues is the lack of data integrity and authenticity, which can lead to the spread of false information and negatively affect patient care [91]. Ensuring data integrity and authenticity can be achieved through implementing secure communication protocols, such as Transport Layer Security and Secure Sockets Layer to protect the data while in transit.

Another common issue is the use of default or weak credentials, which can easily be guessed or brute-forced by attackers, compromising patient privacy and safety [144]. To prevent such attacks, the healthcare industry should establish strong password policies, use multifactor authentication, and ensure that IoT devices are configured with strong passwords [145].

Moreover, several reports of attacks on the application layer in healthcare IoT systems include ransomware attacks that can disrupt critical medical services [54,146] and DDoS attacks [147] that can make the system unavailable. Such attacks can be prevented by implementing network security controls, such as firewalls and intrusion detection systems, to detect and mitigate attacks before they cause damage [148].

Malware attacks on healthcare IoT systems are also a concern. Malware can infect healthcare IoT devices, allowing attackers to steal sensitive patient data, disrupt device operations, and compromise patient safety [124]. To prevent malware attacks, healthcare organizations should ensure that all IoT devices have up-to-date security patches and conduct vulnerability assessments and penetration testing regularly [149].

Another challenge is that healthcare IoT systems often rely on third-party software and services [150], which can introduce additional security risks. Many of these software and services may have vulnerabilities or may not be configured securely, which can allow attackers to exploit them and gain unauthorized access to the system. Healthcare organizations should perform a thorough security assessment of all third-party software and services before integrating them into their IoT systems. Table 6 presents a variety of security issues in the application layer.

Table 6. Security and Privacy Challenges of the IoT Application Layer.

Issue or Attack	Explanation and Highlight	Countermeasure
DDOS Attacks	It can be targeted at medical systems, disrupting access to critical medical information and services [147].	Healthcare organizations can implement anti-DDoS measures such as traffic filtering, rate limiting, and network traffic monitoring. They can also consider using cloud-based anti-DDoS services, which can provide additional protection against DDoS attacks [147,148].
Insider Threats	Employees or contractors in clinical settings can intentionally or accidentally cause a data breach or steal information [86,151].	To mitigate the risk of insider threats, healthcare organizations can implement access controls and monitor user activity [151].
Remote Access Vulnerabilities	Remote access to medical systems can introduce security vulnerabilities if the access is not properly secured [54]. In 2019, a healthcare organization's remote access system was hacked, exposing the PHI of over 2 million patients [152].	To secure remote access to medical systems, healthcare organizations can implement secure authentication methods, such as multifactor authentication, and regularly update remote access software and systems [54].
Outdated Software and Systems	Outdated software and systems can be vulnerable to cyber-attacks, making it important for healthcare organizations to update their technology [54] regularly. In 2020, a healthcare organization's outdated software was found to have a vulnerability that allowed hackers to access sensitive medical information [153].	To mitigate the risk of outdated software and systems, healthcare organizations should regularly review and update their technology, including software, hardware, and systems [54].

Table 6. *Cont.*

Issue or Attack	Explanation and Highlight	Countermeasure
Malicious Apps	Malicious apps can be designed to steal information or launch attacks and can be easily installed on IoT devices [104,124].	To prevent the installation of malicious apps, healthcare organizations can implement strict app-vetting processes and regularly update mobile device management software [104].
Insecure Cloud Storage	If medical information is stored in the cloud, it can be vulnerable to attacks if the cloud storage is not properly secured [104]. In 2020, a healthcare organization's cloud storage system was hacked, exposing the PHI of over 1 million patients [37].	To secure cloud storage, healthcare organizations can encrypt sensitive information, regularly monitor access to cloud storage, and implement strict access controls [104]. They can also consider working with a trusted cloud service provider that specializes in secure cloud storage for the healthcare industry.
Physical Tampering	Physical tampering with IoT devices, such as removing or replacing components, can allow attackers to access sensitive information or launch attacks [54]. In 2021, a report by the U.S. Government Accountability Office found that medical devices such as pacemakers, insulin pumps, and CT scans were vulnerable to hacking due to physical tampering [154].	Healthcare organizations can implement strict access controls and regularly monitor IoT devices for signs of tampering [54,104].
Data Privacy and Identity	IoT interconnects devices from various manufacturers demanding the use of several authentications. Integrating multiple techniques to protect data privacy and identity is challenging [54,116,144].	Using encryption and access controls, implementing secure communication protocols, minimizing data, conducting regular security audits, using strong authentication and passwords, implementing data anonymization, and establishing a privacy policy [54,86].

To mitigate these risks, healthcare organizations must implement appropriate security controls in the application layer, including data encryption, authentication, and access control mechanisms. Healthcare organizations should also use up-to-date software and security patches, conduct regular security assessments and testing, and ensure that default or weak credentials are not used in their IoT systems. Additionally, organizations should provide their employees with cybersecurity training to increase awareness of the importance of security and best practices in IoT security.

In summary, healthcare IoT systems present several security and privacy challenges, particularly at the application layer. To mitigate these risks, healthcare organizations must implement appropriate security controls, including data encryption, access control, and regular security assessments and testing. Emerging technologies such as blockchain and secure software development practices can provide additional layers of security. Additionally, healthcare organizations should ensure that patients are fully informed about the risks and benefits of using IoT devices and provide them with options for controlling the use of their data. By taking these steps, healthcare organizations can ensure the pri-

vacy and confidentiality of patient data and prevent cyberattacks that could compromise patient safety.

4.2. Summary of Key Security and Privacy Threats

The main security and privacy issues, along with potential effects and mitigation options, are summarized in Table 7 below to deliver a clear perspective of the numerous threats found throughout each layer of the Health IoT architecture.

Table 7. Summary of Key Security and Privacy Threats in Health IoT.

IoT Layer	Key Security and Privacy Threats	Impact on Healthcare	Proposed Solutions
Perception Layer	- Device tampering - Data breaches - Replay attacks	- Compromised patient data integrity - Unauthorized access	- Physical security controls - Secure node authentication protocols
Network Layer	- Denial of service (DoS) - Eavesdropping - IP Spoofing	- Disruption of critical healthcare services - Data interception	- Encryption of network communications - Firewalls
Application Layer	- Malware attacks - Ransomware - Weak credentials	- Loss of sensitive patient information - Service downtime	- Regular software updates - Access control mechanisms
General Issues	- Lack of encryption - Inadequate authentication mechanisms	- Vulnerabilities in patient privacy - Data breaches	- Multifactor authentication - Data encryption

This summary table presents a comprehensive resource for the several security issues covered in the previous section. An organized overview of potential vulnerabilities that healthcare organizations need to solve is given by classifying these risks according to the IoT perception, network, and application layers. The potential impacts of these threats on patient safety, data integrity, and system availability are also highlighted in the table, showing how important it is to put in place appropriate countermeasures.

The main findings are presented in the table, highlighting the key areas in which healthcare providers should focus on strengthening their security operations. Organizations can significantly reduce the risk of security breaches and safeguard critical patient data by using the recommended mitigation techniques, improving the general dependability and security of Health IoT systems.

4.3. Taxonomy of Analyzed Vulnerabilities

A taxonomy that offers a clear explanation for selecting particular vulnerabilities for research has been developed, in addition to a review of the significant security and privacy issues. This taxonomy classifies the vulnerabilities according to a number of important factors that affect the performance and security of health-related IoT systems. Among these characteristics are:

- *Impact on Data Integrity:* Issues that could bring incorrect diagnosis or treatment decisions by jeopardizing the availability and integrity of patient data.
- *Threat to Patient Safety:* Challenges include tampered medical equipment or malfunctioning life support systems that threaten the health and safety of patients.
- *System Availability:* Vulnerabilities that impact IoT system availability and cause delays or disruptions in service for critical healthcare operations.
- *Attack Type:* This refers to the type of attack, which can be divided into three categories: application-based, network-based, and physical.

- *Exposure Level:* A measure of an IoT system's vulnerability to outside attacks, which can be impacted by communication protocols, network architecture, and device mobility.

An overview of this taxonomy and the vulnerabilities that belong to each characteristic can be viewed in Table 8 below.

Table 8. Taxonomy of Characteristics and Corresponding Vulnerabilities.

Characteristic	Description	Vulnerabilities
Impact on Data Integrity	Ensures that patient data are accurate and unmodified during its collection, storage, and transmission by focusing a strong focus on its integrity	Data tampering, packet spoofing, man-in-the-middle attacks, malware, replay attacks
Threat to Patient Safety	Detects weaknesses that can directly compromise the health and safety of patients by damaging medical equipment or postponing treatments	Device tampering, ransomware, DoS attacks, physical attacks on medical devices
System Availability	Concerns about risks that could block access to medical data or healthcare services, causing delays in treatment or system failures	Denial-of-service (DoS), distributed DoS (DDoS), congestion attacks, black hole and gray hole attacks
Attack Nature	Classifies vulnerabilities into three categories: application layer based, network layer based, and physical layer based	Physical attacks, malware, phishing, jamming, network attacks, SQL injection, cross-site scripting
Exposure Level	Evaluates the level of system exposure while considering the heterogeneity of networks and devices and how vulnerable they are to outside attacks	Eavesdropping, unauthorized access, sniffing attacks, weak encryption, unpatched vulnerabilities

Healthcare providers can use this taxonomy to prioritize security measures according to the specific threats they face, in addition to deploying it to better understand how risks are determined. A more detailed approach to risk management can be implemented by examining vulnerabilities utilizing these classifications, addressing both short-term threats and long-term security needs.

5. Discussion

In healthcare IoT systems, there are multiple layers of the system vulnerable to security and privacy risks. The architecture of a typical IoT platform in the healthcare domain and the associated threats are illustrated in Figure 4.

The perception layer is essential for data capture and transmission in healthcare IoT systems. However, as shown in Figure 4, the widespread use of devices and sensors in this layer has increased security risks, including unauthorized access, data breaches, and DoS attacks. This includes wearable and wellness devices, implantable medical devices (e.g., insulin pumps), medical equipment, and patient monitoring systems. Securing the perception layer is difficult due to the number of connected devices, limited resources, and lack of industry standards. Continuous research and collaboration among healthcare professionals, cybersecurity experts, and technology vendors are necessary to identify vulnerabilities and develop effective security solutions.

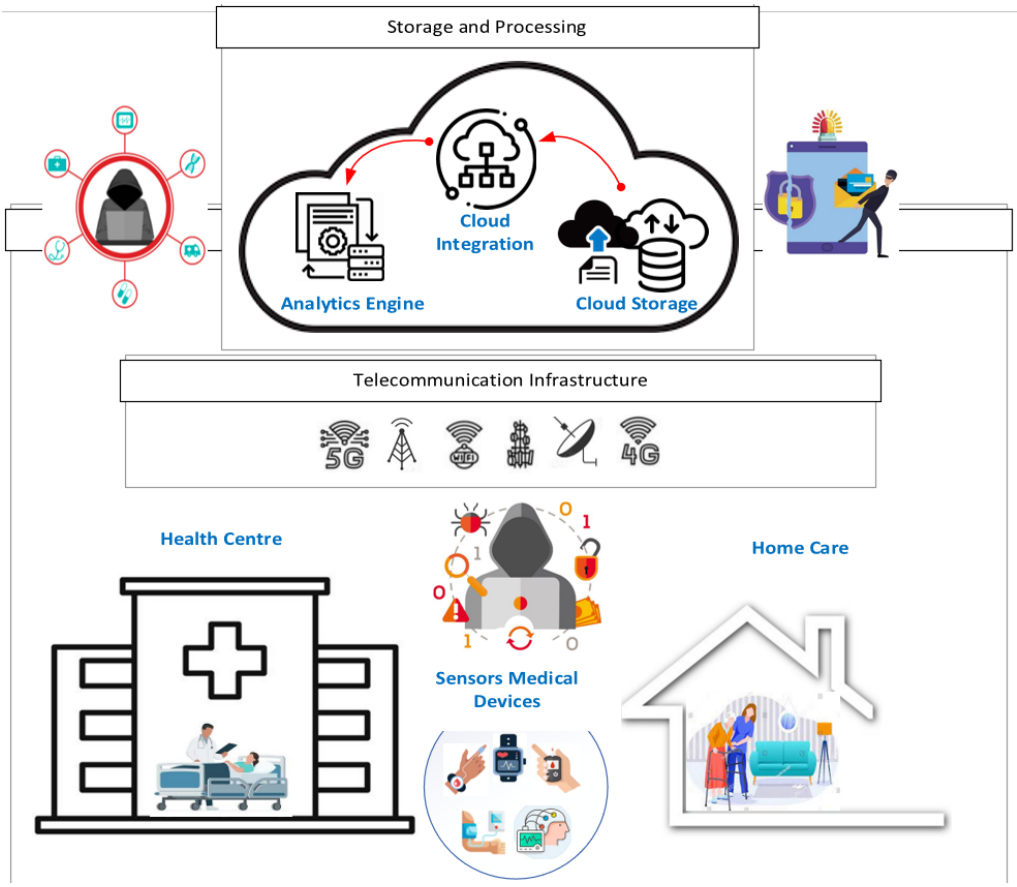

Figure 4. Typical IoT platform in healthcare and associated threats.

The network layer is also vulnerable to cyberattacks due to insecure communication protocols, inadequate authentication mechanisms, and the use of legacy devices and outdated software. Healthcare organizations need to implement appropriate security controls, such as using up-to-date software and security patches, conducting regular security assessments and testing, and ensuring that legacy devices and software are updated and protected against known vulnerabilities.

The application layer of healthcare IoT systems includes both data storage and processing and user interface and services. This layer is vulnerable to various security and privacy issues, including weak credentials, ransomware, and DDoS attacks. Healthcare organizations can mitigate these risks by implementing appropriate security controls, such as data encryption, access control, and regular security assessments and testing. Emerging technologies like blockchain and secure software development practices can provide additional layers of security. Healthcare organizations need to ensure that patients are informed about the risks and benefits of using IoT devices and provided with options for controlling the use of their data. Regular training and awareness programs can also help prevent security incidents and ensure that employees are aware of the risks associated with IoT devices.

Understanding how security threats correspond to each architectural component is crucial for implementing effective security measures. Based on Figure 4, Table 9 presents this mapping.

Table 9. Mapping of Security Threats to Architectural Components.

Architectural Component	Associated Threats	Potential Impact
Medical Devices and Sensors	Physical tampering Node capture Battery drainage attacks Sensor data manipulation	Compromised patient data False medical readings Device malfunction
Communication Infrastructure	Man-in-the-middle attacks DDoS attacks Protocol vulnerabilities Network eavesdropping	Data interception Service disruption Unauthorized access
Data Processing and Storage	Data breaches Malware infections Unauthorized access SQL injection	Privacy violations Data loss System compromise
User Interface and Services	Authentication bypass Session hijacking Cross-site scripting Phishing attacks	Unauthorized access Identity theft Service disruption

Standards and Solutions

The incorporation of IoT in healthcare mandates a strategic approach that goes beyond what our current conventional security measures offer. This involves developing a security-first approach within every healthcare organization, where the importance of data security and patient privacy is ingrained in every aspect of healthcare delivery. In other words, it should be a security [155] and privacy-by-design approach. Practitioners must gain a robust understanding of IoT security's delicate intricacies, including obtaining discernment of the distinctive susceptibilities of different IoT devices and the imperative of preserving such devices with consistent refreshes and protection fixes to mitigate any potential vulnerabilities.

Overall, it is crucial to secure all layers of healthcare IoT systems to safeguard patient data, prevent cyberattacks, and ensure patient safety. Healthcare organizations must take proactive steps to secure their IoT systems, stay informed of the latest security threats and best practices, and implement appropriate security controls at all layers of the system. By doing so, the IoT perception layer can continue to enable the development of innovative healthcare technologies that improve patient outcomes and enhance the quality of care. The National Institute of Standards and Technology guidelines for securing IoT devices in healthcare settings can provide a useful framework for healthcare organizations to improve their security posture. Collaboration between different stakeholders is essential to address the challenges of securing healthcare IoT systems and protecting patient data and safety.

The importance of security and privacy in healthcare IoT cannot be overstated. The systematic literature review highlights that healthcare IoT involves sensitive and personal data, such as patient's health records and biometric data, and breaches can have severe consequences for patients, healthcare providers, and organizations. For example, data breaches can result in identity theft, financial loss, reputational damage, and legal liabilities. Furthermore, compromised healthcare IoT devices can lead to medical errors, delayed diagnoses, and incorrect treatments. Therefore, ensuring the security and privacy of healthcare IoT should be a top priority for all stakeholders involved.

The review emphasizes the need for comprehensive security measures that address security and privacy issues and attacks at multiple layers of the IoT architecture. Single-layer security measures, such as firewalls or encryption, may not be sufficient to protect against sophisticated attacks that exploit vulnerabilities at different layers. Therefore, organizations must adopt a multilayered approach that includes physical security, network security, data security, and access control. This approach should also include periodic

risk assessments, vulnerability scans, and penetration testing to identify and address security gaps.

The review highlights that stakeholders have a shared responsibility to ensure the security and privacy of healthcare IoT. Healthcare organizations, device manufacturers, and software developers must work collaboratively to identify and address security and privacy issues and attacks. This requires implementing security-by-design principles, such as threat modeling, secure coding practices, and regular software updates. Security-by-design principles enable software developers to critically analyze and identify the security needs of the software systems [156]. Subsequently, these security needs can be embedded into the software architecture, so that the software developers can make sure that the developed software systems include all necessary security controls. Healthcare organizations should also provide training and education to staff and end-users to ensure that security and privacy protocols are followed. Healthcare organizations should follow a zero-trust approach, where they understand that the networks are vulnerable to security threats all the time and there are many internal and external security threats in a network regularly. Thus, healthcare organizations should follow the basic principles of the zero-trust approach such as taking necessary measures to ensure user authenticity and allowing users to access company resources only using trusted devices [157]. Additionally, regulatory bodies and policy makers must collaborate with industry stakeholders to establish and enforce standards and regulations that promote the security and privacy of healthcare IoT. These standards should encompass rigorous data privacy regulations to safeguard sensitive patient information [158], robust security certification programs to ensure the integrity of IoT devices and networks [159], and clear incident reporting requirements to address any security breaches or vulnerabilities promptly [160]. Furthermore, it is essential to strike a delicate balance between regulation enforcement and technological advancement to foster innovation in the healthcare IoT sector. Overregulation could stifle innovation and impede the development of new technologies that could significantly benefit patient care and healthcare delivery. Therefore, regulatory frameworks should be flexible enough to accommodate technological advancements while still prioritizing patient safety and privacy [161]. Collaboration among industry stakeholders, regulatory bodies, policy makers, and cybersecurity experts is crucial to developing effective and adaptable regulatory measures that mitigate risks without hindering progress [162].

Our review suggests that ensuring the security and privacy of healthcare IoT requires a coordinated effort among all stakeholders. This includes adopting a multilayered security approach, implementing security-by-design principles, following the basic principles of the zero-trust approach, providing training and education, and complying with relevant regulations and standards. By doing so, stakeholders can mitigate the risk of security and privacy issues and attacks and enhance the trust and reliability of healthcare IoT.

The review identifies several gaps in the current research on IoT security and privacy issues and attacks in healthcare. First, most studies have focused on individual layers of the IoT architecture, rather than examining the entire IoT system. Second, there is a lack of empirical research that evaluates the effectiveness of different security measures and strategies in mitigating security and privacy risks. Third, there is a need for more research on the human factor in IoT security, including end-user behavior, security awareness, and training. Fourth, there is a lack of research on the ethical implications of IoT security and privacy, particularly concerning data ownership, consent, and transparency [163].

To address the gaps in the current literature, future research on IoT security and privacy issues and attacks in healthcare should adopt a more holistic and multidisciplinary approach. This includes examining the entire IoT system, including the devices, network, and applications, and considering the socio-technical and ethical aspects of IoT security and privacy [163]. Future research should also employ more rigorous and empirical research methods, such as experiments and field studies, to evaluate the effectiveness of different security measures and strategies. Additionally, research should explore the role of end-users in IoT security and privacy and identify effective training and awareness programs. Finally,

research should investigate the ethical implications of IoT security and privacy and develop frameworks and guidelines for ensuring data ownership, consent, and transparency.

In addition to the above, there are several areas for further exploration of IoT security and privacy issues and attacks in healthcare. One area is the use of artificial intelligence and machine learning in enhancing IoT security and privacy, as suggested by [164]. Future research exploration should explore the development of inherently flexible security technologies that are amenable to the continuous evolution of IoT systems and how their applications in healthcare are developing. This includes investigating AI-driven security methods that can predict and mitigate potential threats in real-time.

Another area is the impact of emerging technologies, such as 5G and edge computing, on IoT security and privacy. Additionally, research should examine the security and privacy challenges and opportunities of interoperability and data sharing in healthcare IoT. Finally, research should explore the international and cross-cultural aspects of IoT security and privacy, including the role of cultural values and norms in shaping security and privacy attitudes and behaviors.

6. Conclusions and Future Work

In this review, the security and privacy issues and attacks in healthcare IoT were evaluated according to the perception layer, the network layer, and the application layer. This study revealed various threats, such as unauthorized access, data breaches, and DOS attacks, with potentially serious consequences for healthcare providers, organizations, and patients. The review highlighted various security measures, such as encryption, firewalls, and access control, to address these risks.

This study has practical implications, emphasizing that healthcare organizations, software developers, and device manufacturers must prioritize healthcare IoT security and privacy. A comprehensive, multilayered security approach, security-by-design principles, zero-trust principles, and training for staff and end-users must be adopted. Regulators and policy makers must also establish and enforce standards and regulations that promote the security and privacy of healthcare IoT.

This study identified gaps in current literature and areas for further exploration, such as the need for more holistic and empirical research that considers the socio-technical and ethical aspects of IoT security and privacy, the role of emerging technologies, and international and cross-cultural factors that affect security and privacy attitudes and behaviors. Overall, this study underscores the importance of ensuring the security and privacy of healthcare IoT, with stakeholders' coordinated efforts to address the complex and evolving security and privacy threats in this field. This can enhance healthcare IoT trust and reliability, reduce the risks of security and privacy issues and attacks, and ultimately improve healthcare delivery quality and safety.

Author Contributions: The idea of this research is conceptualized by S.M. S.M. developed the research method protocol and involved data collection with T.C. T.C. carried out the data analysis and prepared the first draft of this report under S.M.'s supervision and guidance. The report and findings were enhanced by M.S. contribution. D.A., S.Y. and F.H. provided some technical insights and contributed to revising, editing and formatting this manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by AUT, School of Engineering, Computer and Mathematical Sciences, 2022 Summer Research Scholarships.

Data Availability Statement: All the data to conduct this research were collected from the scientific databases as discussed in the Section 3 and available online.

Acknowledgments: The authors acknowledge the use of AI for English editing. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the contents of the publication.

Conflicts of Interest: Author David Airehrour is employed by the company Together Communications, Auckland 1010, New Zealand. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Sisodia, R.C.; Dankers, C.; Orav, J.; Joseph, B.; Meyers, P.; Wright, P.; Amand, D.S.; Del Carmen, M.; Ferris, T.; Heng, M. Factors Associated With Increased Collection of Patient-Reported Outcomes Within a Large Health Care System. *JAMA Netw. Open* **2020**, *3*, e202764. [CrossRef] [PubMed]
2. Luo, E.; Bhuiyan, M.Z.A.; Wang, G.; Rahman, M.A.; Wu, J.; Atiquzzaman, M. Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun. Mag.* **2018**, *56*, 163–168. [CrossRef]
3. Madanian, S.; Parry, D. Identifying the Potential of RFID in Disaster Healthcare: An International Delphi Study. *Electronics* **2021**, *10*, 2621. [CrossRef]
4. Kiran, D.R. Chapter 35—Internet of Things. In *Production Planning and Control*; Kiran, D.R., Ed.; Butterworth-Heinemann: Oxford, UK, 2019; pp. 495–513.
5. Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Emeishan, China, 14–15 December 2013; pp. 663–667.
6. Al-khafajiy, M.; Baker, T.; Chalmers, C.; Asim, M.; Kolivand, H.; Fahim, M.; Waraich, A. Remote health monitoring of elderly through wearable sensors. *Multimed. Tools Appl.* **2019**, *78*, 24681–24706. [CrossRef]
7. Albahri, A.S.; Alwan, J.K.; Taha, Z.K.; Ismail, S.F.; Hamid, R.A.; Zaidan, A.A.; Albahri, O.S.; Zaidan, B.B.; Alamoodi, A.H.; Alsalem, M.A. IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. *J. Netw. Comput. Appl.* **2021**, *173*, 102873. [CrossRef]
8. Riad, K.; Hamza, R.; Yan, H. Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records. *IEEE Access* **2019**, *7*, 86384–86393. [CrossRef]
9. Vistro, D.M.; Rehman, A.u.; Mehmood, S.; Idrees, M.S.; Munawar, A. An IoT-Based Approach for Smart Ambulance Service Using Thingspeak Cloud. *J. Crit. Rev.* **2020**, *7*, 1697–1703.
10. Yin, X.C.; Liu, Z.G.; Ndibanje, B.; Nkenyereye, L.; Riazul Islam, S. An IoT-based anonymous function for security and privacy in healthcare sensor networks. *Sensors* **2019**, *19*, 3146. [CrossRef]
11. Usak, M.; Kubiatko, M.; Shabbir, M.S.; Viktorovna Dudnik, O.; Jermsittiparsert, K.; Rajabion, L. Health care service delivery based on the Internet of things: A systematic and comprehensive study. *Int. J. Commun. Syst.* **2020**, *33*, e4179. [CrossRef]
12. Bhatt, V.; Chakraborty, S. Improving service engagement in healthcare through internet of things based healthcare systems. *J. Sci. Technol. Policy Manag.* **2023**, *14*, 53–73. [CrossRef]
13. Khattak, H.A.; Shah, M.A.; Khan, S.; Ali, I.; Imran, M. Perception layer security in Internet of Things. *Future Gener. Comput. Syst.* **2019**, *100*, 144–164. [CrossRef]
14. Rghioui, A.; Oumnad, A. Internet of things: Surveys for measuring human activities from everywhere. *Int. J. Electr. Comput. Eng.* **2017**, *7*, 2474.
15. Mouha, R.A. Internet of things (IoT). *J. Data Anal. Inf. Process.* **2021**, *9*, 77–101.
16. Shouran, Z.; Ashari, A.; Priyambodo, T. Internet of things (IoT) of smart home: Privacy and security. *Int. J. Comput. Appl.* **2019**, *182*, 3–8.
17. Chanal, P.M.; Kakkasageri, M.S. Security and Privacy in IoT: A Survey. *Wirel. Pers. Commun.* **2020**, *115*, 1667–1693. [CrossRef]
18. Kumar, S.; Tiwari, P.; Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: A review. *J. Big Data* **2019**, *6*, 111. [CrossRef]
19. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017; pp. 685–690.
20. Sanctis, M.D.; Cianca, E.; Araniti, G.; Bisio, I.; Prasad, R. Satellite Communications Supporting Internet of Remote Things. *IEEE Internet Things J.* **2016**, *3*, 113–123. [CrossRef]
21. Ma, Z.; Xiao, M.; Xiao, Y.; Pang, Z.; Poor, H.V.; Vucetic, B. High-Reliability and Low-Latency Wireless Communication for Internet of Things: Challenges, Fundamentals, and Enabling Technologies. *IEEE Internet Things J.* **2019**, *6*, 7946–7970. [CrossRef]
22. Yassein, M.B.; Shatnawi, M.Q.; Al-zoubi, D. Application layer protocols for the Internet of Things: A survey. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September 2016; pp. 1–4.
23. Hussain, A.; Ali, T.; Althobiani, F.; Draz, U.; Irfan, M.; Yasin, S.; Shafiq, S.; Safdar, Z.; Glowacz, A.; Nowakowski, G.; et al. Security Framework for IoT Based Real-Time Health Applications. *Electronics* **2021**, *10*, 719. [CrossRef]
24. Kavre, M.; Gadekar, A.; Gadhade, Y. Internet of Things (IoT): A Survey. In Proceedings of the 2019 IEEE Pune Section International Conference (PuneCon), Pune, India, 18–20 December 2019; pp. 1–6.
25. Ahmed, Z.; Mohamed, K.; Zeeshan, S.; Dong, X. Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. *Database* **2020**, *2020*, baaa010. [CrossRef]
26. Khatoon, N.; Roy, S.; Pranav, P. A Survey on Applications of Internet of Things in Healthcare. In *Internet of Things and Big Data Applications: Recent Advances and Challenges*; Balas, V.E., Solanki, V.K., Kumar, R., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 89–106.

27. Abiodun, O.I.; Abiodun, E.O.; Alawida, M.; Alkhawaldeh, R.S.; Arshad, H. A Review on the Security of the Internet of Things: Challenges and Solutions. *Wirel. Pers. Commun.* **2021**, *119*, 2603–2637. [CrossRef]
28. Moore, W.; Frye, S. Review of HIPAA, part 1: History, protected health information, and privacy and security rules. *J. Nucl. Med. Technol.* **2019**, *47*, 269–272. [CrossRef] [PubMed]
29. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [CrossRef]
30. De Michele, R.; Furini, M. Iot healthcare: Benefits, issues and challenges. In Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good, Valencia, Spain, 25–27 September 2019; pp. 160–164.
31. Appari, A.; Johnson, M.E. Information security and privacy in healthcare: Current state of research. *Int. J. Internet Enterp. Manag.* **2010**, *6*, 279–314. [CrossRef]
32. Agaku, I.T.; Ayo-Yusuf, O.A.; Connolly, G.N.; Adisa, A.O. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *J. Am. Med. Inform. Assoc.* **2014**, *21*, 374–378. [CrossRef]
33. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet Things J.* **2019**, *6*, 1606–1616. [CrossRef]
34. Maswadi, K.; Ghani, N.B.A.; Hamid, S.B. Systematic Literature Review of Smart Home Monitoring Technologies Based on IoT for the Elderly. *IEEE Access* **2020**, *8*, 92244–92261. [CrossRef]
35. Azeez, N.A.; der Vyver, C.V. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egypt. Inform. J.* **2019**, *20*, 97–108. [CrossRef]
36. Chacko, A.; Hayajneh, T. Security and privacy issues with IoT in healthcare. *EAI Endorsed Trans. Pervasive Health Technol.* **2018**, *4*, e2. [CrossRef]
37. HIPAA. Healthcare Data Breach Statistics. Available online: https://www.hipaajournal.com/healthcare-data-breach-statistics/ (accessed on 20 October 2023).
38. Centers for Disease Control and Prevention. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Available online: https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html (accessed on 20 October 2023).
39. Pramanik, P.K.D.; Pareek, G.; Nayyar, A. Chapter 14—Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards. In *Telemedicine Technologies*; Jude, H.D., Balas, V.E., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 201–225.
40. Awotunde, J.B.; Jimoh, R.G.; Folorunso, S.O.; Adeniyi, E.A.; Abiodun, K.M.; Banjo, O.O. Privacy and Security Concerns in IoT-Based Healthcare Systems. In *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*; Siarry, P., Jabbar, M.A., Aluvalu, R., Abraham, A., Madureira, A., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 105–134.
41. Butpheng, C.; Yeh, K.-H.; Xiong, H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. *Symmetry* **2020**, *12*, 1191. [CrossRef]
42. Coventry, L.; Branley, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* **2018**, *113*, 48–52. [CrossRef] [PubMed]
43. Sadek, I.; Rehman, S.U.; Codjo, J.; Abdulrazak, B. Privacy and security of IoT based healthcare systems: Concerns, solutions, and recommendations. In Proceedings of the How AI Impacts Urban Living and Public Health: 17th International Conference, ICOST 2019, New York City, NY, USA, 14–16 October 2019; Proceedings 17, 2019. pp. 3–17.
44. Paulsen, C. *Glossary of Key Information Security Terms*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
45. Luh, F.; Yen, Y. Cybersecurity in Science and Medicine: Threats and Challenges. *Trends Biotechnol.* **2020**, *38*, 825–828. [CrossRef] [PubMed]
46. Semantha, F.H.; Azam, S.; Yeo, K.C.; Shanmugam, B. A Systematic Literature Review on Privacy by Design in the Healthcare Sector. *Electronics* **2020**, *9*, 452. [CrossRef]
47. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183. [CrossRef]
48. Yeo, L.H.; Banfield, J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspect. Health Inf. Manag.* **2022**, *19*, 1i. [PubMed]
49. Seh, A.H.; Zarour, M.; Alenezi, M.; Sarkar, A.K.; Agrawal, A.; Kumar, R.; Ahmad Khan, R. Healthcare Data Breaches: Insights and Implications. *Healthcare* **2020**, *8*, 133. [CrossRef]
50. McGraw, D.; Mandl, K.D. Privacy protections to encourage use of health-relevant digital data in a learning health system. *NPJ Digit. Med.* **2021**, *4*, 2. [CrossRef]
51. Abouelmehdi, K.; Beni-Hessane, A.; Khaloufi, H. Big healthcare data: Preserving security and privacy. *J. Big Data* **2018**, *5*, 1. [CrossRef]
52. Robinson, J. US Healthcare Data Breach Statistics. Available online: https://www.privacyaffairs.com/healthcare-data-breach-statistics/ (accessed on 15 October 2023).

53. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.-V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.-M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 146. [CrossRef]
54. Elhoseny, M.; Thilakarathne, N.N.; Alghamdi, M.I.; Mahendran, R.K.; Gardezi, A.A.; Weerasinghe, H.; Welhenge, A. Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. *Sustainability* **2021**, *13*, 11645. [CrossRef]
55. Straits Research. IoT Healthcare Market Size Is Projected to Reach USD 486.34 Billion by 2031, Growing at a CAGR of 19.27%: Straits Research. Available online: https://www.globenewswire.com/en/news-release/2022/11/15/2556464/0/en/IoT-Healthcare-Market-Size-is-projected-to-reach-USD-486-34-Billion-by-2031-growing-at-a-CAGR-of-19-27-Straits-Research.html (accessed on 15 October 2023).
56. Kadhim, K.T.; Alsahlany, A.M.; Wadi, S.M.; Kadhum, H.T. An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT). *Wirel. Pers. Commun.* **2020**, *114*, 2235–2262. [CrossRef]
57. Weenk, M.; Bredie, S.J.; Koeneman, M.; Hesselink, G.; van Goor, H.; van de Belt, T.H. Continuous Monitoring of Vital Signs in the General Ward Using Wearable Devices: Randomized Controlled Trial. *J. Med. Internet Res.* **2020**, *22*, e15471. [CrossRef] [PubMed]
58. Al-Rawashdeh, M.; Keikhosrokiani, P.; Belaton, B.; Alawida, M.; Zwiri, A. IoT Adoption and Application for Smart Healthcare: A Systematic Review. *Sensors* **2022**, *22*, 5377. [CrossRef] [PubMed]
59. Babar, S.; Mahalle, P.; Stango, A.; Prasad, N.; Prasad, R. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In *Recent Trends in Network Security and Applications: Third International Conference, CNSA 2010, Chennai, India, 23–25 July 2010. Proceedings*; Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 420–429.
60. Al Ameen, M.; Liu, J.; Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *J. Med. Syst.* **2012**, *36*, 93–101. [CrossRef]
61. Jing, Q.; Lu, J.; Qiu, D.; Vasilakos, A.V.; Wan, J. Security of the Internet of Things: Perspectives and challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [CrossRef]
62. Watzlaf, V.J.M.; Zhou, L.; DeAlmeida, D.R.; Hartman, L.M. A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices Used by Healthcare Providers. *Int. J. Telerehabilitation* **2017**, *9*, 39–58. [CrossRef]
63. Abouzakhar, N.S.; Jones, A.; Angelopoulou, O. Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. In Proceedings of the 2017 IEEE International Conference 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), Exeter, UK, 21–23 June 2017; pp. 373–378.
64. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. *ACM Trans. Comput. Healthc.* **2021**, *2*, 27. [CrossRef]
65. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]
66. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and Privacy in the Medical Internet of Things: A Review. *Secur. Commun. Netw.* **2018**, *2018*, 5978636. [CrossRef]
67. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [CrossRef]
68. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Appl. Sci.* **2019**, *2*, 139. [CrossRef]
69. Abomhara, M.; Køien, G.M. Security and privacy in the Internet of Things: Current status and open issues. In Proceedings of the 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, 11–14 May 2014; pp. 1–8.
70. Vignesh, M.R.; Sivakumar, S. Healthcare sensors issues, challenges & security threats in wireless body area network: A comprehensive survey. *Int. J. Trend Sci. Res. Dev* **2021**, *5*, 989–997.
71. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. [CrossRef]
72. BajriĆ, S. Data Security and Privacy Issues in Healthcare. *Appl. Med. Inform.* **2020**, *42*, 19–27.
73. Alkhatib, S.; Waycott, J.; Buchanan, G.; Bosua, R. Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A Review. *Stud. Health Technol. Inform.* **2018**, *252*, 8–14.
74. Djenna, A.; Saïdouni, D.E. Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure. In Proceedings of the 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, France, 24–26 October 2018; pp. 1–4.
75. Li, C.; Wang, J.; Wang, S.; Zhang, Y. A review of IoT applications in healthcare. *Neurocomputing* **2024**, *565*, 127017. [CrossRef]
76. Zakaria, H.; Abu Bakar, N.A.; Hassan, N.H.; Yaacob, S. IoT Security Risk Management Model for Secured Practice in Healthcare Environment. *Procedia Comput. Sci.* **2019**, *161*, 1241–1248. [CrossRef]
77. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Proceedings of the 2015 IEEE World Congress on Services, New York, NY, USA, 27 June–2 July 2015; pp. 21–28.
78. Abie, H.; Balasingham, I. Risk-based adaptive security for smart IoT in eHealth. In Proceedings of the Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 24–26 February 2012; pp. 269–275.
79. 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]

80. Yaacoub, J.-P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
81. Kumar, P.; Lee, H.J. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* **2012**, *12*, 55–91. [CrossRef]
82. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the Internet of Things: A Review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; pp. 648–651.
83. Priestman, W.; Anstis, T.; Sebire, I.G.; Sridharan, S.; Sebire, N.J. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health Care Inform.* **2019**, *26*, e100031. [CrossRef] [PubMed]
84. Waheed, N.; He, X.; Ikram, M.; Usman, M.; Hashmi, S.S.; Usman, M. Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. *ACM Comput. Surv.* **2020**, *53*, 122. [CrossRef]
85. Chen, F.; Huang, J.; Wang, C.; Tang, Y.; Huang, C.; Xie, D.; Wang, T.; Zhao, C. Data Access Control Based on Blockchain in Medical Cyber Physical Systems. *Secur. Commun. Netw.* **2021**, *2021*, 3395537. [CrossRef]
86. Hasan, M.K.; Ghazal, T.M.; Saeed, R.A.; Pandey, B.; Gohel, H.; Eshmawi, A.A.; Abdel-Khalek, S.; Alkhassawneh, H.M. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Commun.* **2022**, *16*, 421–432. [CrossRef]
87. Alromaihi, S.; Elmedany, W.; Balakrishna, C. Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications. In Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018; pp. 140–145.
88. Wasserman, L.; Wasserman, Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Front. Digit. Health* **2022**, *4*, 862221. [CrossRef]
89. Chattopadhyay, A.K.; Nag, A.; Ghosh, D.; Chanda, K. A Secure Framework for IoT-Based Healthcare System. In Proceedings of the International Ethical Hacking Conference 2018; Springer: Singapore, 2019; pp. 383–393.
90. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.M.; Hamed, H.F.A. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Comput. Secur.* **2021**, *111*, 102491. [CrossRef]
91. Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–6.
92. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017; pp. 112–120.
93. Gupta, B.B.; Dahiya, A. *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*; CRC Press: Boca Raton, FL, USA, 2021.
94. Bediya, A.K.; Kumar, R. A Novel Intrusion Detection System for Internet of Things Network Security. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*; Management Association, I.R., Ed.; IGI Global: Hershey, PA, USA, 2023; pp. 330–348.
95. Sharma, K.; Gupta, B.B. Taxonomy of Distributed Denial of Service (DDoS) Attacks and Defense Mechanisms in Present Era of Smartphone Devices. *Int. J. E-Serv. Mob. Appl. (IJESMA)* **2018**, *10*, 58–74. [CrossRef]
96. Ray, S.; Mishra, K.N.; Dutta, S. Detection and prevention of DDoS attacks on M-healthcare sensitive data: A novel approach. *Int. J. Inf. Technol.* **2022**, *14*, 1333–1341. [CrossRef]
97. Alagar, V.; Alsaig, A.; Ormandjiva, O.; Wan, K. Context-Based Security and Privacy for Healthcare IoT. In Proceedings of the 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, China, 17–19 August 2018; pp. 122–128.
98. Mahjabin, T.; Xiao, Y.; Sun, G.; Jiang, W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717741463. [CrossRef]
99. Imdad, M.; Jacob, D.W.; Mahdin, H.; Baharum, Z.; Shaharudin, S.M.; Azmi, M.S. Internet of things (IoT); security requirements, attacks and counter measures. *Indones. J. Electr. Eng. Comput. Sci.* **2020**, *18*, 1520–1530.
100. Shah, S.; Simnani, S.S.A.; Banday, M.T. A Study of Security Attacks on Internet of Things and Its Possible Solutions. In Proceedings of the 2018 International Conference on Automation and Computational Engineering (ICACE), Noida, India, 3–4 October 2018; pp. 203–209.
101. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
102. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors* **2021**, *21*, 5119. [CrossRef]
103. Alwan, Z.S.; Younis, M.F. Detection and prevention of SQL injection attack: A survey. *Int. J. Comput. Sci. Mob. Comput.* **2017**, *6*, 5–17.
104. Rajendran, G.; Nivash, R.S.R.; Parthy, P.P.; Balamurugan, S. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–6.

105. Tukur, Y.M.; Ali, Y.S. Demonstrating the Effect of Insider Attacks on Perception Layer of Internet of Things (IoT) Systems. In Proceedings of the 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 10–12 December 2019; pp. 1–6.
106. Lee, I. Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. *Information* **2022**, *13*, 404. [CrossRef]
107. Alsowail, R.A.; Al-Shehari, T. Techniques and countermeasures for preventing insider threats. *PeerJ Comput. Sci.* **2022**, *8*, e938. [CrossRef]
108. Albalawi, A.M.; Almaiah, M.A. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol* **2022**, *100*, 2988–3011.
109. Farhin, F.; Kaiser, M.S.; Mahmud, M. Towards Secured Service Provisioning for the Internet of Healthcare Things. In Proceedings of the 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT), Tashkent, Uzbekistan, 7–9 October 2020; pp. 1–6.
110. Rughoobur, P.; Nagowah, L.; Rughoobur, P.; Nagowah, L. A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, United Arab Emirates, 18–20 December 2017; pp. 811–817.
111. What Is RYUK Ransomware? Available online: https://www.trendmicro.com/en_nz/what-is/ransomware/ryuk-ransomware.html#:~:text=Ryuk%20is%20ransomware%20version%20attributed,by%20the%20end%20of%202020 (accessed on 10 December 2023).
112. Swessi, D.; Idoudi, H. A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures. *Wirel. Pers. Commun.* **2022**, *124*, 1557–1592. [CrossRef]
113. Liu, X.; Qian, C.; Hatcher, W.G.; Xu, H.; Liao, W.; Yu, W. Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. *IEEE Access* **2019**, *7*, 79523–79544. [CrossRef]
114. Mahanty, A.; Singh, G.; Som, S.; Khatri, S.K. Security Issues and Challenges in Perception Layer of Smart Healthcare. In Proceedings of the 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 29–31 August 2018; pp. 639–644.
115. Ren, Z.; Liu, X.; Ye, R.; Zhang, T. Security and privacy on internet of things. In Proceedings of the 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), Macau, China, 21–23 July 2017; pp. 140–144.
116. Shrivastava, V.; Namdev, M. A Review on Security and Privacy Issues in Wireless Body Area Networks for Healthcare Applications. *Smart Moves J. Ijoscience* **2019**, *5*, 22–28. [CrossRef]
117. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* **2020**, *20*, 3625. [CrossRef]
118. Habibzadeh, H.; Dinesh, K.; Shishvan, O.R.; Boggio-Dandry, A.; Sharma, G.; Soyata, T. A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective. *IEEE Internet Things J.* **2020**, *7*, 53–71. [CrossRef] [PubMed]
119. Bakar, N.A.A.; Ramli, W.M.W.; Hassan, N.H. The internet of things in healthcare: An overview, challenges and model plan for security risks management process. *Indones. J. Electr. Eng. Comput. Sci. (IJEECS)* **2019**, *15*, 414–420.
120. Amaraweera, S.P.; Halgamuge, M.N. Internet of Things in the Healthcare Sector: Overview of Security and Privacy Issues. In *Security, Privacy and Trust in the IoT Environment*; Mahmood, Z., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 153–179.
121. Fazeldehkordi, E.; Owe, O.; Noll, J. Security and Privacy in IoT Systems: A Case Study of Healthcare Products. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–8.
122. Perwej, Y.; Akhtar, N.; Kulshrestha, N.; Mishra, P. A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends. *J. Emerg. Technol. Innov. Res.* **2022**, *9*, d346–d371.
123. Islam, M.M.; Nooruddin, S.; Karray, F.; Muhammad, G. Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain. *IEEE Internet Things J.* **2023**, *10*, 3611–3641. [CrossRef]
124. Pandey, P.; Pandey, S.C.; Kumar, U. Security issues of internet of things in health-care sector: An analytical approach. In *Advancement of Machine Intelligence in Interactive Medical Image Analysis*; Springer: Singapore, 2020; pp. 307–329.
125. Haque, M.A.; Haque, S.; Kumar, K.; Singh, N.K. A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things. In *Handbook of Research on Digital Transformation and Challenges to Data Security and Privacy*; Anunciação, P.F., Pessoa, C.R.M., Jamil, G.L., Eds.; IGI Global: Hershey, PA, USA, 2021; pp. 63–90.
126. Yousuf, O.; Mir, R.N. A survey on the Internet of Things security. *Inf. Comput. Secur.* **2019**, *27*, 292–323. [CrossRef]
127. Litoussi, M.; Kannouf, N.; El Makkaoui, K.; Ezzati, A.; Fartitchou, M. IoT security: Challenges and countermeasures. *Procedia Comput. Sci.* **2020**, *177*, 503–508. [CrossRef]
128. Bagga, M.; Thakral, P.; Bagga, T. A Study on IoT: Model, Communication Protocols, Security Hazards & Countermeasures. In Proceedings of the 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 20–22 December 2018; pp. 591–598.
129. Chaudhary, J.; Prasad, S. IoT in healthcare sector-a comprehensive analysis of threats and privacy issues. *AIP Conf. Proc.* **2022**, *2519*, 030058. [CrossRef]
130. Akhtar, M.S.; Feng, T. A Systemic Security and Privacy Review: Attacks and Prevention Mechanisms over IOT Layers. *EAI Endorsed Trans. Secur. Saf.* **2022**, *8*, e5. [CrossRef]

131. Sabir, M.A.; Sajid, A.; Ashraf, F. A Systemic Security and Privacy Review: Attacks and Prevention Mechanisms Over IoT Layers. In *Big Data Analytics and Computational Intelligence for Cybersecurity*; Ouaissa, M., Boulouard, Z., Ouaissa, M., Khan, I.U., Kaosar, M., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 69–89.
132. Gautam, S.; Malik, A.; Singh, N.; Kumar, S. Recent Advances and Countermeasures Against Various Attacks in IoT Environment. In Proceedings of the 2019 2nd International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 29–30 March 2019; pp. 315–319.
133. Bahalul Haque, A.K.M.; Bhushan, B.; Nawar, A.; Talha, K.R.; Ayesha, S.J. Attacks and Countermeasures in IoT Based Smart Healthcare Applications. In *Recent Advances in Internet of Things and Machine Learning: Real-World Applications*; Balas, V.E., Solanki, V.K., Kumar, R., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 67–90.
134. Research, Z. Top Cyber Threats to Healthcare Organizations. Available online: https://www.zerofox.com/blog/cyber-threats-to-healthcare-industry/ (accessed on 10 December 2023).
135. Samaila, M.G.; Sequeiros, J.B.F.; Freire, M.M.; Inácio, P.R.M. Security Threats and Possible Countermeasures in IoT Applications Covering Different Industry Domains. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; p. 16.
136. Mehra, D.; Sharma, D.K.; Sharma, S.K. Challenges and vulnerabilities of WSN-based IoT in the healthcare and medical industry. In *Integration of WSNs into Internet of Things*; CRC Press: Boca Raton, FL, USA, 2021; pp. 305–333.
137. Fasunlade, O.; Zhou, S.; Sanders, D. Security Threats and Possible Countermeasure In Digital Healthcare. In Proceedings of the 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17 December 2021; pp. 1297–1302.
138. Saba, T.; Haseeb, K.; Ahmed, I.; Rehman, A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *J. Infect. Public Health* **2020**, *13*, 1567–1575. [CrossRef]
139. Alsaidi, A.; Kausar, F. Security Attacks and Countermeasures on Cloud Assisted IoT Applications. In Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 21–23 September 2018; pp. 213–217.
140. Karunarathne, S.M.; Saxena, N.; Khan, M.K. Security and Privacy in IoT Smart Healthcare. *IEEE Internet Comput.* **2021**, *25*, 37–48. [CrossRef]
141. Qadri, Y.A.; Ali, R.; Musaddiq, A.; Al-Turjman, F.; Kim, D.W.; Kim, S.W. The limitations in the state-of-the-art counter-measures against the security threats in H-IoT. *Clust. Comput.* **2020**, *23*, 2047–2065. [CrossRef]
142. Cilliers, L. Wearable devices in healthcare: Privacy and information security issues. *Health Inf. Manag. J.* **2019**, *49*, 150–156. [CrossRef] [PubMed]
143. Ianculescu, M.; Coardoș, D.; Bica, O.; Vevera, V. Security and Privacy Risks for Remote Healthcare Monitoring Systems. In Proceedings of the 2020 International Conference on e-Health and Bioengineering (EHB), Iasi, Romania, 29–30 October 2020; pp. 1–4.
144. Tyagi, A.K.; Nair, M.M. Internet of Everything (IoE) and Internet of Things (IoTs): Threat Analyses, Possible Opportunities for Future. *J. Inf. Assur. Secur.* **2020**, *15*, 153–177.
145. Aswani Devi, A.; Erukala Suresh, B.; Nayak, S.R.; Sethy, A.; Verma, A. Integrated Industrial Reference Architecture for Smart Healthcare in Internet of Things: A Systematic Investigation. *Algorithms* **2022**, *15*, 309. [CrossRef]
146. Humayun, M.; Jhanjhi, N.Z.; Alsayat, A.; Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. *Egypt. Inform. J.* **2021**, *22*, 105–117. [CrossRef]
147. Khatkar, M.; Kumar, K.; Kumar, B. An overview of distributed denial of service and internet of things in healthcare devices. In Proceedings of the 2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability (INBUSH), Noida, India, 19–21 February 2020; pp. 44–48.
148. Mohapatro, M.; Snigdh, I. An Experimental Study of Distributed Denial of Service and Sink Hole Attacks on IoT based Healthcare Applications. *Wirel. Pers. Commun.* **2021**, *121*, 707–724. [CrossRef]
149. Bikos, A.N.; Sklavos, N. The future of privacy and trust on the internet of Things (IoT) for healthcare: Concepts, Challenges, and Security Threat Mitigations. In *Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2020; pp. 63–90.
150. Gavrilović, N.; Mishra, A. Software architecture of the internet of things (IoT) for smart city, healthcare and agriculture: Analysis and improvement directions. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 1315–1336. [CrossRef]
151. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access* **2018**, *6*, 25167–25177. [CrossRef]
152. Davis, J. The 10 Biggest Healthcare Data Breaches of 2019, So Far. Available online: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far (accessed on 10 December 2023).
153. He, Y.; Aliyu, A.; Evans, M.; Luo, C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J. Med. Internet Res.* **2021**, *23*, e21747. [CrossRef]
154. Burke, G.; Saxena, N. Cyber Risks Prediction and Analysis in Medical Emergency Equipment for Situational Awareness. *Sensors* **2021**, *21*, 5325. [CrossRef]
155. Irshad, R.R.; Sohail, S.S.; Hussain, S.; Madsen, D.Ø.; Zamani, A.S.; Ahmed, A.A.A.; Alattab, A.A.; Badr, M.M.; Alwayle, I.M. Towards enhancing security of IoT-Enabled healthcare system. *Heliyon* **2023**, *9*, e22336. [CrossRef] [PubMed]
156. Bygrave, L.A. Security by Design: Aspirations and Realities in a Regulatory Context. *Oslo Law Rev.* **2022**, *8*, 126–177. [CrossRef]

157. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6476274. [CrossRef]
158. Mishra, V.; Gupta, K.; Saxena, D.; Singh, A.K. A Global Medical Data Security and Privacy Preserving Standards Identification Framework for Electronic Healthcare Consumers. *IEEE Trans. Consum. Electron.* **2024**, *70*, 4379–4387. [CrossRef]
159. Cirne, A.; Sousa, P.R.; Resende, J.S.; Antunes, L. IoT security certifications: Challenges and potential approaches. *Comput. Secur.* **2022**, *116*, 15. [CrossRef]
160. HIPAA. Submitting Notice of a Breach to the Secretary. Available online: https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (accessed on 15 March 2024).
161. Osama, M.; Ateya, A.A.; Sayed, M.S.; Hammad, M.; Pławiak, P.; Abd El-Latif, A.A.; Elsayed, R.A. Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. *Sensors* **2023**, *23*, 7435. [CrossRef]
162. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 698–736. [CrossRef]
163. Madanian, S.; Nakarada-Kordic, I.; Reay, S.; Chetty, T.h. Patients' perspectives on digital health tools. *PEC Innov.* **2023**, *2*, 100171. [CrossRef]
164. Chinbat, T.; Madanian, S.; Airehrour, D.; Hassandoust, F. Machine learning cryptography methods for IoT in healthcare. *BMC Med. Inform. Decis. Mak.* **2024**, *24*, 153. [CrossRef]