sensors

MDPI

*Article*

# Sensors for Context-Aware Smart Healthcare: A Security Perspective

**Edgar Batista [1,2], M. Angels Moncusi [1], Pablo López-Aguilar [3] and Antoni Martínez-Ballesté [1] and Agusti Solanas [1,*]**

[1] Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Av. Països Catalans 26, 43007 Tarragona, Spain; edgar.batista@urv.cat (E.B.); angels.moncusi@urv.cat (M.A.M.); antoni.martinez@urv.cat (A.M.-B.)

[2] SIMPPLE S.L., C. Joan Maragall 1A, 43003 Tarragona, Spain

[3] Anti-Phishing Working Group EU, Av. Diagonal 621–629, 08028 Barcelona, Spain; pablo.lopezaguilar@apwg.eu

* Correspondence: agusti.solanas@urv.cat

check for updates

**Citation:** Batista, M.; Moncusi, A.M.; López-Aguilar, P.; Martínez-Ballesté, A.; Solanas, A. Sensors for Context-Aware Smart Healthcare: A Security Perspective. *Sensors* **2021**, *21*, 6886. https://doi.org/10.3390/s21206886

Academic Editor: Joel J. P. C. Rodrigues

Received: 27 September 2021
Accepted: 14 October 2021
Published: 17 October 2021

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

**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

**Abstract:** The advances in the miniaturisation of electronic devices and the deployment of cheaper and faster data networks have propelled environments augmented with contextual and real-time information, such as smart homes and smart cities. These context-aware environments have opened the door to numerous opportunities for providing added-value, accurate and personalised services to citizens. In particular, smart healthcare, regarded as the natural evolution of electronic health and mobile health, contributes to enhance medical services and people's welfare, while shortening waiting times and decreasing healthcare expenditure. However, the large number, variety and complexity of devices and systems involved in smart health systems involve a number of challenging considerations to be considered, particularly from security and privacy perspectives. To this aim, this article provides a thorough technical review on the deployment of secure smart health services, ranging from the very collection of sensors data (either related to the medical conditions of individuals or to their immediate context), the transmission of these data through wireless communication networks, to the final storage and analysis of such information in the appropriate health information systems. As a result, we provide practitioners with a comprehensive overview of the existing vulnerabilities and solutions in the technical side of smart healthcare.

**Keywords:** smart healthcare; context-aware environments; user-centric sensors; contextual sensors; Internet of Medical Things; wireless body area networks; information security

## 1. Introduction

Smart healthcare (s-health for short) [1] is a paradigm that advocates for the provision of healthcare services through the use of context-aware environments, equipped with complex sensors, infrastructures and communications networks. From sensors and IoT devices to ubiquitous services and decision-making systems, a plethora of information sources provide data able to augment knowledge on patients, their health status and their context, in order to make better decisions, diagnostics and treatments. The technological landscape is, hence, a key enabler of s-health.

During the early 2000s, the synergies between ICTs and medicine and healthcare practice rapidly converged and enabled a key cornerstone in this field: electronic healthcare (e-health) [2]. The e-health paradigm allowed the provision of online medical treatments and disease management, the sharing of electronic health records in a standardised way, and rapid communications between patients and practitioners, among others. Subsequently, with the generalised use of mobile devices (particularly, smartphones), a novel patient-centric highly-personalised healthcare paradigm emerged: mobile healthcare (m-health) [3]. M-health, considered a linchpin of the provision of today's healthcare services, streamlines communications between patients and practitioners, and enables remote-monitoring and self-monitoring. Today, many mobile devices, namely smartphones, smartwatches and fitness trackers, already incorporate many sensors for health-oriented purposes.

With the steady implementation of ICTs in the healthcare domain, cities have also started equipping their infrastructures with ICTs to face important demographic challenges such as the growth of the world's population and the increase in life expectancy. As a result of the progressive integration of sensors in our daily lives, homes, buildings and transportation systems, healthcare facilities and cities as a whole are provided with smart and cognitive capabilities able to collect and analyse vast amounts of heterogeneous data under real-time constraints. The ubiquity and communication capabilities of these environments lead to context-awareness, i.e., environments capable of adapting themselves to users' needs. The meaningful exploitation of user-centric data in combination with contextual data opened the door to smart healthcare services, aiming to acquire advanced high-level knowledge and providing more effective, cost-efficient, personalised and sustainable healthcare models [4–7]. Unlike previous paradigms, s-health was the first paradigm that considered the contextual perspective, so it is seen as a particular case of the e-health and m-health paradigms.

To properly deploy efficient smart healthcare services, stakeholders must be aware of all the concerns surrounding the management of sensor data, including its collection, storage, transmission, analysis and presentation. Nowadays, there exists an overwhelming number and variety of devices with sensing capabilities, with different features, technologies, complexities, dimensions and costs. These sensing devices, able to collect and transmit data from multiple physical locations, are paramount to enable the contextualisation of smart environments, such as smart homes, smart hospitals and smart cities. More specifically, such devices are topologically organised as networks, mostly wireless to endow the system with major flexibility and cost-effectiveness. In this scope, wireless sensor networks (WSNs) and wireless body area networks (WBANs) emerged and attracted the attention of many stakeholders from very different industries, namely healthcare, sport, entertainment, environmental, transportation or manufacturing, among others [8–11]. However, a number of challenges could arise from these communications in terms of throughput, latency, reliability, availability and security.

Concerning the latter, data security stands as one of the most important features in the healthcare domain. Medical data, such as electronic health records, biomedical signals and physiological parameters, are highly sensitive and must be handled with the highest security and privacy standards. Moreover, the high value that such data might generate in the black market motivates attackers to infiltrate themselves into the information systems [12,13]. Despite security safeguards, the history of both communication networks as well as that of the Internet encompasses countless security flaws, vulnerable cryptographic protocols and threatening data breaches. Every information system or communication network is hence virtually prone to be attacked by cybernetic criminals or suffer from irreparable damages because of unintentional human errors. Smart health systems, involving a large number of complex and heterogeneous devices and entities, may present risks from a security and privacy perspective unless properly considered.

The possibilities of s-health applications are many and varied. Hence, facing of all them individually is a daunting task since the use of specific sensors, devices and technologies highly depends on the particular requirements of each application and service. In consequence, the security threats and countermeasures can vary among them. To help readers properly understand all the challenges involved at the time of developing any s-health application, this article adopts a more neutral and high-level approach, by focusing more on the individual actors involved in these scenarios, rather than the very applications. Notwithstanding, numerous examples have been provided to contextualise the topics addressed to the smart health domain. All things considered, it is essential to provide a comprehensive approach to the realistic deployment of smart healthcare services. To this end, the following aspects must be considered:

- The complete variety of attributes related to people's health status and their context must be considered so that the s-health service is as beneficial as possible. Sensing devices must be properly selected in accordance with their inner requirements such as accuracy, reliability, dimensions, computational capabilities, cost or power consumption, among others.
- Proper communication technologies must be favoured according to the specifications of the sensing devices and considering the complex nature of WSNs and WBANs. Scalability, density, coverage area and security are important aspects to be taken in mind for communications.
- All s-health-related ICT components must meet with the highest security requirements to thwart malicious activities. All in all, information security and data privacy, as well as the adequate protection of devices, networks and services, is first and foremost.

There is plenty of literature related to IoT, WBANs and their security concerns. The article in [14] reviewed the most recent sensing techniques for monitoring health conditions, including flexible electronics and textile-based wearables. Similarly, the work in [15] also analysed wearable, non-invasive sensors to monitor vital signs. From a more practical approach, the authors in [16] provided a comprehensive review on the benefits and opportunities of using IoT and wearables in health-oriented applications. In [17], the authors presented a comprehensive survey and classification of commercially available wearables and research prototypes. The articles in [18–20] presented the most common technologies for WBANs and contextualised their applicability in the health domain. In [17,21], the authors presented a comprehensive survey of the attacks and countermeasures to WBANs.

Inspired by this research, this article contextualises all these elements into the smart healthcare paradigm and provides a more comprehensive approach within this domain considering the data life-cycle, from its collection, going through its transmission, to its final exploitation. Often forgotten, this article also surveys the sensors and security concerns related to contextual sensing, a required dimension in smart health. To the best of our knowledge, this is the first article to present a concise and comprehensive review of all the aforementioned smart healthcare research. Therefore, with the aim of contributing to the proper deployment of secure smart health systems, this article provides a down-to-earth landscape of the sensors and communication technologies that could be used to enable these scenarios. More specifically, the contribution of this article is three-fold. First, we provide a detailed review and characterisation of sensors, either user-centric or contextual, that enable smart healthcare services. Second, we discuss the most common wireless communication technologies that allow those sensors to interoperate and transfer the sensed information in a secure manner. Furthermore, third, we also elaborate on the most serious vulnerabilities and threats in such settings, and suggest the corresponding countermeasures. All in all, we hope that this article helps technicians, practitioners, stakeholders and researchers to set the grounds for more secure and private context-aware environments and smart healthcare services.

The rest of the article is organised as follows. Section 2 provides a thorough overview of the sensors used for gathering user and context attributes that are of interest for smart health purposes. Then, Section 3 describes a three-tier WBAN architecture for deploying complex s-health services, and summarises the most relevant wireless communication technologies enabling this architecture. Then, Section 4 analyses the main security aspects associated with smart healthcare environments by discussing the main threats, vulnerabilities and possible countermeasures. Considering the previous observations, Section 5 provides an extensive discussion on open issues and research opportunities to be addressed in the future. Finally, the article closes in Section 6 with some final remarks.

## 2. Sensors: Definition and Taxonomy

Advancements in microelectronics and manufacturing technologies have enabled the development of a large variety of sensors, embedded in electronic small-scale devices, with high sensitivity, low energy consumption and contained costs. This section elaborates on the different sensors to be considered within the s-health paradigm. Sensors are categorised into two groups according to the nature of the sensor data: user-centric data, i.e., referring to personally identifiable individuals; and contextual data, i.e., referring to the context or the immediate environment. Table 1 summarises all the sensor data described in this section.

**Table 1.** Taxonomy of the attributes to be considered for smart health.

| **User-Centric** | | **Contextual** | |
|---|---|---|---|
| Heart rate | Blood oxygen | Air temperature | Air humidity |
| Blood pressure | Blood glucose | Barometric pressure | Air pollution |
| Body temperature | Skin temperature | Water contamination | Acoustic contamination |
| Respiratory rate | Brain activity | Electromagnetic radiation | Seismic activity |
| Muscular activity | Electrodermal activity | | |
| Hydration | Location | | |
| Body motion | | | |

### *2.1. User-Centric Sensors*

User-centric sensors aim to acquire specific data related to the individuals themselves. Within this context, most of these data relate to medical data such as biosignals (i.e., physiological parameters), health status and health conditions. Moreover, sensors collecting the location or the body movements of individuals are also of interest to contextualise individuals. All these sensors have already been seamlessly integrated within wearable devices, whose popularity has grown during the last decade as part of the IoMT technology [14,15,22]. In particular, wearable technology has revolutionised ubiquitous computing with low-cost yet powerful devices, including body-worn accessories, smart textiles, garments, on-skin tattoos, ingestible sensors and implantable appliances, among others [17,23]. This technology, capable of monitoring, analysing and transmitting individuals' data, opens the door to numerous healthcare opportunities, ranging from the remote or self-monitoring of patients' health to the early detection of medical complications. All in all, the generalised use of wearables is contributing to reducing healthcare expenditure and shortening medical times, which leads to more sustainable healthcare models. This section reviews some of the most common methods for the sensing of user-centric attributes (Figure 1) which are summarised in Tables 2–7.

#### 2.1.1. Cardiovascular Activity

Cardiovascular diseases are the first cause of mortality worldwide, responsible for one third of all global deaths [24]. Therefore, the gathering of cardiovascular parameters—namely heart rate, blood pressure, oxygen saturation and blood glucose concentration—has become commonplace in many wearable and IoMT devices [25] (see Table 2). The continuous monitoring of these parameters contributes to cardiac rehabilitation recovery [26] and to early detect abnormal conditions (e.g., tachy/bradycardia, hyper/hypotension, hyper/hypoglycemia...) that might lead to cardiovascular emergencies, such as arrhythmia, stroke or even death [27,28].

One of the most commonly measured vital signs is the heart rate (or pulse), i.e., the number of heartbeats per minute. Electrocardiography (ECG), photoplethysmography (PPG), ballistocardiography (BCG) and phonocardiography (PCG) are common methods of heart rate sensing [29]. On the one hand, ECG sensors record the electrical activity and rhythm of the heart, in the form of electrocardiograms, by attaching a series of electrodes to the skin. Traditional ECG monitoring uses Holter monitors, well-known medical portable units, able to capture long recording periods (from days to weeks) in both home and hospital environments. Despite the high reliability of these devices, they are quite obstructive, invasive and uncomfortable due to their wired architecture. To overcome this, wireless ECG monitoring solutions integrated in wearable devices have already been proposed [30–33]. Alternatively, heart rate data can also be acquired using optical PPG methods by means of pulse oximeter sensors, which measure the intensity of an LED light reflected or transmitted through the skin affected by the changes in the blood volume during each heartbeat. Due to the low-cost and non-invasive nature of this method, most wearables, fitness trackers and commercial devices opt for PPG methods [34–36]. However, the accuracy of PPG measurements is strongly affected by several factors including the measurement procedure, environmental factors and skin pigmentation, among others, and post-processing techniques are desirable to enhance quality [37–39]. Finally, body motion-based BCG methods [40] and sound-based PCG methods [41] are less prominent in wearables. Monitoring a heart's rhythm is particularly important in at-risk patients who may sometimes require an immediate response in a proactive fashion. Hence, actuators are likely to play a key role in the years to come. Today, wearable, non-invasive and non-implantable cardioverter-defibrillators are already a reality [42–44].

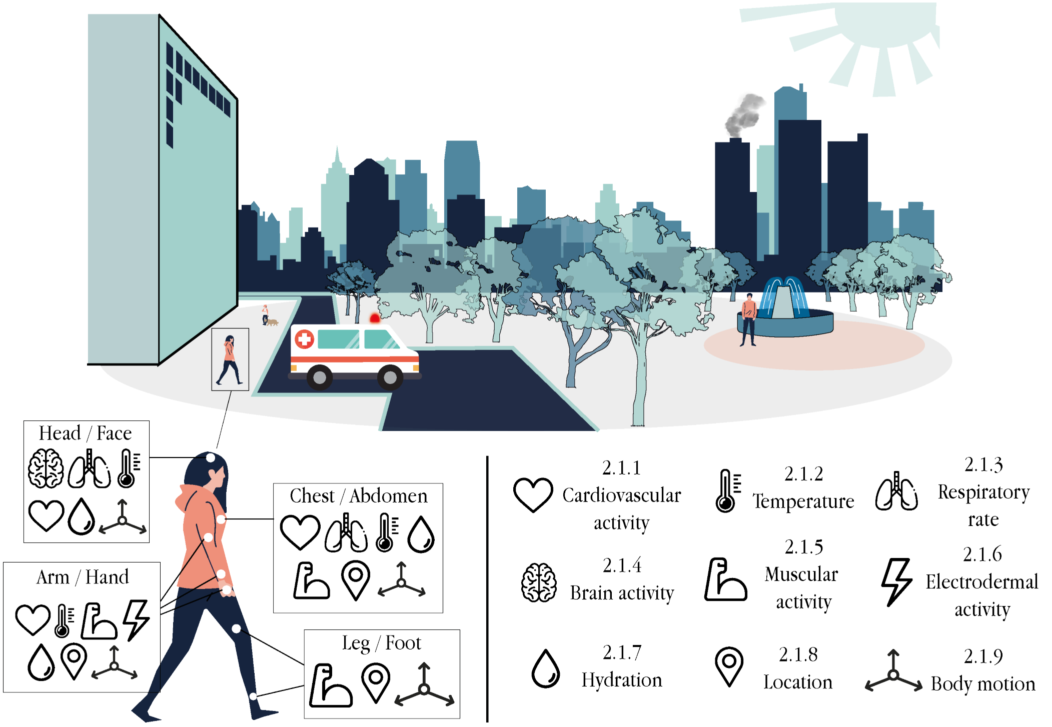

**Figure 1.** User-centric attributes for smart healthcare: each icon, representing the sensors of an attribute, is assigned to a part of the body where that attribute can be collected.

Another popular measurement is the blood oxygen level, which indicates how well the oxygen is distributed to every cell, tissue and organ. Monitoring this attribute is fundamental for people suffering from blood disorders (e.g., anaemia), circulatory problems or respiratory diseases (e.g., asthma and COPD) in order to prevent shortness of breath, hypoxia or cyanosis. The most accurate method to measure the blood oxygen level is the arterial blood gas (ABG) test which analyses blood samples using specific analyser devices. However, this procedure is invasive and painful and it is typically conducted in hospital settings only. More aligned with the smart healthcare paradigm is the use of PPG-based oximeter sensors, already used for heart rate sensing, to measure the blood oxygen saturation ($SpO_2$). Compared to ABG tests, this method is simpler, cheaper, non-invasive and non-painful, but slightly less accurate [45,46]. Many wearables have been designed to monitor this attribute from different parts of the body, such as the wrist, ear and finger [47–50], and even using smart textiles [51].

**Table 2.** Characteristics of the methods for cardiovascular activity sensing.

| Attribute | Method | Sensor | Device/ Wearable | Location | Properties | Suitable for Smart Health |
|---|---|---|---|---|---|---|
| Heart rate | Traditional ECG | Skin electrodes | Holter monitor | Chest | ✓ Accuracy<br>∼ Cost<br>∼ Cont. monit.<br>× Non-invasive | × |
| Heart rate | Wireless ECG | Skin electrodes | Patch<br>Band<br>Textile | Chest<br>Arm | ✓ Accuracy<br>∼ Cost<br>✓ Cont. monit.<br>∼ Non-invasive | ✓ |
| Heart rate | PPG | Pulse oximeter | Smartwatch<br>Wristband<br>Ring | Wrist<br>Finger | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Heart rate | BCG | Tilt<br>Force<br>Pressure | Patch | Chest | × Accuracy<br>∼ Cost<br>∼ Cont. monit.<br>✓ Non-invasive | ∼ |
| Heart rate | PCG | Sound | Microphone<br>Smartphone<br>Electronic stethoscope | Chest | × Accuracy<br>✓ Cost<br>∼ Cont. monit.<br>✓ Non-invasive | ∼ |
| Blood oxygen | ABG | Chemical | Chemical analyser | Arm<br>Wirst | ✓ Accuracy<br>× Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Blood oxygen | PPG | Pulse oximeter | Smartwatch<br>Strap<br>Band<br>Textile | Wrist<br>Earlobe<br>Finger | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Blood pressure | Traditional | Pressure | Sphygmomanometer | Arm | ✓ Accuracy<br>✓ Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Blood pressure | PTT<br>(ECG and PPG) | Pulse oximeter<br>Electrodes | Smartwatch<br>Band<br>Patch | Wrist<br>Arm<br>Ear<br>Chest | ✓ Accuracy<br>∼ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Blood glucose | Traditional (chemical) | Electrochemical | Glucose meter | Finger | ✓ Accuracy<br>✓ Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Blood glucose | Epidermal chemical | Electrochemical | Wristband<br>Patch<br>Tattoo | Wrist<br>Arm | ∼ Accuracy<br>∼ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Blood glucose | Optical spectroscopy | Photo-sensor<br>Infrared | Wristband<br>Patch | Wrist<br>Finger<br>Earlobe | ∼ Accuracy<br>∼ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |

Cardiovascular activity monitoring also considers blood pressure, i.e., the force with which the blood moves through the circulatory system. High blood pressure, called hypertension, is a serious cardiovascular risk with no warning symptoms (popularly known as a "silent killer") that must be fought with healthy lifestyles. Cuff-based sphygmomanometers are the traditional in-hospital devices to measure this attribute. Although they are cheap, accurate and even available in portable electronic devices for home monitoring, they are invasive and unsuitable for outdoor usage, long-term monitoring no real-time monitoring. To overcome this, sensing technologies have contributed to developing non-mechanical and non-invasive solutions [52]. Among others, accurate blood pressure results can be estimated from the pulse transit time (PTT) measure obtained from the combination of PPG and ECG signals [53–55]. Many devices, including smartphones, smartwatches, bands and patches have been designed to this aim [56–59].

Finally, blood glucose concentration is crucial for the management of diabetes. Unless properly managed, diabetic people may experience severe or tragic consequences. Therefore, many m-health applications have emerged with the aim to monitor, suggest and engage diabetic people with their treatment [60–62]. Traditionally, blood glucose is measured using glucose meters, portable devices with electrochemical sensors that chemically analyse a blood drop, typically obtained from the fingertip. Although these devices are easy to use, cheap and accurate, they are invasive and do not provide continuous monitoring. For an s-health oriented approach, several electrochemical-based sensor solutions were implemented in wearable patches, tattoos and implantable sensors [63–65]. Optical-based measurements, already used to measure other attributes, have also been proven for blood glucose monitoring through spectroscopy techniques and infrared technology. Although results are less accurate, solutions are far less invasive and obstructive [66,67]. Complementary to these sensors, diabetes management can reach a higher dimension, by actively monitoring blood glucose in diabetic patients and deliver, when necessary, insulin through in-body insulin pump actuators [68].

### 2.1.2. Temperature

The body temperature (or core temperature) is an indicator of the overall physiological status of an individual and helps determine illnesses such as hypothermia, fever, heat stroke or circulatory shock, among others. Unfortunately, standard medical measurements using thermometers are invasive, obstructive and not aligned with s-health solutions. Nevertheless, these measurements can be estimated in a less-invasive way from one's skin temperature, i.e., the temperature of the outermost surface of the body, generally obtained from the wrist, arm, armpit, chest or forehead [69] (see Table 3).

Thermistors, thermocouples and optical methods are common means of measuring skin temperature [70]. In particular, thermistor sensors are generally popular, cost-efficient and ideal for many wearables, yet their accuracy is influenced by a number of factors including the measurement's location (e.g., wrist, forehead, etc.), ambient temperature (e.g., hot or cold environment), sensor strain, sweating and the distance between the sensor and skin [71–75]. Optical methods, based on FBG or infrared technology, are quite similar to thermistors in terms of accuracy, comfortability and cost [76]. On the other hand, thermocouples' sensors, despite also being cost-efficient, have worse accuracy than the previous methods. Although many sensors have been integrated in traditional wearables, further non-intrusive and more comfortable solutions for temperature sensing have already been proposed by means of stretchable and flexible patches [77–79] and smart textiles [51,76,80,81].

### 2.1.3. Respiratory Rate

The number of breathing cycles per minute determines the respiratory rate, one of the main vital signs of the human body and a clear indicator of overall health. Monitoring this attribute helps identify or keep track of disorders, such as asthma attacks, panic attacks, sleep apnoea, shortness of breath, COPD, pneumonia or anaemia. Although variations can be caused due to the age or the physical activity, abrupt or prolonged abnormal respiration rates can lead to permanent injury or death [82]. In contrast to other vital signs, the recording of one's respiratory rate is less automated (see Table 4). The gold standard technique for its measurement consists of counting the number of times that one's chest or abdomen rises during one minute while the patient is resting. This manual technique is insufficient for smart health.

**Table 3.** Characteristics of the methods for temperature sensing.

| Attribute | Method | Sensor | Device/ Wearable | Location | Properties | Suitable for Smart Health |
|---|---|---|---|---|---|---|
| Body temperature | Traditional<br>(chemical) | Mercury | Mercury-in-glass thermometer | Oral<br>Rectal | ✓ Accuracy<br>✓ Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Skin temperature | Electrical | Thermistor | Patch<br>Band | Arm<br>Chest<br>Ear<br>Forehead | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Skin temperature | Electrical | Thermocouple | Patch<br>Band | Arm<br>Chest<br>Ear<br>Forehead | × Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ∼ |
| Skin temperature | Optical | FBG<br>Infrared | Smartwatch<br>Band<br>Patch<br>Textile | Wrist<br>Chest<br>Ear<br>Forehead | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |

More automated, the most popular monitoring methods are contact-based, i.e., the sensor directly contacts the skin [83]. Breathing can be monitored considering the expansion and contraction movements of the chest walls using strain sensors (e.g., resistive, capacitive and inductive sensors) [84,85], transthoracic impedance sensors [86–88], or motion sensors (e.g., IMUs, later introduced in Section 2.1.9) [89,90]. In general, this technique provides notable accuracy (even though body motion artefacts and environmental factors can diminish the quality) and the small dimensions, low power consumption and contained costs of these sensors facilitate their integration into wearable devices and textiles to be minimally intrusive [91–94].

Further contact-based methods exist for respiratory rate sensing, although they might be less accurate or more obstructive in smart health. For instance, acoustic methods, which aim to characterise the respiratory sounds using microphones [95–97], are promising and suitable in wearable devices, however, unfortunately, they are extremely susceptible to environmental noise, so they should only be considered under very controlled scenarios. Furthermore, one's respiratory rate can also be measured according to the temperature difference between the inhaled air and the exhaled air, by means of electric-based temperature sensors such as thermistors, thermocouples and pyroelectric sensors, placed close to the nose or the mouth [98]. However, this method is quite obstructive and also extremely sensitive to environmental factors. Similarly, inhaled and exhaled air can also be compared in terms of humidity. In this context, electric-based sensors—such as capacitive and resistive sensors—are common, although solutions based on nanoparticles and fibre-optic technology are gaining increasing importance [99]. However, as before, intrusiveness and sensitivity to external factors make this method only suitable for controlled scenarios. Last, there is a growing interest in modulating the cardiac activity recorded from ECG and PPG signals to measure the respiratory rate [100–103]. The lowly invasive, low energy consumption and reduced cost of this method have fostered research in this direction to overcome the main limitations of the aforementioned methods.

Another group of monitoring methods are contactless, i.e., the sensor does not directly contact the skin, which are more comfortable solutions which facilitate long-term monitoring and monitoring during sleep [104]. The main drawback of such methods is their noise sensitivity to environmental or motion artefacts, so they should only be considered under very constrained environments. Most contactless methods are based on camera sensing, which estimate the respiration rate by tracking one's chest movements [105,106]. Other methods have proposed infrared thermal imaging sensors to detect the temperature fluctuations during the respiration cycle [107] or ultrasonic proximity sensors [108,109]:

**Table 4.** Characteristics of the methods for respiratory rate sensing.

| Attribute | Method | Sensor | Device/ Wearable | Location | Properties | Suitable for Smart Health |
|---|---|---|---|---|---|---|
| Respiratory rate | Traditional (observation of chest or abdomen) | - | - | - | ✓ Accuracy<br>✓ Cost<br>× Cont. monit.<br>✓ Non-invasive | × |
| Respiratory rate | Chest wall strain | Resistive<br>Capacitive<br>Inductive | Patch<br>Belt<br>Textile | Chest | ✓ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Respiratory rate | Electrical impedance | Impedance | Patch<br>Belt<br>Textile | Chest | ✓ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Respiratory rate | Motion (contact) | IMU | Patch<br>Belt<br>Textile | Chest<br>Abdomen | ✓ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Respiratory rate | Acoustic | Microphone | Microphone<br>Headset | Nose<br>Mouth<br>Chest | × Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>∼ Non-invasive | ∼ |
| Respiratory rate | Air temp. (electrical) | Thermistor<br>Thermocouple<br>Pyroelectric | Headset<br>Patch | Nose<br>Mouth | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>∼ Non-invasive | ∼ |
| Respiratory rate | Air humid. (electrical) | Capacitive<br>Resistive<br>Nanocrystal | Headset<br>Patch | Nose<br>Mouth | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>∼ Non-invasive | ∼ |
| Respiratory rate | Cardiac act. modulation | Pulse oximeter<br>Electrodes | Smartwatch<br>Band<br>Patch | Wrist<br>Chest | ✓ Accuracy<br>∼ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Respiratory rate | Motion (contactless) | Camera | RGB camera<br>Smartphone | - | ∼ Accuracy<br>✓ Cost<br>× Cont. monit.<br>✓ Non-invasive | ∼ |
| Respiratory rate | Thermal imaging | Camera | Infrared camera | - | ∼ Accuracy<br>× Cost<br>× Cont. monit.<br>✓ Non-invasive | ∼ |
| Respiratory rate | Ultrasonic | Ultrasonic prox.<br>Capacitive | Recording device | - | ∼ Accuracy<br>× Cost<br>× Cont. monit.<br>✓ Non-invasive | ∼ |

### 2.1.4. Brain Activity

Neurological disorders are one of the most prevalent disorders in our society, including Alzheimer's disease or other forms of dementia, epilepsy, meningitis, traumatic brain injury and cerebral palsy. Unfortunately, classical brain activity monitoring methods are highly sophisticated and require large and expensive instrumentation. Hence, developing novel methods considering the size, cost and power constraints so as to be integrated into portable and wearable devices is truly challenging (see Table 5).

One of the most popular methods for assessing the quality of brain activity is electroencephalography (EEG) which measures the electrical activity in the brain by placing small electrodes at multiple locations on the scalp. Conventional EEG measurements, conducted in medical facilities, require a head cap with electrodes connected to a recording instrumentation through long wires. Although accurate, this method is significantly obstructive and invasive. To face these shortcomings, wireless technologies have enabled comfortable EEG monitoring using wearable devices [110,111]. Headset-based solutions are the most prominent [112–114], although there less-obstructive wearables also exist which are placed on the forehead [112,115] or the ear [116,117]—even more discreet solutions include temporary tattoos [118]. In addition to EEG, other methods for brain activity monitoring, albeit less frequently integrated in wearable devices due to their complexity, are based on functional near-infrared spectroscopy (fNIRS) for hemodynamic changes [119,120], magnetoencephalography (MEG) considering magnetic fields [121] and positron-emission tomography (PET) [122].

### 2.1.5. Muscular Activity

Monitoring muscular activity can help detect and evaluate the severity of neurodegenerative diseases such as Parkinson's disease, bradykinesia or dyskinesia symptoms [123,124]. Non-invasive wearable sensor technology can be beneficial in the early detection of these disorders in non-diagnosed patients and to remotely monitor the evolution of these conditions in already-diagnosed patients (see Table 5).

The most popular diagnostic procedure to assess the functioning of the muscles and the nerve cells is electromyography (EMG) which measures the electrical signals generated by the muscles during their movement. There are two kind of methods for EMG recordings. On the one hand, intramuscular EMG methods are invasive, potentially painful, and not well aligned with smart healthcare solutions. On the other hand, surface EMG methods are non-invasive procedures that only require placing some patch electrodes on the muscle's skin, facilitating their integration in wearable devices, such as wristbands, armbands, caps or even textiles, to enable long-term monitoring in real-time [125–128], tracking tremor and dyskinesia symptoms [129], preventing falls [130], recognising gestures and activities [131], controlling robotic prosthetics [132–134] and rehabilitation [135,136]. Although more comfortable, the quality of these measurements is affected by the skin's properties, tissue structure, the adherence of the electrodes to the skin and external electromagnetic interference and noise-filtering techniques are required [137].

In addition to electrical measurements, muscular activity can also be measured from a mechanical perspective through mechanomyography (MMG) [138], which measures the mechanical vibrations of muscles' fibres using accelerometers, condenser microphones, piezoelectric pressure sensors or force-sensitive resistors [139]. This method has been widely used to recognise gestures useful for the control of robot prosthetics or for rehabilitation [139–141], as well as to assess muscles conditions [142].

**Table 5.** Characteristics of the methods for brain activity sensing and muscular activity sensing.

| Attribute | Method | Sensor | Device/ Wearable | Location | Properties | Suitable for Smart Health |
|---|---|---|---|---|---|---|
| Brain activity | Traditional EEG | Skin electrodes | Head cap | Scalp | ✓ Accuracy<br>× Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Brain activity | Wireless EEG | Skin electrodes | Headband<br>Headset<br>Tattoo | Scalp<br>Head<br>Forehead<br>Ear | ∼ Accuracy<br>∼ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Brain activity | fNIRS | Optodes | Head cap | Scalp<br>Head | ✓ Accuracy<br>∼ Cost<br>∼ Cont. monit.<br>∼ Non-invasive | × |
| Brain activity | MEG | Optically pumped magnetometeres | Head cap | Scalp<br>Head | ✓ Accuracy<br>× Cost<br>∼ Cont. monit.<br>∼ Non-invasive | × |
| Brain activity | PET | Photosensor<br>Photodiode | Head cap<br>Helmet | Head | ✓ Accuracy<br>× Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Muscular activity | Intramuscular EMG | Monopolar or concentric electrodes | Needle and recording device | Region of interest | ✓ Accuracy<br>× Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Muscular activity | Surface EMG | Skin electrodes | Patch<br>Band<br>Cap<br>Textile | Region of interest | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Muscular activity | MMG | Accelerometer<br>Pressure<br>Force-sensitive | Patch<br>Band | Region of interest | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |

### 2.1.6. Electrodermal Activity

Electrodermal activity (EDA), also known as skin conductance or galvanic skin response, aims to detect changes in the electrical properties of the skin, especially due to sweating. This property, highly valuable in behavioural medicine, allows detecting emotional states, such as stress, anxiety, depression, fatigue or risk [143–145], characterise sleep activity [146,147] and manage the neurological status [148,149].

The instrumentation required to measure EDA is simple and only requires a couple of electrodes placed next to each other on the skin surface, generally the wrist or fingertip (see Table 6). Different types and materials of electrodes are currently being investigated in order to be integrated into wearable devices, considering both signal quality and comfort aspects for long-term monitoring [150]. Although initial devices were wired, many current solutions, based on wristbands [145,151,152] and finger straps [144,153] are already wireless.

### 2.1.7. Hydration

Hydration plays a significant role in people's health status. Hot environments or strenuous physical exercise (e.g., high-performing athletes or military training recruits) can accelerate the appearance of dehydration, a dangerous condition that leads to physical and cognitive performance loss. Furthermore, monitoring the (de)hydration level in elderly people, a very high-risk group, is crucial to prevent their fragile health condition worsening. Prolonged dehydration periods can lead to serious diseases, such as kidney disease, heart diseases or respiratory infections [154,155].

Traditionally, the method to assess dehydration is qualitative, i.e., looking directly at the patient's eyes or lips. To measure the hydration level in a quantitative way, several techniques based on optical spectroscopic, electromagnetic or electrochemical measurements have been proposed [156–159] (see Table 6). Hydration sensors are commonly integrated in stretchable epidermal sensors [156,157,160] and wristbands [155,158], but they have also been successfully designed as patches and headbands [155,158,161], and even integrated in smart textiles [162].

**Table 6.** Characteristics of the methods for electrodermal activity sensing and hydration sensing.

| Attribute | Method | Sensor | Device/ Wearable | Location | Properties | Suitable for Smart Health |
|---|---|---|---|---|---|---|
| Electrodermal activity | Electrical | Skin electrodes (wired) | Smartwatch<br>Band<br>Strap | Wrist<br>Finger | ✓ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>∼ Non-invasive | ∼ |
| Electrodermal activity | Electrical | Skin electrodes (wireless) | Smartwatch<br>Band<br>Strap | Wrist<br>Finger | ✓ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Hydration | Traditional (observation of eyes or lips) | - | - | - | ✓ Accuracy<br>✓ Cost<br>× Cont. monit.<br>✓ Non-invasive | × |
| Hydration | Optical spectroscopy | Infrared | Band<br>Patch<br>Textile | Wrist<br>Arm<br>Head | ✓ Accuracy<br>∼ Cost<br>∼ Cont. monit.<br>✓ Non-invasive | ✓ |
| Hydration | Electromagnetic | Impedance Capacitive | Band<br>Patch<br>Textile | Wrist<br>Arm<br>Head | ∼ Accuracy<br>✓ Cost<br>∼ Cont. monit.<br>✓ Non-invasive | ✓ |
| Hydration | Epidermal chemical | Electrochemical | Band<br>Patch<br>Tattoo<br>Textile | Wrist<br>Arm | ✓ Accuracy<br>∼ Cost<br>∼ Cont. monit.<br>✓ Non-invasive | ✓ |

### 2.1.8. Location

The provision of health services is not restricted to healthcare facilities only. Checking one's health status or collecting physiological parameters either at home or during walks/exercise by means of wearables is commonplace nowadays. Therefore, other non-medical user-related data are a valuable complement to medical data so as to contextualise users. In particular, thanks to the self-location capabilities integrated in most smartphones and smartwatches, location data are extremely valuable to assist at-risk people, including the elderly, children and people with some certain conditions (see Table 7). More specifically, healthcare-oriented LBS can contribute to finding medical assistance nearby, notify the emergency services of the exact location of the emergency, prevent disorientation and wandering episodes, and even provide walking recommendations to foster healthier lifestyles [5,163,164].

People's location is usually determined using GPS, integrated in most smartphones, wearables and IoT devices. This satellite-based technology is highly accurate for deploying smart health services in outdoor environments—although its accuracy deteriorates indoors or under bad weather conditions. Other satellite-based positioning solutions include GLONASS and Galileo, but their availability in mobile device is less popular. Regarding indoor locating, a number of different technologies have been proposed for precise indoor positioning and proximity-based systems, such as Bluetooth Low Energy (BLE) beacons [165], WiFi-based positioning system (WPS) [166], radio frequency identification (RFID) [167] and ultra-wideband (UWB) [168] technologies (further details can be found in Section 3.2). These technologies help locate and keep track of the people's trajectories in indoor environments, such as the elderly in nursing homes or patients in a smart hospital.

#### 2.1.9. Body Motion

Human motion analysis helps physicians and physiotherapists identify abnormal movements and plan and assess the correctness of rehabilitation programmes [169] (see Table 7). More specifically, applications of body motion measurements in healthcare are diverse, including the analysis of gait patterns and the assessment of gait abnormalities [170–172]; the development of corrective posture systems for rehabilitation purposes; enhance athletes' performance [173–175]; the detection of falls (especially for the elderly) [176–178]; and the recognition of gestures and activities [179,180].

Many solutions are based on optical motion capture methods, aiming to track human motions in a 3D space using multiple cameras triangulating markers attached to different parts of the body. Although being largely used in computer-generated special effects in cinema and TV and their high potential, these systems are very complex and require expensive time-consuming operations. Moreover, their use in indoor settings is only feasible under very controlled environments [181,182]. There are alternative optical methods that use RGB-depth cameras that do not require the attachment of markers to the body. Although these methods are more practical and less invasive, they do not provide spatio-temporal information (i.e., there is no way to know whether the gesture is beginning or finishing) and they are also only viable under controlled environments [183–185]. Hence, capturing body motion and human movements in real-life, uncontrolled environments is not straightforward. The use of inertial measurement units (IMUs), which considers a triaxial accelerometer, a triaxial gyroscope and a non-inertial triaxial magnetometer, enable the recreation of the motion of the movements [186]. This method, which works in both indoors and outdoors, can be integrated in wearable devices for enhancing people's comfort while enabling long-term monitoring [170,187,188].

### *2.2. Contextual Sensors*

The deployment of massive networks of IoT devices collecting contextual parameters in real-time has enabled context-aware environments, where smart health applications can be deployed. Whereas this information is rarely used in classical healthcare paradigms, it plays a key role in the s-health paradigm to provide more efficient and effective health services and improve people's health status and welfare. This section reviews the most popular methods for the sensing of contextual attributes (see Figure 2), which are summarised in Table 8–10.

#### 2.2.1. Air Temperature

Air temperature is one of the main contextual parameters contributing to the comfort, welfare and health of people. Extreme temperatures or high temperature variations can have negative consequences for human health. Especially important with the incoming climate change effects, several studies have aimed to establish a relationship between air temperature and the mortality rate [189–192] or the appearance of diseases and disorders [193–196].

There are different types of temperature sensors integrated in a large number and variety of IoT devices [197] (as can be seen in Table 8). Thermocouples are popular sensing solutions due to their contained costs, rapid responses to temperature changes and large range of temperature detection values. However, accuracy is the main drawback of this kind of sensors, and they should not be used when very precise measurements are needed.

Resistance temperature detectors, with a metal core, are more accurate, but their response to temperature changes is slower and their cost is higher compared to other sensors. Similarly, thermistors are low-cost sensors with a ceramic or polymer core that lead to faster responses to temperature changes with notable accuracy. Last, several devices prefer semiconductor-based sensors using integrated circuits because of their low cost, low energy consumption and fair accuracy.

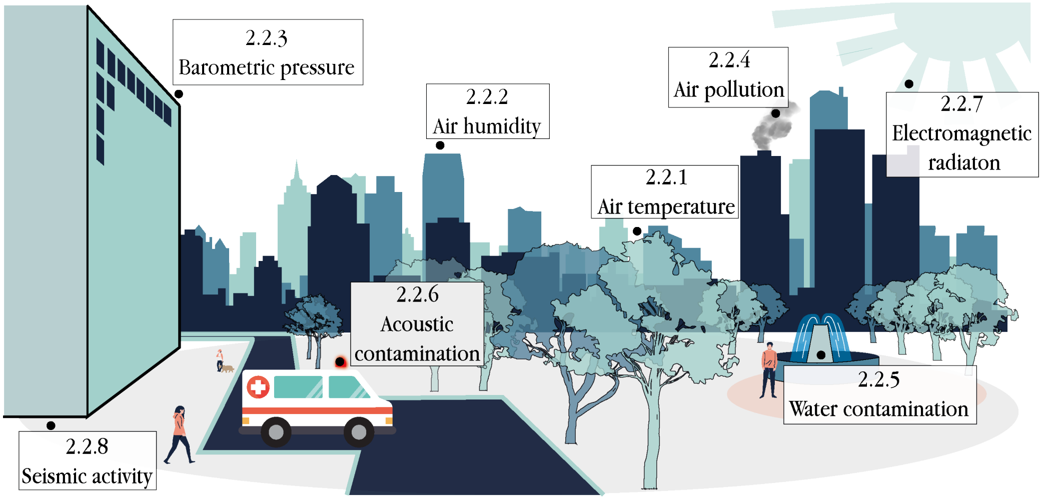

**Figure 2.** Contextual attributes for smart healthcare that can be sensed from context-aware environments.

**Table 7.** Characteristics of the methods for location sensing and body motion sensing.

| Attribute | Method | Sensor | Device/ Wearable | Location | Properties | Suitable for Smart Health |
|---|---|---|---|---|---|---|
| Location | Satellite (outdoor) | GPS<br>GLONASS<br>Galileo | Smartphone<br>Smartwatch<br>Band | Any | ✓ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |
| Location | Proximity (indoor) | BLE beacon<br>WPS<br>RFID<br>UWB | IoT<br>Access point<br>Tag | - | ✓ Accuracy<br>✓ Cost<br>∼ Cont. monit.<br>✓ Non-invasive | ✓ |
| Body motion | Optical motion capture | Camera | Camera<br>Marker | Markers distributed in the body | ✓ Accuracy<br>× Cost<br>× Cont. monit.<br>× Non-invasive | × |
| Body motion | Optical | Camera | RGB-depth camera | - | ∼ Accuracy<br>∼ Cost<br>∼ Cont. monit.<br>✓ Non-invasive | ∼ |
| Body motion | Kinematic | IMU | Band<br>Patch<br>Textile | Region of interest | ∼ Accuracy<br>✓ Cost<br>✓ Cont. monit.<br>✓ Non-invasive | ✓ |

**Table 8.** Characteristics of the methods for air temperature sensing, air humidity sensing and barometric pressure sensing.

| Attribute | Method | Sensor/ Device | Properties | Suitable for Smart Health |
|---|---|---|---|---|
| Air temperature | Electrical | Thermocouple | × Accuracy<br>✓ Cost<br>✓ Response time<br>✓ Energy consumption | ∼ |
| Air temperature | Electrical | Resistance temperature detector | ✓ Accuracy<br>∼ Cost<br>× Response time<br>✓ Energy consumption | ∼ |
| Air temperature | Electrical | Thermistor | ✓ Accuracy<br>∼ Cost<br>✓ Response time<br>✓ Energy consumption | ✓ |
| Air temperature | Electrical | Semiconductor integrated circuit | ∼ Accuracy<br>✓ Cost<br>✓ Response time<br>✓ Energy consumption | ✓ |
| Air humidity | Electrical | Capacitive | ✓ Accuracy<br>× Cost<br>✓ Response time<br>✓ Energy consumption | ∼ |
| Air humidity | Electrical | Resistive | ∼ Accuracy<br>✓ Cost<br>∼ Response time<br>✓ Energy consumption | ✓ |
| Air humidity | Optical | Fibre-optic | ✓ Accuracy<br>× Cost<br>∼ Response time<br>✓ Energy consumption | ∼ |
| Barometric pressure | MEMS | Piezoresistive pressure | ✓ Accuracy<br>✓ Cost<br>✓ Response time<br>✓ Energy consumption | ✓ |

### 2.2.2. Air Humidity

Abnormal humidity values can cause physical discomfort and lead to serious health outcomes [198]. On the one hand, low humidity can cause nasal congestion which increases the risk of flu and other respiratory infections [199,200]. On the other hand, high humidity together with high temperatures can lead to hyperthermia, dehydration, heat exhaustion and heat stroke. Interestingly enough, high humidity also fosters the appearance, growth and spread of bacteria and viruses that can aggravate health conditions, including infectious diseases, allergies and respiratory problems, among others [200,201].

Similarly to air temperature sensing, many IoT devices integrated mechanisms for air humidity monitoring, which can be measured using different types of sensors (see Table 8). Capacitive humidity sensors are commonly used in the market due to their accuracy (although it decreases in extreme environments), small dimensions, low power consumption and wide measurement range. Furthermore, resistive sensors were inexpensive and suitable solutions in non-extreme environments that do not require extremely precise results [202]. More recently, optical methods based on fibre-optic sensors offer several advantages regarding the aforementioned sensors in terms of durability, higher accuracy, reduced temperature dependency and electromagnetic immunity [203,204]. Although this method is less used in commercial devices, its future is encouraging.

### 2.2.3. Barometric Pressure

Differences in barometric pressure because of weather shifts or altitude changes may harmfully affect the human body. Headache, migraine attacks or joint pain, such as arthritis, are common symptoms appearing due to pressure changes [205–208]. Current barometric pressure sensors are based on microelectromechanical systems (MEMS), based on the piezo-resistive effect, which offer high accuracy, low power consumption, low cost and can be manufactured at low cost and small dimensions so that they could be seamlessly integrated into portable IoT devices [209–211] (see Table 8).

### 2.2.4. Air Pollution

Air pollution is a global public health emergency: nine out of ten people breath air containing high levels of pollutants, resulting in the death of approximately seven million people worldwide annually [212]. The most harmful pollutants include particulate matter ($PM_{10}$, $PM_{2.5}$ and $PM_{0.1}$), ozone ($O_3$), carbon monoxide (CO), nitrogen oxide ($NO_2$), sulphur dioxide ($SO_2$), lead, polycyclic aromatic hydrocarbons (PAHs), volatile organic compounds (VOCs) and dioxins, which are more concentrated in large urban areas or industrialised regions. These pollutants contribute to respiratory problems, such as COPD, asthma and bronchitis, cardiovascular diseases, neurological disorders, reproductive dysfunctions, skin diseases and a variety of cancers in long-term exposures [213–216]. Smart health applications can intelligently manage this information to reduce the exposure of citizens to pollutants.

Optical spectroscopy methods are standard analytical techniques to detect gas pollutants in the air, although they are time-consuming, expensive and cannot be used in real-time. More interestingly, for smart health, there are two main low-cost sensing methods for measuring this information more efficiently [217,218] (see Table 9). Commonly used in the industry are metal oxide semiconductor (MOS) sensors, characterised by their low cost, small dimensions, fast response times, low power consumption and high durability. However, they are sensitive to changes in environmental conditions and to interfering gases. Such limitations are overcome using electrochemical sensors, even though their cost and dimension are significantly higher in comparison to MOS sensors [219–221].

### 2.2.5. Water Contamination

In addition to air, water is another vital resource that may contain microbiological or chemical contamination. Poor quality water, especially abundant in low-income countries, can lead to waterborne parasitic infections (e.g., cholera, dysentery and typhoid), chronic diseases, reproductive complications and adverse neurodevelopment procedures [222].

Traditional methods for measuring water quality are based on laboratory chemical analyses of water samples, which are manually collected at various locations and at different time periods. Despite being accurate, this procedure is inefficient, resource-consuming and offline because no real-time information is provided—which is essential to detect outbreaks of contaminated water (see Table 9). To evaluate the quality of water in real-time, electrochemical sensors can monitor changes in water parameters that become affected by chemical and biological pollutants, such as turbidity, free/total chlorine, oxidation-reduction potential, electrical conductivity, pH, nitrates level and temperature [223–225]. Furthermore, further approaches have proposed the detection of floating debris in contaminated water by means of aquatic sensors embedding a CMOS camera [226].

### 2.2.6. Acoustic Contamination

Regular exposure to acoustic contamination, this is, elevated sound levels and environmental noise, can result in adverse health outcomes, including hearing impairments, sleep disturbance, chronic stress and an increased incidence of suffering cardiovascular and metabolic diseases [227–229]. Today, the continuous and real-time monitoring of noise levels is possible using low-cost and small microphones embedded in IoT devices [230,231] (as can be seen in Table 9).

**Table 9.** Characteristics of the methods for air pollution sensing, water contamination sensing and acoustic contamination sensing.

| Attribute | Method | Sensor/ Device | Properties | Suitable for Smart Health |
|---|---|---|---|---|
| Air pollution | Optical spectroscopy | Infrared Fluorescence | ✓ Accuracy<br>× Cost<br>× Response time<br>∼ Energy consumption | × |
| Air pollution | Chemiresistive | MOS | ∼ Accuracy<br>✓ Cost<br>✓ Response time<br>∼ Energy consumption | ✓ |
| Air pollution | Electrochemical | Electrochemical | ✓ Accuracy<br>× Cost<br>✓ Response time<br>✓ Energy consumption | ∼ |
| Water contamination | Traditional (chemical) | In-lab instrumentation | ✓ Accuracy<br>× Cost<br>× Response time<br>× Energy consumption | × |
| Water contamination | Electrochemical | Resistive<br>Capacitive<br>Conductance | ∼ Accuracy<br>∼ Cost<br>✓ Response time<br>✓ Energy consumption | ✓ |
| Water contamination | Optical | CMOS camera | ∼ Accuracy<br>✓ Cost<br>✓ Response time<br>✓ Energy consumption | ✓ |
| Acoustic contamination | Acoustic | Microphone | ✓ Accuracy<br>✓ Cost<br>✓ Response time<br>✓ Energy consumption | ✓ |

### 2.2.7. Electromagnetic Radiation

Electromagnetic radiation has become a popular form of pollution due to the omnipresent telecommunication equipment. In short, two types of radiation exist: non-ionising radiation and ionising radiation. On the one hand, ionising radiation (e.g., Gamma rays, X-rays and higher UV light band) can cause tissue damage since rays contain sufficient electromagnetic energy to detach electrons from atoms or molecules. Numerous studies state the adverse health outcomes due to prolonged exposures to ionising radiation: UV exposures can lead to sunburns, eye damage and skin cancer, X-rays can modify cells' genetic material and cause mutations and cancer and Gamma rays can cause disorders, such as leukaemia and bone, breast and lung cancer. Moreover, syndromes related to the nervous system and neuropsychiatric-related problems, including insomnia, chronic fatigue, sexual dysfunction and memory problems, have also been associated with electromagnetic radiation [232–234]. On the other hand, non-ionising radiation (e.g., radio-frequency, microwaves, infrared, visible light and low UV band) may generate thermal energy and excite molecules, but it does not contain sufficient energy to remove electrons from atoms or molecules [233], although concerns have also been raised about its impact on human health [235].

To protect against radiation exposure, portable and affordable devices are being developed to detect Gamma radiation using Geiger–Müller tubes or fibre-optic radiation sensors [236–240] and to detect infrared and UV lights through optical sensors as well [241] (see Table 10).

### 2.2.8. Seismic Activity

Tremors on the Earth's surface involve seismic activity resulting from natural disasters, such as earthquakes, volcanic eruptions and explosions. Surface vibrations are a common daily phenomenon, but they are imperceptible for humans due to their low intensity and do not suppose an apparent risk. However, sudden high-intensity shakes can produce seismic waves able to collapse buildings and trigger catastrophic consequences for people, including death. Continuous seismic monitoring does not contribute to people's health status per se under normal conditions, but it can be essential for alerting or predicting seismic events so to guarantee people's safety.

Traditional sensing solutions use seismometers, which are reliable and high-performance instruments though nonetheless bulky, expensive and sensitive to electromagnetic interference (see Table 10). In recent years, this activity has being monitored using the inexpensive tri-axial accelerometer sensors that, in combination with machine learning techniques, allows detecting or predicting seismic events [242–244]. Additionally, opto-mechanical sensors based on optical fibre technology have already been assessed to monitor ground motions [245].

**Table 10.** Characteristics of the methods for electromagnetic radiation sensing and seismic activity sensing.

| Attribute | Method | Sensor/ Device | Properties | Suitable for Smart Health |
|---|---|---|---|---|
| Electromagnetic radiation | Electrical | Geiger–Müller tubes | ✓ Accuracy<br>× Cost<br>∼ Response time<br>∼ Energy consumption | ∼ |
| Electromagnetic radiation | Optical | Fibre-optic | ✓ Accuracy<br>∼ Cost<br>✓ Response time<br>∼ Energy consumption | ✓ |
| Seismic activity | Traditional (motion) | Seismometer | ✓ Accuracy<br>× Cost<br>∼ Response time<br>∼ Energy consumption | × |
| Seismic activity | Kinematic | Accelerometer | ∼ Accuracy<br>✓ Cost<br>∼ Response time<br>✓ Energy consumption | ✓ |
| Seismic activity | Optical | Opto-mechanical | ∼ Accuracy<br>∼ Cost<br>∼ Response time<br>✓ Energy consumption | ✓ |

## 3. Communication Architecture and Technologies

Smart healthcare services are not fed from a single sensing device, but from many of them. To ease this management, devices are logically structured as networks, generally wireless. In this scope, WSNs provide a contextualisation-enabling infrastructure within physical environments for real-time applications. For instance, the coverage of a region with a WSN composed of multiple temperature, humidity and air pollution sensors enables the transmission of real-time data to a smart health service aiming to alert nearby patients with respiratory diseases. Despite the huge potential of WSNs as a whole, it is worth mentioning that each single sensor was generally resource constrained in terms of computation, memory, storage and battery capacity. To increase the life expectancy of the sensors and prevent rapid battery depletion, their power consumption must be as low as possible and the implementation of lightweight protocols is a must—this is particularly the case for data transmission, the most energy-consuming task [246,247].

With the rise of wearable technology, WSNs evolved towards a more user-centric approach: WBANs. WBANs are designed to collect user-centric attributes such as physiological parameters, location and motions, and communicate them to external entities to provide efficient, personalised and real-time health services. Furthermore, actuators within WBANs can receive feedback or commands from other devices and act accordingly. For instance, a diabetes-oriented WBAN enables continuous blood glucose monitoring, and when abnormal values are detected, communicates to an external smart healthcare service and/or activates an insulin pump actuator that delivers insulin into the body. WBANs offer enhanced opportunities concerning active patient monitoring, biofeedback, telemedicine and rehabilitation [18] that can irreversibly shift traditional healthcare models. However, in addition to the technical challenges inherited from WSNs (e.g., latency, throughput, energy consumption…), WBANs have to face additional obstacles for their practical adoption, including reliability, accuracy, fault tolerance, interoperability and security, among others [9,19,248]. The non-compliance of these additional requirements can certainly endanger people's health. For example, incorrect medical decisions could be taken in the case of the inaccurate sensing of physiological parameters, or transmitting the information through an insecure communication channel.

### 3.1. WBAN Communication Architecture

The low-power and resource-constrained devices involved in WBANs require communication architectures to transmit data in a time- and energy-efficient manner. Fulfilling all of these conditions is one of the most prominent communication architectures for WBAN, which is based on three tiers [19] (as can be seen in Figure 3):

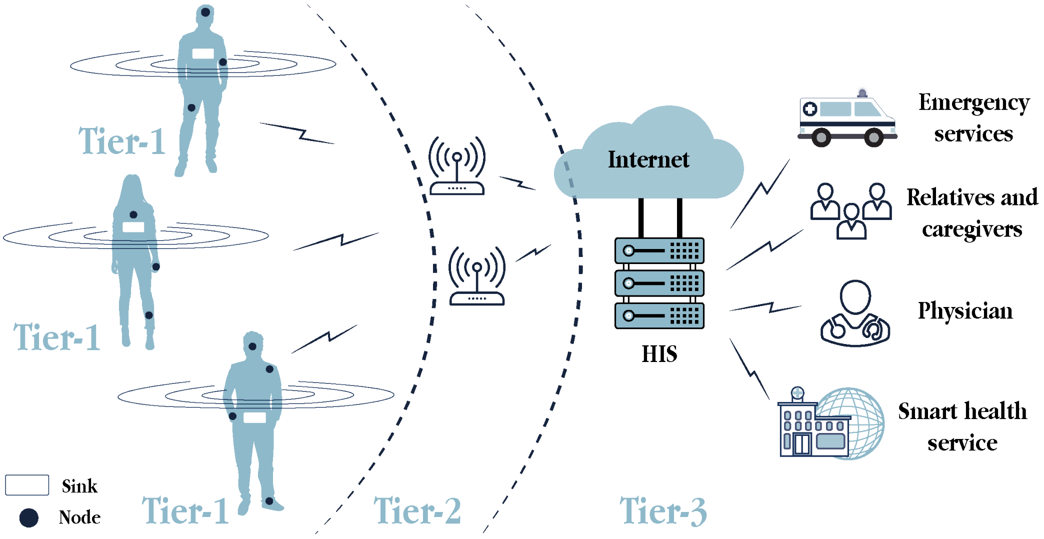

**Figure 3.** Component-based representation of the 3-tier communication architecture for WBANs.

- Intra-WBAN communications (Tier 1): This tier enables communications between the sensors and actuators (i.e., nodes) placed in, on and around the human body, in a range of approximately two meters. In addition to the direct communications among these nodes, they can also communicate with a sink, a portable device attached to the body, to transmit the user-centric data. The sink, which usually refers to a smartphone in the s-health context, is the WBAN coordinator and gateway to the next tier. Short-range and low-energy communication technologies are desirable in this tier.
- Inter-WBAN communications (Tier 2): This tier aims to connect the users' WBANs with external networks that are easily accessible for other users, such as the Internet

and cellular networks. Hence, the communications in this tier take place between the sink and one or more access points, which are gateways to those networks. Large-range communication technologies, such as ZigBee, BLE, Wi-Fi and cellular, were adopted in this tier.

- Beyond-WBAN communications (Tier 3): The communications in this tier refer to those from the health provider. Having received the user-centric data from the previous tier, it was stored in the healthcare information system (HIS) and then, analysed by physicians, medical staff or automatised systems may act accordingly. With the medical records and the profiles of patients, smart healthcare systems can automate real-time diagnosis, adjust medical treatments or alert the emergency services, relatives and caregivers if needed.

Conceptually, four main actors participate in this architecture (see Figure 4). First, as reviewed in Section 2, nodes are a primary information source in s-health systems. Second, these systems are supported by the HIS, responsible for the storage, retrieval, analysis and presentation of all the data in accordance with the services provided. Third, users intended to use the s-health services, either patients and physicians and must be also considered as crucial actors. Furthermore, fourth, all these actors are able to interact among them thanks to the deployment of communications networks, whose technologies are described as follows.

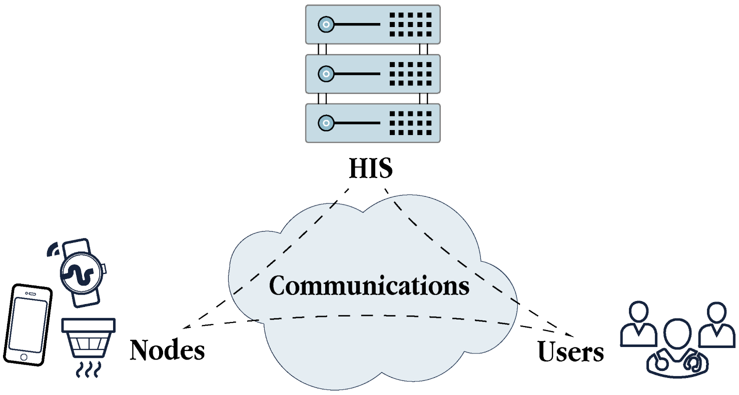

**Figure 4.** Relationship among the actors involved in smart healthcare systems.

### *3.2. Wireless Communication Technologies*

Plenty of wireless technologies are available to deploy smart healthcare systems, each one with its own properties in terms of radio coverage, data transmission rates, frequency, latency, power consumption, etc. All these features must be considered when envisaging smart health solutions. The landscape of wireless communication technologies for smart healthcare is described in what follows, and a comparison between these technologies and their suitability in the aforementioned WBAN architecture is summarised in Tables 11 and 12.

#### 3.2.1. Bluetooth

One of the most popular short-range wireless communication technologies is Bluetooth (see Table 11). Previously standardised under the IEEE 802.15.1, currently known as the Bluetooth Special Interest Group, it has established its specifications and developments. Bluetooth enables transmitting data between two wireless devices, one of them acting as a master (commonly the sink) and the other as a slave, in a range of, at most, 100 m at a data rate up of to 3 Mbps. This technology operates in the 2.4 GHz ISM band, also used by Wi-Fi and ZigBee technologies, and frequency hopping-related techniques were applied to reduce potential interference. This technology reached its popularity in the early 2000s with the emergence of mobile devices, and even today is extensively used in numerous general-purpose portable devices, including smartphones, smartwatches, fitness trackers, laptops and computer peripherals. However, with the advent of resource-constrained devices, a very low-power Bluetooth specification was developed: BLE (see Table 11) [15,18,249], able to transmit data with a very low power consumption and latency at 2 Mbps in a range of 400 m. The BLE characteristics are well aligned with s-health applications, such as critical emergency response, so to communicate with wearables, IoT, IoMT and other devices deployed in WSNs and WBANs. For instance, this technology has been a great ally to develop contact tracing applications during the COVID-19 outbreak [250]. Hence, we foresee BLE as an excellent technology for the next-generation medical purpose oriented devices.

#### 3.2.2. ZigBee

ZigBee [8,18,249], designed by the ZigBee Alliance and built on the IEEE 802.15.4 standard, is another outstanding wireless technology (see Table 11). This technology was advantageous for its low power consumption, so battery-powered devices can be operational for several years before battery depletion. Different characteristics in terms of coverage, data rate, power consumption and operational frequency bands are offered upon the selected ZigBee module, with XBee being the simplest one. The coverage radio is generally up to 100 m (similar to Bluetooth's), but data are transmitted at a low data rate up to 250 kbps. Hence, ZigBee might not be suitable for transmitting user-centric data in real-time which requires immediate action. Notwithstanding, this technology could be considered for battery-powered IoT devices oriented towards contextual sensing in WSNs.

**Table 11.** Comparison of the main wireless communication technologies for smart healthcare (I).

| | **Bluetooth** | **BLE** | **ZigBee** | **IEEE 802.15.6** | **Wi-Fi** |
|---|---|---|---|---|---|
| **Frequency bands** | 2.4 GHz | 2.4 GHz | 868/915 MHz<br>2.4 GHz | 14–29 MHz (HBC)<br>400–2400 MHz (NB)<br>3.2–10.3 GHz (UWB) | 2.4/5 GHz |
| **Radio coverage** | Short/medium | Medium | Short/medium | Short | Medium |
| | 10–100 m | 400 m | 10–100 m | 2 m | 50–100 m |
| **Data rate** | Moderate | Moderate | Low | Low/moderate | High |
| | 1–3 Mbps | 1–2 Mbps | 20–250 kbps | 10 kbps–15 Mbps | 400 Mbps–10 Gbps |
| **Latency** | Moderate | Very low | Very low/Low | Low/moderate | Low |
| | 100 ms | 10 ms | 10–30 ms | 125 ms | 50 ms |
| **Power** | Moderate | Very low | Very low/low | Very low | High |
| | 0.2–0.5 W | 10 mW | 1–60 mW | 0.1–3 mW | 0.8–1 W |
| **Size** | 8 | 32.000 | 65.000 | 256 | 250 |
| **Topology** | Scatternet | Star, mesh | Star, tree, mesh | Star, multi-hop | Star, mesh, ad hoc |
| **Security** | 56,64,128-bit AES | 128-bit AES | 128-bit AES | Level 1/Level 2 | 128,256-bit AES |
| **Cost** | Medium | Low | Low | Low | High |
| **WBAN tier** | Tier 1/Tier 2 | Tier 1/Tier 2 | Tier 2 | Tier 1 | Tier 2/Tier 3 |
| **Suitable for smart health** | ∼ | ✓ | ∼ | ✓ | ✓ |

#### 3.2.3. IEEE 802.15.6

IEEE 802.15.6, the latest international standard for WBAN communications, is oriented towards short-distance communications between devices operating on, in or around the human body [8,18,251]. The standard defines three physical layers, each operating at different frequency bands for different purposes (see Table 11). First, the narrowband (NB) comprises seven frequency bands between 400 MHz and 2.4 GHz with low data rates of up to 900 kbps (e.g., the 400 MHz band is used for implant communication and the 600 MHz band for medical telemetry). Second, the ultra-wideband (UWB) operating at higher frequencies between the 3.2–4.7 GHz and the 6.2–10.3 GHz band enable higher data rates of several Mbps (up to 15 Mbps) between on-body devices and on/off-body devices, such as for entertainment systems. Third, the human body communication (HBC) using the human body as a channel operates in low bands between the 14–18 MHz and the 25–29 MHz and transmits data at a maximum rate of 2 Mbps in an energy-efficient way.

In addition to the low power requirements, communications must be reliable, considering that devices are continuously changing their location due to humans' movements. Furthermore, regarding securing communications, three security levels are defined [252]: level 0 does not provide any security mechanisms and unsecured communications are established, level 1 provides message authentication and integrity assurance, but no encryption mechanisms, and level 2 provides message authentication, integrity assurance and encryption. This standard is expected to be adopted by miniaturised and resource-constrained medical devices to properly communicate the user-centric data.

#### 3.2.4. Wi-Fi

One of the most used general-purpose wireless technology is Wi-Fi, available in most devices from the digital ecosystem [18,249]. Wi-Fi encompassed within the IEEE 802.11 standards family for wireless communications in local area networks, is suitable for transmitting large volumes of data in a range of tens of meters at very high data rates (in the order of Mbps or even Gbps at latest specifications), where power consumption is not a critical issue (see Table 11). IEEE 802.11n, also known as Wi-Fi 4, operates in the frequency band between 2.4 GHz and 5 GHz and supports a theoretical data rate of up to 600 Mbps. IEEE 802.11ac (Wi-Fi 5) exhibits better performance and better radio coverage compared to its predecessors, operating in the 5 GHz band and providing data rates from 400 Mbps up to 1 Gbps. Recently introduced, the latest specification IEEE 802.11ax (Wi-Fi 6) increases data rates up to 10 Gbps, strengthens security with WPA3 and reduces the energy consumption compared to its predecessors, hence opening the door to its possible use in some resource-constrained devices in the coming years [253]. These characteristics make Wi-Fi technology a suitable solution for large-scale real-time smart health services.

#### 3.2.5. Cellular Networks

The tremendous popularity of smartphones during the last decade motivated the evolution of cellular networks, originally devoted to providing telephony services, towards high-bit rate transmissions of data. Today, the LTE-based 4G technology is available in many off-the-shelf smartphones and other portable devices (see Table 12). This technology operates at different bands between the 700 MHz and the 2.6 GHz frequencies (different among countries) and supports high data rates of hundreds of Mbps at a relatively low latency. Similarly to Wi-Fi, the main limitation of 4G is its high energy consumption, which limits its implementation in resource-constrained devices, although most current smartphones and smartwatches (i.e., the sinks) implemented this technology. Fourth Generation (4G) technology perfectly fits long-range communications in the outdoors, where secure Wi-Fi access points are less available.

The fifth generation of mobile networks, 5G, has undoubtedly been one of the main buzzwords of recent years. Expected to enable the massive deployment of IoT in a truly connected world with billions of devices [254], 5G promises very high data rates of up to several Gbps (especially at higher frequency bands of millimetre waves) in an almost negligible latency (1 ms ideally), using only a fraction of the energy consumption of 4G (see Table 12). To make 5G a reality, lots of antennas will need to be installed in order to manage an unprecedented coverage density of approximately a million devices per square kilometre. However, this requires a substantial investment in infrastructure. 5G will certainly open the door to numerous s-health opportunities, even though some of them could sound futuristic today, such as augmented/virtual reality assistance for blind people, remote collaboration in surgical interventions or video-enabled medication adherence [255–257].

### 3.2.6. Low-Power Wide-Area Networks

Long-range communications can be hardly implemented in sensors and IoT devices due to its aggressive power consumption. To fill this gap, the low-power wide-area networks (LPWANs) emerged as a novel communication paradigm (see Table 12). These kinds of technologies are able to transmit data along large distances (up to several kilometres) at a very low power consumption. However, these communications were conducted at a low data rate and high latency [258,259]. These technologies are hence not suitable for real-time applications, although they could be adopted for contextual sensing, whose values vary slightly over time and real-time constraints are relaxed or for non-critical healthcare monitoring, such as rehabilitation.

Some of the most prominent LPWAN technologies are LoRa, SigFox and NB-IoT [15,249,255,260]. In short, SigFox is an easy-to-deploy technology enabling large network connectivity at low infrastructure costs. However, the data transmission rate is very low (between 100 and 600 bps) and the latency is the highest in comparison to similar technologies. Interestingly enough, LoRa offers an excellent trade-off between distance coverage, data rate and energy consumption, and its popularity in IoT arenas has significantly grown in later years and it is expected to grow further. NB-IoT, although enhancing LoRa's properties in terms of latency and data rate, is scarcely adopted in IoT devices and lacks deployment readiness.

**Table 12.** Comparison of the main wireless communication technologies for smart healthcare (and II).

| | **4G/LTE** | **5G** | **LoRa** | **SigFox** | **NB-IoT** |
|---|---|---|---|---|---|
| **Frequency bands** | 0.7–2.6 GHz | 600–700 MHz<br>2.5–3.8 GHz<br>25–100 GHz | 863–928 MHz | 868/915 MHz | 800–900 MHz |
| **Radio coverage** | High | Medium/high | High | High | High |
| | 10 km | 300m–1 km | 5–20 km | 10–50 km | 15 km |
| **Data rate** | High | Very high | Very low | Very low | Low |
| | 10–300 Mbps | 1–20 Gbps | 37.5 kbps | 100–600 bps | 250 kbps |
| **Latency** | Low | Very low | High | High | High |
| | 50–70 ms | 1–10 ms | 3 s | 10 s | 1 s |
| **Power** | Moderate | Low | Low | Low | Low |
| | 250–700 mW | N/A | 25 mW | 10–100 mW | 20–200 mW |
| **Size** | Thousands<br>per km$^2$ | 1 million<br>per km$^2$ | 1000 | 1,000,000 | 50,000 |
| **Topology** | Cellular | Cellular | Star of stars | Star | Star |
| **Security** | 128-bit | 256-bit | 128-bit AES | Optional | 128,256-bit |
| **Cost** | Medium | High | Low | Low | Low |
| **WBAN tier** | Tier 2/Tier 3 | Tier 2/Tier 3 | Tier 2 | Tier 2 | Tier 2 |
| **Suitable for smart health** | ✓ | ✓ | ∼ | × | ∼ |

### 3.2.7. Other Technologies

In addition to the aforementioned wireless communication technologies, there are further technologies that could be well suited for smart health purposes. RFID and NFC are popular solutions for very short-range communications, particularly interesting for indoors. Other promising low-power technologies that could complement or even replace ZigBee or Bluetooth in the coming years are, among others, Z-Wave, ANT and RuBee. Within the LPWAN-related standards, weightless could be an interesting solution for communicating devices in the industrial and medical field. Finally, WiMAX (IEEE 802.16) could contribute to establishing the long-range transmissions of several kilometres where energy consumption is not critical.

### *3.3. Evaluation of Wireless Technologies*

Many wireless technologies are available for deploying smart healthcare solutions. As shown in Tables 11 and 12, each of them is suitable at different tiers of the aforementioned WBAN architecture due to its inner characteristics of radio coverage or power consumption, among others. However, to select the most adequate technology for each tier, other aspects must be considered.

One of the most important characteristics is the throughput of each technology, whose evaluation is not straightforward. Although the throughput could naively be approximated to the data rate, it diminishes in real environments due to interference or packet losses. For instance, whereas SigFox and LoRa enable high interference resilience, NB-IoT lacks interference immunity [261]. Therefore, although NB-IoT has a higher data rate than the other LPWAN technologies, a non-negligible number of frames could be lost and decrease its throughput consequently. Another key aspect to consider is the message size and the message frequency, i.e., the payload capacity. For instance, SigFox messages can carry a payload of 12 bytes and SigFox limits each SigFox device to 140 messages per day [262]. Finally, media access control also plays a crucial role in a network's throughput. For example, the RTS/CTS mechanisms can be used by 802.11 standards' family to avoid transmission collision, but at the price of lowering its throughput, especially in dense networks. Finally, scalability is another fundamental aspect once deploying smart healthcare systems intended for large populations. Whereas ZigBee and LPWAN technologies have a great scalability [261], scalability in 4G and 5G networks depends on the density of base stations deployed, and on the number of sinks and access points in BLE and Wi-Fi networks.

## 4. Information Security: Requirements, Attacks and Solutions

Security and privacy issues are critical concerns in any type of information system. However, these issues are even further strengthened in smart healthcare systems due to the high confidentiality of the information managed. More specifically, security and privacy aspects must be considered throughout the entire system: from the very sensing devices where data are collected, through the network where the data are transmitted, to the HIS where data are stored, analysed and presented to end users.

This section addresses the issue of information security in smart healthcare services from a global scope, by describing the security requirements that all s-health systems must fulfil in Section 4.1, categorising the most common attacks in these systems in Section 4.2, and proposing appropriate solutions to avert those attacks in Section 4.3.

### *4.1. Security Requirements*

As any other information system, smart healthcare systems must pursue a number of security requirements and put in place the appropriate protection mechanisms to guarantee them. Then, the main security requirements that must be considered are briefly discussed:

- Confidentiality: Data confidentiality is the property that guarantees that data are only disclosed to authorised entities (e.g., people, devices, processes. . . ), whilst remaining unintelligible to unauthorised entities. User-centric data, but especially the medical, must be kept confidential during storage periods (susceptible to data leakages) and while being conveyed through the communication networks (susceptible to eavesdropping). The most widely used technique to achieve confidentiality is encryption, in which only authorised entities have access to the secret key required to decode the data.
- Integrity: Data integrity ensures the accuracy, trustworthiness and completeness of data, guaranteeing that the data have not been modified or destroyed by unauthorised entities. For instance, attackers might tamper the data without authorisation during its transmission over the network. Unless properly detected, smart healthcare

systems would react to users upon faux data, and potentially endanger their health. Moreover, other non-related human events can also threat integrity, such as hardware glitches. Integrity-oriented protections include cryptographic hashes for detecting data modifications, and redundancy and backup policies enable restoring any affected data if necessary.

- Availability: Data availability guarantees that authorised entities have constant access to the data regardless of their location and time. This property allows the proper functioning of the sensing devices, the communication channels and the information systems at a whole. Smart healthcare systems must guarantee the availability of medical data, since decisions might be made anytime and anywhere. Hence, they must be resilient to service disruptions: either intentional from attackers denying services to legitimate users, or accidental due to natural disasters, hardware failures or system upgrades that require systems breakdowns. Redundancy, recovery policies and fail-over strategies should be considered to avoid availability issues.
- Non-repudiation: Non-repudiation is the guarantee that a particular interaction between two entities actually occurred. This means that, given the communication of a message between two authorised entities in a system, the sender cannot deny having sent a message to the receiver in the future, and the receiver cannot deny having received the message from the sender in the future. Although cryptographic digital signatures can help achieve this property, it is noteworthy that their use in some sensing devices might be limited due to their computational constraints.
- Authentication and authorisation: Authentication and authorisation mechanisms are commonly misconceived or interchanged. On the one hand, authentication refers to the process of confirming the identity of an entity, i.e., determining whether the entity is who it claims to be. On the other hand, authorisation refers to the process of determining whether the authenticated entity has access to the particular resources and services of the system. Within smart healthcare systems, authentication procedures are mandatory in order to establish communications only with properly authenticated entities, and avoiding any communication with illegitimate entities. In general, this is achieved through credentials, e.g., passwords, biometrics or digital certificates. In the case of successful authentication, then systems must ensure whether the entities have permission to do the actions that aim to (e.g., access, modify or delete medical information).
- Privacy: Privacy is a fundamental right that has to be protected. Smart healthcare systems must process personal data in a lawful, fair and transparent manner for a specific, limited and legitimate purpose. Besides, due to the sensitivity of the data, they require the explicit individuals' consent for their managing and be compliant with the current regulations on data privacy. These systems must adopt the appropriate safeguards to reduce disclosure risks, including identity disclosure, i.e., the direct re-identification of individuals, and attribute disclosure, i.e., the inference of confidential information to a certain individual. Hence, in the case of data leakages or eavesdropping, people's privacy is not jeopardised. One of the most common data sanitisation techniques for privacy protection is data anonymisation.

### *4.2. Security Attacks, Threats and Vulnerabilities*

The impact of attacks against smart healthcare systems may go beyond the leakage of medical records and the loss of privacy, and life-threatening situations may arise in the case of hijacking implantable devices, such as insulin pumps or pacemakers [263–266]. Unfortunately, attacks against vulnerabilities discovered in medical devices are unexceptional [267,268]. In addition, wireless technologies and the proper HIS may also entail a number of security flaws depending on the design and implementation of the system: insecure programming practices, vulnerable communication protocols or obsolete technologies open the door to numerous security attacks [269–271].

As observed, smart healthcare systems are susceptible to different types of security attacks. In the literature, different taxonomies were proposed to classify them. Then, the most popular classification methods are outlined:

- Based on the attack's nature: passive attacks and active attacks [21]. In passive attacks, attackers monitor and collect information from the system and exploit it to launch further attacks. This kind of attacks does not harm the system, hence victims are not aware of them. On the contrary, active attacks are intended to modify or damage the system by injecting, altering or destroying data or services. Since these attacks impact the systems, victims are informed of them.
- Based on the attack's origin: internal attacks and external attacks [21]. Internal attacks are initiated by malicious entities located inside the system, i.e., insider attackers. In contrast, external attacks are launched by external entities located outside the system, i.e., outsider attackers.
- Based on the attack's launch method: physical methods, logical/software-based methods and side-channel methods [272]. Physical methods refer to the attacker's ability to have physical access to the cyber-physical system in an unauthorised way. Logical or software-based methods exploit vulnerabilities and expose errors in logical systems, such as software, operating systems, applications or protocols, to gain illegitimate access. Side-channel methods observe the indirect physical effects of the systems during their functioning to acquire advanced knowledge.
- Based on the TCP/IP model layer: application layer, transport layer, network layer and network interface layer [272]. Attackers can target different layers of the TCP/IP model to find weaknesses and infiltrate the system. Similar classifications can be performed using the OSI model.

Complementing the taxonomies above, this article presents a classification of security attacks based on the actors involved in the smart healthcare systems, namely nodes, communications, HIS and users. It is noteworthy that the list of attacks below is not exhaustive, and only covers the most widely known attacks related to smart healthcare. In short, Table 13 classifies the security attacks reviewed in this article according to the aforementioned taxonomies, and indicates which security requirements are compromised as a consequence. In addition, a graphical summary is provided in Figure 5.

#### 4.2.1. Attacks against Nodes

The resource-constrained nature of most of the nodes deployed in WBANs and WSNs limits the incorporation of robust security mechanisms. Hence, nodes become the primary target of many attackers. In particular, attacks related to node compromising, including node capture attacks, false data injection attacks and sleep deprivation attacks are explained. Furthermore, side-channel attacks and firmware update attacks are also considered within this scope.

##### Node Capture Attacks

One of the most popular attacks is node capture attacks, in which attackers take control of a node after successfully exploiting a vulnerability [273–275]. These attacks need to be rapidly detected to disconnect the compromised node from the network as soon as possible. Otherwise, attackers may seek for further vulnerabilities within the system to elevate their privileges and eventually, gain control over the entire system. These attacks mainly compromise the confidentiality of the system because attackers could extract the private information from the captured node, such as user-centric data in the case of wearable devices or the cryptographic keys stored in the nodes to encrypt and decrypt the communications. Within the s-health scenario, this attack can indirectly threaten people's privacy because raw sensitive data might be disclosed to attackers.

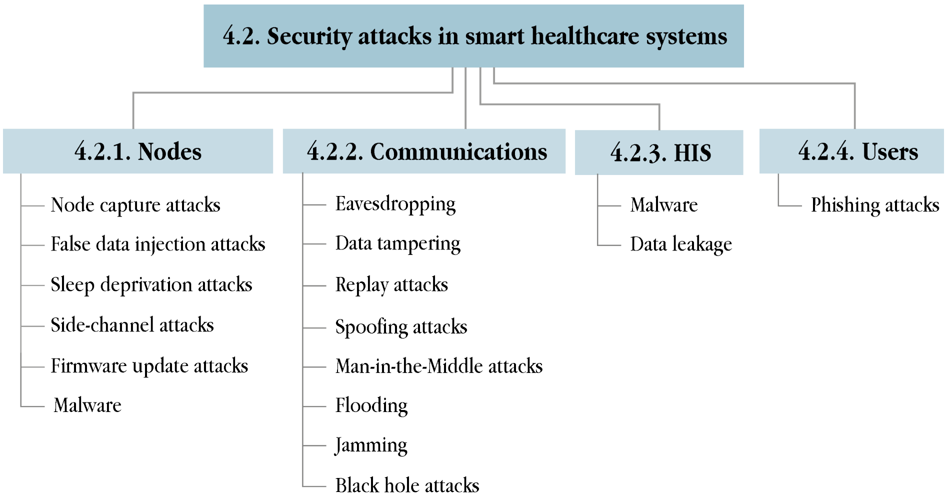

**Figure 5.** The taxonomy of security attacks in smart healthcare systems.

False Data Injection Attacks

Once a node has been compromised, attackers can inject malicious code in the captured node and redeploy it in the network (as if it was a legitimate node) with the aim to perform unintended functions. Usually, attackers can use the captured node to conduct false data injection attacks, i.e., fabricating erroneous data as if they were true or preventing passing true data [276]. Hence, the integrity of smart healthcare systems could be compromised because they would naively react to fake data and take unsuitable health decisions that might put people's lives at risk [277,278]. For example, the injection of false physiological parameters could lead to wrong medical diagnosis and consequentially to inadequate medical treatments based on these data. The severity of these attacks increases in critical operations such as surgeries, where the injection of real-time parameters could result in a loss of life. Furthermore, false medical records may cause illegal insurance claims, thus opening the door to potential financial fraud.

Sleep Deprivation Attacks

More aggressive attacks which damage (either physically or logically) the sensor network and disrupt network communications are sleep deprivation attacks (also known as energy drain attacks) [279,280]. These attacks aim to increase the power consumption of captured nodes with useless tasks, such as running infinite loops, so as to accelerate the battery draining of the devices and hence, force their disconnection from the sensor network. By disconnecting nodes, the system's availability becomes affected, and dramatic consequences could arise within the healthcare domain. In particular, stopping vulnerable life-assistance devices, such as pacemakers [281] or cardiac defibrillators [282], can impact human lives.

Side-Channel Attacks

Whereas most attacks aim to exploit the weakness of algorithms and protocols implemented in the nodes, the family of side-channel attacks concentrate on exploiting the physical effects of computing devices during their normal functioning to infer sensitive information, namely cryptographic keys and passwords [283]. Such attacks can leak relevant information about these devices through physical side signals, such as timing analysis (i.e., time taken to perform computations), power analysis (i.e., variations on the power consumption to perform computations), electromagnetic emanation (i.e., radiation emitted by the system to perform computations) and acoustic attack (i.e., sounds produced during computations), among others [272]. All in all, side-channel attacks are difficult to handle and pose serious threats due to their non-invasive nature, the generally passive mode, and the fact that they evaluate the physics, rather than the implementation, of the computing elements.

The numerous nodes deployed in smart health systems open the door to a plethora of side-channel attacks [284]. For instance, several studies have shown the feasibility of inferring the key-based security system of smartphones or smartwatches by means of motion sensors [285–287]. In this scenario, attackers would gain the additional advantage of bypassing the security mechanisms defending the system and thus, break into it more easily. More active side-channel attacks might also put people's lives at risk, such as by injecting electromagnetic signals that might bogus the legitimate signals of cardiac implantable devices [288].

**Table 13.** Summary and classification of security attacks in smart healthcare systems.

| Attack | Target Actor | Nature | Origin | Launch Method | TCP/IP Layer | Requirements Threats |
|---|---|---|---|---|---|---|
| Node capture | Nodes | Active | External | Physical | Network interface | Confidentiality<br>Non-repudiation<br>Authentication<br>Privacy |
| False data injection | Nodes | Active | Internal | Physical | Network interface | Integrity |
| Sleep deprivation | Nodes | Active | External | Physical<br>Logical | Network interface | Availability |
| Side-channel | Nodes | Passive<br>Active | External | Side-channel | Network interface | Confidentiality<br>Availability |
| Firmware update | Nodes | Active | External | Logical | Network interface | Confidentiality<br>Non-repudiation<br>Authentication<br>Authorisation |
| Eavesdropping | Communications | Passive | External | Logical | Network interface<br>Network | Confidentiality<br>Privacy |
| Data tampering | Communications | Active | Internal | Physical | Network interface | Integrity |
| Replay | Communications | Active | Internal | Physical | Network | Integrity<br>Authentication<br>Authorisation |
| Spoofing | Communications | Active | Internal<br>External | Physical | Network interface<br>Network<br>Transport<br>Application | Integrity |
| Man-in-the-middle | Communications | Active | Internal<br>External | Logical | Network<br>Transport | Confidentiality<br>Integrity<br>Authentication<br>Privacy |
| Flooding | Communications | Active | Internal<br>External | Logical | Network<br>Transport<br>Application | Availability |

**Table 13.** *Cont.*

| Attack | Target Actor | Nature | Origin | Launch Method | TCP/IP Layer | Requirements Threats |
|---|---|---|---|---|---|---|
| Jamming | Communications | Active | External | Physical | Network interface | Availability |
| Black hole | Communications | Active | Internal | Physical | Network | Availability |
| Malware | HIS<br>Nodes | Active | External | Logical | Application | Confidentiality<br>Integrity<br>Availability<br>Non-repudiation<br>Authentication<br>Authorisation<br>Privacy |
| Data leakage | HIS | Passive | External | Logical | Application | Confidentiality<br>Privacy |
| Phishing | Users | Active | External | Logical | Application | Confidentiality<br>Authentication<br>Authorisation<br>Privacy |

#### Firmware Update Attacks

Modern nodes require firmware updates to support the latest technological developments and improve performance. For time inefficiencies, these updates are no longer performed physically between the manufacturer and the device, but remotely, in which the devices are able to automatically download the latest firmware version and upgrade themselves. However, the security of firmware updates is generally insufficient due to the lack of encryption and/or authentication mechanisms [289], opening the door to firmware update attacks. This attack consists of injecting a malicious firmware into the vulnerable device so as to grant attackers total control over them. The main severity of these attacks is that they are capable of affecting entire families of nodes, e.g., if a manufacturer uses the same firmware update mechanism, then all its devices would be vulnerable. Particularly, numerous commercial wearable devices, especially fitness trackers, are susceptible to this kind of attacks due to their computational constraints [290–294]. Even worse, vulnerabilities in the firmware update procedure, able to execute arbitrary code, of automated external defibrillators and implantable devices have been reported [265,295].

### 4.2.2. Attacks against Communications

The distributed nature of smart healthcare systems requires communication networks to transmit the information between the different actors within the system. Most of the existing attacks aim to target the communications, mostly wireless, which are prone to hijacking unless properly secured. Eavesdropping, data tampering, replay attacks, spoofing attacks, man-in-the-middle attacks and denial of service attacks are subsequently described within the s-health paradigm.

#### Eavesdropping

Continuous communications among entities are exposed to be intercepted by eavesdrop attackers. Eavesdropping (or sniffing) attacks aim to secretly capture and listen to the data packets transiting the communications, without the knowledge of the legitimate entities [296]. During eavesdropping, all messages are compromised and attackers can analyse the traffic to learn private information from the whole system (e.g., data, protocols, communicating entities…) [297]. For this reason, messages must never be transmitted in plain-text or encrypted with vulnerable algorithms. This passive attack undermines the confidentiality of the communications and might jeopardise people’s privacy.

Some Bluetooth and BLE communications, extensively used in the s-health domain, might be vulnerable to eavesdropping attacks, where encryption might be bypassed [298–300]. Indeed, a variety of medical devices, including hospital equipment [301], wearables [302–306] and implantable devices [282,307], have been compromised through eavesdropping, by disclosing private data or serving to obtain insights for further active attacks. Eavesdropping attacks are also common in other popular technologies, namely Wi-Fi and ZigBee [308,309].

Data Tampering

More actively, attackers can deliberately alter or destroy data transiting through the network. This attack, commonly known as data tampering or modification attack, aims to compromise the integrity of the data and as a consequence, the system's [310]. By means of data tampering attacks, attackers could modify the data at their convenience in order to manipulate the system's functioning or gain access to it. For instance, systems would malfunction in the case of modifying data packets properties, such as their timestamps (i.e., the flow of events would be erroneous from the system's perspective) or their destination address (i.e., redirecting them to illegitimate destinations) [311].

More threatening, the unauthorised modification of more sensitive data, such as medical, could cause physical damage on people's health, because systems would react upon malicious data. This situation might lead to overtreatment, undertreatment or even death [312]. Several data tampering attacks have been successfully conducted using medical equipment [301,311], fitness trackers [291,293,306,313] and even implantable devices [265,266,314]. No less important, tampering with contextual data can also negatively impact the lifestyles of large populations, as smart healthcare systems would adapt themselves to false contextual conditions covering a certain geographical area. In short, tampering user-centric data leads to individual damages, but tampering contextual data might lead to large-scale damages.

Replay Attacks

During eavesdropping, attackers capture valid data packets that are sent between two legitimate entities. Even though their messages could be encrypted (and thus unreadable for attackers), these messages have an effect on the recipient entity. Attackers can exploit this to mislead legitimate entities and acquire the trust of the system with the aim to maliciously duplicate transactions, impersonate entities or raise confusion within the system. Thus, replay attacks occur when unauthorised entities re-send legitimate captured data packets at a later time while acting as the original sender, hoping to repeat some action that benefits the attacker [315]. For instance, if attackers intercept the messages related to a valid login procedure, they could try to replay them later on and, unless detected by the system, obtain access to the system without knowing the actual credentials. This attack clearly threatens data freshness, another important attribute in information systems [316].

The consequences of successful replay attacks in smart healthcare systems can be tragic, especially when replaying messages describing users medical data [317–320]. Systems would naively react to old physiological parameters rather than to the current physiological parameters of users in that moment. Replaying old messages for a long period of time may bring mistreatment. Among others, studies have demonstrated the possibility of targeting diabetic people by launching replay attacks with false glucose readings [321] or exploiting the validation limitations regarding integrity and authentication in cardioverter-defibrillator devices [282] and other implantable medical devices [263,266]. Similarly, replay attacks were also detected in a number of fitness trackers due to the lack of authentication mechanisms [293].

Spoofing Attacks

Identity theft is undoubtedly one of the primary security concerns in information systems. Spoofing attacks consist of masquerading attackers acting as legitimate entities by using forged data [322]. If the legitimate entities within the system trust in the incoming (malign) entity, attackers can gain access to once inaccessible resources, and conduct further insider attacks. There exist different spoofing attacks targeting different OSI layers, namely ARP spoofing (i.e., attackers link their MAC address to a legitimate network IP address), IP spoofing (i.e., attackers send IP packets from a spoofed source IP address to disguise themselves) and DNS spoofing (i.e., attackers re-route specific domain name requests to different IP addresses under their control) [323,324].

The computational, size and power limitations of most nodes prevent the implementation of spoofing countermeasures. Hence, these devices may be vulnerable to spoofing attacks, hence compromising the entire s-health system. Successful spoofing attacks enable attackers retrieve medical data gathered from the sensing devices, such as fitness trackers [294] and even trigger life-threatening situations in the case of spoofing insulin pumps [325]. Beyond medical data, the ability to spoof GPS data was also pointed out [326,327], forging the real location of devices (and hence, the users as well).

Man-in-the-Middle Attacks

One of the most popular and devastating attacks in networks are man-in-the-middle attacks (MitM) [328]. Such attacks consist of intercepting the communication between two legitimate entities who believe that they are directly communicating with each other. Once a communication is hijacked, attackers are free to passively eavesdrop the data packets seeking for private data or actively manipulate the data packets by tampering data or injecting false data. Moreover, attackers can exploit this illegitimate advantage for redirecting traffic to malicious resources or spreading malware through the network. With the lack of security of many sensing devices, MitM attacks can be feasibly exploited in sensor networks [329,330]. Indeed, some Bluetooth communications have been proven to be vulnerable to MitM attacks [299,331,332]. As a result, there is a need to evaluate the trustworthiness of entities within sensor networks so as to ensure the confidentiality and integrity of the transmitted data through such networks [333–335].

The impact of MitM attacks on smart healthcare systems can be tremendous. Attackers could intercept medical records shared between two legitimate healthcare providers, or intercept physiological data collected from sensing devices without the knowledge of the actors. Numerous nodes are vulnerable to this kind of attack due to the security flaws and weak authentication mechanisms. For instance, the lack of encryption of some devices enables attackers to seamlessly hijack communications and capture private data such as session identifiers, passwords and health data [291,293,303,305,313,336–338]. Of further concern, studies HAVE also discovered MitM-enabling vulnerabilities in protocols integrated in implantable medical devices [339,340].

Denial of Service Attacks

Attacks against availability prevent the normal performance of information systems and threaten network functioning and resources responsiveness. Denial-of-service attacks (DoS) aim to make resources unavailable to the legitimate users by temporarily or indefinitely disrupting the services provided [341]. A more sophisticated version is that of distributed denial-of-service attacks (DDoS) which require multiple and coordinated sources controlled by an attacker targeting a victim, who cannot stop the attack by just blocking a single source. In addition to the aforementioned sleep deprivation attacks at the node level, there exist further DDoS-oriented attacks at the communication level. Usually, the most prominent attack is flooding which overwhelms legitimate resources with purposeless requests, in such a way that they are not able to handle all the incoming packets (even the legitimate ones) and then collapse. Attackers can flood the network with data packets from different layers of the OSI model, such as HTTP flood, ICMP flood, SYN flood, DNS flood and HELLO flood. Another well-known type of DDoS attack is jamming, which uses specific jammer devices to generate random radio-frequency signals that deliberately cause interference and hence, disrupt the network's functioning [342]. Another DDoS attack at the network layer is the black hole attack (also called packet drop attack), where a malicious node exploits vulnerabilities in routing protocols to redirect the traffic towards itself and then, drop the incoming packets [343].

Many DDoS attacks have been launched in the recent years with the Mirai botnet, which exploits the low-security implementations of IoT devices to disrupt services [344,345]. This kind of disruptive attack could lead to terrifying consequences in smart healthcare systems, which need to be constantly on for real-time monitoring and act immediately in the case of emergencies [293,303]. Unfortunately, availability is particularly crucial in certain critical-mission medical devices, such as implantable devices, wherein availability-threatening attacks can lead to the loss of people's lives [266,282,346].

#### 4.2.3. Attacks against HIS

Certain security attacks aim to target the very HIS infrastructure of the healthcare service providers, i.e., the servers, databases, routers, firewalls and computers that manage the system's applications, data and flows. These attacks are likely to be more sophisticated since these systems, which are not resource-constrained, are able to implement more robust countermeasures. More specifically, malware and data leakage attacks are outlined as follows.

##### Malware

Malware, short for malicious software, encompasses all different types of unwanted and hostile programs, used to invade, damage, disrupt or disable computer systems and networks [347]. This creates chaos and compromises confidentiality, integrity and availability, by exploiting the vulnerabilities of the systems [348]. Infected systems are partly (or completely) under the control of attackers and therefore are susceptible to data theft, hijacking and propagating the malware into other systems. Malware can be divided into different categories, including worms, trojans, rootkits, viruses, spyware, keyloggers, botnets and ransomware [329]. In particular, ransomware attacks have become popular in recent years with the aim of hijacking a system whose files are encrypted with an attacker's key, and ask for some payment in cryptocurrencies to restore them [349].

For decades, many malware have been developed to target conventional computing devices. However, with the advent of sensing devices, wearables and IoT devices, different malware variants emerged to target these more vulnerable devices. In particular, the lack of strong security mechanisms makes these devices highly vulnerable to malware infection [293,301]. The Mirai botnet, VPNFilter, BrickerBot or Reaper are some examples of malware targeting large networks of IoT devices [329,344,345,350]. In addition, the popular WannaCry ransomware-based attack threatened millions of organisations in 2017 and hijacked multiple healthcare systems, including the British National Health Service [351]. Hence, smart healthcare systems must monitor the functioning of their entities, seeking for abnormal malware-derived conditions, and, once detected apply the proper countermeasures to prevent the malware spread and mitigate the impact on the entire system.

##### Data Leakage

Data leakages (or data breaches) occur when personal and/or confidential data from an organisation is released to an untrusted environment by an unauthorised entity. Most data leakages involve financial information, medical records, trade secrets or intellectual property, whose value on the black market may be significant [13]. Unfortunately, these incidents are far too common [352–354]. These attacks constitute a threat to the confidentiality and privacy, essential principles that users expect from organisations once managing their personal information. It is noteworthy that leakages are not only due to malicious attacks, but they may also be due to unintentional human actions (e.g., unintentional emailing to wrong recipients) or system glitches. However, this does not extinguish organisations from legal liabilities and economical sanctions, in addition to the considerable reputational damage.

#### 4.2.4. Attacks against Users

The weakest link in the security chain of a system is the human factor [355]. Hence, attackers can attempt to infiltrate themselves into target systems by taking advantage of the lack of knowledge of most users regarding computer security, instead of seeking for vulnerabilities in their infrastructure, network and nodes. To this aim, attackers conduct social engineering activities to exploit humans error, among which phishing attacks are the most prominent.

##### Phishing Attacks

Phishing attacks aim to deceive users and obtain sensitive data wherein attackers disguise themselves as a legitimate entity [356]. The most common phishing is by e-mail, where attackers forge the sender's address to seem legitimate, hoping that users trust it and introduce private data or download some malware. In the case of successfully deceiving users, then attackers can impersonate the victims, acquire confidential data from the systems or launch further malicious activities on their behalf for raising their privileges. Phishing has evolved towards more sophisticated attacks, namely spear phishing (i.e., targeted phishing attacks using OSINT tools), whaling (i.e., targeted phishing attacks to high-privilege corporation's users), vishing (i.e., voice phishing) or smishing (i.e., SMS phishing), among others. With the worldwide COVID-19 pandemic, attackers have used the opportunity to intensify phishing campaigns for deceiving users with fraudulent messages [357–359]. Phishing attacks in the healthcare domain are common: attackers can impersonate legitimate users and gain access into the HIS [360–362]. In such cases, systems should be able to detect abnormal accesses (e.g., the source IP address or country is not the usual one) and prevent the entrance of users into the system unless performing a second authentication.

### *4.3. Security Solutions*

Achieving a high level of security in smart healthcare systems is challenging because this requires the implementation of many security mechanisms at different layers. Then, the most popular security solutions and safeguards to be considered in these systems are described. For the sake of clarity, these solutions were classified into four groups: secure communications, always-on systems, trust management and data protection (see Figure 6). Moreover, Table 14 summarises the proposed solutions and indicates which security requirements are protected when adopting them.

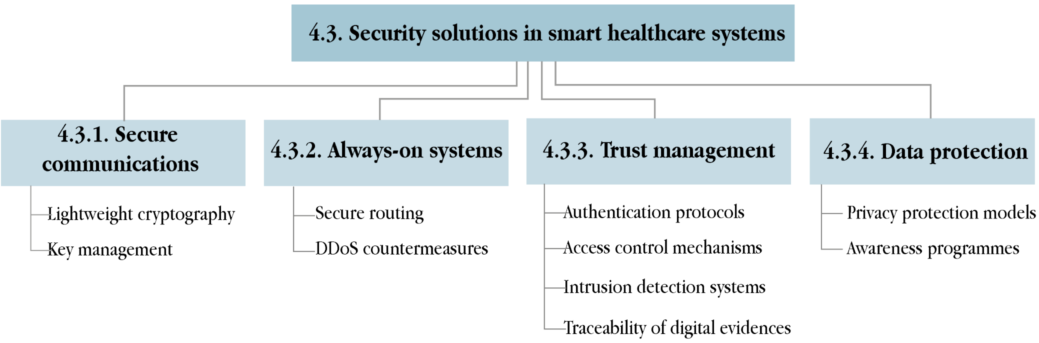
4.3. Security solutions in smart healthcare systems
4.3.1. Secure communications
Lightweight cryptography
Key management
4.3.2. Always-on systems
Secure routing
DDoS countermeasures
4.3.3. Trust management
Authentication protocols
Access control mechanisms
Intrusion detection systems
Traceability of digital evidences
4.3.4. Data protection
Privacy protection models
Awareness programmes

**Figure 6.** Taxonomy of security solutions in smart healthcare systems.

#### 4.3.1. Secure Communications

Many security attacks are communication and network oriented. Although securing these channels is always paramount, it is of utmost importance in smart healthcare systems. To this end, all the entities involved in the storage and transmission of data must consider the use of cryptography. Solutions based on lightweight cryptography and key management are discussed below.

### Lightweight Cryptography

Servers, desktop computers, tablets or smartphones are powerful enough to implement state-of-the-art cryptographic solutions. However, conventional cryptography is unsuitable for resource-constrained devices. Hence, they must rely on lightweight cryptography [363,364], which focuses on the design of simpler and faster cryptographic primitives, standardised under the ISO/IEC 29192 [365].

In recent years, many symmetric key solutions were proposed to ensure confidentiality [366]. Whereas AES remains the standard algorithm in conventional cryptography, many block ciphers have simplified their properties for lightweight cryptography (i.e., smaller block sizes, key sizes and number of rounds) in order to improve their efficiency. PRESENT, CLEFIA and LEA are the current block cipher algorithms within ISO/IEC 29192-2:2019 [367–369]. Although lightweight stream ciphers can be used in constrained environments, they are less prominent compared to block ciphers. The two standardised algorithms in ISO/IEC 29192-3:2012 are Enocoro and Trivium [370,371].

Regarding public-key cryptography, lightweight techniques based on Elliptic-curve cryptography (ECC) have been presented [372]. In general, ECC-based implementations are more efficient compared to classical approaches such as RSA, since ECC can reach the same level of security with significantly shorter key lengths and moreover, are not based on computationally demanding complex operations [373–376]. For instance, TinyECC is a configurable and publicly-available ECC library suitable for supporting public-key cryptography in sensor networks and IoT devices [377]. With a view on the post-quantum era, where RSA and ECC algorithms can be vulnerable, lattice-based cryptography [378] is becoming increasingly important and its feasibility in lightweight IoT devices is promising [379,380].

Cryptographic primitives can also provide data integrity assurance by means of hash functions, which help determine integrity-oriented attacks. However, conventional hash functions, such as SHA-2 and SHA-3, might not be efficient enough for constrained devices, and lightweight hash functions using shorter messages and outputs have been proposed. PHOTON, SPONGENT and Lesamanta-LW are standardised within ISO/IEC 29192-5:2016 [381–383]. Furthermore, lightweight message authentication codes (MACs), used to verify the authenticity and the integrity of the message have also been defined in ISO/IEC 29192-6:2019: LightMAC and Chaskey [384,385].

### Key Management

As long as the cryptographic keys are securely managed, the security of the communications is guaranteed. Key management deals with the generation, exchange, storage, use and revocation of the cryptographic keys in a distributed system. In particular, smart healthcare systems must deploy robust key management policies to safeguard confidentiality.

Randomness is an important factor in computer security, since the generation of cryptographic keys requires random values to ensure their uniqueness and unpredictability. The implementation of random number generators in resource-constrained environments is challenging due to the hardware and software limitations, despite the fact that the design of lightweight algorithms is currently on the rise [386–388]. In the specific context of wearable devices, different private key generation schemes have been proposed based on the randomness of user-centric attributes, including heart rate [389–393] and body motion [394,395].

### 4.3.2. Always-On Systems

Smart healthcare systems must be uninterruptedly available. However, due to the increasing sophistication of attacks against systems' availability, fulfilling this requirement is challenging. More specifically, this section addresses two major solutions against systems' availability, namely secure routing and DDoS countermeasures.

### Secure Routing

Routing is fundamental to enable communications in any kind of network. In smart healthcare, routing information must be properly communicated in a time and energy-efficient way [247,396]. As nodes can join and leave the network on-the-fly (e.g., a new sensor is introduced, a sensor has crashed, or a sensor has been compromised and removed from the network), routing solutions must be autonomous, scalable and dynamically adapt to these changes [397,398]. Routing protocols must also be resilient to attackers who can inject malicious routing information into the network (e.g., when a node is captured) to cause routing inconsistencies and disrupt communications. Numerous studies have been defined to secure routing protocols within sensor networks, based on the trustworthiness of neighbour nodes, clustering or hierarchical methods and genetic evolutionary techniques [399–402].

**Table 14.** Summary and classification of security solutions in smart healthcare systems.

| Type | Solution | Actor | TCP/IP Layer | Requirements Protected |
|---|---|---|---|---|
| Secure communications | Lightweight cryptography | Nodes<br>Communications<br>HIS | Network interface | Confidentiality<br>Integrity<br>Non-repudiation<br>Authentication |
| | Key management | Nodes<br>HIS | Network interface | Confidentiality<br>Authentication |
| Always-on systems | Secure routing | Communications | Network | Availability |
| | DDoS countermeasures | Nodes<br>Communications<br>HIS | Network | Availability |
| Trust management | Authentication protocols | Nodes<br>HIS | Transport<br>Application | Authentication<br>Confidentiality<br>Privacy |
| | Access control mechanisms | HIS | Application | Authentication<br>Confidentiality<br>Privacy |
| | Intrusion detection systems | Communications<br>HIS | Network<br>Transport<br>Application | Confidentiality<br>Integrity<br>Availability<br>Authentication<br>Privacy |
| | Traceability of digital evidence | HIS | Application | Integrity |
| Data protection | Privacy protection models | HIS | Application | Privacy |
| | Awareness programmes | Users | - | Privacy |

### DDoS Countermeasures

Different defensive DDoS countermeasures must be adopted at different stages to avert these attacks, categorised into preventive measures, detection measures and responsive measures [341,403].

Prevention mechanisms are intended to decrease the probability of suffering DDoS attacks. These methods can be generally classified as filtering-based or capacity-based [404]. Filtering-based mechanisms aim to decrease the network traffic by distinguishing legitimate traffic from attacking traffic, which is dropped. To do this, the IP traceback method determines the true IP origin address of a data packet, rather than its spoofed IP address. Probabilistic/deterministic packet marking, route-based packet filtering, history-based IP filtering or ingress/egress filtering approaches are used to filter data packets using different criteria, such as their source or destination address or their reachability [405–407].

The monitoring of the system's metrics serves to detect abnormal behaviour. Under DDoS attacks, these metrics are abnormal because the system would be overwhelmed and would degrade its quality of services. For years, most DDoS detection methods were based on statistical analysis, but several machine learning solutions have recently been proposed. Statistical methods can effectively and efficiently detect DDoS attacks by monitoring the incoming traffic at different time periods through entropy, principal component analysis and hidden Markov models [408,409]. With regards to machine learning techniques, many classifiers have succeeded in identifying DDoS attacks (e.g., support vector machines, neural networks, random forest...) from data packets' features, such as their size, origin and destination addresses, ports, protocols or time interval between them [410–412].

Finally, but no less importantly, the detection of DDoS attacks must be immediately followed by a proactive response. Smart healthcare systems must be designed to be fault-tolerant and limit DDoS damage. Among other strategies, scaling hardware resources, queuing techniques or migration-enabling services should be considered.

#### 4.3.3. Trust Management

Systems require mechanisms to be trustworthy, i.e., by producing reliable and authentic data and communications and being accountable. Implementing authentication protocols and access control mechanisms, considering intrusion detection systems and tracing digital evidence are some solutions to this aim.

##### Authentication Protocols

Authentication is paramount to prevent disclosing information to unauthorised entities. Indeed, both users and devices must be authenticated in smart healthcare systems. Traditionally, user authentication mechanisms were password based. However, weak passwords or the systematic reuse of passwords are common malpractices that facilitate the task of attackers to overcome these authentication mechanisms. Current authentication mechanisms combine possession factors (e.g., smart cards, one-time password tokens), knowledge factors (e.g., passwords, PINs) and biometric factors (e.g., fingerprint, iris scan, facial recognition) to strengthen the robustness of the authentication procedure. The combination of all three authentications is generally known as a three-factor authentication. In particular, biometric authentication has gained increasing importance during the last decade with the advent of smartphones and wearables. In addition, several studies have reported the feasibility of using wearables to authenticate users' identity from the continuous collection of user-centric data, such as heart rate, body temperature, ECG signals or body motion [413–415]. Concerning device authentication, which cannot implement traditional protocols due to their energy and time consumption, a number of lightweight authentication protocols have already been presented [416–419].

##### Access Control Mechanisms

Access control limits the access of users or devices (i.e., subjects) to the resources (i.e., objects) of the system, by establishing a subject-to-object segregation [420]. For instance, patients may only access to their own information, physicians may only have access to the medical information of their patients, whereas nodes may only have access to the services associated to their own task. With scalability and flexibility in mind, numerous fine-grained access policies have been defined to enforce different access privileges to the system's subjects. Extensively used, role-based access control (RBAC) models associate each subject to a role, and each role has a set of access permissions. Thus, a subject has as many permissions as the role indicates. This scheme combines both security and privacy to the system's objects with usability and flexibility at the time to define the privileges and roles [421]. Alternatively, cryptography can also help define access control mechanisms in a more secure way with the attribute-based encryption (ABE)-based fine-grained access control. In this context, the information is encrypted with a set of attributes (e.g., department, age, gender...), and only the users fulfilling those attributes are able to decrypt the information and hence, gain access [422]. Furthermore, the work in [423] proposed the use of blockchain technology to decentralise the access control within an IoT environment with a privacy-preserving component.

### Intrusion Detection Systems

The deployment of preventive mechanisms, such as intrusion detection systems (IDS), can help detect attacks at an early stage. IDS monitor and analyse the activities happening within a system, and alert once detecting unknown or potentially malicious activities. Depending on the deployment of the IDS, they can be network-based (NIDS), i.e., monitor data packets across the network for malicious activities, or host-based (HIDS), i.e., monitor all the activities occurring within an end device, such as the modification of files, operating system calls, running processes and the utilisation of resources. IDS are a mature technology in traditional environments, however, they might not yet be adequate in context-aware environments. In this context, IDS must be as lightweight as possible to minimise the overhead introduced in the system's infrastructure, so that they do not interfere or significantly impact with the proper functioning of the system [424].

The most popular IDS method is based on anomaly detection. By properly defining the normal behaviour of the system (captured during a training phase), the real-time activity can be compared against the normal behaviour. When the distance between the normal and the real-time behaviour exceeds a predefined threshold, an alarm is raised. Although this method allows the detection of new kinds of attacks and malware, it is susceptible to high false alarm rates as the accuracy of the method depends on the behaviour captured during the training phase, which may be incomplete in some cases [425]. Another method is based on signatures, referring to the effects and patterns suffered by a system due to an attack. Storing all the signatures of known attacks in a database, IDS are able to detect whether the real-time behaviour of the system matches with any stored signature. Despite the high accuracy of this method, unknown attacks remain undetectable [426]. With the aim of combining the advantages of these two approaches, hybrid specification-based IDS methods have emerged [427].

### Traceability of Digital Evidence

When systems are compromised, specific information about the attacks might remain in the systems, unless attackers have been able to completely destroy their footprint. Preserving the traceability of these digital evidence is paramount to report the incident to the judicial authorities and initiate an investigation to prosecute the criminals. However, this represents a challenge for judiciary forces that should be able to face these criminals' behaviours in an efficient way and, in some case, from an international perspective. The procedure needed to obtain digital evidence, along with their recognition in a court of justice, should follow a standardised procedure accepted by most jurisdictions. This procedure should guarantee the origin of the evidence and the integrity of the chain of custody. As such, the lack of standardisation in the process of sharing and handling digital evidence among jurisdictions entails several disparities on how forensic reports are presented. Therefore, standardising the process used in the preparation of digital forensic reports is a crucial step towards producing high-quality reports and a way to facilitate the sharing and admissibility of reports across jurisdictions [428].

Despite the complexity of implementing similar mechanisms for the management and presentation of digital evidence in different jurisdictions, a series of international standards have been provided by ISO/IEC institutions with the aim to properly manage potential digital evidence from its collection to its reporting. For example, the ISO/IEC 27037 provides guidance with respect to the identification, collection, acquisition and preservation of digital evidence from different devices, such as storage media and mobile phones, among others [429]. In line with this standard, the ISO/IEC 27041 provides guidance to assure that the performed investigative process has been properly tested and meets the requirements of the investigation [430]; the ISO/IEC 27042 describes the correct conduct for analysis and interpretation of potential digital evidence to allow the correct evaluation, interpretation and reporting of the potential digital evidence [431]; and the ISO/IEC 27043 provides an overview of the investigation principles from the incident identification to its closure [432]. The correct implementation of these standards may be helpful to build trust and therefore, foster cross-border cooperation [433].

#### 4.3.4. Data Protection

In the management of personal information, there are a number of privacy concerns which arise throughout the entire data life cycle: from the storage and transmission over the network to their analysis and exploitation for secondary use. To prevent data misuse scandals and mitigate the impact of data leakages, legal privacy regulations, such as GDPR in Europe [434] and HIPAA in the United States [435], lay the foundations for the proper management and processing of personal information in the digital universe. Particularly, the enforcement of GDPR has strengthened people's privacy rights and forced organisations to adopt privacy-by-design principles, including data minimisation, transparent and lawful processing, accountability and pseudonymisation or encryption. As medical and biometric data are categorised as highly sensitive data, the privacy issues are even more apparent, and smart healthcare systems must carefully implement all the proper privacy-preserving safeguards to ensure both data confidentiality and privacy [436]. In this section, some privacy-preserving models are introduced, and the usefulness of awareness programmes are outlined.

##### Privacy Protection Models

From a privacy perspective, the main objective was to break the link between personally identifiable information (e.g., ID number, full name, social security number...) with its corresponding confidential information (e.g., physiological parameters, biometric data...). Therefore, in the case of a data leakage, people's identities cannot be seamlessly associated to confidential information. Pseudonymisation, a GDPR-friendly practice, can reduce privacy risks by masking individuals' identities with artificial identifiers, called pseudonyms [437]. This strategy has to be considered when communicating medical data between two entities among the network, so that only the legitimate entities can correlate the pseudonym with its identity. In the case of eavesdropping, attackers are not able to identify the source belonging to the captured sensitive data.

Once information is stored within the HIS for secondary use or statistical purposes, data should undergo an anonymisation process ensuring that a third-party is not able to re-identify the individual's identity from the data stored. In this context, in addition to the removal of personally identifiable information, a number of techniques can be applied to the data, such as noise addition (e.g., the physiological values are slightly different regarding the original ones) or micro-aggregation (e.g., creating groups of similar values and conserving only their centroids) [438]. In this aim, several privacy protection models have been proposed within the privacy protection literature, namely $k$-anonymity, $l$-diversity, $t$-closeness or differential privacy [439,440]. It is worth noting that the anonymisation procedure implies a trade-off between data quality and privacy: the more privacy, the lower the data quality.

##### Awareness Programmes

Organisations and public administrations should foster awareness programmes on cybersecurity and data protection to educate non-expert users. These programmes must provide high-quality updated information, tips, recommendations and campaigns that users could easily apply in their daily routines to prevent or mitigate user-oriented attacks. Among others, these programmes could be oriented for phishing, home/work computer security, mobile device security, secure remote working, best practices on strong passwords or Wi-Fi security. Unfortunately, these actions are often not applied in most organisations and when conducted, they are considered from a very generic perspective. Thus, in an intent to clarify the relationship between the human factor in phishing victimisation, the most recent research has been exploring the role of psychological traits and users' susceptibility to phishing attacks. The results of this research will facilitate the creation of more effective awareness campaigns and therefore, contribute to protect people, companies and infrastructures [441].

## 5. Future Challenges and Research Opportunities

Despite the progressive adoption of context-aware environments, smart healthcare applications and services are still constrained to very specific scenarios and cannot exploit all their potential. Thanks to the latest developments in the manufacturing of IoT and high-speed communications networks, the implementation of these environments will certainly accelerate in the years to come, and when they are a reality, the ecosystem of smart healthcare will reach a higher dimension.

Consumer electronics, by means of wearables, IoT and IoMT devices, have been the linchpin of most health-oriented services to enhance one's quality of life in the last decade. Significant advancements in the miniaturisation of sensors have opened the door to nanotechnology, which can revolutionise myriad aspects of healthcare and open the door to new frontiers and research opportunities, including disease diagnostics and monitoring, surgical devices, drug delivery and vaccine development. Although initial nanotechnology-based devices have already been set in the form of ingestible sensors and textile-based wearables, their use is still not generalised yet due to their costly manufacturing. Next-generation nanotechnology-based devices may consider smart pills with sensing, imaging and drug delivery capabilities for nanomedicine purposes, nanobots working as miniature surgeons with repairing capabilities of cellular structures, and nanofibres for regenerative medicine [442–444]. For instance, nanotechnology could play a key role in the fight against COVID-19 [445]. The optimism regarding nanotechnology has already enabled coining the term of the Internet of Nano-Things (IoNT) [446], whose success in the smart healthcare domain will mostly depend on the success to address its security concerns, not only regarding the safety of human lives, but also from the technological side. The development of security countermeasures in such technologies will certainly be a major technical challenge.

The increase in mobile devices integrating wireless communication capabilities adds complexity to the already challenging electromagnetic spectrum of context-aware environments. In these scenarios, the placement of the different devices from WSNs and WBANs can determine the correct performance of the entire system. Inadequate configurations can dramatically decrease the quality of service of devices operating in context-aware environments, leading to severe consequences in sensitive contexts, such as smart hospitals or smart ICUs. However, the continuous movement of both humans and wireless devices in these settings hinders the analysis of such communications systems. To this aim, radio-planning analyses in terms of coverage/capacity relations, power distribution, potential interference, power delay profiles and delay spread should be considered. Deterministic simulations based on ray optics, such as ray launching or ray tracing, are popular methods offering a reasonable trade-off between precision and computational cost. Many wireless technologies, including ZigBee, BLE and Bluetooth, have been studied in complex and highly dense environments such as hospitals and ICUs [447,448]. These analyses might not only help evaluate appropriate configurations of context-aware environments, but also anticipate and protect networks from malicious interference-based attacks, such as jamming attacks. Another inevitable challenge of next-generation communication networks is their evolution towards green communications. With the aim of reducing the alarming carbon footprint of current technologies due to their intensive demand, decreasing the energy consumption of communications is currently in the spotlight [449]. A number of low-power and green communication technologies are expected to gain popularity in the near future, including LPWAN and 5G models, which have already been evaluated under this model [450,451], as well as the 6G networks of tomorrow [452]. Energy-efficient lightweight security solutions will hence be a mandatory requirement in the wireless communication technologies of the future.

There are multiple emerging architectures that can enhance the security robustness of most current systems. However, their adoption in the smart healthcare domain is still at an embryonic stage. On the one hand, zero trust architectures [453] can be seen as an interesting solution to enhance security in systems. These architectures offer a security model based on the premise of not trusting any entity until a validation, legitimation and authorisation process has been passed. The model supports the implementation of least privileged access and continually requires the identification of actors who have gained access to the network. Although the adoption of zero trust models is not trivial [454], its application in smart healthcare applications might provide several benefits for users and bring new levels of security. On the other hand, the use of blockchain technology could provide a new model in the smart healthcare industry, by making electronic health records more efficient, transparent and secure. Thus, to secure information, smart contracts can be seen as an interesting alternative to existing systems as they remove the need for a mediator. In the near future, this technology could allow organisations creating a secure system to store patient records and therefore enabling faster diagnosis and interventions to each patient. However, despite the numerous opportunities that blockchain could provide in the smart healthcare sector, it also raises several challenges that should be addressed in future research. In this line, [455] highlighted the need to address issues such as patient data interoperability, secure storage in Cloud systems and data control in blockchain, among others.

Equally impressive is the evolution of artificial intelligence (AI) in the last decade, particularly that machine learning and deep learning. The maturity of this field enables influencing other areas. Today, with fast-evolving security threats and attacks, AI-based applications for cybersecurity offer a strategic advantage to thwart malicious endeavours of attackers at contained costs [456]. Many systems, including HIS and other components involved in smart healthcare environments, can enhance their robustness, response and resilience through AI [457]. For example, security attacks could be mitigated or defeated autonomously, including zero-day attacks whose value in the black market would decrease, security countermeasures could be launched on-the-fly according to attack severity, and honeypots could be dynamically generated. Moreover, AI can also fuel novel cybersecurity countermeasures to enable the detection of sophisticated malware and phishing, and the development of advanced IDS with excellent accuracy rates [458]. Recently introduced, multi-agent systems are expected to be promising solutions to face security threats in distributed architectures [459,460]. Although AI can significantly improve security solutions, it is a double-edged sword because it could also facilitate novel sorts of attacks that adversaries might exploit to generate new categories of vulnerabilities and unforeseen security threats may arise. With the aim of making AI reliable for cybersecurity, some development and monitoring practices should be followed [457], and ethical and legal challenges must be properly addressed [461].

Technology has irreversibly transformed healthcare systems and it is apparent to expect that it will still reshape them even more in the future. Future developments of healthcare systems will be partly influenced by the context where these health services will be provided. Hence, since smart healthcare was founded under the concept of smart cities and context-aware environments, next-generation healthcare paradigms might be founded under the contexts and environments of tomorrow. In particular, the conceptualisation of connected learning theories, such as connectivism [462], along with recent technological shifts, such as IoT, ubiquitous computing, IA and big data, have allowed the development of cognitive cities, a novel augmented urban paradigm that is gathering the attention of the research community. Cognitive cities [463], a particular implementation of a cognitive system at a very large scale, are able to learn, adapt their behaviour based on past experiences, and sense, understand and respond to changes in their immediate environment. Note that cognitive cities augment smart cities with learning and behavioural capabilities to face the challenges of future mega-cities. In this specific context, one might find appropriate coining a specific healthcare paradigm for cognitive environments: cognitive healthcare. To make cognitive healthcare a reality, numerous challenges will need to be addressed, including security and privacy issues inherited from the very cognitive environments [464]. Although cognitive healthcare is still ahead in the future, setting the ground for potential security and privacy problems can be achieved at present.

## 6. Conclusions

This article has addressed the deployment of effective and secure smart healthcare services in context-aware environments from a technical perspective. More specifically, we addressed the issue facing devices in the sensing layer, able to collect both user-centric attributes, such as cardiovascular activity, respiratory rate or location, and contextual attributes, such as air temperature or air pollution. These devices must be met with adequate accuracy, size, cost and power consumption to be suitable for smart health scenarios. As a result, all data can be conveyed, either using specific sensors networks, namely WBANs or WSNs, to the healthcare information systems that provide the corresponding services. Likewise, with the aim of enabling physicians, medical staff and automated processes to analyse these data and provide real-time diagnosis, suggest personalised treatments and raise alarms to emergency services in specific situations, this study provides a throughout description of a large number of wireless technologies. In particular, we observed that Bluetooth/BLE is a prominent technology in WBANs, and ZigBee can be used in such networks as well as in wider sensor networks. Promising technologies including 5G cellular networks are paving the way for scalable architectures for the transmission of large volumes of data under real-time constraints.

Moreover, we also addressed the issue of information security in the smart healthcare context, which is paramount due to the high sensitivity of the information handled. Indeed, sensor networks are prone to attacks and if no specific measures are considered, smart healthcare services are doomed to fail. To address this aspect, we anatomised and classified the information security requirements, attacks and solutions in smart healthcare systems. Attacks against sensing devices, communications, information systems and users were also detailed. In order to provide the whole system with security properties, the capabilities of the constrained resources and the networks scalability must be considered. Hence, proposals such as lightweight cryptography, DDoS countermeasures and authentication protocols are bound to be the basis of security protocols in smart healthcare scenarios. Moreover, since the management of personal information arises a number of privacy concerns, we also recalled the basics of data protection, either from a technical perspective using privacy models and from a non-technical perspective with educational awareness programmes.

In a nutshell, in this article, we described a wide range of technologies and protocols, and we demonstrated that there exist a number of alternatives to be considered when designing and deploying smart healthcare services. However, we omitted some other aspects that could also be of interest. For instance, the interoperability problem related to the complex ecosystem of protocols, standards and manufacturers, specifically in sensor devices. Furthermore, education on the right use of technology, awareness programmes about cybersecurity and data privacy, ethical aspects of smart healthcare and their corresponding legal initiatives are only in their very early stages.

**Author Contributions:** Conceptualisation, E.B., M.A.M. and A.S.; writing—original draft preparation, E.B., M.A.M., P.L.-A. and A.M.-B.; writing—review and editing, E.B., P.L.-A., A.M.-B. and A.S.; visualisation, E.B.; supervision, A.M.-B. and A.S.; funding acquisition, A.M.-B. and A.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by grant IoTrain RTI2018-095499-B-C32 funded by MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe". Also, this research was supported by the Government of Catalonia with projects 2017-DI-002, 2017-SGR-896 and ACTUA 2020PANDE00103, by Universitat Rovira i Virgili with project 2017PFR-URV-B2-41, by the European

Commission with LOCARD project under grant number 832735, and by GoodBrother COST action 19121.

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

**Informed Consent Statement:** Not applicable.

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

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| ABE | Attribute-Based Encryption |
| ABG | Arterial Blood Gas |
| AES | Advanced Encryption Standard |
| AI | Artificial Intelligence |
| ARP | Address Resolution Protocol |
| BCG | Ballistocardiography |
| BLE | Bluetooth Low Energy |
| COPD | Chronic Obstructive Pulmonary Disease |
| DDoS | Distributed Denial of Service |
| DNS | Domain Name System |
| DoS | Denial of Service |
| ECC | Elliptic-Curve Cryptography |
| ECG | Electrocardiography |
| EDA | Electrodermal Activity |
| EEG | Electroencephalography |
| EMG | Electromyography |
| FBG | Fibre Bragg Grating |
| fNIRS | Functional Near-Infrared Spectroscopy |
| GDPR | General Data Protection Regulation |
| GPS | Global Positioning System |
| HBC | Human Body Communication |
| HIDS | Host-Based Intrusion Detection Systems |
| HIPAA | Health Insurance Portability and Accountability Act |
| HIS | Healthcare Information System |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| ICT | Information and Communication Technologies |
| ICU | Intensive Care Unit |
| IDS | Intrusion Detection Systems |
| IEC | International Electrotechnical Commission |
| IMU | Inertial Measurement Units |
| IoMT | Internet of Medical Things |
| IoT | Internet of Things |
| IP | Internet Protocol |
| ISO | International Organisation for Standardisation |
| LPWAN | Low-Power Wide-Area Networks |
| LTE | Long-Term Evolution |
| MAC (address) | Media Access Control |
| MAC (code) | Message Authentication Code |
| MEG | Magnetoencephalography |
| MEMS | Microelectromechanical Systems |
| MitM | Man-in-the-Middle |
| MMG | Mechanomyography |
| MOS | Metal Oxide Semiconductor |
| NB | Narrowband |

| | |
|---|---|
| NFC | Near-Field Communication |
| NIDS | Network-Based Intrusion Detection Systems |
| OSI | Open Systems Interconnection |
| OSINT | Open Source Intelligence |
| PCG | Phonocardiography |
| PET | Positron-Emission Tomography |
| PPG | Photoplethysmography |
| PTT | Pulse Transit Time |
| RBAC | Role-Based Access Control |
| RFID | Radio Frequency Identification |
| RGB | Red Green Blue |
| RSA | Rivest–Shamir–Adleman |
| RTS/CTS | Request to Send/Clear To Send |
| SHA | Secure Hash Algorithm |
| TCP | Transmission Control Protocol |
| UV | Ultraviolet |
| UWB | Ultra Wideband |
| WBAN | Wireless Body Area Networks |
| WPA | Wi-Fi Protected Access |
| WPS | WiFi-based Positioning System |
| WSN | Wireless Sensor Networks |

## References

1. 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]
2. Eysenbach, G. What is e-health? *J. Med. Internet Res.* **2001**, *3*, e20. [CrossRef]
3. Istepanian, R.S.; Laxminarayan, S.; Pattichis, C. (Eds). *M-Health—Emerging Mobile Health Systems*; Topics in Biomedical Engineering; Springer: New York, NY, USA, 2006.
4. Solanas, A.; Casino, F.; Batista, E.; Rallo, R. Trends and Challenges in Smart Healthcare Research: A Journey from Data to Wisdom. In Proceedings of the IEEE 3rd International Forum on Research and Technologies for Society and Industry, Modena, Italy, 11–13 September 2017; pp. 1–6.
5. Casino, F.; Patsakis, C.; Batista, E.; Borràs, F.; Martínez-Ballesté, A. Healthy Routes in the Smart City. *IEEE Softw.* **2017**, *34*, 42–47. [CrossRef]
6. Patsakis, C.; Papageorgiou, A.; Falcone, F.; Solanas, A. s-Health as a driver towards better emergency response systems in urban environments. In Proceedings of the 10th IEEE International Symposium on Medical Measurements and Application, Turin, Italy, 7–9 May 2015; pp. 214–218.
7. Sundaravadivel, P.; Kougianos, E.; Mohanty, S.P.; Ganapathiraju, M.K. Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health. *IEEE Consum. Electron. Mag.* **2017**, *7*, 18–28. [CrossRef]
8. Movassaghi, S.; Abolhasan, M.; Lipman, J.; Smith, D.; Jamalipour, A. Wireless Body Area Networks: A Survey. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 1658–1686. [CrossRef]
9. Salayma, M.; Al-Dubai, A.; Romdhani, I.; Nasser, Y. Wireless Body Area Network (WBAN) A Survey on Reliability, Fault Tolerance, and Technologies Coexistence. *ACM Comput. Surv.* **2017**, *50*, 1–38. [CrossRef]
10. Aguirre, E.; Lopez-Iturri, P.; Azpilicueta, L.; Redondo, A.; Astrain, J.J.; Villadangos, J.; Bahillo, A.; Perallos, A.; Falcone, F. Design and Implementation of Context Aware Applications WITH Wireless Sensor Network Support in Urban Train Transportation Environments. *IEEE Sens. J.* **2016**, *17*, 169–178. [CrossRef]
11. Lombardo, L.; Corbellini, S.; Parvis, M.; Elsayed, A.; Angelini, E.; Grassini, S. Wireless Sensor Network for Distributed Environmental Monitoring. *IEEE Trans. Instrum. Meas.* **2017**, *67*, 1214–1222. [CrossRef]
12. Czeschik, C. Black Market Value of Patient Data. In *Digital Marketplaces Unleashed*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 883–893.
13. Yao, M. Your Electronic Medical Records Could Be Worth $1000 To Hackers. Available online: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/ (accessed on 1 August 2021).
14. Yetisen, A.K.; Martinez-Hurtado, J.L.; Ünal, B.; Khademhosseini, A.; Butt, H. Wearables in Medicine. *Adv. Mater.* **2018**, *30*, 1706910. [CrossRef] [PubMed]
15. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
16. Dian, F.J.; Vahidnia, R.; Rahmati, A. Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey. *IEEE Access* **2020**, *8*, 69200–69211. [CrossRef]

17. Seneviratne, S.; Hu, Y.; Nguyen, T.; Lan, G.; Khalifa, S.; Thilakarathna, K.; Hassan, M.; Seneviratne, A. A survey of wearable devices and challenges. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 2573–2620. [CrossRef]
18. Negra, R.; Jemili, I.; Belghith, A. Wireless Body Area Networks: Applications and technologies. *Procedia Comput. Sci.* **2016**, *83*, 1274–1281. [CrossRef]
19. Khan, R.A.; Pathan, A.S.K. The state-of-the-art wireless body area sensor networks: A survey. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1550147718768994. [CrossRef]
20. Ahad, A.; Tahir, M.; Aman Sheikh, M.; Ahmed, K.I.; Mughees, A.; Numani, A. Technologies Trend towards 5G Network for Smart Health-Care Using IoT: A Review. *Sensors* **2020**, *20*, 4047. [CrossRef] [PubMed]
21. Hajar, M.S.; Al-Kadri, M.O.; Kalutarage, H.K. A survey on wireless body area networks: Architecture, security challenges and research opportunities. *Comput. Secur.* **2021**, *104*, 102211. [CrossRef]
22. Qureshi, F.; Krishnan, S. Wearable Hardware Design for the Internet of Medical Things (IoMT). *Sensors* **2018**, *18*, 3812. [CrossRef] [PubMed]
23. Xu, S.; Jayaraman, A.; Rogers, J.A. Skin sensors are the future of health care. *Nature* **2019**, *571*, 319–321. [CrossRef] [PubMed]
24. World Health Organization. Cardiovascular Diseases (CVDs). Available online: https://www.who.int/health-topics/cardiovascular-diseases (accessed on 27 September 2021).
25. Michard, F. A sneak peek into digital innovations and wearable sensors for cardiac monitoring. *J. Clin. Monit. Comput.* **2017**, *31*, 253–259. [CrossRef]
26. Redfern, J. Can Older Adults Benefit from Smart Devices, Wearables, and Other Digital Health Options to Enhance Cardiac Rehabilitation? *Clin. Geriatr. Med.* **2019**, *35*, 489–497. [CrossRef]
27. Kiranyaz, S.; Ince, T.; Gabbouj, M. Personalized Monitoring and Advance Warning System for Cardiac Arrhythmias. *Sci. Rep.* **2017**, *7*, 9270. [CrossRef]
28. Ousaka, D.; Sakano, N.; Morita, M.; Shuku, T.; Sanou, K.; Kasahara, S.; Oozawa, S. A new approach to prevent critical cardiac accidents in athletes by real-time electrocardiographic tele-monitoring system: Initial trial in full marathon. *J. Cardiol. Cases* **2019**, *20*, 35–38. [CrossRef]
29. Nedoma, J.; Fajkus, M.; Martinek, R.; Kepak, S.; Cubik, J.; Zabka, S.; Vasinek, V. Comparison of BCG, PCG and ECG Signals in Application of Heart Rate Monitoring of the Human Body. In Proceedings of the 40th International Conference on Telecommunications and Signal Processing, Barcelona, Spain, 5–7 July 2017; pp. 420–424.
30. Spanò, E.; Di Pascoli, S.; Iannaccone, G. Low-Power Wearable ECG Monitoring System for Multiple-Patient Remote Monitoring. *IEEE Sens. J.* **2016**, *16*, 5452–5462. [CrossRef]
31. Yang, Z.; Zhou, Q.; Lei, L.; Zheng, K.; Xiang, W. An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. *J. Med. Syst.* **2016**, *40*, 286. [CrossRef]
32. Rachim, V.P.; Chung, W.Y. Wearable Noncontact Armband for Mobile ECG Monitoring System. *IEEE Trans. Biomed. Circuits Syst.* **2016**, *10*, 1112–1118. [CrossRef] [PubMed]
33. Ankhili, A.; Tao, X.; Cochrane, C.; Coulon, D.; Koncar, V. Washable and Reliable Textile Electrodes Embedded into Underwear Fabric for Electrocardiography (ECG) Monitoring. *Materials* **2018**, *11*, 256. [CrossRef]
34. Biswas, D.; Simões-Capela, N.; Van Hoof, C.; Van Helleputte, N. Heart Rate Estimation From Wrist-Worn Photoplethysmography: A Review. *IEEE Sens. J.* **2019**, *19*, 6560–6570. [CrossRef]
35. Fiorini, L.; Cavallo, F.; Martinelli, M.; Rovini, E. Characterization of a PPG Wearable Sensor to be Embedded into an Innovative Ring-Shaped Device for Healthcare Monitoring. In *Ambient Assisted Living: Italian Forum 2019*; Springer: Cham, Switzerland, 2021; pp. 49–63.
36. Jo, E.; Lewis, K.; Directo, D.; Kim, M.J.; Dolezal, B.A. Validation of Biofeedback Wearables for Photoplethysmographic Heart Rate Tracking. *J. Sport. Sci. Med.* **2016**, *15*, 540.
37. Chowdhury, S.S.; Hyder, R.; Hafiz, M.S.B.; Haque, M.A. Real-Time Robust Heart Rate Estimation From Wrist-Type PPG Signals Using Multiple Reference Adaptive Noise Cancellation. *IEEE J. Biomed. Health Inform.* **2016**, *22*, 450–459. [CrossRef] [PubMed]
38. Bent, B.; Goldstein, B.A.; Kibbe, W.A.; Dunn, J.P. Investigating sources of inaccuracy in wearable optical heart rate sensors. *NPJ Digit. Med.* **2020**, *3*, 1–8. [CrossRef]
39. Temko, A. Accurate Heart Rate Monitoring During Physical Exercises Using PPG. *IEEE Trans. Biomed. Eng.* **2017**, *64*, 2016–2024. [CrossRef] [PubMed]
40. Albukhari, A.; Lima, F.; Mescheder, U. Bed-Embedded Heart and Respiration Rates Detection by Longitudinal Ballistocardiography and Pattern Recognition. *Sensors* **2019**, *19*, 1451. [CrossRef] [PubMed]
41. Ismail, S.; Siddiqi, I.; Akram, U. Localization and classification of heart beats in phonocardiography signals—A comprehensive review. *EURASIP J. Adv. Signal Process.* **2018**, *2018*, 26. [CrossRef]
42. Cheung, C.C.; Olgin, J.E.; Lee, B.K. Wearable cardioverter-defibrillators: A review of evidence and indications. *Trends Cardiovasc. Med.* **2021**, *31*, 196–201. [CrossRef]
43. Wäßnig, N.K.; Günther, M.; Quick, S.; Pfluecke, C.; Rottstädt, F.; Szymkiewicz, S.J.; Ringquist, S.; Strasser, R.H.; Speiser, U. Experience with the Wearable Cardioverter-Defibrillator in Patients at High Risk for Sudden Cardiac Death. *Circulation* **2016**, *134*, 635–643. [CrossRef]

44. Kutyifa, V.; Moss, A.J.; Klein, H.; Biton, Y.; McNitt, S.; MacKecknie, B.; Zareba, W.; Goldenberg, I. Use of the Wearable Cardioverter Defibrillator in High-Risk Cardiac Patients: Data From the Prospective Registry of Patients Using the Wearable Cardioverter Defibrillator (WEARIT-II Registry). *Circulation* **2015**, *132*, 1613–1619. [CrossRef]
45. Phattraprayoon, N.; Sardesai, S.; Durand, M.; Ramanathan, R. Accuracy of pulse oximeter readings from probe placement on newborn wrist and ankle. *J. Perinatol.* **2012**, *32*, 276–280. [CrossRef]
46. Seifi, S.; Khatony, A.; Moradi, G.; Abdi, A.; Najafi, F. Accuracy of pulse oximetry in detection of oxygen saturation in patients admitted to the intensive care unit of heart surgery: Comparison of finger, toe, forehead and earlobe probes. *BMC Nurs.* **2018**, *17*, 1–7. [CrossRef]
47. Chen, Q.; Tang, L. A wearable blood oxygen saturation monitoring system based on bluetooth low energy technology. *Coputer Commun.* **2020**, *160*, 101–110. [CrossRef]
48. Davies, H.J.; Williams, I.; Peters, N.S.; Mandic, D.P. In-Ear SpO2: A Tool for Wearable, Unobtrusive Monitoring of Core Blood Oxygen Saturation. *Sensors* **2020**, *20*, 4879. [CrossRef]
49. Ma, G.; Zhu, W.; Zhong, J.; Tong, T.; Zhang, J.; Wang, L. Wearable Ear Blood Oxygen Saturation and Pulse Measurement System Based on PPG. In Proceedings of the IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, Guangzhou, China, 8–12 October 2018; pp. 111–116.
50. Lochner, C.M.; Khan, Y.; Pierre, A.; Arias, A.C. All-organic optoelectronic sensor for pulse oximetry. *Nat. Commun.* **2014**, *5*, 5745. [CrossRef]
51. Coyle, S.; Lau, K.T.; Moyna, N.; O'Gorman, D.; Diamond, D.; Di Francesco, F.; Costanzo, D.; Salvo, P.; Trivella, M.G.; De Rossi, D.E.; et al. BIOTEX — Biosensing Textiles for Personalised Healthcare Management. *IEEE Trans. Inf. Technol. Biomed.* **2010**, *14*, 364–370. [CrossRef]
52. Arakawa, T. Recent Research and Developing Trends of Wearable Sensors for Detecting Blood Pressure. *Sensors* **2018**, *18*, 2772. [CrossRef] [PubMed]
53. Kachuee, M.; Kiani, M.M.; Mohammadzade, H.; Shabany, M. Cuffless Blood Pressure Estimation Algorithms for Continuous Health-Care Monitoring. *IEEE Trans. Biomed. Eng.* **2016**, *64*, 859–869. [CrossRef] [PubMed]
54. Liu, H.; Ivanov, K.; Wang, Y.; Wang, L. Toward a Smartphone Application for Estimation of Pulse Transit Time. *Sensors* **2015**, *15*, 27303–27321. [CrossRef] [PubMed]
55. Carek, A.M.; Conant, J.; Joshi, A.; Kang, H.; Inan, O.T. SeismoWatch: Wearable Cuffless Blood Pressure Monitoring Using Pulse Transit Time. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*; Association for Computing Machinery: New York, NY, USA, 2017; Volume 1, pp. 1–16.
56. Kario, K. Management of Hypertension in the Digital Era: Small Wearable Monitoring Devices for Remote Blood Pressure Monitoring. *Hypertension* **2020**, *76*, 640–650. [CrossRef]
57. Ringrose, J.; Padwal, R. Wearable Technology to Detect Stress-Induced Blood Pressure Changes: The Next Chapter in Ambulatory Blood Pressure Monitoring? *Am. J. Hypertens.* **2021**, *34*, 330–331. [CrossRef] [PubMed]
58. Lin, H.; Xu, W.; Guan, N.; Ji, D.; Wei, Y.; Yi, W. Noninvasive and Continuous Blood Pressure Monitoring Using Wearable Body Sensor Networks. *IEEE Intell. Syst.* **2015**, *30*, 38–48. [CrossRef]
59. Holz, C.; Wang, E.J. Glabella: Continuously Sensing Blood Pressure Behavior using an Unobtrusive Wearable Device. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2017**, *1*, 58. [CrossRef]
60. Chang, S.H.; Chiang, R.D.; Wu, S.J.; Chang, W.T. A Context-Aware, Interactive M-Health System for Diabetics. *IT Prof.* **2016**, *18*, 14–22. [CrossRef]
61. Valenzuela, F.; García, A.; Vázquez, M.; Cortez, J.; Espinoza, A. An IoT-Based Glucose Monitoring Algorithm to Prevent Diabetes Complications. *Appl. Sci.* **2020**, *10*, 921. [CrossRef]
62. Al-Taee, M.A.; Al-Nuaimy, W.; Muhsin, Z.J.; Al-Ataby, A. Robot Assistant in Management of Diabetes in Children Based on the Internet of Things. *IEEE Internet Things J.* **2016**, *4*, 437–445. [CrossRef]
63. Kim, J.; Campbell, A.S.; Wang, J. Wearable non-invasive epidermal glucose sensors: A review. *Talanta* **2018**, *177*, 163–170. [CrossRef] [PubMed]
64. Bandodkar, A.J.; Jia, W.; Yardımcı, C.; Wang, X.; Ramirez, J.; Wang, J. Tattoo-Based Noninvasive Glucose Monitoring: A Proof-of-Concept Study. *Anal. Chem.* **2015**, *87*, 394–398. [CrossRef] [PubMed]
65. Xiao, Z.; Tan, X.; Chen, X.; Chen, S.; Zhang, Z.; Zhang, H.; Wang, J.; Huang, Y.; Zhang, P.; Zheng, L.; et al. An Implantable RFID Sensor Tag toward Continuous Glucose Monitoring. *IEEE J. Biomed. Health Inform.* **2015**, *19*, 910–919. [CrossRef] [PubMed]
66. Ali, H.; Bensaali, F.; Jaber, F. Novel Approach to Non-Invasive Blood Glucose Monitoring Based on Transmittance and Refraction of Visible Laser Light. *IEEE Access* **2017**, *5*, 9163–9174. [CrossRef]
67. Haxha, S.; Jhoja, J. Optical Based Noninvasive Glucose Monitoring Sensor Prototype. *IEEE Photonics J.* **2016**, *8*, 1–11. [CrossRef]
68. Yadav, K.S.; Kapse-Mistry, S.; Peters, G.J.; Mayur, Y.C. E-drug delivery: A futuristic approach. *Drug Discov. Today* **2019**, *24*, 1023–1030. [CrossRef] [PubMed]
69. Eggenberger, P.; MacRae, B.A.; Kemp, S.; Bürgisser, M.; Rossi, R.M.; Annaheim, S. Prediction of Core Body Temperature Based on Skin Temperature, Heat Flux, and Heart Rate Under Different Exercise and Clothing Conditions in the Heat in Young Adult Males. *Front. Physiol.* **2018**, *9*, 1780. [CrossRef]

70. de Andrade Fernandes, A.; dos Santos Amorim, P.R.; Brito, C.J.; de Moura, A.G.; Moreira, D.G.; Costa, C.M.A.; Sillero-Quintana, M.; Marins, J.C.B. Measuring skin temperature before, during and after exercise: A comparison of thermocouples and infrared thermography. *Physiol. Meas.* **2014**, *35*, 189. [CrossRef]
71. Huang, M.; Tamura, T.; Tang, Z.; Chen, W.; Kanaya, S. A Wearable Thermometry for Core Body Temperature Measurement and Its Experimental Verification. *IEEE J. Biomed. Health Inform.* **2016**, *21*, 708–714. [CrossRef]
72. Atallah, L.; Ciuhu, C.; Wang, C.; Bongers, E.; Blom, T.; Paulussen, I.; Noordergraaf, G.J. An Ergonomic Wearable Core Body Temperature Sensor. In Proceedings of the IEEE 15th International Conference on Wearable and Implantable Body Sensor Networks, Las Vegas, NV, USA, 4–7 March 2018; pp. 70–73.
73. Shin, J.; Jeong, B.; Kim, J.; Binh Nam, V.; Yoon, Y.; Jung, J.; Hong, S.; Lee, H.; Eom, H.; Yeo, J.; et al. Sensitive Wearable Temperature Sensor with Seamless Monolithic Integration. *Adv. Mater.* **2020**, *32*, 1905527. [CrossRef]
74. Mizuno, T.; Kume, Y. Development of a Glasses-Like Wearable Device to Measure Nasal Skin Temperature. In Proceedings of the International Conference on Human—Computer Interaction, Los Angeles, CA, USA, 2–7 August 2015; Springer: Cham, Switzerland, 2015; pp. 727–732.
75. Xu, X.; Karis, A.J.; Buller, M.J.; Santee, W.R. Relationship between core temperature, skin temperature, and heat flux during exercise in heat. *Eur. J. Appl. Physiol.* **2013**, *113*, 2381–2389. [CrossRef] [PubMed]
76. Li, H.; Yang, H.; Li, E.; Liu, Z.; Wei, K. Wearable sensors in intelligent clothing for measuring human body temperature based on optical fiber Bragg grating. *Opt. Express* **2012**, *20*, 11740–11752. [CrossRef] [PubMed]
77. Chen, X.; Ren, Z.; Guo, H.; Cheng, X.; Zhang, H. Self-powered flexible and transparent smart patch for temperature sensing. *Appl. Phys. Lett.* **2020**, *116*, 043902. [CrossRef]
78. Shi, X.; Wu, P. A Smart Patch with On-Demand Detachable Adhesion for Bioelectronics. *Small* **2021**, *17*, 2101220. [CrossRef] [PubMed]
79. Chen, Y.; Lu, B.; Chen, Y.; Feng, X. Breathable and Stretchable Temperature Sensors Inspired by Skin. *Sci. Rep.* **2015**, *5*, 11505. [CrossRef]
80. Rajan, G.; Morgan, J.J.; Murphy, C.; Torres Alonso, E.; Wade, J.; Ott, A.K.; Russo, S.; Alves, H.; Craciun, M.F.; Neves, A.I.S. Low Operating Voltage Carbon–Graphene Hybrid E-textile for Temperature Sensing. *ACS Appl. Mater. Interfaces* **2020**, *12*, 29861–29867. [CrossRef]
81. Fleury, A.; Sugar, M.; Chau, T. E-textiles in Clinical Rehabilitation: A Scoping Review. *Electronics* **2015**, *4*, 173–203. [CrossRef]
82. Fleming, S.; Thompson, M.; Stevens, R.; Heneghan, C.; Plüddemann, A.; Maconochie, I.; Tarassenko, L.; Mant, D. Normal ranges of heart rate and respiratory rate in children from birth to 18 years of age: A systematic review of observational studies. *Lancet* **2011**, *377*, 1011–1018. [CrossRef]
83. Massaroni, C.; Nicolò, A.; Lo Presti, D.; Sacchetti, M.; Silvestri, S.; Schena, E. Contact-Based Methods for Measuring Respiratory Rate. *Sensors* **2019**, *19*, 908. [CrossRef] [PubMed]
84. Chu, M.; Nguyen, T.; Pandey, V.; Zhou, Y.; Pham, H.N.; Bar-Yoseph, R.; Radom-Aizik, S.; Jain, R.; Cooper, D.M.; Khine, M. Respiration rate and volume measurements using wearable strain sensors. *NPJ Digit. Med.* **2019**, *2*, 1–9. [CrossRef] [PubMed]
85. Naranjo-Hernández, D.; Talaminos-Barroso, A.; Reina-Tosina, J.; Roa, L.M.; Barbarov-Rostan, G.; Cejudo-Ramos, P.; Márquez-Martín, E.; Ortega-Ruiz, F. Smart Vest for Respiratory Rate Monitoring of COPD Patients Based on Non-Contact Capacitive Sensing. *Sensors* **2018**, *18*, 2144. [CrossRef]
86. Chen, R.; Chen, K.; Dai, Y.; Zhang, S. Utility of transthoracic impedance and novel algorithm for sleep apnea screening in pacemaker patient. *Sleep Breath.* **2019**, *23*, 741–746. [CrossRef]
87. Heydari, F.; Ebrahim, M.P.; Yuce, M.R. Chest-based Real-Time Pulse and Respiration Monitoring Based on Bio-Impedance. In Proceedings of the 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society, Montreal, QC, Canada, 20–24 July 2020; pp. 4398–4401.
88. Wang, F.T.; Chan, H.L.; Wang, C.L.; Jian, H.M.; Lin, S.H. Instantaneous Respiratory Estimation from Thoracic Impedance by Empirical Mode Decomposition. *Sensors* **2015**, *15*, 16372–16387. [CrossRef]
89. Lapi, S.; Lavorini, F.; Borgioli, G.; Calzolai, M.; Masotti, L.; Pistolesi, M.; Fontana, G.A. Respiratory rate assessments using a dual-accelerometer device. *Respir. Physiol. Neurobiol.* **2014**, *191*, 60–66. [CrossRef] [PubMed]
90. Ferreira, A.G.; Fernandes, D.; Branco, S.; Monteiro, J.L.; Cabral, J.; Catarino, A.P.; Rocha, A.M. A Smart Wearable System for Sudden Infant Death Syndrome Monitoring. In Proceedings of the IEEE International Conference on Industrial Technology, Taipei, Taiwan, 14–17 March 2016; pp. 1920–1925.
91. Sharma, P.; Hui, X.; Zhou, J.; Conroy, T.B.; Kan, E.C. Wearable radio-frequency sensing of respiratory rate, respiratory volume, and heart rate. *NPJ Digit. Med.* **2020**, *3*, 1–10. [CrossRef]
92. Al-Halhouli, A.; Al-Ghussain, L.; El Bouri, S.; Habash, F.; Liu, H.; Zheng, D. Clinical Evaluation of Stretchable and Wearable Inkjet-Printed Strain Gauge Sensor for Respiratory Rate Monitoring at Different Body Postures. *Appl. Sci.* **2020**, *10*, 480. [CrossRef]
93. Piuzzi, E.; Pisa, S.; Pittella, E.; Podestà, L.; Sangiovanni, S. Wearable Belt With Built-In Textile Electrodes for Cardio—Respiratory Monitoring. *Sensors* **2020**, *20*, 4500. [CrossRef] [PubMed]
94. Jun, Z.; Chun-na, L.; Wen-liang, Z.; Hong, Z.; Yong-feng, L.; Xue-feng, H. Wearable respiratory strain monitoring system based on textile-based capacitive strain sensor. *J. Physics Conf. Ser.* **2020**, *1570*, 012033. [CrossRef]

95. Oletic, D.; Bilas, V. Energy-Efficient Respiratory Sounds Sensing for Personal Mobile Asthma Monitoring. *IEEE Sensors J.* **2016**, *16*, 8295–8303. [CrossRef]
96. Corbishley, P.; Rodriguez-Villegas, E. Breathing Detection: Towards a Miniaturized, Wearable, Battery-Operated Monitoring System. *IEEE Trans. Biomed. Eng.* **2007**, *55*, 196–204. [CrossRef] [PubMed]
97. Larson, E.C.; Goel, M.; Boriello, G.; Heltshe, S.; Rosenfeld, M.; Patel, S.N. SpiroSmart: Using a Microphone to Measure Lung Function on a Mobile Phone. In Proceedings of the ACM Conference on Ubiquitous Computing, Pittsburgh, PA, USA, 5–8 September 2012; pp. 280–289.
98. Milici, S.; Lorenzo, J.; Lázaro, A.; Villarino, R.; Girbau, D. Wireless Breathing Sensor Based on Wearable Modulated Frequency Selective Surface. *IEEE Sens. J.* **2016**, *17*, 1285–1292. [CrossRef]
99. Kano, S.; Kim, K.; Fujii, M. Fast-Response and Flexible Nanocrystal-Based Humidity Sensor for Monitoring Human Respiration and Water Evaporation on Skin. *ACS Sens.* **2017**, *2*, 828–833. [CrossRef] [PubMed]
100. Varon, C.; Caicedo, A.; Testelmans, D.; Buyse, B.; Van Huffel, S. A novel algorithm for the automatic detection of sleep apnea from single-lead ECG. *IEEE Trans. Biomed. Eng.* **2015**, *62*, 2269–2278. [CrossRef]
101. Varon, C.; Morales, J.; Lázaro, J.; Orini, M.; Deviaene, M.; Kontaxis, S.; Testelmans, D.; Buyse, B.; Borzée, P.; Sörnmo, L.; et al. A Comparative Study of ECG-derived Respiration in Ambulatory Monitoring using the Single-lead ECG. *Sci. Rep.* **2020**, *10*, 1–14. [CrossRef]
102. Touw, H.R.W.; Verheul, M.H.; Tuinman, P.R.; Smit, J.; Thöne, D.; Schober, P.; Boer, C. Photoplethysmography respiratory rate monitoring in patients receiving procedural sedation and analgesia for upper gastrointestinal endoscopy. *J. Clin. Monit. Comput.* **2017**, *31*, 747–754. [CrossRef] [PubMed]
103. Karlen, W.; Raman, S.; Ansermino, J.M.; Dumont, G.A. Multiparameter Respiratory Rate Estimation From the Photoplethysmogram. *IEEE Trans. Biomed. Eng.* **2013**, *60*, 1946–1953. [CrossRef]
104. AL-Khalidi, F.Q.; Saatchi, R.; Burke, D.; Elphick, H.; Tan, S. Respiration Rate Monitoring Methods: A Review. *Pediatr. Pulmonol.* **2011**, *46*, 523–529. [CrossRef]
105. Massaroni, C.; Lo Presti, D.; Formica, D.; Silvestri, S.; Schena, E. Non-Contact Monitoring of Breathing Pattern and Respiratory Rate via RGB Signal Measurement. *Sensors* **2019**, *19*, 2758. [CrossRef]
106. Massaroni, C.; Lopes, D.S.; Lo Presti, D.; Schena, E.; Silvestri, S. Contactless Monitoring of Breathing Patterns and Respiratory Rate at the Pit of the Neck: A Single Camera Approach. *J. Sens.* **2018**, *2018*, 4567213. [CrossRef]
107. Pereira, C.B.; Yu, X.; Goos, T.; Reiss, I.; Orlikowsky, T.; Heimann, K.; Venema, B.; Blazek, V.; Leonhardt, S.; Teichmann, D. Noncontact Monitoring of Respiratory Rate in Newborn Infants Using Thermal Imaging. *IEEE Trans. Biomed. Eng.* **2018**, *66*, 1105–1114. [CrossRef]
108. Kusche, R.; John, F.; Cimdins, M.; Hellbrück, H. Contact-Free Biosignal Acquisition via Capacitive and Ultrasonic Sensors. *IEEE Access* **2020**, *8*, 95629–95641. [CrossRef]
109. Min, S.D.; Kim, J.K.; Shin, H.S.; Yun, Y.H.; Lee, C.K.; Lee, M. Noncontact Respiration Rate Measurement System Using an Ultrasonic Proximity Sensor. *IEEE Sens. J.* **2010**, *10*, 1732–1739.
110. Casson, A.J.; Yates, D.C.; Smith, S.J.M.; Duncan, J.S.; Rodriguez-Villegas, E. Wearable Electroencephalography: What Is It, Why Is It Needed, and What Does It Entail? *IEEE Eng. Med. Biol. Mag.* **2010**, *29*, 44–56. [CrossRef]
111. Apicella, A.; Arpaia, P.; Frosolone, M.; Moccaldi, N. High-wearable EEG-based distraction detection in motor rehabilitation. *Sci. Rep.* **2021**, *11*, 1–9. [CrossRef]
112. Byrom, B.; McCarthy, M.; Schueler, P.; Muehlhausen, W. Brain Monitoring Devices in Neuroscience Clinical Research: The Potential of Remote Monitoring Using Sensors, Wearables, and Mobile Devices. *Clin. Pharmacol. Ther.* **2018**, *104*, 59–71. [CrossRef] [PubMed]
113. Lau-Zhu, A.; Lau, M.P.H.; McLoughlin, G. Mobile EEG in research on neurodevelopmental disorders: Opportunities and challenges. *Dev. Cogn. Neurosci.* **2019**, *36*, 100635. [CrossRef]
114. Mihajlović, V.; Grundlehner, B.; Vullers, R.; Penders, J. Wearable, Wireless EEG Solutions in Daily Life Applications: What are we Missing? *IEEE J. Biomed. Health Inform.* **2014**, *19*, 6–21. [CrossRef] [PubMed]
115. Lin, C.T.; Chuang, C.H.; Cao, Z.; Singh, A.K.; Hung, C.S.; Yu, Y.H.; Nascimben, M.; Liu, Y.T.; King, J.T.; Su, T.P.; et al. Forehead EEG in Support of Future Feasible Personal Healthcare Solutions: Sleep Management, Headache Prevention, and Depression Treatment. *IEEE Access* **2017**, *5*, 10612–10621. [CrossRef]
116. Athavipach, C.; Pan-ngum, S.; Israsena, P. A Wearable In-Ear EEG Device for Emotion Monitoring. *Sensors* **2019**, *19*, 4014. [CrossRef] [PubMed]
117. Gu, Y.; Cleeren, E.; Dan, J.; Claes, K.; Van Paesschen, W.; Van Huffel, S.; Hunyadi, B. Comparison between Scalp EEG and Behind-the-Ear EEG for Development of a Wearable Seizure Detection System for Patients with Focal Epilepsy. *Sensors* **2018**, *18*, 29. [CrossRef] [PubMed]
118. Casson, A.J. Wearable EEG and beyond. *Biomed. Eng. Lett.* **2019**, *9*, 53–71. [CrossRef] [PubMed]
119. von Lühmann, A.; Zimmermann, B.B.; Ortega-Martinez, A.; Perkins, N.; Yücel, M.A.; Boas, D.A. Towards Neuroscience in the Everyday World: Progress in wearable fNIRS instrumentation and applications. In Proceedings of the Biophotonics Congress: Biomedical Optics 2020, Ford Lauderdale, FL, USA, 20–23 April 2020; OSA Technical Digest (Optical Society of America, US. 2020), paper BM3C.2.

120. Kassab, A.; Le Lan, J.; Tremblay, J.; Vannasing, P.; Dehbozorgi, M.; Pouliot, P.; Gallagher, A.; Lesage, F.; Sawan, M.; Nguyen, D.K. Multichannel Wearable fNIRS-EEG System for Long-Term Clinical Monitoring. *Hum. Brain Mapp.* **2018**, *39*, 7–23. [CrossRef] [PubMed]
121. Boto, E.; Seedat, Z.A.; Holmes, N.; Leggett, J.; Hill, R.M.; Roberts, G.; Shah, V.; Fromhold, T.M.; Mullinger, K.J.; Tierney, T.M.; et al. Wearable neuroimaging: Combining and contrasting magnetoencephalography and electroencephalography. *NeuroImage* **2019**, *201*, 116099. [CrossRef]
122. Melroy, S.; Bauer, C.; McHugh, M.; Carden, G.; Stolin, A.; Majewski, S.; Brefczynski-Lewis, J.; Wuest, T. Development and Design of Next-Generation Head-Mounted Ambulatory Microdose Positron-Emission Tomography (AM-PET) System. *Sensors* **2017**, *17*, 1164. [CrossRef]
123. Ossig, C.; Antonini, A.; Buhmann, C.; Classen, J.; Csoti, I.; Falkenburger, B.; Schwarz, M.; Winkler, J.; Storch, A. Wearable sensor-based objective assessment of motor symptomsin Parkinson's disease. *J. Neural Transm.* **2016**, *123*, 57–64. [CrossRef]
124. Vescio, B.; Nisticò, R.; Augimeri, A.; Quattrone, A.; Crasà, M.; Quattrone, A. Development and Validation of a New Wearable Mobile Device for the Automated Detection of Resting Tremor in Parkinson's Disease and Essential Tremor. *Diagnostics* **2021**, *11*, 200. [CrossRef]
125. Mazzetta, I.; Gentile, P.; Pessione, M.; Suppa, A.; Zampogna, A.; Bianchini, E.; Irrera, F. Stand-Alone Wearable System for Ubiquitous Real-Time Monitoring of Muscle Activation Potentials. *Sensors* **2018**, *18*, 1748. [CrossRef]
126. Song, M.S.; Kang, S.G.; Lee, K.T.; Kim, J. Wireless, Skin-Mountable EMG Sensor for Human–Machine Interface Application. *Micromachines* **2019**, *10*, 879. [CrossRef]
127. Cerone, G.L.; Botter, A.; Vieira, T.; Gazzoni, M. Design and Characterization of a Textile Electrode System for the Detection of High-Density sEMG. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2021**, *29*, 1110–1119. [CrossRef]
128. Pino, E.J.; Arias, Y.; Aqueveque, P. Wearable EMG Shirt for Upper Limb Training. In Proceedings of the 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Honolulu, HI, USA, 18–21 July 2018; pp. 4406–4409.
129. Cole, B.T.; Roy, S.H.; De Luca, C.J.; Nawab, S.H. Dynamical Learning and Tracking of Tremor andDyskinesia From Wearable Sensors. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2014**, *22*, 982–991. [CrossRef]
130. Leone, A.; Rescio, G.; Caroppo, A.; Siciliano, P. A Wearable EMG-based System Pre-fall Detector. *Procedia Eng.* **2015**, *120*, 455–458. [CrossRef]
131. Jung, P.G.; Lim, G.; Kim, S.; Kong, K. A Wearable Gesture Recognition Devicefor Detecting Muscular Activities Basedon Air-Pressure Sensors. *IEEE Trans. Ind. Inform.* **2015**, *11*, 485–494.
132. Ghassemi, M.; Triandafilou, K.; Barry, A.; Stoykov, M.E.; Roth, E.; Mussa-Ivaldi, F.A.; Kamper, D.G.; Ranganathan, R. Development of an EMG-controlled Serious Game for Rehabilitation. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2019**, *27*, 283–292. [CrossRef]
133. Leonardis, D.; Barsotti, M.; Loconsole, C.; Solazzi, M.; Troncossi, M.; Mazzotti, C.; Castelli, V.P.; Procopio, C.; Lamola, G.; Chisari, C.; et al. An EMG-controlled robotic hand exoskeleton for bilateral rehabilitation. *IEEE Trans. Haptics* **2015**, *8*, 140–151. [CrossRef] [PubMed]
134. Hussain, I.; Salvietti, G.; Spagnoletti, G.; Prattichizzo, D. The Soft-SixthFinger: A Wearable EMG Controlled Robotic Extra-Finger for Grasp Compensation in Chronic Stroke Patients. *IEEE Robot. Autom. Lett.* **2016**, *1*, 1000–1006. [CrossRef]
135. Bi, Z.; Wang, Y.; Wang, H.; Zhou, Y.; Xie, C.; Zhu, L.; Wang, H.; Wang, B.; Huang, J.; Lü, X.; et al. Wearable EMG Bridge-a Multiple-Gesture Reconstruction System Using Electrical Stimulation Controlled by the Volitional Surface Electromyogram of a Healthy Forearm. *IEEE Access* **2020**, *8*, 137330–137341. [CrossRef]
136. Freed, A.; Chan, A.D.C.; Lemaire, E.D.; Parush, A. Wearable EMG Analysis for Rehabilitation (WEAR)—Surface electromyography in clinical gait analysis. In Proceedings of the IEEE International Symposium on Medical Measurements and Applications, Bari, Italy, 30–31 May 2011; pp. 601–604.
137. Chowdhury, R.H.; Reaz, M.B.I.; Ali, M.A.B.M.; Bakar, A.A.A.; Chellappan, K.; Chang, T.G. Surface Electromyography Signal Processing and Classification Techniques. *Sensors* **2013**, *13*, 12431–12466. [CrossRef] [PubMed]
138. Plewa, K.; Samadani, A.; Chau, T. Comparing electro-and mechano-myographic muscle activation patterns in self-paced pediatric gait. *J. Electromyogr. Kinesiol.* **2017**, *36*, 73–80. [CrossRef]
139. Booth, R.; Goldsmith, P. A Wrist-Worn Piezoelectric Sensor Array for Gesture Input. *J. Med. Biol. Eng.* **2018**, *38*, 284–295. [CrossRef]
140. Wilson, S.; Vaidyanathan, R. Upper-Limb Prosthetic Control using Wearable Multichannel Mechanomyography. In Proceedings of the International Conference on Rehabilitation Robotics, London, UK, 17–20 July 2017; pp. 1293–1298.
141. Esposito, D.; Andreozzi, E.; Fratini, A.; Gargiulo, G.D.; Savino, S.; Niola, V.; Bifulco, P. A Piezoresistive Sensor to Measure Muscle Contraction and Mechanomyography. *Sensors* **2018**, *18*, 2553. [CrossRef] [PubMed]
142. Krueger, E.; Popović-Maneski, L.; Nohama, P. Mechanomyography-Based Wearable Monitor of Quasi-Isometric Muscle Fatigue for Motor Neural Prostheses. *Artif. Organs* **2018**, *42*, 208–218. [CrossRef] [PubMed]
143. Martínez-Rodrigo, A.; Fernández-Caballero, A.; Silva, F.; Novais, P. Monitoring Electrodermal Activity for Stress Recognition Using a Wearable. In Proceedings of the 12th International Conference on Intelligent Environments, London, UK, 12–13 September 2016; pp. 416–425.

144. Zangróniz, R.; Martínez-Rodrigo, A.; Pastor, J.M.; López, M.T.; Fernández-Caballero, A. Electrodermal Activity Sensor for Classification of Calm/Distress Condition. *Sensors* **2017**, *17*, 2324. [CrossRef] [PubMed]
145. Choi, B.; Jebelli, H.; Lee, S. Feasibility analysis of electrodermal activity (EDA) acquired from wearable sensors to assess construction workers' perceived risk. *Saf. Sci.* **2019**, *115*, 110–120. [CrossRef]
146. Herlan, A.; Ottenbacher, J.; Schneider, J.; Riemann, D.; Feige, B. Electrodermal activity patterns in sleep stages and their utility for sleep versus wake classification. *J. Sleep Res.* **2019**, *28*, e12694. [CrossRef]
147. Arriba-Pérez, D.; Caeiro-Rodríguez, M.; Santos-Gago, J.M. Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios. *Sensors* **2016**, *16*, 1538. [CrossRef] [PubMed]
148. Nagai, Y.; Jones, C.I.; Sen, A. Galvanic Skin Response (GSR)/Electrodermal/Skin Conductance Biofeedback on Epilepsy: A Systematic Review and Meta-Analysis. *Front. Neurol.* **2019**, *10*, 377. [CrossRef]
149. Nagai, Y.; Critchley, H.D. Novel Therapeutic Application of Galvanic Skin Response (GSR) Biofeedback to a Neurological Disorder: Mechanisms Underlying Biofeedback in Epilepsy Management. In *Epilepsy Res. Prog.*; Nova Science Publishers: New York, NY, USA, 2008; pp. 175–205.
150. Posada-Quintero, H.F.; Chon, K.H. Innovations in Electrodermal Activity Data Collection and Signal Processing: A Systematic Review. *Sensors* **2020**, *20*, 479. [CrossRef] [PubMed]
151. Pope, G.C.; Halter, R.J. Design and Implementation of an Ultra-Low Resource Electrodermal Activity Sensor for Wearable Applications. *Sensors* **2019**, *19*, 2450. [CrossRef] [PubMed]
152. Gjoreski, M.; Lustrek, M.; Gams, M.; Gjoreski, H. Monitoring stress with a wrist device using context. *J. Biomed. Informatics* **2017**, *73*, 159–170. [CrossRef]
153. Geršak, G.; Drnovšek, J. Electrodermal activity patient simulator. *PLoS ONE* **2020**, *15*, e0228949. [CrossRef]
154. Trafton, A. Hydration Sensor Could Improve Dialysis. Available online: http://news.mit.edu/2019/hydration-sensor-dialysis-0724 (accessed on 1 August 2021).
155. Yao, S.; Myers, A.; Malhotra, A.; Lin, F.; Bozkurt, A.; Muth, J.F.; Zhu, Y. A Wearable Hydration Sensor with Conformal Nanowire Electrodes. *Adv. Healthc. Mater.* **2017**, *6*, 1601159. [CrossRef] [PubMed]
156. Koh, A.; Kang, D.; Xue, Y.; Lee, S.; Pielak, R.M.; Kim, J.; Hwang, T.; Min, S.; Banks, A.; Bastien, P.; et al. A Soft, Wearable Microfluidic Device for the Capture, Storage, and Colorimetric Sensing of Sweat. *Sci. Transl. Med.* **2016**, *8*, 366ra165. [CrossRef] [PubMed]
157. Huang, X.; Yeo, W.H.; Liu, Y.; Rogers, J.A. Epidermal Differential Impedance Sensor for Conformal Skin Hydration Monitoring. *Biointerphases* **2012**, *7*, 1–9. [CrossRef] [PubMed]
158. Gao, W.; Emaminejad, S.; Nyein, H.Y.Y.; Challa, S.; Chen, K.; Peck, A.; Fahad, H.M.; Ota, H.; Shiraki, H.; Kiriya, D.; et al. Fully integrated wearable sensor arrays for multiplexed in situ perspiration analysis. *Nature* **2016**, *529*, 509–514. [CrossRef] [PubMed]
159. Liu, G.; Alomari, M.; Sahin, B.; Snelgrove, S.E.; Edwards, J.; Mellinger, A.; Kaya, T. Real-time sweat analysis via alternating current conductivity of artificial and human sweat. *Appl. Phys. Lett.* **2015**, *106*, 133702. [CrossRef]
160. Huang, X.; Liu, Y.; Cheng, H.; Shin, W.J.; Fan, J.A.; Liu, Z.; Lu, C.J.; Kong, G.W.; Chen, K.; Patnaik, D.; et al. Materials and Designs for Wireless Epidermal Sensors of Hydration and Strain. *Adv. Funct. Mater.* **2014**, *24*, 3846–3854. [CrossRef]
161. Schiavoni, R.; Monti, G.; Tedesco, A.; Tarricone, L.; Piuzzi, E.; de Benedetto, E.; Masciullo, A.; Cataldo, A. Microwave Wearable System for Sensing Skin Hydration. In Proceedings of the IEEE International Instrumentation and Measurement Technology Conference, Glasgow, UK, 17–20 May 2021; pp. 1–6.
162. Yokus, M.A.; Daniele, M.A. Skin Hydration Sensor for Customizable Electronic Textiles. *MRS Adv.* **2016**, *1*, 2671–2676. [CrossRef]
163. Batista, E.; Borras, F.; Martínez-Ballesté, A. Monitoring People with MCI: Deployment in a Real Scenario for Low-Budget Smartphones. In Proceedings of the International Conference on Information, Intelligence, Systems and Applications, Corfu, Greece, 6–8 July 2015; pp. 1–6.
164. Cao, H.R.; Zhan, C. A Novel Emergency Healthcare System for Elderly Community in Outdoor Environment. *Wirel. Commun. Mob. Comput.* **2018**, *2018*. [CrossRef]
165. Nguyen, Q.H.; Johnson, P.; Nguyen, T.T.; Randles, M. A novel architecture using iBeacons for localization and tracking of people within healthcare environment. In *Global IoT Summit*; IEEE: New York, NY, USA, 2019; pp. 1–6.
166. Torres, J.; Belmonte, Ó.; Montoliu, R.; Trilles, S.; Calia, A. How feasible is WiFi fingerprint-based indoor positioning for in-home monitoring? In Proceedings of the 12th International Conference on Intelligent Environments;, London, UK, 14–16 September 2016; pp. 68–75.
167. Kim, S.C.; Jeong, Y.S.; Park, S.O. RFID-based indoor location tracking to ensure the safety of the elderly in smart home environments. *Pers. Ubiquitous Comput.* **2013**, *17*, 1699–1707. [CrossRef]
168. Shi, G.; Ming, Y. Survey of indoor positioning systems based on ultra-wideband (UWB) technology. In *Wireless Communications, Networking and Applications*; Springer: New Delhi, India, 2016; pp. 1269–1278.
169. Ferre, M.; Batista, E.; Solanas, A.; Martínez-Ballesté, A. Smart Health-Enhanced Early Mobilisation in Intensive Care Units. *Sensors* **2021**, *21*, 5408. [CrossRef]
170. Chang, H.C.; Hsu, Y.L.; Yang, S.C.; Lin, J.C.; Wu, Z.H. A Wearable Inertial Measurement System With Complementary Filter for Gait Analysis of Patients With Stroke or Parkinson's Disease. *IEEE Access* **2016**, *4*, 8442–8453. [CrossRef]

171. Lin, F.; Wang, A.; Zhuang, Y.; Tomita, M.R.; Xu, W. Smart Insole: A Wearable Sensor Device for Unobtrusive Gait Monitoring in Daily Life. *IEEE Trans. Ind. Inform.* **2016**, *12*, 2281–2291. [CrossRef]
172. Chen, S.; Lach, J.; Lo, B.; Yang, G.Z. Toward Pervasive Gait Analysis With WearableSensors: A Systematic Review. *IEEE J. Biomed. Health Inform.* **2016**, *20*, 1521–1537. [CrossRef]
173. Bisio, I.; Garibotto, C.; Lavagetto, F.; Sciarrone, A. When eHealth Meets IoT: A Smart Wireless System for Post-Stroke Home Rehabilitation. *IEEE Wirel. Commun.* **2019**, *26*, 24–29. [CrossRef]
174. Ding, Z.Q.; Luo, Z.Q.; Causo, A.; Chen, I.M.; Yue, K.X.; Yeo, S.H.; Ling, K.V. Inertia sensor-based guidance system for upperlimb posture correction. *Med Eng. Phys.* **2013**, *35*, 269–276. [CrossRef]
175. Wang, Q.; Chen, W.; Timmermans, A.A.A.; Karachristos, C.; Martens, J.B.; Markopoulos, P. Smart Rehabilitation Garment for posture monitoring. In Proceedings of the 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Milan, Italy, 25–29 August 2015; pp. 5736–5739.
176. Khojasteh, S.B.; Villar, J.R.; Chira, C.; González, V.M.; de la Cal, E. Improving Fall Detection Using an On-Wrist Wearable Accelerometer. *Sensors* **2018**, *18*, 1350. [CrossRef] [PubMed]
177. Sucerquia, A.; López, J.D.; Vargas-Bonilla, J.F. Real-Life/Real-Time Elderly Fall Detection with a Triaxial Accelerometer. *Sensors* **2018**, *18*, 1101. [CrossRef] [PubMed]
178. Cippitelli, E.; Fioranelli, F.; Gambi, E.; Spinsante, S. Radar and RGB-Depth Sensors for Fall Detection: A Review. *IEEE Sensors J.* **2017**, *17*, 3585–3604. [CrossRef]
179. Bisio, I.; Delfino, A.; Lavagetto, F.; Sciarrone, A. Enabling IoT for In-Home Rehabilitation: Accelerometer Signals Classification Methods for Activity and Movement Recognition. *IEEE Internet Things J.* **2016**, *4*, 135–146. [CrossRef]
180. Lu, Y.; Wei, Y.; Liu, L.; Zhong, J.; Sun, L.; Liu, Y. Towards unsupervised physical activity recognition using smartphone accelerometers. *Multimed. Tools Appl.* **2017**, *76*, 10701–10719. [CrossRef]
181. Fleron, M.K.; Ubbesen, N.C.H.; Battistella, F.; Dejtiar, D.L.; Oliveira, A.S. Accuracy between optical and inertial motion capture systems for assessing trunk speed during preferred gait and transition periods. *Sport. Biomech.* **2019**, *18*, 366–377. [CrossRef]
182. Robert-Lachaine, X.; Mecheri, H.; Muller, A.; Larue, C.; Plamondon, A. Validation of a low-cost inertial motion capture system for whole-body motion analysis. *J. Biomech.* **2020**, *99*, 109520. [CrossRef]
183. Hesse, N.; Pujades, S.; Romero, J.; Black, M.J.; Bodensteiner, C.; Arens, M.; Hofmann, U.G.; Tacke, U.; Hadders-Algra, M.; Weinberger, R.; et al. Learning an Infant Body Model from RGB-D Data for Accurate Full Body Motion Analysis. In Proceedings of the International Conference on Medical Image Computing and Computer-Assisted Intervention; Granada, Spain, 16–20 September 2018; pp. 792–800.
184. de Vries, N.M.; Smilowska, K.; Hummelink, J.; Abramiuc, B.; van Gilst, M.M.; Bloem, B.R.; Overeem, S. Exploring the Parkinson patients' perspective on home-based video recording for movement analysis: A qualitative study. *BMC Neurol.* **2019**, *19*, 71. [CrossRef]
185. Gaglio, S.; Re, G.L.; Morana, M. Human Activity Recognition Process Using 3-D Posture Data. *IEEE Trans.-Hum.-Mach. Syst.* **2014**, *45*, 586–597. [CrossRef]
186. Collin, J.; Davidson, P.; Kirkko-Jaakkola, M.; Leppäkoski, H. Inertial Sensors and Their Applications. In *Handbook of Signal Processing Systems*; Springer, New York, NY, USA, 2019; pp. 51–85.
187. Martínez-Ballesté, A.; Gimeno, P.; Mariné, A.; Batista, E.; Solanas, A. e-PEMICU: An e-Health Platform to Support Early Mobilisation in Intensive Care Units. In Proceedings of the 10th International Conference on Information, Intelligence, Systems and Applications, Patras, Greece, 15–17 July 2019; pp. 1–6.
188. Villeneuve, E.; Harwin, W.; Holderbaum, W.; Janko, B.; Sherratt, R.S. Reconstruction of Angular Kinematics From Wrist-Worn Inertial Sensor Data for Smart Home Healthcare. *IEEE Access* **2017**, *5*, 2351–2363. [CrossRef]
189. Gasparrini, A.; Guo, Y.; Hashizume, M.; Kinney, P.L.; Petkova, E.P.; Lavigne, E.; Zanobetti, A.; Schwartz, J.D.; Tobias, A.; Leone, M.; et al. Temporal Variation in Heat–Mortality Associations: A Multicountry Study. *Environ. Health Perspect.* **2015**, *123*, 1200–1207. [CrossRef]
190. Zeng, W.; Lao, X.; Rutherford, S.; Xu, Y.; Xu, X.; Lin, H.; Liu, T.; Luo, Y.; Xiao, J.; Hu, M.; et al. The effect of heat waves on mortality and effect modifiers in four communities of Guangdong Province, China. *Sci. Total. Environ.* **2014**, *482*, 214–221. [CrossRef]
191. Ou, C.Q.; Song, Y.F.; Yang, J.; Chau, P.Y.K.; Yang, L.; Chen, P.Y.; Wong, C.M. Excess Winter Mortality and Cold Temperatures in a Subtropical City, Guangzhou, China. *PLoS ONE* **2013**, *8*, e77150. [CrossRef]
192. Yang, C.; Meng, X.; Chen, R.; Cai, J.; Zhao, Z.; Wan, Y.; Kan, H. Long-term variations in the association between ambient temperature and daily cardiovascular mortality in Shanghai, China. *Sci. Total. Environ.* **2015**, *538*, 524–530. [CrossRef]
193. Cui, L.; Geng, X.; Ding, T.; Tang, J.; Xu, J.; Zhai, J. Impact of ambient temperature on hospital admissions for cardiovascular disease in Hefei City, China. *Int. J. Biometeorol.* **2019**, *63*, 723–734. [CrossRef]
194. Phung, D.; Thai, P.K.; Guo, Y.; Morawska, L.; Rutherford, S.; Chu, C. Ambient temperature and risk of cardiovascular hospitalization: An updated systematic review and meta-analysis. *Sci. Total. Environ.* **2016**, *550*, 1084–1102. [CrossRef]
195. Xu, Z.; Crooks, J.L.; Davies, J.M.; Khan, A.F.; Hu, W.; Tong, S. The association between ambient temperature and childhood asthma: A systematic review. *Int. J. Biometeorol.* **2018**, *62*, 471–481. [CrossRef]
196. Mullins, J.T.; White, C. Temperature and Mental Health: Evidence from the Spectrum of Mental Health Outcomes. *J. Health Econ.* **2019**, *68*, 102240. [CrossRef]

197. Kamat, R.K.; Naik, G.M. Thermistors – in search of new applications, manufacturers cultivate advanced NTC techniques. *Sens. Rev.* **2002**, *22*, 334–340. [CrossRef]
198. Wolkoff, P. Indoor air humidity, air quality, and health—An overview. *Int. J. Hyg. Environ. Health* **2018**, *221*, 376–390. [CrossRef]
199. Lukcso, D.; Guidotti, T.L.; Franklin, D.E.; Burt, A. Indoor environmental and air quality characteristics, building-related health symptoms, and worker productivity in a federal government building complex. *Arch. Environ. Occup. Health* **2016**, *71*, 85–101. [CrossRef]
200. Angelon-Gaetz, K.A.; Richardson, D.B.; Marshall, S.W.; Hernandez, M.L. Exploration of the effects of classroom humidity levels on teachers' respiratory symptoms. *Int. Arch. Occup. Environ. Health* **2016**, *89*, 729–737. [CrossRef]
201. Ijaz, M.K.; Zargar, B.; Wright, K.E.; Rubino, J.R.; Sattar, S.A. Generic aspects of the airborne spread of human pathogens indoors and emerging air decontamination technologies. *Am. J. Infect. Control.* **2016**, *44*, S109–S120. [CrossRef]
202. Najeeb, M.A.; Ahmad, Z.; Shakoor, R.A. Organic Thin-Film Capacitive and Resistive Humidity Sensors: A Focus Review. *Adv. Mater. Interfaces* **2018**, *5*, 1800969. [CrossRef]
203. Ascorbe, J.; Corres, J.M.; Arregui, F.J.; Matias, I.R. Recent Developments in Fiber Optics Humidity Sensors. *Sensors* **2017**, *17*, 893. [CrossRef] [PubMed]
204. Han, Y.G. Relative Humidity Sensors Based on Microfiber Knot Resonators—A Review. *Sensors* **2019**, *19*, 5196. [CrossRef]
205. Maini, K.; Schuster, N.M. Headache and Barometric Pressure: A Narrative Review. *Curr. Pain Headache Rep.* **2019**, *23*, 87. [CrossRef]
206. Kimoto, K.; Aiba, S.; Takashima, R.; Suzuki, K.; Takekawa, H.; Watanabe, Y.; Tatsumoto, M.; Hirata, K. Influence of Barometric Pressure in Patients with Migraine Headache. *Intern. Med.* **2011**, *50*, 1923–1928. [CrossRef]
207. McAlindon, T.; Formica, M.; Schmid, C.H.; Fletcher, J. Changes in Barometric Pressure and Ambient Temperature Influence Osteoarthritis Pain. *Am. J. Med.* **2007**, *120*, 429–434. [CrossRef]
208. Brennan, S.A.; Harney, T.; Queally, J.M.; McGoona, J.O.; Gormley, I.C.; Shannon, F.J. Influence of weather variables on pain severity in end-stage osteoarthritis. *Int. Orthop.* **2012**, *36*, 643–646. [CrossRef]
209. Song, P.; Ma, Z.; Ma, J.; Yang, L.; Wei, J.; Zhao, Y.; Zhang, M.; Yang, F.; Wang, X. Recent Progress of Miniature MEMS Pressure Sensors. *Micromachines* **2020**, *11*, 56. [CrossRef]
210. Javed, Y.; Mansoor, M.; Shah, I.A. A review of principles of MEMS pressure sensing with its aerospace applications. *Sens. Rev.* **2019**, *39*, 652–664. [CrossRef]
211. Tenzer, Y.; Jentoft, L.P.; Howe, R.D. The Feel of MEMS Barometers: Inexpensive and Easily Customized Tactile Array Sensors. *IEEE Robot. Autom. Mag.* **2014**, *21*, 89–95. [CrossRef]
212. World Health Organization. Air Pollution. Available online: https://www.who.int/health-topics/air-pollution (accessed on 1 July 2021).
213. Manisalidis, I.; Stavropoulou, E.; Stavropoulos, A.; Bezirtzoglou, E. Environmental and Health Impacts of Air Pollution: A Review. *Front. Public Health* **2020**, *8*, 14. [CrossRef]
214. Anderson, J.O.; Thundiyil, J.G.; Stolbach, A. Clearing the Air: A Review of the Effects of Particulate Matter Air Pollution on Human Health. *J. Med. Toxicol.* **2012**, *8*, 166–175. [CrossRef] [PubMed]
215. Kurt, O.K.; Zhang, J.; Pinkerton, K.E. Pulmonary Health Effects of Air Pollution. *Curr. Opin. Pulm. Med.* **2016**, *22*, 138. [CrossRef] [PubMed]
216. Ye, D.; Klein, M.; Chang, H.H.; Sarnat, J.A.; Mulholland, J.A.; Edgerton, E.S.; Winquist, A.; Tolbert, P.E.; Sarnat, S.E. Estimating acute cardiorespiratory effects of ambient volatile organic compounds. *Epidemiology* **2017**, *28*, 197–206. [CrossRef] [PubMed]
217. Idrees, Z.; Zheng, L. Low cost air pollution monitoring systems: A review of protocols and enabling technologies. *J. Ind. Inf. Integr.* **2020**, *17*, 100123. [CrossRef]
218. Baron, R.; Saffell, J. Amperometric Gas Sensors as a Low Cost Emerging Technology Platform for Air Quality Monitoring Applications: A Review. *ACS Sens.* **2017**, *2*, 1553–1566. [CrossRef]
219. Rai, A.C.; Kumar, P.; Pilla, F.; Skouloudis, A.N.; Di Sabatino, S.; Ratti, C.; Yasar, A.; Rickerby, D. End-user perspective of low-cost sensors for outdoor air pollution monitoring. *Sci. Total. Environ.* **2017**, *607*, 691–705. [CrossRef]
220. Karagulian, F.; Gerboles, M.; Barbiere, M.; Kotsev, A.; Lagler, F.; Borowiak, A. *Review of Sensors for Air Quality Monitoring*; European Commission: Luxembourg, 2019.
221. Lewis, A.C.; Lee, J.D.; Edwards, P.M.; Shaw, M.D.; Evans, M.J.; Moller, S.J.; Smith, K.R.; Buckley, J.W.; Ellis, M.; Gillot, S.R.; et al. Evaluating the performance of low cost chemical sensors for air pollution research. *Faraday Discuss.* **2016**, *189*, 85–103. [CrossRef]
222. Levallois, P.; Villanueva, C.M. Drinking Water Quality and Human Health: An Editorial. *Int. J. Environ. Res. Public Health* **2019**, *16*, 631. [CrossRef]
223. Højris, B.; Kornholt, S.N.; Christensen, S.C.B.; Albrechtsen, H.J.; Olesen, L.S. Detection of drinking water contamination by an optical real-time bacteria sensor. *$H_2$Open J.* **2018**, *1*, 160–168. [CrossRef]
224. Hatiboruah, D.; Das, T.; Chamuah, N.; Rabha, D.; Talukdar, B.; Bora, U.; Ahamad, K.U.; Nath, P. Estimation of trace-mercury concentration in water using a smartphone. *Measurement* **2020**, *154*, 107507. [CrossRef]
225. Lambrou, T.P.; Anastasiou, C.C.; Panayiotou, C.G.; Polycarpou, M.M. A Low-Cost Sensor Network for Real-Time Monitoring and Contamination Detection in Drinking Water Distribution Systems. *IEEE Sens. J.* **2014**, *14*, 2765–2772. [CrossRef]

226. Wang, Y.; Zhang, X.; Chen, J.; Cheng, Z.; Wang, D. Camera sensor-based contamination detection for water environment monitoring. *Environ. Sci. Pollut. Res.* **2019**, *26*, 2722–2733. [CrossRef]
227. Münzel, T.; Schmidt, F.P.; Steven, S.; Herzog, J.; Daiber, A.; Sørensen, M. Environmental Noise and the Cardiovascular System. *J. Am. Coll. Cardiol.* **2018**, *71*, 688–697. [CrossRef]
228. Hahad, O.; Kröller-Schön, S.; Daiber, A.; Münzel, T. The Cardiovascular Effects of Noise. *Dtsch. ÄRzteblatt Int.* **2019**, *116*, 245. [CrossRef] [PubMed]
229. Van Kempen, E.; Casas, M.; Pershagen, G.; Foraster, M. WHO Environmental Noise Guidelines for the European Region: A Systematic Review on Environmental Noise and Cardiovascular and Metabolic Effects: A Summary. *Int. J. Environ. Res. Public Health* **2018**, *15*, 379. [CrossRef] [PubMed]
230. Kazmi, A.; Tragos, E.; Serrano, M. Underpinning IoT for Road Traffic Noise Management in Smart Cities. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications, Athens, Greece, 19–23 March 2018; pp. 765–769.
231. Segura Garcia, J.; Pérez Solano, J.J.; Cobos Serrano, M.; Navarro Camba, E.A.; Felici Castell, S.; Soriano Asensi, A.; Montes Suay, F. Spatial Statistical Analysis of Urban Noise Data from a WASN Gathered by an IoT System: Application to a Small City. *Appl. Sci.* **2016**, *6*, 380. [CrossRef]
232. Moan, J.; Grigalavicius, M.; Baturaite, Z.; Dahlback, A.; Juzeniene, A. The relationship between UV exposure and incidence of skin cancer. *Photodermatol. Photoimmunol. Photomed.* **2015**, *31*, 26–35. [CrossRef]
233. Genuis, S.J. Fielding a current idea: Exploring the public health impact of electromagnetic radiation. *Public Health* **2008**, *122*, 113–124. [CrossRef] [PubMed]
234. Xiang, F.; Lucas, R.; Hales, S.; Neale, R. Incidence of Nonmelanoma Skin Cancer in Relation to Ambient UV Radiation in White Populations, 1978-2012 Empirical Relationships. *JAMA Dermatol.* **2014**, *150*, 1063–1071. [CrossRef] [PubMed]
235. Hardell, L. World Health Organization, radiofrequency radiation and health—A hard nut to crack. *Int. J. Oncol.* **2017**, *51*, 405–413. [CrossRef]
236. Kržanović, N.; Stanković, K.; Živanović, M.; Đaletić, M.; Ciraj-Bjelac, O. Development and testing of a low cost radiation protection instrument based on an energy compensated Geiger-Müller tube. *Radiat. Phys. Chem.* **2019**, *164*, 108358. [CrossRef]
237. Wang, P.; Tang, X.B.; Gong, P.; Huang, X.; Wen, L.S.; Han, Z.Y.; He, J.P. Des. Portable Dose Rate Detect. Based Double -Geiger -Mueller Count.. *Nucl. Instruments Methods Phys. Res. Sect. Accel. Spectrometers Detect. Assoc. Equip.* **2018**, *879*, 147–152. [CrossRef]
238. Tocchi, A.; Roca, V.; Angrisani, L.; Bonavolontà, F.; Moriello, R.S.L. First step towards an IoT implementation of a wireless sensors network for environmental radiation monitoring. In Proceedings of the IEEE International Instrumentation and Measurement Technology Conference, Turin, Italy, 22–25 May 2017; pp. 1–6.
239. Joo, H.; Kim, R.; Moon, J.H. Radioactivity Measurement of Radioactive Contaminated Soil by Using a Fiber-Optic Radiation Sensor. *J. Korean Phys. Soc.* **2016**, *68*, 1287–1290. [CrossRef]
240. Kim, R.; Lee, S.B.; Kim, J.W.; Moon, J.H. Development and Comparison of Fiber-Optic Beta Radiation Sensors with Different Diameters of Their Sensing Probes. *J. Sens.* **2017**, *2017*, 1452765. [CrossRef]
241. McGrath, M.J.; Scanaill, C.N.; Nafus, D. *Sensor Technologies: Healthcare, Wellness and Environmental Applications*; Apress: New York, NY, USA, 2014.
242. Lee, J.; Khan, I.; Choi, S.; Kwon, Y.W. A Smart IoT Device for Detecting and Responding to Earthquakes. *Electronics* **2019**, *8*, 1546. [CrossRef]
243. Zambrano, A.M.; Perez, I.; Palau, C.; Esteve, M. Technologies of Internet of Things applied to an Earthquake Early Warning System. *Future Gener. Comput. Syst.* **2017**, *75*, 206–215. [CrossRef]
244. Alphonsa, A.; Ravi, G. Earthquake Early Warning System by IOT using Wireless Sensor Networks. In Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking, Chennai, India, 23–25 March 2016; pp. 1201–1205.
245. Pisco, M.; Bruno, F.A.; Galluzzo, D.; Nardone, L.; Gruca, G.; Rijnveld, N.; Bianco, F.; Cutolo, A.; Cusano, A. Opto-mechanical lab-on-fibre seismic sensors detected the Norcia earthquake. *Sci. Rep.* **2018**, *8*, 1–14. [CrossRef]
246. Alzaid, H.; Foo, E.; Gonzalez Nieto, J.M. Secure Data Aggregation in Wireless Sensor Network: A survey. In Proceedings of the 6th Australasian Information Security Conference, Wollongong, NSW, Australia, 1 January 2008; Volume 81, pp. 93–105.
247. Anwar, M.; Abdullah, A.H.; Altameem, A.; Qureshi, K.N.; Masud, F.; Faheem, M.; Cao, Y.; Kharel, R. Green Communication for Wireless Body Area Networks: Energy Aware Link Efficient Routing Approach. *Sensors* **2018**, *18*, 3237. [CrossRef]
248. Filipe, L.; Fdez-Riverola, F.; Costa, N.; Pereira, A. Wireless Body Area Networks for Healthcare Applications: Protocol Stack Review. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 213705. [CrossRef]
249. Jawad, H.M.; Nordin, R.; Gharghan, S.K.; Jawad, A.M.; Ismail, M. Energy-Efficient Wireless Sensor Networks for Precision Agriculture: A Review. *Sensors* **2017**, *17*, 1781. [CrossRef]
250. Ahmed, N.; Michelin, R.A.; Xue, W.; Ruj, S.; Malaney, R.; Kanhere, S.S.; Seneviratne, A.; Hu, W.; Janicke, H.; Jha, S.K. A Survey of COVID-19 Contact Tracing Apps. *IEEE Access* **2020**, *8*, 134577–134601. [CrossRef]
251. IEEE. IEEE Standard for Local and metropolitan area networks—Part 15.6: Wireless Body Area Networks. In *IEEE Standards Association*; IEEE: New York, NY, USA, 2012; pp. 1–271.
252. Toorani, M. Security analysis of the IEEE 802.15.6 standard. *Int. J. Commun. Syst.* **2016**, *29*, 2471–2489. [CrossRef]

253. Afaqui, M.S.; Garcia-Villegas, E.; Lopez-Aguilera, E. IEEE 802.11ax: Challenges and requirements for future high efficiency Wi-Fi. *IEEE Wirel. Commun.* **2016**, *24*, 130–137. [CrossRef]
254. Al-Absi, M.A.; Al-Absi, A.A.; Sain, M.; Lee, H.J. A State of the Art: Future Possibility of 5G with IoT and Other Challenges. In *Smart Healthcare Analytics in IoT Enabled Environment*; Springer: Cham, Switzerland, 2020; pp. 35–65.
255. Ahad, A.; Tahir, M.; Yau, K.L.A. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. *IEEE Access* **2019**, *7*, 100747–100762. [CrossRef]
256. Lloret, J.; Parra, L.; Taha, M.; Tomás, J. An architecture and protocol for smart continuous eHealth monitoring using 5G. *Comput. Netw.* **2017**, *129*, 340–351. [CrossRef]
257. Jusak, J.; Pratikno, H.; Putra, V.H. Internet of Medical Things for Cardiac Monitoring: Paving The Way to 5G Mobile Networks. In Proceedings of the 5th IEEE International Conference on Communication, Networks and Satellite, Surabaya, Indonesia, 8–10 December 2016; pp. 75–79.
258. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 855–873. [CrossRef]
259. del Campo, G.; Gomez, I.; Cañada, G.; Piovano, L.; Santamaria, A. Guidelines and criteria for selecting the optimal low-power wide-area network technology. In *LPWAN Technologies for IoT and M2M Applications*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 281–305.
260. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Le Moullec, Y. A Survey on the Roles of Communication Technologies in IoT-Based Personalized Healthcare Applications. *IEEE Access* **2018**, *6*, 36611–36631. [CrossRef]
261. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2019**, *5*, 1–7. [CrossRef]
262. Aernouts, M.; Berkvens, R.; Van Vlaenderen, K.; Weyn, M. Sigfox and LoRaWAN Datasets for Fingerprint Localization in Large Urban and Rural Areas. *Data* **2018**, *3*, 13. [CrossRef]
263. Li, C.; Raghunathan, A.; Jha, N.K. Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System. In Proceedings of the IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, MO, USA, 13–15 June 2011; pp. 150–156.
264. Kuehn, B.M. Pacemaker Recall Highlights Security Concerns for Implantable Devices. *Circulation* **2018**, *138*, 1597–1598. [CrossRef] [PubMed]
265. Liebowitz, J.; Schaller, R. Biological Warfare: Tampering with implantable medical devices. *IT Prof.* **2015**, *17*, 70–72. [CrossRef]
266. Halperin, D.; Heydt-Benjamin, T.S.; Ransford, B.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 18–22 May 2008; pp. 129–142.
267. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 3723–3768. [CrossRef]
268. Fiaidhi, J.; Mohammed, S. Security and Vulnerability of Extreme Automation Systems: The IoMT and IoA Case Studies. *IT Prof.* **2019**, *21*, 48–55. [CrossRef]
269. Papageorgiou, A.; Strigkos, M.; Politou, E.; Alepis, E.; Solanas, A.; Patsakis, C. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* **2018**, *6*, 9390–9403. [CrossRef]
270. Aliasgari, M.; Black, M.; Yadav, N. Security Vulnerabilities in Mobile Health Applications. In Proceedings of the IEEE Conference on Application, Information and Network Security, Langkawi, Malaysia, 21–22 November 2018; pp. 21–26.
271. Zuo, C.; Wen, H.; Lin, Z.; Zhang, Y. Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 1469–1483.
272. Aloseel, A.; He, H.; Shaw, C.; Khan, M.A. Analytical Review of Cybersecurity for Embedded Systems. *IEEE Access* **2020**, *9*, 961–982. [CrossRef]
273. Agrawal, S.; Das, M.L.; Lopez, J. Detection of Node Capture Attack in Wireless Sensor Networks. *IEEE Syst. J.* **2018**, *13*, 238–247. [CrossRef]
274. Wang, C.; Wang, D.; Tu, Y.; Xu, G.; Wang, H. Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks. *IEEE Trans. Dependable Secur. Comput.* **2020**, 1–20. [CrossRef]
275. Lin, C.; Wu, G.; Qiu, T.; Deng, J. A low-cost node capture attack algorithm for wireless sensor networks. *Int. J. Commun. Syst.* **2016**, *29*, 1251–1268. [CrossRef]
276. Bostami, B.; Ahmed, M.; Choudhury, S. False Data Injection Attacks in Internet of Things. In *Performability in Internet of Things*; Springer: Cham, Switzerland, 2019; pp. 47–58.
277. Ahmed, M.; Pathan, A.S.K. False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adapt. Syst. Model.* **2020**, *8*, 1–14. [CrossRef]
278. Ahmed, M.; Barkat Ullah, A.S.S.M. False Data Injection Attacks in Healthcare. In Proceedings of the 15th Australasian Conference on Data Mining, Melbourne, VIC, Australia, 19–20 August 2017; Springer: Singapore, 2017; pp. 192–202.
279. Pirretti, M.; Zhu, S.; Vijaykrishnan, N.; McDaniel, P.; Kandemir, M.; Brooks, R. The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. *Int. J. Distrib. Sens. Netw.* **2006**, *2*, 267–287. [CrossRef]

280. Nguyen, V.L.; Lin, P.C.; Hwang, R.H. Energy Depletion Attacks in Low Power Wireless Networks. *IEEE Access* **2019**, *7*, 51915–51932. [CrossRef]
281. Hei, X.; Du, X.; Wu, J.; Hu, F. Defending Resource Depletion Attacks on Implantable Medical Devices. In Proceedings of the 53th IEEE Global Telecommunications Conference, Miami, FL, USA, 6–10 December 2010; pp. 1–5.
282. Marin, E.; Singelee, D.; Garcia, F.D.; Chothia, T.; Willems, R.; Preneel, B. On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them. In Proceedings of the 32nd Annual Conference on Computer Security Applications, Los Angeles, CA USA, 5–8 December 2016; pp. 226–236.
283. Spreitzer, R.; Moonsamy, V.; Korak, T.; Mangard, S. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Commun. Surv. Tutorials* **2017**, *20*, 465–488. [CrossRef]
284. Spence, A.; Bangay, S. Side-Channel Sensing: Exploiting Side-Channels to Extract Information for Medical Diagnostics and Monitoring. *IEEE J. Transl. Eng. Health Med.* **2020**, *8*, 1–13. [CrossRef]
285. Maiti, A.; Jadliwala, M.; He, J.; Bilogrevic, I. Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2180–2194. [CrossRef]
286. Maiti, A.; Heard, R.; Sabra, M.; Jadliwala, M. Towards Inferring Mechanical Lock Combinations using Wrist-Wearables as a Side-Channel. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Stockholm, Sweden, 18–20 June 2018; pp. 111–122.
287. Liu, X.; Zhou, Z.; Diao, W.; Li, Z.; Zhang, K. When Good Becomes Evil: Keystroke Inference with Smartwatch. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015 ; pp. 1273–1285.
288. Kune, D.F.; Backes, J.; Clark, S.S.; Kramer, D.; Reynolds, M.; Fu, K.; Kim, Y.; Xu, W. Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 145–159.
289. HP Inc. HP Study Reveals Smartwatches Vulnerable to Attack. Available online: https://www8.hp.com/us/en/hp-news/press-release.html?id=2037386 (accessed on 1 August 2021).
290. Shim, J.; Lim, K.; Jeong, J.; Cho, S.j.; Park, M.; Han, S. A Case Study on Vulnerability Analysis and Firmware Modification Attack for a Wearable Fitness Tracker. *IT Converg. Pract.* **2017**, *5*, 25–33.
291. Rieck, J. Attacks on Fitness Trackers Revisited: A Case-Study of Unfit Firmware Security. *arXiv* **2016**, arXiv:1604.03313.
292. Arias, O.; Wurm, J.; Hoang, K.; Jin, Y. Privacy and Security in Internet of Things and Wearable Devices. *IEEE Trans. -Multi-Scale Comput. Syst.* **2015**, *1*, 99–109. [CrossRef]
293. Classen, J.; Wegemer, D.; Patras, P.; Spink, T.; Hollick, M. Anatomy of a Vulnerable Fitness Tracking System: Dissecting the Fitbit Cloud, App, and Firmware. *Proc. ACM Interactive Mobile Wearable Ubiquitous Technol.* **2018**, *2*, 1–24. [CrossRef]
294. Kim, D.; Park, S.; Choi, K.; Kim, Y. BurnFit: Analyzing and Exploiting Wearable Devices. In Proceedings of the International Workshop on Information Security Applications, Jeju Island, Korea, 20–22 August 2015; Springer: Cham, Switzerland, 2015; pp. 227–239.
295. Hanna, S.; Rolles, R.; Molina-Markham, A.; Poosankam, P.; Blocki, J.; Fu, K.; Song, D. Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices. In Proceedings of the 2nd USENIX Workshop on Health Security and Privacy, San Francisco, CA, USA, 9 August, 2011.
296. Zou, Y.; Wang, G. Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack. *IEEE Trans. Ind. Inform.* **2015**, *12*, 780–787. [CrossRef]
297. Xu, Q.; Ren, P.; Song, H.; Du, Q. Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations. *IEEE Access* **2016**, *4*, 2840–2853. [CrossRef]
298. Zorz, Z. Critical Bluetooth Flaw Opens Millions of Devices to Eavesdropping Attacks. Available online: https://www.helpnetsecurity.com/2019/08/16/bluetooth-cve-2019-9506/ (accessed on 1 August 2021).
299. Ryan, M. Bluetooth: With Low Energy comes Low Security. In Proceedings of the 7th USENIX Workshop on Offensive Technologies, Washington, DC, USA, 13 August 2013; pp. 1–7.
300. Fawaz, K.; Kim, K.H.; Shin, K.G. Protecting Privacy of BLE Device Users. In Proceedings of the 25th USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016; pp. 1205–1221.
301. Moses, V.; Korah, I. Lack of Security of Networked Medical Equipment in Radiology. *Am. J. Roentgenol.* **2015**, *204*, 343–353. [CrossRef]
302. Cusack, B.; Antony, B.; Ward, G.; Mody, S. Assessment of security vulnerabilities in wearable devices. In Proceedings of 15th Australian Information Security Management Conference, Edith Cowan University, Perth, Australia, 5–6 December 2017; pp. 42–48.
303. Goyal, R.; Dragoni, N.; Spognardi, A. Mind The Tracker You Wear—A Security Analysis of Wearable Health Trackers. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016; pp. 131–136.
304. Das, A.K.; Pathak, P.H.; Chuah, C.N.; Mohapatra, P. Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers. In Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, St. Augustine, FL, USA, 23–24 February 2016; pp. 99–104.
305. Lotfy, K.; Hale, M.L. Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things. In Proceedings of the IEEE International Conference on Mobile Services, San Francisco, CA, USA, 27 June–2 July 2016; pp. 25–32.

306. Rahman, M.; Carbunar, B.; Topkara, U. Secure Management of Low Power Fitness Trackers. *IEEE Trans. Mob. Comput.* **2015**, *15*, 447–459. [CrossRef]
307. Hei, X.; Du, X.; Lin, S.; Lee, I.; Sokolsky, O. Patient Infusion Pattern based Access Control Schemes for Wireless Insulin Pump System. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 3108–3121. [CrossRef]
308. Li, Y.; Barthelemy, J.; Sun, S.; Perez, P.; Moran, B. A Case Study of WiFi Sniffing Performance Evaluation. *IEEE Access* **2020**, *8*, 129224–129235. [CrossRef]
309. Morgner, P.; Mattejat, S.; Benenson, Z.; Müller, C.; Armknecht, F. Insecure to the Touch: Attacking ZigBee 3.0 via Touchlink Commissioning. In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Boston, MA, USA, 18–20 July 2017; pp. 230–240.
310. Bodei, C.; Galletta, L. Tracking sensitive and untrustworthy data in IoT. In Proceedings of the The Italian Conference on Cybersecurity, Venice, Italy, 17–20 January 2017 ; Volume 1816, pp. 38–52.
311. Siddiqi, M.; Sivaraman, V.; Jha, S. Timestamp Integrity in Wearable Healthcare Devices. In Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems, Bangalore, India, 6–9 November 2016; pp. 1–6.
312. Kimergård, A.; Breindahl, T.; Hindersson, P.; Deluca, P. Tampering of opioid analgesics: A serious challenge for public health? *Addiction* **2016**, *111*, 1701–1702. [CrossRef]
313. Fereidooni, H.; Frassetto, T.; Miettinen, M.; Sadeghi, A.R.; Conti, M. Fitness Trackers: Fit for Health but Unfit for Security and Privacy. In Proceedings of the IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, Philadelphia, PA, USA, 17–19 July 2017; pp. 19–24.
314. Morgner, P.; Pfennig, S.; Salzner, D.; Benenson, Z. Malicious IoT Implants: Tampering with Serial Communication over the Internet. In Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses; Heraklion, Crete, Greece, 10–12 September 2018; pp. 535–555.
315. Kim, J.; Song, J. A Simple and Efficient Replay Attack Prevention Scheme for LoRaWAN. In Proceedings of the 7th International Conference on Communication and Network Security, Tokyo, Japan, 24–26 November 2017; pp. 32–36.
316. Jin, H.; Zhou, K.; Jiang, H.; Lei, D.; Wei, R.; Li, C. Full integrity and freshness for cloud data. *Future Gener. Comput. Syst.* **2018**, *80*, 640–652. [CrossRef]
317. Belkhouja, T.; Du, X.; Mohamed, A.; Al-Ali, A.K.; Guizani, M. New Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control. In Proceedings of the IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–5.
318. Rughoobur, P.; Nagowah, L. A Lightweight Replay Attack Detection Framework for Battery Depended IoT Devices Designed for Healthcare. In Proceedings of the International Conference on Infocom Technologies and Unmanned Systems, Dubai, United Arab Emirates, 18–20 December 2017; pp. 811–817.
319. Spring, R.; Freudenthal, E.; Estevez, L. Practical Techniques for Limiting Disclosure of RF-Equipped Medical Devices. In Proceedings of the IEEE Dallas Engineering in Medicine and Biology Workshop, Dallas, TX, USA, 11–12 November 2007; pp. 82–85.
320. Ali, A.; Khan, F.A. Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP J. Wirel. Commun. Netw.* **2013**, *2013*, 216. [CrossRef]
321. Radcliffe, J. Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System. In Proceedings of the Black Hat Conference, Las Vegas, NV, USA, 30 July–4 August, 2011; Volume 2011.
322. Yılmaz, M.H.; Arslan, H. A Survey: Spoofing Attacks in Physical Layer Security. In Proceedings of the IEEE 40th Local Computer Networks Conference, Clearwater Beach, FL, USA, 26–29 October 2015; pp. 812–817.
323. Mirkovic, J.; Kline, E.; Reiher, P. RESECT: Self–Learning Traffic Filters for IP Spoofing Defense. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, FL, USA, 4–8 December 2017; pp. 474–485.
324. Zhang, C.; Hu, G.; Chen, G.; Sangaiah, A.K.; Zhang, P.; Yan, X.; Jiang, W. Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack. *IEEE Access* **2017**, *6*, 22764–22777. [CrossRef]
325. Park, Y.; Son, Y.; Shin, H.; Kim, D.; Kim, Y. This ain't your dose: Sensor Spoofing Attack on Medical Infusion Pump. In Proceedings of the 10th USENIX Workshop on Offensive Technologies, Austin, TX, USA, 8–9 August 2016; pp. 1–11.
326. Zhang, P.; Nagarajan, S.G.; Nevat, I. Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things. *IEEE Internet Things J.* **2017**, *4*, 2199–2206. [CrossRef]
327. Tippenhauer, N.O.; Pöpper, C.; Rasmussen, K.B.; Capkun, S. On the Requirements for Successful GPS Spoofing Attacks. In Proceedings of the 18th ACM Conference on Computer and communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 75–86.
328. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2027–2051. [CrossRef]
329. Wazid, M.; Das, A.K.; Rodrigues, J.J.P.C.; Shetty, S.; Park, Y. IoMT Malware Detection Approaches: Analysis and Research Challenges. *IEEE Access* **2019**, *8*, 182459–182476. [CrossRef]
330. Navas, R.E.; Le Bouder, H.; Cuppens, N.; Cuppens, F.; Papadopoulos, G.Z. Do not trust your neighbors! A small IoT platform illustrating a man-in-the-middle attack. In Proceedings of the International Conference on Ad-Hoc Networks and Wireless, Saint-Malo, France, 5–7 September 2018; pp. 120–125.

331. Hale, M.L.; Lotfy, K.; Gamble, R.F.; Walter, C.; Lin, J. Developing a platform to evaluate and assess the security of wearable devices. *Digit. Commun. Netw.* **2019**, *5*, 147–159. [CrossRef]
332. Sun, D.Z.; Mu, Y.; Susilo, W. Man-in-the-Middle Attacks on Secure Simple Pairing in Bluetooth Standard V5.0 and Its Countermeasure. *Pers. Ubiquitous Comput.* **2018**, *22*, 55–67. [CrossRef]
333. Belkhouja, T.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Guizani, M. Light-Weight Solution to Defend Implantable Medical Devices against Man-In-The-Middle Attack. In Proceedings of the IEEE Global Communications Conference, Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–5.
334. Ahmad, F.; Adnane, A.; Franqueira, V.N.L.; Kurugollu, F.; Liu, L. Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. *Sensors* **2018**, *18*, 4040. [CrossRef]
335. Ahmad, F.; Kurugollu, F.; Adnane, A.; Hussain, R.; Hussain, F. MARINE: Man-in-the-middle Attack Resistant trustmodel IN connEcted vehicles. *IEEE Internet Things J.* **2020**, *7*, 3310–3322. [CrossRef]
336. Kazlouski, A.; Marchioro, T.; Manifavas, H.; Markatos, E.P. I still See You! Inferring Fitness Data from Encrypted Traffic of Wearables. In Proceedings of the 14th International Joint Conference on Biomedical Engineering Systems and Technologies, Lisbon, Portugal, 11–13 February 2021; pp. 369–376.
337. Fereidooni, H.; Classen, J.; Spink, T.; Patras, P.; Miettinen, M.; Sadeghi, A.R.; Hollick, M.; Conti, M. Breaking Fitness Records without Moving: Reverse Engineering and Spoofing Fitbit. In Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses, Atlanta, GA, USA, 18–20 September 2017; pp. 48–69.
338. Pournaghshband, V.; Sarrafzadeh, M.; Reiher, P. Securing Legacy Mobile Medical Devices. In Proceedings of the International Conference on Wireless Mobile Communication and Healthcare, Paris, France, 21–23 November 2012; Springer: Berlin/Heidelberg, Germany, 2012, pp. 163–172.
339. Marin, E.; Argones-Rúa, E.; Singelée, D.; Preneel, B. A survey on physiological-signal-based security for medical devices. *IACR Cryptol. Eprint Arch.* **2016**, *2016*, 867.
340. Rostami, M.; Burleson, W.; Koushanfar, F.; Juels, A. Balancing Security and Utility in Medical Devices? In Proceedings of the 50th Annual Design Automation Conference, Austin, TX, USA, 29 May 2013–7 June 2013; pp. 1–6.
341. Hoque, N.; Bhattacharyya, D.K.; Kalita, J.K. Botnet in DDoS Attacks: Trends and Challenges. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2242–2270. [CrossRef]
342. Vadlamani, S.; Eksioglu, B.; Medal, H.; Nandi, A. Jamming attacks on wireless networks: A taxonomic survey. *Int. J. Prod. Econ.* **2016**, *172*, 76–94. [CrossRef]
343. Subasini, C.A.; Karuppiah, S.P.; Sheeba, A.; Padmakala, S. Developing an attack detection framework for wireless sensor network-based healthcare applications using hybrid convolutional neural network. *Trans. Emerg. Telecommun. Technol.* **2021**, e4336.
344. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and Other Botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
345. De Donno, M.; Dragoni, N.; Giaretta, A.; Spognardi, A. DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Secur. Commun. Netw.* **2018**, *2018*, 7178164. [CrossRef]
346. Ellouze, N.; Allouche, M.; Ahmed, H.B.; Rekhis, S.; Boudriga, N. Security of implantable medical devices: Limits, requirements, and proposals. *Secur. Commun. Netw.s* **2014**, *7*, 2475–2491. [CrossRef]
347. Ye, Y.; Li, T.; Adjeroh, D.; Iyengar, S.S. A Survey on Malware Detection Using Data Mining Techniques. *ACM Comput. Surv.* **2017**, *50*, 1–40. [CrossRef]
348. Or-Meir, O.; Nissim, N.; Elovici, Y.; Rokach, L. Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *ACM Comput. Surv.* **2019**, *52*, 1–48. [CrossRef]
349. Hernandez-Castro, J.; Cartwright, A.; Cartwright, E. An economic analysis of ransomware and its welfare consequences. *R. Soc. Open Sci.* **2020**, *7*, 190023. [CrossRef] [PubMed]
350. Vignau, B.; Khoury, R.; Hallé, S. 10 Years of IoT Malware: A Feature-Based Taxonomy. In Proceedings of the IEEE 19th International Conference on Software Quality, Reliability and Security Companion, Sofia, Bulgaria, 22–26 July 2019; pp. 458–465.
351. Martin, G.; Ghafur, S.; Kinross, J.; Hankin, C.; Darzi, A. WannaCry—A year on. *BMJ* **2018**, *361*, 1–2. [CrossRef] [PubMed]
352. Isaak, J.; Hanna, M.J. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer* **2018**, *51*, 56–59. [CrossRef]
353. Newcomb, A. Hacked MyFitnessPal Data Goes on Sale on the Dark Web—One Year After the Breach. Available online: https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach/ (accessed on 1 August 2021).
354. Thielman, S. Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History. Available online: https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached (accessed on 1 August 2021).
355. Mitnick, K.D.; Simon, W.L. *The art of Deception: Controlling the Human Element of Security*; John Wiley & Sons: Hoboken, NJ, USA, 2003.
356. Chiew, K.L.; Yong, K.S.C.; Tan, C.L. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Syst. Appl.* **2018**, *106*, 1–20. [CrossRef]
357. Anti-Phishing Working Group. Phishing Activity Trends Report—3rd Quarter 2020; Technical Report; Anti-Phishing Working Group: Washington, DC, USA, 2020.

358. The US Department of Justice. Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams—Hundreds of Domains Disrupted Through Public and Private Sector Cooperative Efforts. Available online: https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-COVID-19-related-scams, (accessed on 1 August 2021).
359. Symanovich, S. Coronavirus Phishing Emails: How to Protect against COVID-19 Scams. Available online: https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html (accessed on 1 August 2021).
360. 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]
361. Wright, A.; Aaron, S.; Bates, D.W. The Big Phish: Cyberattacks Against U.S. Healthcare Systems. *J. Gen. Intern. Med.* **2016**, *31*, 1115–1118. [CrossRef] [PubMed]
362. Jalali, M.S.; Bruckes, M.; Westmattelmann, D.; Schewe, G. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *J. Med. Internet Res.* **2020**, *22*, e16775. [CrossRef] [PubMed]
363. McKay, K.A.; Bassham, L.; Sönmez Turan, M.; Mouha, N. *Report on Lightweight Cryptography*; Technical Report DRAFT NISTIR 8114; National Institute of Standards and Technology, Gaithersburg, MD, USA, 2016.
364. Buchanan, W.J.; Li, S.; Asif, R. Lightweight cryptography methods. *J. Cyber Secur. Technol.* **2017**, *1*, 187–201. [CrossRef]
365. ISO Central Secretary. *Information Technology—Security Techniques—Lightweight Cryptography*; Technical Report ISO/IEC Standard 29192; International Organization for Standardization: Geneva Switzerland, 2012.
366. Biryukov, A.; Perrin, L. State of the Art in Lightweight Symmetric Cryptography. Cryptology ePrint Archive, Report 2017/511. 2017. Available online: https://eprint.iacr.org/2017/511 (accessed on 1 August 2021).
367. Bogdanov, A.; Knudsen, L.R.; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.B.; Seurin, Y.; Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 450–466.
368. Shirai, T.; Shibutani, K.; Akishita, T.; Moriai, S.; Iwata, T. The 128-Bit Blockcipher CLEFIA. In *International Workshop on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 181–195.
369. Hong, D.; Lee, J.K.; Kim, D.C.; Kwon, D.; Ryu, K.H.; Lee, D.G. LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In *International Workshop on Information Security Applications*; Springer: Cham, Switzerland, 2013; pp. 3–27.
370. Watanabe, D.; Ideguchi, K.; Kitahara, J.; Muto, K.; Furuichi, H.; Kaneko, T. Enocoro-80: A Hardware Oriented Stream Cipher. In Proceedings of the 3rd International Conference on Availability, Reliability and Security, Barcelona, Spain, 4–7 March 2008; pp. 1294–1300.
371. De Canniere, C.; Preneel, B. Trivium. In *New Stream Cipher Designs*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 244–266.
372. Lara-Nino, C.A.; Diaz-Perez, A.; Morales-Sandoval, M. Elliptic Curve Lightweight Cryptography: A Survey. *IEEE Access* **2018**, *6*, 72514–72550. [CrossRef]
373. Suárez-Albela, M.; Fraga-Lamas, P.; Fernández-Caramés, T.M. A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices. *Sensors* **2018**, *18*, 3868. [CrossRef] [PubMed]
374. Suárez-Albela, M.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Castedo, L. A Practical Performance Comparison of ECC and RSA for Resource-Constrained IoT Devices. In Proceedings of the Global Internet of Things Summit, Bilbao, Spain, 4–7 June 2018; pp. 1–6.
375. Liu, Z.; Huang, X.; Hu, Z.; Khan, M.K.; Seo, H.; Zhou, L. On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age. *IEEE Trans. Dependable Secur. Comput.* **2016**, *14*, 237–248. [CrossRef]
376. Marin, L.; Pawlowski, M.P.; Jara, A. Optimized ECC Implementation for Secure Communication between Heterogeneous IoT Devices. *Sensors* **2015**, *15*, 21478–21499. [CrossRef] [PubMed]
377. Liu, A.; Ning, P. TinyECC: A Configurable Library for Elliptic Curve Cryptographyin Wireless Sensor Networks. In Proceedings of the International Conference on Information Processing in Sensor Networks, St. Louis, MO, USA, 22–24 April 2008; pp. 245–256.
378. Nejatollahi, H.; Dutt, N.; Ray, S.; Regazzoni, F.; Banerjee, I.; Cammarota, R. Post-Quantum Lattice-Based Cryptography Implementations: A Survey. *ACM Comput. Surv.* **2019**, *51*, 1–41. [CrossRef]
379. Liu, Z.; Azarderakhsh, R.; Kim, H.; Seo, H. Efficient Software Implementation of Ring-LWE Encryption on IoT Processors. *IEEE Trans. Comput.* **2017**, *69* 1424 –1433
380. Xiao, D.; Yu, Y. Cryptanalysis of Compact-LWE and Related Lightweight Public Key Encryption. *Secur. Commun. Netw.* **2018**, *2018*, 4957045. [CrossRef]
381. Guo, J.; Peyrin, T.; Poschmann, A. The PHOTON Family of Lightweight Hash Functions. In *Proceedings of the Annual Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 222–239.
382. Bogdanov, A.; Knežević, M.; Leander, G.; Toz, D.; Varıcı, K.; Verbauwhede, I. SPONGENT: A Lightweight Hash Function. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 312–325.
383. Hirose, S.; Ideguchi, K.; Kuwakado, H.; Owada, T.; Preneel, B.; Yoshida, H. A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Korea, 1–3 December 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 151–168.

384. Luykx, A.; Preneel, B.; Tischhauser, E.; Yasuda, K. A MAC Mode for Lightweight Block Ciphers. In *Proceedings of the 23rd International Conference on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 43–59.
385. Mouha, N.; Mennink, B.; Van Herrewege, A.; Watanabe, D.; Preneel, B.; Verbauwhede, I. Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In *Proceedings of the International Conference on Selected Areas in Cryptography*; Springer: Cham, Switzerland, 2014; pp. 306–323.
386. Bakiri, M.; Guyeux, C.; Couchot, J.F.; Marangio, L.; Galatolo, S. A Hardware and Secure Pseudorandom Generator for Constrained Devices. *IEEE Trans. Ind. Informatics* **2018**, *14*, 3754–3765. [CrossRef]
387. Orúe López, A.B.; Hernández Encinas, L.; Martín Muñoz, A.; Montoya Vitini, F. A Lightweight Pseudorandom Number Generator for Securing the Internet of Things. *IEEE Access* **2017**, *5*, 27800–27806. [CrossRef]
388. Wallace, K.; Moran, K.; Novak, E.; Zhou, G.; Sun, K. Toward Sensor-Based Random Number Generation for Mobile and IoT Devices. *IEEE Internet Things J.* **2016**, *3*, 1189–1201. [CrossRef]
389. Xu, F.; Qin, Z.; Tan, C.C.; Wang, B.; Li, Q. IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian. In Proceedings of the IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 1862–1870.
390. Zhang, Z.; Wang, H.; Vasilakos, A.V.; Fang, H. ECG-Cryptography and Authentication in Body Area Networks. *IEEE Trans. Inf. Technol. Biomed.* **2012**, *16*, 1070–1078. [CrossRef]
391. Yao, L.; Liu, B.; Yao, K.; Wu, G.; Wang, J. An ECG-Based Signal Key Establishment Protocol in Body Area Networks. In Proceedings of the 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing, Xi'an, China, 26–29 October 2010; pp. 233–238.
392. Rushanan, M.; Rubin, A.D.; Kune, D.F.; Swanson, C.M. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 524–539.
393. Hu, C.; Cheng, X.; Zhang, F.; Wu, D.; Liao, X.; Chen, D. OPFKA: Secure and Efficient Ordered-Physiological-Feature-based Key Agreement for Wireless Body Area Networks. In Proceedings of the IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 2274–2282.
394. Xu, W.; Javali, C.; Revadigar, G.; Luo, C.; Bergmann, N.; Hu, W. Gait-Key: A Gait-Based Shared Secret Key Generation Protocol for Wearable Devices. *ACM Trans. Sens. Netw.* **2017**, *13*, 1–27. [CrossRef]
395. Revadigar, G.; Javali, C.; Xu, W.; Vasilakos, A.V.; Hu, W.; Jha, S. Accelerometer and Fuzzy Vault-Based Secure Group Key Generation and Sharing Protocol for Smart Wearables. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2467–2482. [CrossRef]
396. Effatparvar, M.; Dehghan, M.; Rahmani, A.M. A comprehensive survey of energy-aware routing protocols in wireless body area sensor networks. *J. Med. Syst.* **2016**, *40*, 201. [CrossRef]
397. Bhanumathi, V.; Sangeetha, C.P. A guide for the selection of routing protocols in WBAN for healthcare applications. *Hum.-Centric Comput. Inf. Sci.* **2017**, *7*, 24. [CrossRef]
398. Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. *J. Netw. Comput. Appl.* **2016**, *66*, 198–213. [CrossRef]
399. Boudargham, N.; Abdo, J.B.; Demerjian, J.; Guyeux, C.; Atechian, T. Efficient Cluster-Based Routing Algorithm for Body Sensor Networks. In Proceedings of the IEEE Middle East and North Africa Communications Conference, Jounieh, Lebanon, 18–20 April 2018; pp. 1–6.
400. Rajagopalan, R. Energy Efficient Routing Algorithm for Patient Monitoring in Body Sensor Networks. In Proceedings of the IEEE 13th International Conference on Wearable and Implantable Body Sensor Networks, San Francisco, CA, USA, 14–17 June 2016; pp. 141–146.
401. Nidhya, R.; Karthik, S.; Smilarubavathy, G. An End-to-End Secure and Energy-Aware Routing Mechanism for IoT-Based Modern Health Care System. In *Soft Computing and Signal Processing*; Springer: Singapore, 2019; pp. 379–388.
402. Su, H.; Wang, Z.; An, S. MAEB: Routing Protocol for IoT Healthcare. *Adv. Internet Things* **2013**, *3*, 8–15. [CrossRef]
403. Zargar, S.T.; Joshi, J.; Tipper, D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Commun. Surv. Tutorials* **2013**, *15*, 2046–2069. [CrossRef]
404. Kalkan, K.; Gür, G.; Alagöz, F. Filtering-Based Defense Mechanisms Against DDoS Attacks: A Survey. *IEEE Syst. J.* **2016**, *11*, 2761–2773. [CrossRef]
405. Yu, S.; Zhou, W.; Guo, S.; Guo, M. A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking. *IEEE Trans. Comput.* **2015**, *65*, 1418–1427. [CrossRef]
406. Bhuyan, M.H.; Bhattacharyya, D.K.; Kalita, J.K. E-LDAT: A lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric. *Secur. Commun. Netw.* **2016**, *9*, 3251–3270. [CrossRef]
407. Kalkan, K.; Alagöz, F. A distributed filtering mechanism against DDoS attacks: ScoreForCore. *Comput. Netw.* **2016**, *108*, 199–209. [CrossRef]
408. Nooribakhsh, M.; Mollamotalebi, M. A review on statistical approaches for anomaly detection in DDoS attacks. *Inf. Secur. J. Glob. Perspect.* **2020**, *29*, 118–133. [CrossRef]
409. Jian-Qi, Z.; Feng, F.; Ke-Xin, Y.; Yan-Heng, L. Dynamic entropy based DoS attack detection method. *Comput. Electr. Eng.* **2013**, *39*, 2243–2251. [CrossRef]
410. Doshi, R.; Apthorpe, N.; Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In Proceedings of the IEEE Security and Privacy Workshops, San Francisco, CA, USA, 24 May 2018; pp. 29–35.

411. Idhammad, M.; Afdel, K.; Belouch, M. Semi-supervised machine learning approach for DDoS detection. *Appl. Intell.* **2018**, *48*, 3193–3208. [CrossRef]
412. Yuan, X.; Li, C.; Li, X. DeepDefense: Identifying DDoS Attack via Deep Learning. In Proceedings of the IEEE International Conference on Smart Computing, Hong Kong, China, 29–31 May 2017; pp. 1–8.
413. Wu, G.; Wang, J.; Zhang, Y.; Jiang, S. A Continuous Identity Authentication Scheme Based on Physiological and Behavioral Characteristics. *Sensors* **2018**, *18*, 179. [CrossRef] [PubMed]
414. Enamamu, T.S.; Clarke, N.; Haskell-Dowland, P.; Li, F. Smart Watch based Body-Temperature Authentication. In Proceedings of the International Conference on Computing Networking and Informatics, Lagos, Nigeria, 29–31 October 2017; pp. 1–7.
415. Rostami, M.; Juels, A.; Koushanfar, F. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. In Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 1099–1112.
416. Kim, Y.; Lee, W.S.; Raghunathan, V.; Jha, N.K.; Raghunathan, A. Vibration-based Secure Side Channel for Medical Devices. In Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference, San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
417. Das, A.K.; Wazid, M.; Kumar, N.; Khan, M.K.; Choo, K.K.R.; Park, Y. Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment. *IEEE J. Biomed. Health Inform.* **2017**, *22*, 1310–1322. [CrossRef] [PubMed]
418. Kumar, D.; Grover, H.S. A secure authentication protocol for wearable devices environment using ECC. *J. Inf. Secur. Appl.* **2019**, *47*, 8–15. [CrossRef]
419. Bilal, M.; Kang, S.G. An Authentication Protocol for Future Sensor Networks. *Sensors* **2017**, *17*, 979. [CrossRef] [PubMed]
420. Liu, Y.; Zhang, Y.; Ling, J.; Liu, Z. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 1020–1026. [CrossRef]
421. de Carvalho Junior, M.A.; Bandiera-Paiva, P. Health Information System Role-Based Access Control Current Security Trends and Challenges. *J. Healthc. Eng.* **2018**, *2018*. [CrossRef] [PubMed]
422. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October 2006–3 November 2006; pp. 89–98.
423. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*; Springer: Cham, Switzerland, 2017; pp. 523–533.
424. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
425. Ioannou, C.; Vassiliou, V.; Sergiou, C. An Intrusion Detection System for Wireless Sensor Networks. In Proceedings of the 24th International Conference on Telecommunications, Montreal, QC, Canada, 24–22 August 2005; pp. 1–5.
426. Ioulianou, P.; Vasilakis, V.; Moscholios, I.; Logothetis, M. A Signature-based Intrusion Detection Systemfor the Internet of Things. In Proceedings of the Information and Communication Technology Form, Graz, Austria, 11–13 July 2018; pp. 1–5.
427. Bostani, H.; Sheikhan, M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. *Comput. Commun.* **2017**, *98*, 52–71. [CrossRef]
428. Karie, N.M.; Kebande, V.R.; Venter, H.S.; Choo, K.K.R. On the importance of standardising the process of generating digital forensic reports. *Forensic Sci. Int. Rep.* **2019**, *1*, 100008. [CrossRef]
429. ISO Central Secretary. *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*; Technical Report ISO/IEC Standard 27037; International Organization for Standardization: Vernier/Geneva, Switzerland, 2012.
430. ISO Central Secretary. *Information Technology—Security Techniques—Guidance on Assuring Suitability and Adequacy of Incident Investigative Method*; Technical Report ISO/IEC Standard 27041; International Organization for Standardization: Vernier/Geneva, Switzerland, 2015.
431. ISO Central Secretary. *Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence*; Technical Report ISO/IEC Standard 27042; International Organization for Standardization: Vernier/Geneva Switzerland, 2015.
432. ISO Central Secretary. Information Technology—Security Techniques—Incident Investigation Principles and Processes; Technical Report ISO/IEC Standard 27043; International Organization for Standardization: Vernier/Geneva Switzerland, 2015.
433. López-Aguilar, P.; Solanas, A. An Effective Approach to the Cross-Border Exchange of Digital Evidence Using Blockchain. In Proceedings of the 9th International Conference on Applications in Electronics Pervading Industry, Environment and Society, Pisa, Italy, 21–22 September 2021; pp. 1–5.
434. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**, *L119*, 1–88.
435. Annas, G.J. HIPAA Regulations—A New Era of Medical-Record Privacy? *N. Engl. J. Med.* **2003**, *348*, 1486–1490. [CrossRef]
436. Muchagata, J.; Ferreira, A. Translating GDPR into the mHealth Practice. In Proceedings of the International Carnahan Conference on Security Technology, Montreal, QC, Canada, 22–25 October 2018; pp. 1–5.
437. Bolognini, L.; Bistolfi, C. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Comput. Law Secur. Rev.* **2017**, *33*, 171–181. [CrossRef]

438. Domingo-Ferrer, J.; Mateo-Sanz, J.M. Practical Data-Oriented Microaggregation for Statistical Disclosure Control. *IEEE Trans. Knowl. Data Eng.* **2002**, *14*, 189–201. [CrossRef]
439. Sweeney, L. k-anonymity: A model for protecting privacy. *Int. J. Uncertainty, Fuzziness-Knowl.-Based Syst.* **2002**, *10*, 557–570. [CrossRef]
440. Lin, C.; Song, Z.; Song, H.; Zhou, Y.; Wang, Y.; Wu, G. Differential Privacy Preserving in Big Data Analytics for Connected Health. *J. Med. Syst.* **2016**, *40*, 97. [CrossRef] [PubMed]
441. López-Aguilar, P.; Solanas, A. Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism. In Proceedings of the IEEE 45th Annual Computers, Software, and Applications Conference, Madrid, Spain, 12–16 July 2021; pp. 1363–1368.
442. Abramson, A.; Caffarel-Salvador, E.; Soares, V.; Minahan, D.; Tian, R.Y.; Lu, X.; Dellal, D.; Gao, Y.; Kim, S.; Wainer, J.; et al. A luminal unfolding microneedle injector for oral delivery of macromolecules. *Nat. Med.* **2019**, *25*, 1512–1518. [CrossRef]
443. Flores, A.M.; Hosseini-Nassab, N.; Jarr, K.U.; Ye, J.; Zhu, X.; Wirka, R.; Koh, A.L.; Tsantilas, P.; Wang, Y.; Nanda, V.; et al. Pro-efferocytic nanoparticles are specifically taken up by lesional macrophages and prevent atherosclerosis. *Nat. Nanotechnol.* **2020**, *15*, 154–161. [CrossRef]
444. Zamani, R.; Aval, S.F.; Pilehvar-Soltanahmadi, Y.; Nejati-Koshki, K.; Zarghami, N. Recent Advances in Cell Electrospining of Natural and Synthetic Nanofibers for Regenerative Medicine. *Drug Res.* **2018**, *68*, 425–435. [CrossRef]
445. Vahedifard, F.; Chakravarthy, K. Nanomedicine for COVID-19: The role of nanotechnology in the treatment and diagnosis of COVID-19. *Emergent Mater.* **2021**, *4*, 75–99. [CrossRef]
446. Miraz, M.H.; Ali, M.; Excell, P.S.; Picking, R. Internet of Nano-Things, Things and Everything: Future Growth Trends. *Future Internet* **2018**, *10*, 68. [CrossRef]
447. Lopez-Iturri, P.; Aguirre, E.; Trigo, J.D.; Astrain, J.J.; Azpilicueta, L.; Serrano, L.; Villadangos, J.; Falcone, F. Implementation and Operational Analysis of an Interactive Intensive Care Unit within a Smart Health Context. *Sensors* **2018**, *18*, 389. [CrossRef] [PubMed]
448. Aguirre, E.; Lopez-Iturri, P.; Azpilicueta, L.; Rivarés, C.; Astrain, J.J.; Villadangos, J.; Falcone, F. Design and performance analysis of wireless body area networks in complex indoor e-Health hospital environments for patient remote monitoring. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 1–17. [CrossRef]
449. Yu, F.R.; Zhang, X.; Leung, V.C.M. *Green Communications and Networking*; CRC Press: Boca Raton, FL, USA, 2016.
450. Ali, Z.; Henna, S.; Akhunzada, A.; Raza, M.; Kim, S.W. Performance Evaluation of LoRaWAN for Green Internet of Things. *IEEE Access* **2019**, *7*, 164102–164112. [CrossRef]
451. Gandotra, P.; Jha, R.K.; Jain, S. Green Communication in Next Generation Cellular Networks: A Survey. *IEEE Access* **2017**, *5*, 11727–11758. [CrossRef]
452. Huang, T.; Yang, W.; Wu, J.; Ma, J.; Zhang, X.; Zhang, D. A Survey on Green 6G Network: Architecture and Technologies. *IEEE Access* **2019**, *7*, 175758–175768. [CrossRef]
453. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*; Technical Report Special Publication 800-207; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
454. Bertino, E. Zero Trust Architecture: Does It Help? *IEEE Secur. Priv.* **2021**, *19*, 95–96. [CrossRef]
455. Dasaklis, T.K.; Casino, F.; Patsakis, C. Blockchain Meets Smart Health: Towards Next Generation Healthcare Services. In Proceedings of the 9th International Conference on Information, Intelligence, Systems and Applications, Zakynthos, Greece, 23–25 July 2018; pp. 1–8.
456. Kroll, J.A.; Michael, J.B.; Thaw, D.B. Enhancing Cybersecurity via Artificial Intelligence: Risks, Rewards, and Frameworks. *Computer* **2021**, *54*, 64–71. [CrossRef]
457. Taddeo, M.; McCutcheon, T.; Floridi, L. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nat. Mach. Intell.* **2019**, *1*, 557–560. [CrossRef]
458. Truong, T.C.; Zelinka, I.; Plucar, J.; Čandík, M.; Šulc, V. Artificial Intelligence and Cybersecurity: Past, Presence, and Future. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*; Springer: Singapore, 2020; pp. 351–363.
459. Choi, I.S.; Hong, J.; Kim, T.W. Multi-Agent Based Cyber Attack Detection and Mitigation for Distribution Automation System. *IEEE Access* **2020**, *8*, 183495–183504. [CrossRef]
460. Zeadally, S.; Adi, E.; Baig, Z.; Khan, I.A. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access* **2020**, *8*, 23817–23837. [CrossRef]
461. Gerke, S.; Minssen, T.; Cohen, G. Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial Intelligence in Healthcare*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 295–336.
462. Siemens, G. Connectivism: A Learning Theory for the Digital Age. *Int. J. Instr. Technol. Distance Learn.* **2005**, *2*, 3–10.
463. Mostashari, A.; Arnold, F.; Mansouri, M.; Finger, M. Cognitive cities and intelligent urban governance. *Netw. Ind. Q.* **2011**, *13*, 4–7.
464. Machin, J.; Batista, E.; Martínez-Ballesté, A.; Solanas, A. Privacy and Security in Cognitive Cities: A Systematic Review. *Appl. Sci.* **2021**, *11*, 4471. [CrossRef]