applied sciences

Review

Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)

Jahanzeb Shahid [1], Rizwan Ahmad [1,*], Adnan K. Kiani [2], Tahir Ahmad [3], Saqib Saeed [4] and Abdullah M. Almuhaideb [5]

[1] School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan; 13msccsjshahid@seecs.edu.pk
[2] Essex Pathways Department, University of Essex, Colchester CO4 3SQ, UK; a.kiani@essex.ac.uk
[3] Security and Trust Unit, Fondazione Bruno Kessler, 38123 Trento, Italy; ahmad@fbk.eu
[4] SAUDI ARAMCO Cybersecurity Chair, Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; sbsaed@iau.edu.sa
[5] SAUDI ARAMCO Cybersecurity Chair, Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; amalmuhaideb@iau.edu.sa
* Correspondence: rizwan.ahmad@seecs.edu.pk

Abstract: The Internet of Things (IoT) is an emerging field consisting of Internet-based globally connected network architecture. A subset of IoT is the Internet of Healthcare Things (IoHT) that consists of smart healthcare devices having significant importance in monitoring, processing, storing, and transmitting sensitive information. It is experiencing novel challenges regarding data privacy protection. This article discusses different components of IoHT and categorizes various healthcare devices based on their functionality and deployment. This article highlights the possible points and reasons for data leakage, such as conflicts in laws, the use of sub-standard devices, lack of awareness, and the non-availability of dedicated local law enforcement agencies. This article draws attention to the escalating demand for a suitable regulatory framework and analyzes compliance problems of IoHT devices concerning healthcare data privacy and protection regulations. Furthermore, the article provides some recommendations to improve the security and privacy of IoHT implementation.

Keywords: IoHT; data privacy; healthcare systems; security and privacy; healthcare regulations

check for updates

Citation: 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. https://doi.org/10.3390/app12041927

Academic Editors: Hamid Mcheick and Gianluca Lax

Received: 10 October 2021
Accepted: 27 January 2022
Published: 12 February 2022

1. Introduction

The IoT is an emerging technology that facilitates consumers by exchanging information with devices connected to the Internet. The International Telecommunication Union (ITU) [1] defines IoT as the network of sensor devices interacting with the environment. The spectrum of IoT has been broadened and encloses many applications that are used in different scenarios like security, remote monitoring, electrical appliances control, military use, and other electronic equipment. One primary use case of IoT is in the healthcare sector, i.e., the Internet of Healthcare Things (IoHT), designed to monitor, store, or transmit healthcare information. In simple words, IoHT is a sub-class of IoT specifically dealing with healthcare that includes devices, services, and software [2].

The IoHT describes uniquely identifiable devices connected to the Internet, communicating with each other, used in the medical area. IoHT devices help to monitor individuals' medical conditions by generating clinical data by forwarding it to a remote server or service with the help of wireless network infrastructure [3]. Like any other Internet-based device, IoHT devices have a unique identifier such as an IP address which enables them to connect with the network and to forward/receive data to/from intended devices [4]. The central server manages this collected information and responds accordingly to diagnose patients' diseases. A high-level general working flow diagram of an IoHT implementation is presented in Figure 1. The idea is to provide reliable, efficient, and cost-effective healthcare services by facilitating physicians and medical staff by remotely monitoring their patients. IoHT implementations also enable individuals to manage their health data easily and assist them in how to use wearable health monitors [5,6].

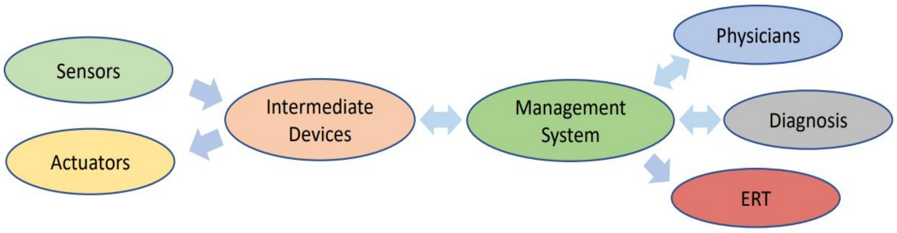

Figure 1. High-Level Architecture of IoHT Implementation.

Data privacy is considered to be a fundamental requirement for consumer acceptance, which can be ensured through the data flow representation, authentication, and authorization of the performed activities such as data collection, retention, processing, and transmission. Data privacy risks are directly related to unauthorized collection, usage, access, storage, and sharing activities. These activities might be the reason for personal data leakage and compromising the user's privacy, especially concerning healthcare data, as it has different priorities and is highly valuable and sensitive. In this regard, appropriate protection and security measures are required [7–10].

Moreover, accessibility and availability of personal healthcare information on the Internet also cause privacy problems. In June 2015, a censorious privacy violation attack was launched when malware exploited vulnerabilities in blood gas analyzer devices to gain access to hospital networks and leaked private data [11]. Despite this, the privacy framework for IoHT systems and services is expected to be transparent to patients, making available updated information to ensure the protection of patients' data [6]. The healthcare systems collect most of the data from the sensing devices and forward it via intermediate devices to the management layer. During this process, several protocols and encoding schemes are used to communicate data reliably. It is easier to find vulnerabilities in different components of the healthcare system by using search engines like Shodan, which assists attackers in searching the connected vulnerable devices on the Internet [12]. Similarly, a worksheet containing millions of records with user healthcare information can be exchanged in a fraction of a second, seamlessly, and without leaving any consistent trace [10].

Some IoT-related data privacy and protection policies are used to protect data and users' privacy. However, these legal frameworks have not produced the intended results and the actual level of healthcare data privacy protection is insufficient for the issues mentioned earlier [9]. There are also some limitations and missing aspects of healthcare data privacy laws that do not provide a particular set of instructions to protect IoHT data.

In this paper, we discuss technological, legal, and structural problems of IoHT systems with some analysis, and compliance issues of the healthcare data privacy and protection framework in the developing countries. The paper uses a layered architecture to highlight the data protection and privacy issues in the IoHT. It further identifies protection and privacy issues at different layers from technical and legal perspectives. Furthermore, the study of different components of the existing healthcare system in terms of security related to data protection discusses possible points of data leakage, missing aspects of healthcare policies, and issues in the enforcement of healthcare systems and policies. To highlight the utility of this work we compare it with recent similar works in the IoHT literature in Table 1. The main contributions of this work can be summarized as follows:

- We define a five-layer reference architecture for IoHT, which is derived from known architectures used in other IoHT related research articles [13–15];

- We present IoHT classification, identify the vulnerabilities in IoHT implementation and map the security problem on the defined five-layer IoHT architecture;
- We discuss major existing healthcare legislative and regulatory initiatives, compare various legislative approaches and identify the gaps and governance challenges.
- We conclude with the recommendations on both frontiers (i.e., technical and legislative).

Table 1. Comparison of this work with the recent IoHT literature.

Papers with Authors	**IoHT Architecture**	**Legislative and Regulatory**	**Communication Technologies**	**Standards**	**Security and Privacy**	
					Challenges	Countermeasures
S. Ketu et al., 2021 [16]	✔			✔	✔	✔
M. Mamdouh, 2021 [17]	✔				✔	✔
R. Somasundaram, 2021 [18]					✔	✔
R. Sivan et al., 2021 [19]	✔				✔	✔
This Paper	✔	✔	✔	✔	✔	✔

The remainder of the paper is organized as follows. Section 2 introduces the Internet of Healthcare Things (IoHT) and presents a layered architecture and working of IoHT. Section 3 highlights the vulnerabilities in the healthcare system and identifies the possible points from where the data can be leaked. Section 4 presents various global governance initiatives regarding privacy and data protection in IoHT and also identifies the gaps and governance challenges that hinder the widespread adoption of IoHT. Section 5 recommends some measures for effective IoHT implementation, while Section 6 draws some conclusions.

2. Internet of Healthcare Things (IoHT)

Health management problems are increasing with the growing population, especially with the increasingly larger aging population. Sometimes no response from the hospital for emergencies creates social issues. Similarly, the medical staff in rural areas do not have sufficient resources for treatment and do not have the expertise to diagnose complex diseases. Due to these reasons, people in rural areas focus on big hospitals for proper medical attention, increasing the load on hospitals. The late detection of diseases and severe health problems of older people also complicate the diagnosis process. Therefore, there is a need to provide better medical facilities using an optimized healthcare system that includes body sensors and medical devices to remotely monitor and diagnose medical problems [20,21].

2.1. IoHT Classification Based on Architecture

In this subsection, we present a detailed classification of IoHT based on the IoHT architecture in Figure 2. A generic IoHT architecture consists of IoHT devices [22–30], communication protocols [31–36], and networks [37–40]. The IoHT devices are further classified as wearable devices and implant devices. The data of IoHT devices are then transmitted by using different communication protocols like IEEE 802.15.6, WBAN, IEEE 802.15.1 Bluetooth, IEEE 802.11 WiFi, and LoRaWAN. The destination of this medical data is a cloud service, or a remote server designed for intensive processing tasks. Finally, data can be transmitted to a physician or an Emergency Response Team (ERT) via a mobile communication service such as 4G or 5G.

Once the information is collected from different IoHT devices where the sensors exist, it travels toward the near and far edge of the network to be stored, analyzed, and additionally processing [41].

Using a fog node network can give a health care system more computing power that smaller and battery-oriented IoHT devices might not be able to achieve. In the IoHT architecture, data operations, such as classification and compression, are completed on the intermediate devices or often single remote servers that allow for the fast processing of data that mobile devices cannot do. In cloud-based networks, the majority of the computation is performed on the cloud servers because the cloud has a higher computing capacity than the fog node networks. Cloud-based networks utilize multiple servers for parallel computing and data analysis. Moreover, the cloud has data centers that allow for more data storage that is sometimes needed for patient records.

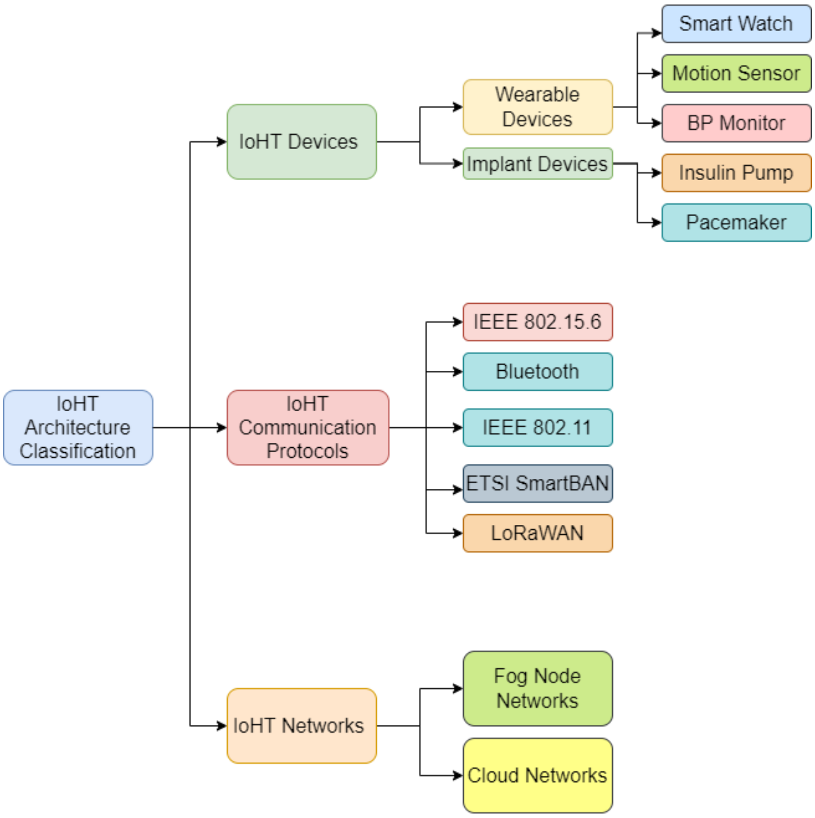

Figure 2. IoHT Architecture Classification.

2.2. IoHT Components

An IoHT implementation can simply consist of a single sensor device like a heartbeat monitor connected to a mobile device via Bluetooth. The mobile device should have a specific application to generate alarms after analyzing data. It could be complex, consisting of multiple sensors, intermediate devices, and centralized servers connected with a central management system. The medical Emergency Response Team (ERT) monitors the patient's health conditions and responds in the case of any emergency.

Figure 3 shows a generic IoHT implementation where different devices at different layers communicate with each other with the help of various protocols. Intermediate devices like cell phones or PDAs communicate with sensors/actuators using short-range protocols and with healthcare servers with the help of the Internet. Servers take the appropriate actions by updating the database or contacting the relevant physicians or quick response teams in case of an emergency. It is a simple architecture used in IoT application development [41]. Each connected device has limitations like limited processing, memory, and battery resources, etc., and the applications are developed for better utilization of these limited resources. The reference architecture model shown in Figure 3 highlights a layered approach for describing IoHT functionalities and their problems. In addition, the layered architecture is used for identifying IoHT data security and privacy issues in technical and legal aspects. This five-layer architecture helps to identify IoHT data security and privacy issues at different layers, what type of devices and entities (medical team, physician, and emergency services) are involved at a specific layer, and what threat vectors are involved at each layer.

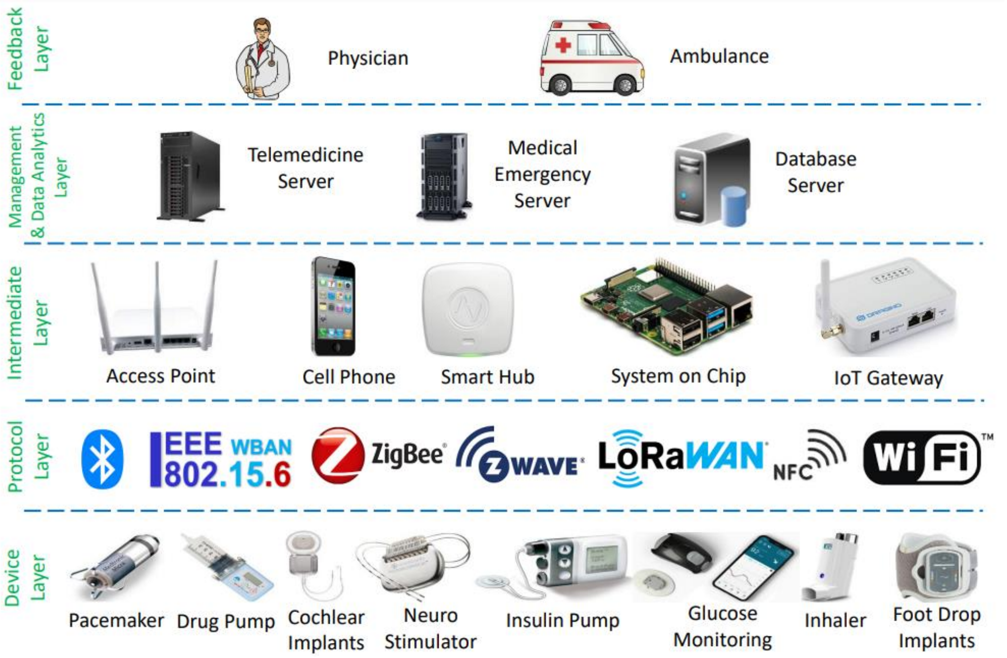

Figure 3. Five-Layer Architecture for IoHT.

Here, we will discuss each layer with its components.

2.2.1. Device Layer

Actuators are devices that can perform some actions based on the data generated by sensors, e.g., electronic motors, drug pumps, etc. On the other hand, according to their installation type, these devices can be divided into three categories (i.e., implantable, wearable, and fixed devices). These categories are briefly discussed here.

Implantable Medical Devices are implanted into the human body as shown in Figure 4. The most common devices belonging to this category are the Pacemaker [42], Neurostimulators [43], Insulin Pumps, Glucose Monitoring Systems [44], Gastric Stimulators [45], Foot Drop Implants [46], Cochlear Implants [47], and Drug Pumps [48], etc.

Fixed Medical Devices are related to the third category of devices that can be used for different tests in the laboratory, such as X-ray machines. The medical devices in this layer can be classified according to their functionalities or installation type. According to their functionalities, these devices can be divided into two types (i.e., sensors and actuators) briefly discussed here.

Sensors generate data by sensing physical parameters from their environment, e.g., temperature, pressure, etc. [49], ventilators, and ECG machines installed in medical labs and diagnostics rooms. These machines are not mobile because of their sizeable physical dimension. These machines are computerized, controlled, and connected to the networks for remote monitoring. The data sent from these devices are not secure and prone to data-stealing threats. It is essential to ensure the security of these devices because these devices gather and forward the data of multiple patients on an hourly basis compared to the devices working remotely. Therefore, these devices draw more attention from the intruders. A summary of data transmission rate, frequency spectrum, range, etc., is given in Table 2.

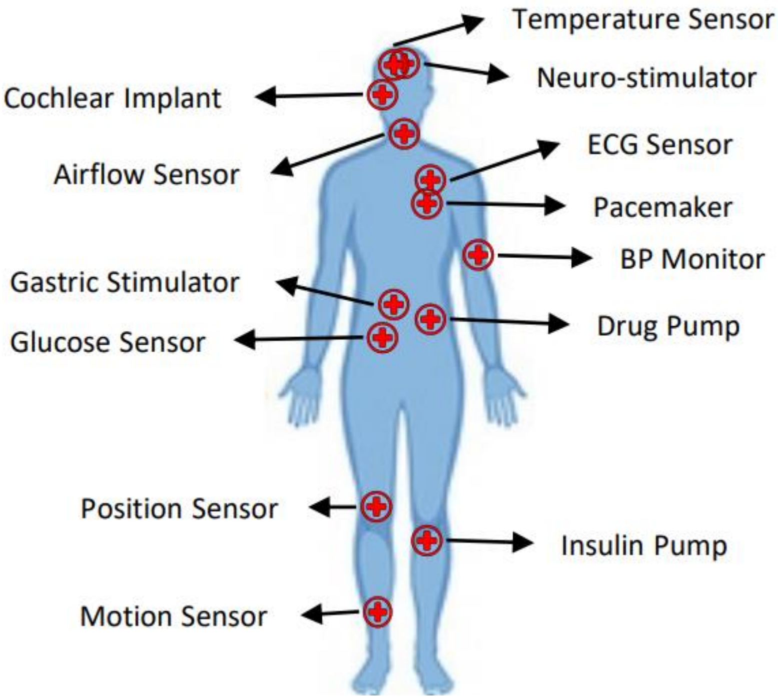

Figure 4. Implantable and Wearable IoHT Devices.

Table 2. IoHT Devices Technical Details.

IoHT Devices	Protocol	Range	Frequency Spectrum	Data Transmission Rate	Security Protocols
Pacemaker	BLE/WiFi/Cellular	400–500 m	2.4-5 GHz, ISM Band, 700–2100 MHz	1–3 Mbit/s	Secure SDN, NIST Standard
Hear Rate Monitor	ANT +/BLE	400 m	2.5 GHz	60 Kbps–3 Mbit/s	8-Byte Network Key, 128-bit AES
Temperature Sensor	IEEE 802.15.4/Zigbee	10 m	2.4-2.48 GHz	250 Kbps	Symmetric Cryptography
ECG Sensor	WiFi	50 m	2.4–2.5 GHz, ISM Band	1–3 Mbit/s	WPA-2
Blood Pressure Monitor	Bluetooth 3.0 + EDR Technology	10 m	2.45 GHz	3 Mbit/s	AES-CMAC Encryption
EMG Sensors	BLE	400 m	2.45 GHz	1 Mbit/s	Link Layer Encryption
PPG Sensors	BLE	400 m	2.45 GHz	1 Mbit/s	Link Layer Encryption
Position Sensors	BLE	400 m	2.45 GHz	1 Mbit/s	Link Layer Encryption
Cuffless B.P. Sensors	BLE	400 m	2.45 GHz	1 Mbit/s	Link Layer Encryption
Motion Sensors	Radio Frequency	150 m	433.92 MHz	10 Kbps	SPECK/SIMON
Air Flow Sensors	Bluetooth 3.0	100–150 m	2.45 GHz	1–3 Mbit/s	Symmetric Cryptography

2.2.2. Protocol Layer

The protocol layer consists of communication protocols and wireless standards used to enable communication for wireless devices. The first dedicated standard for Wireless Body Area Networks (WBANs) is the IEEE 802.15.6 released in 2012 [31]. IEEE 802.15.6 is designed to support both medical and non-medical applications and can be easily configured based on application requirements [50]. It ensures communication inside and around the human body and is specifically designed keeping in mind sensor devices that consume less energy and have a low transmission range. Another upcoming standard in this context is the European Telecommunications Standards Institute (ETSI) SmartBan [27,30]. In addition to IEEE 802.15.6, there are other commonly used standards and technologies such as IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee), IEEE 802.11 (WiFi) [35], Bluetooth Low Energy (BLE), NFC, LoRaWAN, UWB [36], RuBee [51], and Z-Wave [52]. The choice of the standard used is based on many factors like data rate, transmission range, number of devices supported, interference due to the coexistence of different technologies, etc. The technical details about these protocols, such as frequency, communication range, data transfer rate, energy consumption, and its security features, are summarized in Table 3.

Table 3. IoHT Devices Technical Details.

Protocol	Frequency	Range	Data Transfer Rate	Energy Consumption	Security
Bluetooth	2.40–2.48 GHz	10–50 m	1–3 Mbps	0.01–50 W	SAFER Block Cipher
BLE	2.40 GHz	400–1000 m	125 Kbps–2 Mbps	50–100 micro W	AES-CCM Cipher
ZigBee	860 MHz–2.40 GHz	10–100 m	20–250 Kbps	10–100 micro W	AES-CCM/CBC
LoRaWAN	433–923 MHz	2–7 km	27 Kbps	50–80 micro W	AEA-CMAC
ANT	2.40 GHz	30 m	60 Kbps	42–72 micro W	AES-CBC
UWB	4.3 GHz	10 m	1 Mbps	5.31 micro W	CRC
RuBee	131 kHz	15 m	9.6 Kbps	40 nano W	AES

2.2.3. Intermediate Layer

Devices in this layer have the responsibility to transmit data to potent computing resources like cloud servers. These devices act like gateways that enable data flow from the sensor devices to the cloud or central servers for storage and further analysis. These devices can run multiple communication protocols such as WiFi, Bluetooth, GSM, etc., [53] and forward the collected data to the server. Some intermediate devices can store data as well for pre-processing algorithms to evaluate whether the data is clinically relevant or not [45]. Some of the intermediate devices are discussed here briefly.

Smart Hub is used to make communication easy with smart IoT devices but has many vulnerabilities that draw the attention of attackers into sniffing the traffic of the smart hub. If they can access networks, they will be able to spot IoT healthcare devices in the network [54].

Access Points facilitate a wireless connection between different healthcare devices and connect them with remote servers.

IoT Gateways primarily act as the bridge to connect sensor networks with conventional communication networks, enabling protocol conversion and device management.

The System on Chip (SoC) is a device that integrates all components of a computer system, helps to normalize data collected from different sensors, and controls actuators based on applications. In this way, it reduces the load on a central server and minimizes the communication [55].

Personal Digital Assistants (PDAs) are extensively used in the healthcare domain to support healthcare providers [56]. Such systems receive data from different wearable and implanted devices and process them through a variety of software applications [57].

2.2.4. Management and Data Link Layer

Management and database servers are the centralized part of the healthcare system that receives and updates the patient's data collected by the sensors and can also help the physicians manage the quantity of medicine or prescribe a new one for the patient. In emergencies, the servers send alerts to physicians and the emergency response teams for appropriate actions.

2.2.5. Feedback Layer

The physicians and the emergency response teams (ERT) provide feedback in any emergency and play a significant role in the healthcare system. At this layer, doctors and ERT respond to the system when they receive an alert from it.

Physicians are an integral part of the healthcare system and can observe their patients anytime, anywhere, and change treatment when required. An IoT device for a physician gives real-time information about the patient under observation. The IoT gateway device gathers information from different healthcare devices and forwards it to PDA devices held by physicians.

Emergency Response Team (ERT): In case of any medical emergency, the responsibility of the ERT is to provide medical attention to patients on-premises or remotely. In the context of IoHT, medical devices monitor patients' conditions and generate alerts in case of a medical emergency. Emergency care is a critical part of medical services and is influenced by the contextual information's time, availability, and accuracy [58].

2.3. IoHT Working

Figure 4 presents the data workflow diagram of a generic IoHT implementation system. This figure follows the conventions of a workflow diagram where the Start and End processes are shown with an oval shape. Different systems processes are demonstrated with rectangle shapes, and conditional methods are shown with the diamond shapes. The IoHT system consists of a Sensor, Intermediate System, Actuator, Server, and ERT module. A physician is also a part of the system that receives information from the server about a patient's health condition.

Figure 5 presents a three-level generic IoHT implementation framework. Level 1 consists of sensors and actuators reading physiological parameters and at times performing interventions. The acquired data is then processed in level 2 before it is forwarded to level 3 for decision-making.

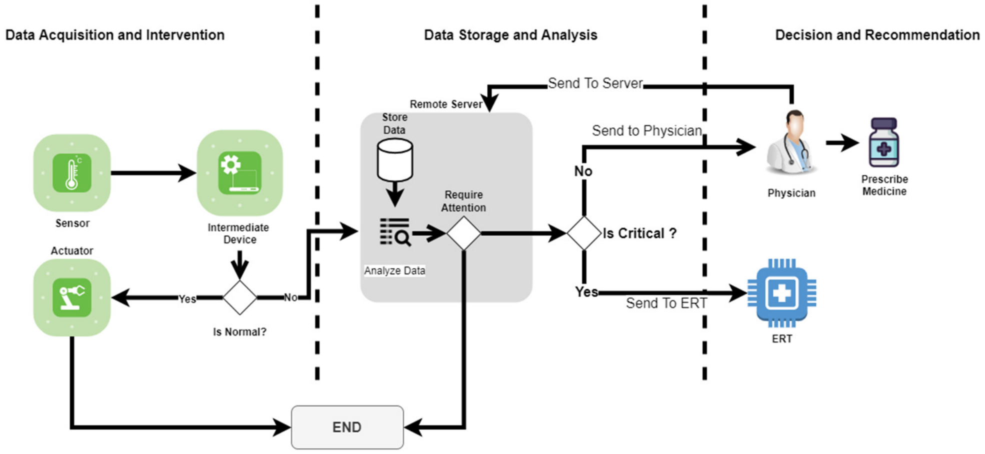

Figure 5. Workflow Diagram of IoHT Implementation.

3. IoHT Security Landscape

IoHT security goes beyond device security, therefore, rather than only physical interfaces and firmware on the device, its scope must include web, mobile/cloud interfaces, network services, local storage, and 3rd party APIs as well. Furthermore, diverse needs and varied intended usage of healthcare devices by residential and industrial consumers makes it more complex [59]. A list of top ten vulnerabilities related to IoHT devices has been published by The Open Web Application Security Project (OWASP). This includes lack of authorization/insufficient authentication, insecure web interfaces, lack of transport encryption, insecure network services, privacy concerns, insecure cloud interfaces, inadequate security configuration, insecure software or firmware, poor physical security, and insecure mobile interfaces [60]. Interested readers can refer to [61,62] for detailed security issues concerning IoHT.

3.1. Security Vulnerabilities in IoHT Implementations

There are several known security vulnerabilities in the existing IoHT implementations [12,63]. It is essential to discuss them to get a better understanding of the resulting security problems.

3.1.1. IoT Device's Operating System

Due to the specialized requirements of IoHT devices and limitations of existing operating systems, specialized operating systems such as RIOT, Contiki, FreeRTOS, and TinyOS have been developed for IoT devices [64,65]. The constrained computational power, memory, and limited power of IoT devices make them vulnerable to the system and network attacks. Furthermore, constrained resources do not allow the implementation of complex encryption and authentication schemes on these devices as they may significantly consume the computational resources and cause a long delay, resulting in the degraded performance of the regular operation of these devices which is critical, especially for real-time IoT devices. This scenario facilitates attackers in using memory vulnerabilities and compromises the security of such devices [66]. With inadequate resources on lightweight IoT devices, it becomes challenging to implement strong encryption and authentication schemes.

3.1.2. Communication Protocols

IoHT devices come with fewer safety checks, and it is the firmware of these devices that have security vulnerabilities like hardcoded keys. The urgency to roll out IoHT cloud platforms and the limited user experience of new IoT applications may result in the development of protocols by I.T. companies having many potential security loopholes. Due to the diversity of IoT devices, it is not easy to develop a standard security protocol for heterogeneous devices and it leads to problems of how to discover and urgently address the security vulnerabilities among IoT devices.

3.1.3. Insecure Middleware

To make IoT applications development more manageable, various IoT middleware platforms have been developed. These platforms offer distributed system services with standard programming interfaces and protocols and minimize problems associated with heterogeneity, distribution, and scale in IoT applications development. These services are called 'middleware' as they sit 'in the middle', in a layer above the operating system and networking software and below domain-specific applications [67,68].

3.2. Possible Points for Data Leakage

In the healthcare system, there are two states of data from where it can be stolen. These states are the persistent data (i.e., data at rest) and transient data (i.e., in motion). The overall description of data leakage points in a healthcare system is given in Figure 5. The arrows with dotted lines represent transient data whereas the arrows with solid lines represent persistent data. The details of each state are as follows.

3.2.1. Persistent Data

Persistent data refers to the data stored on different healthcare system components, such as sensing and actuating devices, etc., and is prone to theft. Here, the features of the healthcare system where the data can be stolen are discussed.

Healthcare devices such as sensors and actuators store the events logs (latest reading, configuration change, connection history, etc.) in the memory. As these devices usually have weak security configurations and store data in non-encrypted forms, an attacker can steal the data by exploiting these weaknesses.

IoHT servers are the most attractive components of healthcare systems for attackers to steal health care data from as they contain the complete history of all the patients with their biodata.

Physicians/Response Team devices are mostly mobile devices that physicians or response teams use to monitor and process healthcare data. These devices are susceptible to memory leakage attacks. Personal computers, mobile phones, tablets, or any specific devices to monitor healthcare data fall into this category. Due to direct communication with IoHT data servers, these devices are highly vulnerable to different security attacks. Figure 6 is presenting attacks an attacker can execute on devices operating at different layers. Effect of one compromised device can propagate at different layers because these devices are communicating with each other.

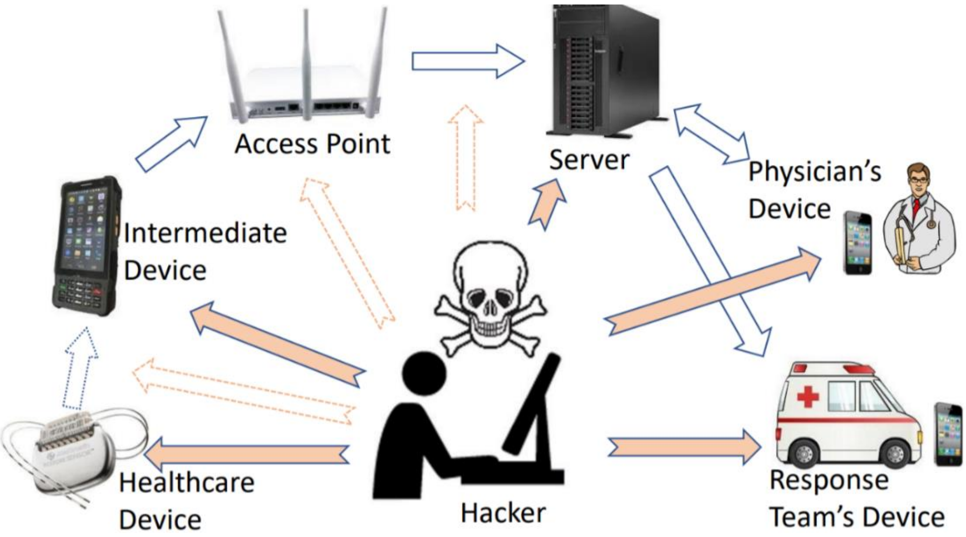

Figure 6. Possible Sites for Data Leakage in an IoHT implementation.

3.2.2. Transient Data

Transient data refers to the data on the move, as in the IoHT implementations, the information is transferred from devices to servers using different protocols and networking devices. Here, we discuss such devices and protocols from where the data can be stolen during transmission.

Communication protocols are used to transmit data from an IoT device to a device. IoT devices are primarily lightweight, low computational, and battery-oriented. Low-range protocols with weak security features transfer data from IoT devices to a gateway device.

Intermediate devices collect data from end devices using a specific protocol to aggregate and transform this data into another format that can be understood by the next device. A mobile phone or a PDA connected to the wearer acts like an intermediate device. These intermediate devices use multiple protocols to communicate with IoT endpoint devices, data servers, and monitoring devices. These protocols have security issues; IoT gateways, smart hubs, mobile phones, and WiFi devices enable IoT devices to connect with the Internet. These devices are limited in storage and are not used to store data; therefore, they forward it as it is received by changing its format. These devices communicate with IoT devices with different designs like LoRaWAN, ZigBee, Bluetooth, etc., but forward this collected data by using TCP/IP or UDP to the Internet.

Access Points/Smart Hubs/IoT Gateways enable communication between IoT and data servers. They are not storage devices; however, they forward received data to the intended destination. Due to the contact with different types of IoT devices, these devices operate multiple protocols. Security features like encryption, hashing, and password checking are used with these protocols. However, there are no established guidelines to comply with any healthcare laws describing the security levels needed for IoT healthcare intermediate devices.

3.3. Essential Security Features of IoHT

Following are some of the essential security features of IoHT.

Use of Standardized Devices: To ensure data privacy and security in healthcare systems, it is essential to use standardized devices with reliable security features. These devices should meet healthcare standards and policies. Data storage, transmission, format interchanges, terminologies, and presentation standards should be well-defined. No medical devices, either implantable or wearable, are allowed to be manufactured if they do not meet data standards.

Log Management and Compliance: Every management activity performed on these healthcare devices should be appropriately logged on the healthcare servers. For data privacy, there is a need to know who is accessing what data from which system. The best practices are gathering log files and saving them for future references as long as you need them. In distributed systems, these reports should be shared with other systems to prove compliance.

Updating Technologies: Technologies are considered the workforce behind the advancement in healthcare systems, and recent innovations have proven this. Technologies have changed the healthcare system to increase the accessibility of treatment that leads to improved care and efficiency. The latest components are more efficient and secure as compared to the previous ones. Therefore, the new devices with the latest technologies should be preferred over the old ones.

Patch Management: In addition to upgrading hardware, updating the software of IoT device's firmware is also essential; if it is not updated, it may be vulnerable. The software vendors release patches from time to time to overcome the flaws and loopholes. Every device which is connected to the Internet needs to be updated, whether it is a personal computer, smartphone, or any other device such as IoT [20].

User's Profiling: The users should be identified and authenticated; the system must know what resources a user can access. This process is called authorization. This process ensures that the behavior of the users is constrained according to the user's permission. User profiling is more critical in healthcare applications. Healthcare organizations must comply with international standards and procedures regarding user authentication and authorization. The exchange of patient data must permanently preserve privacy constraints with professional liabilities.

Generate Alerts: There should be some proper mechanism for IoHT to generate alerts for any kind of malicious event. Intermediate devices can play an essential role in this regard with the help of some applications. Warnings should be raised for critical events and emergencies. These devices can analyze received data; after the detection of any malicious activity, alerts can be directly transmitted to the monitoring server or system. Availability of IoHT should be the top priority; if any critical IoHT device goes off for any reason, intermediate devices communicate with them directly; therefore, generating alerts by these devices could help the emergency response team to respond more quickly.

Fines and Penalties: A mechanism should be implemented in the healthcare sector against attackers that attack healthcare systems and devices and try to leak or steal healthcare information. Healthcare data is confidential, and if an attacker tries to breach the healthcare system for the purpose of data-stealing by any means they should be charged with penalties or imprisonment.

4. Healthcare Data Protection Legislation and Framework

In developed countries, there are data privacy and protection laws implemented to securely process citizens' personal data. In this section, we discuss some of them briefly to highlight their aims and features. These laws and legislations are compared with each other to see how they provide security features at different layers of the proposed healthcare architecture. Implementation of IoT data privacy regulations is very important for legal matters, human rights, and social norms. Generally, IoT data privacy regulations are required to support core privacy goals like fairness, purpose satisfaction, proportionality, and accountability. Government and private organizations can work together to achieve these goals. American, European, and other leading countries' law enforcement organizations are working to find a common ground for solving healthcare data privacy problems while also making a more effective existing legal framework. An effective legal framework should ensure the user's awareness and their control over the IoT healthcare products with their services. Compliance with other international data privacy frameworks makes it more adequate [6,69].

4.1. Major Healthcare Initiative

A brief overview of healthcare initiatives related to data protection, for different regions, is given below.

4.1.1. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was enacted by the US government to implement the security and privacy of healthcare data for American citizens. It has separate rule sets for security and privacy. The privacy rules enable the privacy of the health data to protect the data from disclosure. The security rules provide security of the individuals' health information by adopting advanced technologies to acquire more efficient means of patient care. The HIPAA security and privacy rules are implemented to healthcare and non-healthcare organizations that store, transmit, and process healthcare data of US citizens by any means.

The privacy rule protects the following health information processed by concerned entities:

- Common Identifier (e.g., name, address, birth date);
- Past, present, or future physical and mental health or condition;
- Past, present, or future payment provision for healthcare;
- Provision of healthcare to individuals.

The mentioned entities are allowed to be processed or disclosed for research and public interest and should have the authorization to process or disclose health information except for treatment purposes, like payment and relevant health care operations.

The Security Rule protects personal health information that has been created, received, transmitted, and managed electronically. These security rules have the following characteristics:

- Making sure of the integrity and availability of personal healthcare information;
- Detects and protects against known threats to confidentiality, integrity, and availability;
- Protect against processes not permitted and the disclosure of information.

The security rule requires the administrative protection of management processes personnel. Proper administrative controls should be maintained for devices and personnel. This rule also includes audit control, access control, integrity control, and transmission security.

4.1.2. The Health Information Technology for Economic and Clinical Health Act (HITECH)

The Health Information Technology for Economic and Clinical Health Act (HITECH) is an extension of security and privacy guidelines described in HIPAA signed in 2009. However, it has not been completely enforced in the healthcare industry. It only provides legal liability for noncompliance. Besides applying the HIPAA rules, it is responsible for the notification of breaches and unauthorized access to healthcare data. It enables individuals with a right to get their electronic healthcare data and they can grant privileges to others to receive healthcare information [70].

4.1.3. Personal Information Protection and Electronic Document Act (PIPEDA)

The federal government of Canada introduced the Personal Information Protection and Electronic Document Act (PIPEDA) in 2001. Its main purpose is to provide individuals control, to some extent, over their personal information by enforcing policies on organizations that process and disclose the personal information of Canadian citizens. These policies include informing citizens concerning personal information processed or disclosed and this information is protected by using adequate security measures. The PIPEDA applies to all personal data, healthcare data, and other data that holds the private information of individuals. If any organization collects data, then it is fully accountable for the protection of the collected data. The PIPEDA is not applicable in all states of Canada. Every province has the right to enforce rules and policies as long as they are similar to PIPEDA [71]. PIPEDA provides basic guidelines to organizations for collecting and processing personal information for business purposes. The interconnected devices should use the security standards of data privacy principles according to PIPEDA.

4.1.4. EUROHEALTH

In late 1990, the WHO Regional Committee for Europe established a healthcare program called EUROHEALTH. It provides medium-term needs for the Countries of Central and Eastern Europe (CCEE) for material, managerial, and technical resources for long-term health strategies. The primary objectives of this program are to make collaborative agreements with CCEE, fundraising, and coordination with international organizations. The program's work has generated an information flow for better cooperation and coordination between all the organizations working in the health sector. This program is realistic, flexible, and accessible to the CCEE [72].

4.1.5. General Data Protection Regulation (GDPR)

In May 2018, a new General Data Protection Regulation (GDPR) replaced directive 95/46 [73], consolidating and innovating data protection rules. The introduced GDPR is considerably more comprehensive and establishes requirements for internal compliance mechanisms that did not exist in the legislation. It applies to all sectors of the economy, all broadly defined personal data, and every sector that controls or processes data. Moreover, it applies protective standards throughout the lifespan of the data. GDPR is designed to enable people to better control their data. Although the EU already established its data protection directive in 1995, it was not completely reasonable for all the member states of the EU. To remove all the reservations, the GDPR has been established and is applicable throughout the EU.

The liability of the GDPR's impact is likely to be for health organizations, hospitals, and other healthcare organizations that process healthcare data. GDPR requires accountability for how healthcare data is processed. Data controllers are not only responsible for the compliance, but processors are also accountable for any data breach of their work and direction. Furthermore, health organizations will need to be clearer and attentive in profiling data processing activities and will require their staff to ensure a secure flow of data [74].

4.1.6. The Privacy Act (Australia)

It entails the set of principles of Australian legislation to protect the personal information of Australian citizens. These principles refer to the usage, storage, and disclosure of personal information. Moreover, individuals have the right to the access and correction of their personal information. This law also includes data security, data quality, and cross-border data flow policies [75].

Healthcare data is a subset of personal information and needs extra security policies and protection. All organizations that provide a health service and hold health information (other than an employee record) are covered by the Privacy Act, whether or not they are small businesses. In certain circumstances, the Privacy Act permits the handling of health information and personal information for health and medical research purposes, where it is impracticable for researchers to obtain individuals' consent.

4.1.7. Saudi Health Information Exchange Policies (SHIEP)

The main objective of this policy is to present the permissible usage of the KSA (Kingdom of Saudi Arabia) health information exchange like patient care, public health, and quality. This policy applies to all individuals and organizations who have access to the Saudi Health Information Exchange managed records such as participating healthcare subscribers, business associates, health information services providers, and subcontractors [76].

Personal Health Information (PHI) will be available for treatment, healthcare operations, and public health, but it may be permitted for research and education. This policy shall not permit the usage of healthcare information for market studies and legal investigation or inquiry.

Table 4 presents a comparison of regulations in light of the proposed five layers architecture for IoHT. It is interesting to observe that none of the above regulations are providing security at the intermediate and feedback layer. However, both these layers are vulnerable to data leakage threats due to human intervention accessibility to physical devices.

Table 4. Comparison of Healthcare Regulations.

Regulation	Country/ Region	Device Layer	Protocol Layer	Intermediate Layer	Management Layer	Feedback Layer
HIPAA	America	Yes	Yes	No	Yes	No
PIPEDA	Canada	Yes	No	No	No	No
EURO HEALTH	EU	Yes	No	No	No	No
GDPR	EU	Yes	Yes	No	No	No
The Privacy Act	Australia	Yes	Yes	No	No	No
SHIEP	KSA	Yes	Yes	No	Yes	No

4.2. Data Protection Issues/Aspects Not Covered in Healthcare Laws

There are various issues and aspects of IoHT that are not covered in the already discussed legislative initiatives.

Big Data Issues Integrating healthcare data notably raises security and privacy issues. Patient information is processed at different levels of security in data centers. In America, most organizations have HIPAA certification, but this does not guarantee a patient's record safety because HIPAA is more inclined towards ensuring security policies rather than implementation. Moreover, the transmission of large data sets from different locations poses an extra burden on processing and storage. Conventional security solutions are inadequate for large and inherently changing data sets. With the emergence of cloud healthcare solutions, security demands are becoming more complex and there are no specified policies written in existing healthcare data protection laws [77].

Data Governance related to the governance of healthcare data should be the initial step in managing healthcare data. It is due to the need of moving the healthcare industry towards a value-based business model. It demands common data representation that encircles different security standards (e.g., ICD, CPT, and LOINC) [78]. Currently, data generated in the healthcare industry is diverse and would demand a proper governance model. There are no policies for healthcare data standardization and normalization for proper data governance.

Privacy-preserving analytics in the healthcare industry is grasping IoT devices to monitor and transmit vitals to healthcare clouds. Therefore, it needs to process and analyze data in an ad-hoc decentralized manner. However, the execution of resource-exhausting operations with privacy preservation is becoming a challenge. As new healthcare data analytics are becoming popular, healthcare data privacy laws need revision, and new laws should be drafted to illustrate all processes involved in the usage of patients' private data.

Identification of the Relevant Privacy Violation privacy in IoT-based devices can be violated at many stages. Firstly, it is violated by collecting data by third parties. Secondly, the usage and distribution of private data, and thirdly, the data is combined with other data. The third possibility is not known by the users who are using IoT-based medical devices to process and generate data. By combining newly generated information with existing data about a patient or health activity, it raises the high commercial value for many data-hungry organizations and commercial firms. Most of the data is often generated by automated medical devices, therefore, a higher trust level should be maintained for this data than on manually entered human data. This is important because medical insurance companies are monitoring the health conditions of their customers with the help of medical devices to ascertain the specific risks associated with their customer's health. These devices are also tracking users' geo-locations and such data must be protected through adequate device safety measures as well as legislative limitations on data usage.

Data and context quality are mostly overlooked issues even if these facts play a significant role in the privacy debates in the context of IoT. The quality of data highly depends on the environment in which it is collected. The quality of context may be unknown where there is no or incomplete information about the context. It may also be ambivalent as there is a chance of contradictory information from different context sources. Context quality generates new problems of confidentiality that have not been addressed by current research. Context quality is related to the information that is not to be processed by hardware components that likely provide the information. It is better to protect context quality as it is sensitive information. Change in context quality is also sensitive information. IoT devices generate data based on context and do not allow users to shut down the system or to easily disconnect from it.

To enhance transparency of the healthcare systems, not only healthcare data that is propagated from different devices need to be controlled, but also the data generated automatically by the healthcare devices need to be managed. Despite this important issue, no law has been made in this regard. There is a need to develop a combined approach with technical standards and existing regulatory frameworks to ensure data transparency.

Privacy violating interactions and presentation in IoT-based healthcare applications like heartbeat monitors, geo-tracking devices, automated insulin pumps, and other healthcare devices envisage and require strong interaction with the patient. In such devices, the information will be provided through sensors or other recorded medical device readings. This information goes through different devices to reach its ultimate destination and becomes a threat to privacy when this sensitive information is exchanged through different systems. In smart cities, for instance, an individual could make a query for the way to a specific health clinic. Such a query should not be answered, for instance, by showing the way to a health clinic nearby, visible to any passerby, another example of such medical devices that do not encrypt data while transmitting to the remote server. Any adversary intending to sniff that data could easily use this information for a malicious purpose. Due to the close interaction and presentation techniques, the threat of privacy-violating interaction and presentation is a major challenge in healthcare laws.

Life cycle transition privacy is compromised when private information is disclosed by IoT devices during the life cycle transition. These devices hold information like vital sign readings, drug dosage, and actuator functions. Healthcare data is highly sensitive, but also the collection of simple usage data (e.g., location, duration, frequency) could disclose a lot about the life cycle of people. Despite evident problems with healthcare devices, the life cycle transition problem has never been addressed. The life cycle of healthcare devices is still modeled as buy-once-own-forever and solutions have not evolved beyond a total memory wipe (e.g., before selling a wearable) or physical destruction. There is a need to identify the requirements for flexible solutions to implement convenient privacy life cycle management mechanisms.

Linkage refers to the linkage of different previously separated systems like combining forms of revealed data sources. When data is gathered from different sources with different permissions and contexts it causes loss of context and poor judgment. Threats of linking different systems and data sources are not novel. Online social networks and integrated third-party applications are facing the same problems. However, IoT networks and services rely on the interaction and collaboration of many coequal systems. Managing the numerous devices in IoHT systems and their connectivity with other systems will raise more challenges in linkage threats. The threat of linkage will cause problems in the IoT evolution process. There are mainly two reasons for it. First, the horizontal linkage of different companies and manufacturers systems to create a heterogeneous distributed system-of-systems delivering new services that no single system can provide. Successful linkage will make data exchange more agile and controllable between different parties. However, horizontal linkage also causes more local data flows than vertical linkage that could improve privacy. These problems should be properly addressed in IoT healthcare laws to prevent passive monitoring and intrusive data collection by IoT devices.

4.3. IoHT Governance Challenges

Based on the analysis of the major global healthcare initiatives, we identified the following IoHT governance challenges that hinder the widespread adoption of IoHT systems.

4.3.1. Conflicts in Laws

After the implementation of the General Data Protection Regulation (GDPR) for the enforcement of data security and privacy, standards have been widened. For the protection of European citizens' data outside of Europe, their data is allowed to be used under strict conditions: If any data privacy legislation enacted by a non-EU country accepts Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR). These terms and conditions cause challenges for developing countries because BCR's and SCC are time-consuming and costly [79].

A country may or may not have a law for user data protection, but the healthcare system should follow the laws of the country from which the user belongs. The same thing applies to the social and cultural norms, which should be applied according to the laws of the state to which the user belongs. In the case of data residing on cloud servers, again, the privacy laws will be applied according to the region of the patients.

4.3.2. Data Protection Issues in Healthcare Systems

The above discussion leads us to find the four major issues in protecting healthcare data from the national policy level to an organizational level. These issues are (i) the absence of laws for healthcare data protection, (ii) the use of non-standard healthcare devices and communication protocols by a healthcare facility, (iii) compliance issues to implement healthcare policies locally, (iv) and the absence of a dedicated enforcement agency for inspection and to deal with complaints and violations [80].

4.3.3. Absence of Conflict of Laws for Healthcare Data Protection

As we have discussed, the most common reason for violations in healthcare laws is the absence of law in many developing countries. There is no law for healthcare data protection, therefore, patients' data can be used by the government and private agencies. They use patients' medical records for research purposes without their consent. No monitoring facility can ensure the integrity of the medical records after being used by these organizations.

4.3.4. Non-Standard Healthcare Devices and Protocols

The development and production process of various smart devices over a short period reduces the security considerations. Small businesses have less expertise and resources in terms of security implementations and testing the devices as well as applications for the healthcare domain. Usage of non-standard healthcare devices and protocols is the major concern of healthcare data privacy and protection, which, in context, is the usage of locally manufactured healthcare devices that do not have sufficient security features according to healthcare standards. Most of these devices are unable to update or patch against new threats and attacks. There must be some laws and policies included in these healthcare care laws that declare guidelines for manufacturing healthcare devices and security features must be included in them [81].

4.3.5. Other Considerations

Apart from the above-mentioned challenges, there are several local issues worth consideration for the adoption of IoHT governance initiatives.

- Awareness: There is a lack of awareness among the users of healthcare systems about the importance of the security of healthcare data;
- System Management Staff: Most of the time healthcare data is processed and forwarded by system management staff in healthcare institutes. They work on intermediate devices like data servers and gateway devices. The staff is not qualified enough to understand the complexities of data privacy and legal aspects. They are unaware of the latest threats because their primary tasks are network configurations and the availability of data at the endpoints. Mostly, they do not update healthcare systems and leave them unpatched until an issue is raised. They have little exposure to awareness programs and practices for data security and privacy;
- Doctors and Healthcare staff: One of the critical facts is not knowing much about the security and privacy laws of healthcare data by the healthcare staff and emergency response teams in hospitals. Specifically, the doctor uses personal devices such as cell phones or laptops to view the data, therefore, these personal devices also need to be secure. Moreover, they are not even familiar with the consequences of healthcare data leakage. There is no proper framework implemented that enforces healthcare staff to follow rules and policies to share and process patients' healthcare data legally and securely;
- Patients: These are the central entities in the healthcare system. However, they are less attractive to attackers due to having less information i.e., about themselves only. They are conscious about their privacy and all these legalities are there to protect their healthcare privacy. However, they do not have any idea about how their data is shared with other organizations and what their rights are regarding their healthcare data. If their data is shared without conferring with them, it begs the question of what the legal liberties are that can be taken by concerned organizations about data sharing;
- Enforcement Difficulties: There is no enforcement authority or body established that helps to enforce data privacy laws in the healthcare sector. All the healthcare institutes should be obliged to follow instructions by some authority. The authority should implement healthcare laws;
- Low Budget: In developing countries, the medical budget is very limited. The trend of using IoHT devices is emerging in big cities. Mostly, there is no central system or facility provided to facilitate data privacy in developing countries. A very low or limited budget is allocated for new and innovative technologies in the healthcare sector. Therefore, the authorities consider that there is no need to enforce data privacy policies if the usage of such devices is limited;
- Lack of Qualified Staff: The IT staff does not configure/enable security functions in IoHT due to inadequate qualifications and expertise. The main reason behind it is the lack of security training programs for medical staff. They are only interested in the functional requirements of medical devices but do not take care of non-functional requirements of a medical device like communication security and data privacy;
- No Internal Auditing: There is no IoHT audit like IT audit, conducted in healthcare organizations and hospitals. If any organization is processing healthcare data, then it

is unlikely to make checks and balance the healthcare data. The internal audit ensures what data is being processed by which organization for what purposes. The auditing activities reduce the risk of data leakage and unauthorized usage;

- No Special Enforcement Authority: One of the difficulties in the enforcement of data privacy laws and regulations is the absence of special enforcement authorities in the healthcare sector. Formation and implementation of data privacy laws should be the primary responsibilities of the authority. It can also ensure the compliance of state-level or national-level policies with international policies.

5. Recommendations

After careful analysis of data privacy and protection policies and compliance issues for IoHT-based systems, some recommendations can assist in improving this system. These recommendations assist in resolving healthcare data security problems due to compliance issues between different legal frameworks.

- Fines and Penalties: IoT devices gather a huge amount of information and there are several privacy risks associated with the usage and access of the data. Specifically, individual identification and behavior monitoring are major concerns. As the usage of IoT devices is increasing in the healthcare sector, a huge amount of private data is processed and stored. There is a need to introduce new privacy safeguards. The health information collected from devices like Fitbit/Jawbone [82] can be used to detect disease correlations with new treatment options with remote monitoring;
- Data Anonymization: IoT devices gather most of the data aggregated from the environment and forward it via a router or intermediate device for processing. During this process, several protocols and compression schemes are used as the storage space on the devices is limited and cannot handle big headers like that used for Internet Protocol IPv6. This data is sanitized as closely as possible to the device that created it since this communication avoids safety risks;
- Healthcare System Design: The healthcare system should be designed in such a way that it provides the controls in a user-friendly manner. An end-user must have full control over his/her collected data at any moment i.e., to whom it can be or cannot be shared. At any moment, the user should be given the possibility to know and control who has his data, what data have been collected, and for what purposes they will be used for the legitimate initial purpose;
- Privacy by Design: Privacy embedded into the design is an essential component integrated into the whole IoHT core system. The privacy safeguard framework must be implemented from the beginning of the system engineering process. The healthcare devices operate with user interactions or web interfaces. There are no privacy protection guidelines available while designing device interfaces. There are several vulnerabilities in web-based interfaces that are prone to data leakage and information leakage attacks. Most of the devices do not have authentication features or have default passwords that are difficult to enter due to their small size interfaces;
- Communication Security: There are several communication protocols used in IoT healthcare devices. There are no specific guidelines provided in data privacy laws about protocol security or what type of encryption or anonymity standards should be adopted for IoT devices, which operate on low memory and computation resources. These privacy laws should provide transparent policies about the communication security of these devices, especially for use in hospitals;
- Dispute Resolution: There is a need to resolve regional and international disputes regarding data protection. There are different versions of healthcare data privacy laws enforced regionally and internationally. If the healthcare data of a citizen is processed in a different country or state where different data privacy laws are enforced, then what are the possible legal issues that should apply to that person's processed data? These types of disputes should be resolved in the national healthcare policies;

- Awareness Programs: Awareness programs are very significant to highlight the importance of data privacy, especially in the healthcare sector. IT staff, management staff, and other related staff of a healthcare facility should be aware and carry out the practices of secure processing of healthcare data. They must be aware of the consequences in the case of data leakage and what penalties they would be charged in the case of carelessness. Doctor and emergency response teams should be trained for the secure usage of their devices (i.e., laptops and cellphones, etc.) linked to healthcare systems, and they should share their experiences and difficulties while using these devices securely with healthcare organizations.

6. Conclusions

In this paper, we presented a detailed IoHT classification along with the general architecture of IoHT systems. The architecture aids in highlighting data security and privacy challenges. Along with discussion about the known security vulnerabilities, we also discussed the healthcare regulations and affiliated issues. We also highlighted major reasons causing the failure of data protection and possible points of data leakage in IoHT systems. The study also discussed and compared various data protection regulations and highlighted their limitations. Lastly, we proposed some recommendations regarding data privacy and security for IoHT implementations. We believe this research will help the industrial and governing bodies to design and implement IoT-enabled healthcare systems while protecting the security and privacy of individuals.

As future work, we plan to explore cybersecurity risk assessment approaches with respect to IoHT to aid organizations and governments in better protecting themselves against pertinent risks. The risk with simply extending existing assessment methodologies will be possibly being blind to new risks arising in the healthcare ecosystem. These risks could be related to the high sensitivity of healthcare data, the flow of information, and compliance with regional and global regulatory approaches.

Author Contributions: J.S. and R.A. were involved in the conceptualization of the key idea; A.K.K. and T.A. helped with the methodology and defining the contents of the paper; J.S., R.A., A.K.K. and T.A. were involved in the writing—original draft preparation; J.S., R.A., A.K.K., T.A., S.S. and A.M.A. were involved in reviewing and editing. The improvements in the write-up were contributed to by all. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University for funding this project.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. *International Telecommunication Union Yearbook of Statistics, 1991–2000*; ITU: Geneva, Switzerland, 2001.
2. Ahmad, T.; Ranise, S. Validating Requirements of Access Control for Cloud-Edge IoT Solutions (Short Paper). In *International Symposium on Foundations and Practice of Security*; Springer: Cham, Switzerland, 2018.
3. Culler, D.; Chakrabarti, S.; Infusion, I.P. 6LoWPAN: Incorporating IEEE 802.15. 4 into the IP Architecture, IPSO Alliance; White Paper. 2009. Available online: https://www.omaspecworks.org/wp-content/uploads/2018/03/6lowpan.pdf (accessed on 1 October 2021).
4. Al Alkeem, E.; Yeun, C.Y.; Zemerly, M.J. Security and privacy framework for ubiquitous healthcare IoT devices. In Proceedings of the 10th IEEE International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 8–10 December 2015; pp. 70–75.
5. Miorandi, D.; Sicari, S.; de Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad. Hoc. Netw.* **2012**, *10*, 1497–1516. [CrossRef]
6. Porambage, P.; Ylianttila, M.; Schmitt, C.; Kumar, P.; Gurtov, A.; Vasilakos, A.V. The quest for privacy in the internet of things. *IEEE Cloud Comput.* **2016**, *3*, 36–45. [CrossRef]

7. Solanas, A.; Patsakis, C.; Conti, M.; Vlachos, I.S.; Ramos, V.; Falcone, F.; Postolache, O.; Pérez-Martínez, P.A.; Di Pietro, R.; Perrea, D.N.; et al. Smart health: A context-aware health paradigm within smart cities. *IEEE Commun. Mag.* **2014**, *52*, 74–81. [CrossRef]
8. Martinz-Ballest, A.; Pérez-Martínez, P.A.; Solanas, A. The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Commun. Mag.* **2013**, *51*, 136–141. [CrossRef]
9. Eckhoff, D.; Wagner, I. Privacy in the smart city- applications, technologies, challenges, and solutions. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 489–516. [CrossRef]
10. Alghanim, A.A.; Rahman, S.M.M.; Hossain, M.A. Privacy analysis of smart city healthcare services. In Proceedings of the 2017 IEEE International Symposium on Multimedia (ISM), Taichung, Taiwan, 11–13 December 2017; pp. 394–398.
11. Storm, D. MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks Computer World. 2015. Available online: https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html (accessed on 1 October 2021).
12. McMahon, E.; Williams, R.; El, M.; Samtani, S.; Patton, M.; Chen, H. Assessing medical device vulnerabilities on the Internet of Things. In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; pp. 176–178.
13. Wang, L.; Ali, Y.; Nazir, S.; Niazi, M. ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods. *IEEE Access* **2020**, *8*, 152316–152332. [CrossRef]
14. Rahman, M.A.; Hossain, M.S.; Showail, A.J.; Alrajeh, N.A.; Alhamid, M.F. A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city. *Sustain. Cities Soc.* **2021**, *72*, 103083. [CrossRef]
15. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and provenance enhanced Internet of health things framework: A blockchain managed federated learning approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef]
16. Ketu, S.; Mishra, P.K. Mishra Internet of Healthcare Things: A contemporary survey. *J. Netw. Comput. Appl.* **2021**, *192*, 103179. [CrossRef]
17. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Comput. Secur.* **2021**, *111*, 102491. [CrossRef]
18. Somasundaram, R.; Thirugnanam, M. Review of security challenges in healthcare internet of things. *Wirel. Netw.* **2021**, *27*, 5503–5509. [CrossRef]
19. Sivan, R.; Zukarnain, Z.A. Security and Privacy in Cloud-Based E-Health System. *Symmetry* **2021**, *13*, 742. [CrossRef]
20. Parashar, A.; Rishishwar, S. Security challenges in IoT. In Proceedings of the Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 27–28 February 2017; pp. 446–449.
21. Morghan, H.; Hashmi, U.S.; Imran, A. Edge computing in smart health care systems: Review, challenges, and research directions. *Trans. Emerg. Telecommun. Technol.* **2019**, e3710. [CrossRef]
22. Cao, Y.; Hou, P.; Brown, D.; Wang, J.; Chen, S. Distributed analytics and edge intelligence: Pervasive health monitoring at the era of fog computing. In Proceedings of the 2015 Workshop on Mobile Big Data (Mobidata), Hangzhou, China, 21 June 2015.
23. Hu, R.; Pham, H.; Buluschek, P.; Gatica-Perez, D. Elderly people living alone: Detecting home visits with ambient and wearable sensing. In Proceedings of the 2nd International Workshop on Multimedia for Personal Health and Health Care (MMHealth), Mountain View, CA, USA, 23 October 2017.
24. Baktir, A.C.; Tunca, C.; Ozgovde, A.; Salur, G.; Ersoy, C. SDN-based multi-tier computing and communication architecture for pervasive healthcare. *IEEE Access* **2018**, *6*, 56765–56781. [CrossRef]
25. Brito, C.; Pinto, L.; Marinho, V.; Paiva, S.; Pinto, P. A Review on Recent Advances in Implanted Medical Devices Security. In Proceedings of the 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), 2021, Chaves, Portugal, 23–26 June 2021; pp. 1–6. [CrossRef]
26. Thakar, A.T.; Pandya, S. Survey of IoT enables healthcare devices. In Proceedings of the 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 18–19 July 2017.
27. Li, X.; Huang, X.; Li, C.; Yu, R.; Shu, L. EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems. *IEEE Access* **2019**, *7*, 22011–22025. [CrossRef]
28. Perez, A.J.; Zeadally, S. Recent Advances in Wearable Sensing Technologies. *Sensors* **2021**, *21*, 6828. [CrossRef] [PubMed]
29. Qu, Y.; Zheng, G.; Ma, H.; Wang, X.; Ji, B.; Wu, H. A Survey of Routing Protocols in WBAN for Healthcare Applications. *Sensors* **2019**, *19*, 1638. [CrossRef]
30. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
31. Saboor, A.; Mustafa, A.; Ahmad, R.; Khan, M.A.; Haris, M.; Hameed, R. Evolution of Wireless Standards for Health Monitoring. In Proceedings of the 2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON), Jaipur, India, 13–15 March 2019; pp. 268–272. [CrossRef]
32. Saboor, A.; Ahmad, R.; Ahmed, W.; Kiani, A.K.; Moullec, Y.L.; Alam, M.M. On Research Challenges in Hybrid Medium-Access Control Protocols for IEEE 802.15.6 WBANs. *IEEE Sens. J.* **2019**, *19*, 8543–8555. [CrossRef]
33. Taleb, H.; Nasser, A.; Andrieux, G. Wireless technologies, medical applications and future challenges in WBAN: A survey. *Wirel. Netw.* **2021**, *27*, 5271–5295. [CrossRef]

34. Hämäläinen, M.; Paso, T.; Mucchi, L. ETSI SmartBAN in Medical IoT. In Proceedings of the 2021 XXXIVth General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS), Rome, Italy, 28 August–4 September 2021. [CrossRef]
35. Negra, R.; Jemili, I.; Belghith, A. Wireless body area networks: Applications and technologies. *Procedia Comput. Sci.* **2016**, *83*, 1274–1281. [CrossRef]
36. Khajenasiri, I.; Zhu, P.; Verhelst, M.; Gielen, G. A low-energy ultra-wideband internet-of-things radio system for multi-standard smart-home energy management. *IEIE Trans. Smart Process. Comput.* **2015**, *4*, 354–365. [CrossRef]
37. Mukherjee, A.; Ghosh, S.; Behere, A.; Ghosh, S.K.; Buyya, R. Internet of Health Things (IoHT) for personalized health care using integrated edge-fog-cloud network. *J. Ambient. Intell. Hum. Comput.* **2021**, *12*, 943–959. [CrossRef]
38. Mamdouh, M.; Awad, A.I.; Hamed, H.F.A.; Khalaf, A.A.M. Outlook on Security and Privacy. In *IoHT: Key Challenges and Future Vision, Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV 2020). Advances in Intelligent Systems and Computing, Cairo, Egypt, 8–10 April, 2020*; Hassanien, A.E., Azar, A., Gaber, T., Oliva, D., Tolba, F., Eds.; Springer: Cham, Switzerland, 2020; p. 1153. [CrossRef]
39. Meyer, J.; Kazakova, A.; Büsing, M.; Boll, S. Visualization of complex health data on mobile devices. In Proceedings of the 2016 ACM Workshop on Multimedia for Personal Health and Health Care (MMHealth), Amsterdam, The Netherlands, 16 October 2016.
40. Rolim, C.O.; Koch, F.L.; Westphall, C.B.; Werner, J.; Fracalossi, A.; Salvador, G.S. A cloud computing solution for patient's data collection in health care institutions. In Proceedings of the 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine, St. Maarten, The Netherlands, 2–16 October 2010.
41. Perera, C.; McCormick, C.; Bandara, A.K.; Price, B.A.; Nuseibeh, B. Privacy-by-design framework for assessing internet of things applications and platforms. In Proceedings of the 6th International Conference on the Internet of Things, Stuttgart, Germany, 7–9 November 2016; pp. 83–92.
42. Stork, M.; Vancura, V. Hidden pacemaker pulses detection based on wavelet and Hilbert-Huang transform. In Proceedings of the IEEE International Conference on Applied Electronics, Pilsen, Czech Republic, 9–10 September 2014; pp. 285–288.
43. Samani, M.M.; Mahnam, A. Design and implementation of an ultra low power wireless neuro-stimulator system. In Proceedings of the 17th Iranian Conference of Biomedical Engineering (ICBME), Isfahan, Iran, 3–4 November 2010; pp. 1–4.
44. Lucisano, J.Y.; Routh, T.L.; Lin, J.T.; Gough, D.A. Glucose monitoring in individuals with diabetes using a long-term implanted sensor/telemetry system and mode. *IEEE Trans. Biomed. Eng.* **2016**, *64*, 198–1993.
45. Hiremath, S.; Yang, G.; Mankodiya, K. Wearable internet of things: Concept, architectural components and promises for person-centered healthcare. In Proceedings of the International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), Athens, Greece, 3–5 November 2014; pp. 304–307.
46. Birgit, L.; Andrei, P. ActiGait®: A Partly Implantable Drop-Foot Stimulator System. In *Introduction to Neural Engineering for Motor Rehabilitation*; Farina, D., Jensen, W., Akay, M., Eds.; IEEE: Piscataway, NJ, USA, 2013; pp. 421–423.
47. Hansen, J.H.; Ali, H.; Saba, J.N.; Charan, M.R.; Mamun, N.; Ghosh, R.; Brueggeman, A. Cci-mobile: Design and evaluation of a cochlear implant and hearing aid research platform for speech scientists and engineers. In Proceedings of the 2019 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Chicago, IL, USA, 19–22 May 2019; pp. 1–4.
48. Caffey, S.; Po-Ying, L.; Jeffrey, B. Remote-Controlled Drug Pump Devices. U.S. Patent 8,285,328, 9 October 2012.
49. Zhao, Y.; Wang, J.; Zhang, Y.; Liu, H.; Chen, Z.A.; Lu, Y.; Dai, Y.; Xu, L.; Gao, S. Flexible and Wearable EMG and PSD Sensors Enabled Locomotion Mode Recognition for IoHT Based In-home Rehabilitation. *IEEE Sens. J.* **2021**, *21*, 26311–26319. [CrossRef]
50. Rao, S.; Dubey, S.; Deb, S.; Hughes, Z.; Seo, Y.S.; Nguyen, M.Q.; Tang, S.J.; Abell, T.; Lahr, C.; Chiao, J.C. Wireless gastric stimulators. In Proceedings of the Texas Symposium on Wireless and Microwave Circuits and Systems, Waco, TX, USA, 3–4 April 2014; pp. 1–4.
51. Zareei, M.; Zarei, A.; Budiarto, R.; Omar, M.A. A comparative study of short range wireless sensor network on high density networks. In Proceedings of the 17th Asia-Pacific Conference on Communications, APCC, Sabah, Malaysia, 2–5 October 2011; pp. 247–252.
52. Fouladi, B.; Ghanoun, S. *Security Evaluation of the Z-Wave Wireless Protocol*; Black Hat: Las Vegas, NV, USA, 2013; Volume 24, pp. 1–2.
53. Fatima, I.; Ahmad, A.; Ali, S.; Ali, M.; Baig, M. ITriple-Band circular polarized antenna for WLAN/WiFi/Bluetooth/WiMAX applications. *Prog. Electromagn. Res. C* **2021**, *109*, 65–75. [CrossRef]
54. Varshney, G.; Gupta, H. A security framework for IOT devices against wireless threats. In Proceedings of the 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, India, 10–11 August 2017; pp. 1–6.
55. Xie, L.; Yang, G.; Mantysalo, M.; Xu, L.L.; Jonsson, F.; Zheng, L.R. Heterogeneous integration of bio-sensing system-on-chip and printed electronics. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2012**, *4*, 672–682. [CrossRef]
56. Lindquist, A.; Johansson, P.; Petersson, G.; Saveman, B.I.; Nilsson, G. The use of the personal digital assistant (PDA) among personnel and students in health care: A review. *J. Med. Internet Res.* **2008**, *10*, e1038. [CrossRef]
57. Jung, J.Y.; Lee, J. Automatic discovery and installation of wearable bio signal devices in ubiquitous healthcare system. In Proceedings of the 9th International Conference on Advanced Communication Technology, Gangwon, Korea, 12–14 February 2007; pp. 412–414.
58. da Costa, C.A.; Pasluosta, C.F.; Eskofier, B.; da Silva, D.B.; Righi, R.d. Internet of health things: Toward intelligent vital signs monitoring in hospital wards. *Artif. Intell. Med.* **2018**, *89*, 61–69. [CrossRef]

59. Rajit, N.; Thanachayanont, A. A 1-V CMOS low-power resistor-based temperature sensor for human body temperature monitoring. In Proceedings of the 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), JeJu, Korea, 23–26 June 2019; pp. 1–4.
60. Yousefzadeh, B.; Shalmany, S.H.; Makinwa, K.A. A BJT-based temperature-to-digital converter with inaccuracy from −55 °C to +125 °C in 0.16. *IEEE J. Solid State Circuits* **2017**, *52*, 1044–1052. [CrossRef]
61. Bai, B.; Nazir, S.; Bai, Y.; Anees, A. Security and provenance for Internet of Health Things: A systematic literature review. *J. Softw. Evol. Process.* **2021**, *33*, e2335. [CrossRef]
62. Esha, N.H.; Tasmim, M.R.; Huq, S.; Mahmud, M.; Kaiser, M.S. Trust IoHT: A Trust Management Model for Internet of Healthcare Things. In Proceedings of the International Conference on Data Science and Applications, Kolkata, India, 10–11 April 2021; 2021; pp. 47–57.
63. MacDermott, A.; Kendrick, P.; Idowu, I.; Ashall, M.; Shi, Q. Securing things in the healthcare internet of things. In Proceedings of the Global IoT Summit (GIoTS), New York, NY, USA, 7–21 June 2019; pp. 1–6.
64. Baccelli, E.; Hahm, O.; Günes, M.; Wählisch, M.; Schmidt, T. OS for the IoT-goals, challenges, and solutions. In Proceedings of the Interdisciplinaire sur la Sécurité Globale (WISG2013) Workshop, Troyes, France, 22 January 2013; pp. 1–6.
65. Chung, B.; Kim, J.; Jeon, Y. On-demand security configuration for IoT devices. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 19–21 October 2016; pp. 1082–1084.
66. 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.* **2018**, *6*, 1606–1616. [CrossRef]
67. Foukia, N.; Billard, D.; Solana, E. PISCES: A framework for privacy by design in IoT. In Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 706–713.
68. van Rest, J.; Boonstra, D.; Everts, M.; van Rijn, M.; van Paassen, R. Designing privacy-by-design. In Proceedings of the 1st Annual Privacy Forum, Lecture Notes in Computer Science, Limassol, Cyprus, 10–11 October 2012; Springer: Berlin/Heidelberg, Germany, 2012; Volume 8319, pp. 55–72.
69. Weber, R.H. Internet of things-new security and privacy challenges. *Comput. Law Secur.* **2010**, *26*, 23–30. [CrossRef]
70. Neuhaus, C.; Polze, A.; Chowdhury, M.M. *Survey on Healthcare IT Systems: Standards, Regulations and Security*; University Potsdam: Potsdam, Germany, 2011.
71. Swartz, N. Canada reviews PIPEDA. *Inform. Manag.* **2007**, *41*(2), 8.
72. Danzon, M.; Litvinov, S.K. EUROHEALTH Programme. *World Health Stat. Q. Rapp. Trimest. De Stat. Sanit. Mond.* **1993**, *46*, 153–157.
73. de Hert, P.; Papakonstantinou, V. The proposed data protection regulation replacing directive 95/46/EC: A sound system for the protection of individuals. *Comput. Law Secur. Rev.* **2012**, *28*, 130–142. [CrossRef]
74. Georgiou, D.; Lambrinoudakis, C. Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR). *Information* **2020**, *11*, 586. [CrossRef]
75. Maeve, M. E-government in Australia: The challenge to privacy of personal information. *Int. J. Inf. Technol.* **2002**, *10*, 327.
76. Balkhair, A. Kingdom of Saudi Arabia The National eHealth Program. 2014. Available online: https://www.itu.int/ITU-D/cyb/events/2012/e-health/Nat_eH_Dev/Session%204/KSA-MOH-Presentation-SaudiArabia%20FINAL.pdf (accessed on 1 October 2021).
77. Zheng, M. Surveillance and disease control in COVID-19: Big data application in public health. In *Proceeding of the International Conference on Applications and Techniques in Cyber Security and Intelligence, Fuyang, China, 19–21 June 2021*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 565–570.
78. Overhage, J.M.; Ryan, P.B.; Reich, C.G.; Hartzema, A.G.; Stang, P.E. Validation of a common data model for active safety surveillance research. *J. Am. Med. Inform. Assoc.* **2012**, *19*, 54–60. [CrossRef]
79. Mattoo, A.; Meltzer, J.P. International data flows and privacy: The conflict and its resolution. *J. Int. Econ. Law* **2018**, *21*, 769–789. [CrossRef]
80. Hemalatha, P. Monitoring and securing the healthcare data harnessing IOT and blockchain technology. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 2554–2561.
81. Lydahl, D. Standard tools for non-standard care: The values and scripts of a person-centred assessment protocol. *Health* **2021**, *25*, 103–120. [CrossRef] [PubMed]
82. Huang, Y.; Xu, J.; Yu, B.; Shull, P.B. Validity of FitBit, Jawbone UP, Nike+ and other wearable devices for level and stair walking. *Gait Posture* **2016**, *48*, 36–41. [CrossRef] [PubMed]