

Old Dominion University

ODU Digital Commons

School of Cybersecurity Faculty Publications

School of Cybersecurity

5-2023

IoT Health Devices: Exploring Security Risks in the Connected Landscape

Abasi-amefon Obot Affia

Hilary Finch

Woosub Jung

Issah Abubakari Samori

Lucas Potter

See next page for additional authors

Follow this and additional works at: <https://digitalcommons.odu.edu/cybersecurity-pubs>





Part of the [Data Storage Systems Commons](#), [Digital Communications and Networking Commons](#), [Graphics and Human Computer Interfaces Commons](#), and the [Information Security Commons](#)

Authors

Abasi-amefon Obot Affia, Hilary Finch, Woosub Jung, Issah Abubakari Samori, Lucas Potter, and Xavier-Lewis Palmer

Review

IoT Health Devices: Exploring Security Risks in the Connected Landscape

Abasi-amefon Obot Affia ^{1,*}, Hilary Finch ^{2,3,*} , Woosub Jung ⁴ , Issah Abubakari Samori ⁵, Lucas Potter ⁶ and Xavier-Lewis Palmer ^{3,6}

¹ Institute of Computer Science, University of Tartu, 51005 Tartu, Estonia

² School of Cybersecurity, Old Dominion University, Norfolk, VA 23529, USA

³ CYBER Solutions Academy, Franklin, VA 23851, USA

⁴ LENS Laboratory, Department of Computer Science, William & Mary, Williamsburg, VA 23185, USA

⁵ MinoHealth AI Labs, Accra 00233, Ghana

⁶ School of Engineering and Technology, Biomedical Engineering Institute, Old Dominion University, Norfolk, VA 23529, USA

* Correspondence: amefon.affia@ut.ee (A.-a.O.A.); hfinc003@odu.edu (H.F.)

Abstract: The concept of the Internet of Things (IoT) spans decades, and the same can be said for its inclusion in healthcare. The IoT is an attractive target in medicine; it offers considerable potential in expanding care. However, the application of the IoT in healthcare is fraught with an array of challenges, and also, through it, numerous vulnerabilities that translate to wider attack surfaces and deeper degrees of damage possible to both consumers and their confidence within health systems, as a result of patient-specific data being available to access. Further, when IoT health devices (IoTHDs) are developed, a diverse range of attacks are possible. To understand the risks in this new landscape, it is important to understand the architecture of IoTHDs, operations, and the social dynamics that may govern their interactions. This paper aims to document and create a map regarding IoTHDs, lay the groundwork for better understanding security risks in emerging IoTHD modalities through a multi-layer approach, and suggest means for improved governance and interaction. We also discuss technological innovations expected to set the stage for novel exploits leading into the middle and latter parts of the 21st century.



Citation: Affia, A.-a.O.; Finch, H.; Jung, W.; Samori, I.A.; Potter, L.; Palmer, X.-L. IoT Health Devices: Exploring Security Risks in the Connected Landscape. *IoT* **2023**, *4*, 150–182. <https://doi.org/10.3390/iot4020009>

Academic Editor: Amiya Nayak

Received: 26 February 2023

Revised: 21 April 2023

Accepted: 24 April 2023

Published: 25 May 2023



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

Keywords: biocybersecurity; cyberbiosecurity; healthcare; IoT; security risk management

1. Introduction

The Internet of Things (IoT) has been steadily rolled out to numerous devices worldwide since the mid-late 2000s, starting largely with benign consumer items and increasingly into more sensitive areas, including healthcare, transportation, and more sensitive services [1]. With the inclusion of the IoT into healthcare, significant gains were realized in that patients experienced ease in reporting their health status [2,3]. In some cases, those confined gained autonomy [2,3]. This applies to institutions adopting the IoT, gradual, sparing legislation adopted in the past 20 years to fast-track and improve the digitalization and reporting of medical information. It has not been just healthcare facilities that have boomed with IoT adoption. Modern labs, warehouses, schools, transport equipment, and agricultural plots use IoT devices in the 21st century [4], and these remain critical in consideration of healthcare impacts as their inputs and interactions impact operations. However, consumers and institutions alike have raised significant concerns about the continued digitalization of healthcare. The issues causing these concerns have occurred, from simple oversights in design to complex implementations of IoT health devices (IoTHDs). These have been accompanied by the discovery of numerous security vulnerabilities and high volumes of attacks that have been carried out [5–14]. Vulnerabilities in IoTHD design and implementation pose immediate data-based threats. These threats include mass data leaks,

improper forwarding of data, and sometimes even indirectly disrupting the operation of other connected devices through a lack of communication or coordination [15–17]. We found vulnerabilities in production-scale and patched devices that have stored data in unencrypted, non-proprietary, and easy-to-access formats. However, it is worth noting that proprietary formats can frustrate open-source efforts and are usually financially motivated but more secure. Alternatively, some vulnerabilities leak access to other connected devices, which is problematic for any roll-out [17]. Relating to attacks, an increasing amount of health and manufacturing infrastructure has been open [17,18] and subject to attacks, such as Advanced Persistent Threats (APTs), ransomware, trojans, worms, and loggers [19]. These persistent problems within the IoTHD supply chain and health chain of actions pose numerous threats to patient health, caregiver service, and national security. Strielkina et al. [15] noted the significant problems networked devices posed, including random failures, privacy compromise, and deliberate operations disruptions.

This paper examines the architecture components of IoTHD systems dissected in terms of devices, connected software technologies, the backbone infrastructure, and the individuals involved—IoTHD stakeholders. The discussion of the devices targets medical imaging, medical sensors (used to derive data from being taken advantage of and facilitate processes in modern healthcare), external and implanted devices, and virtual home assistants. The software discussion is split between legacy systems and AI-based software technologies that enable functions within these IoTHDs. The infrastructure discussion covers the communication and application backbone relevant to achieving medical services. Lastly, using IoTHDs requires a discussion of the relevant people and communities. These refer to nation-state actors, healthcare facility personnel, and independent and unorthodox communities. With knowledge of the landscape, we explore the vulnerabilities in healthcare infrastructure as a subset of the international bioeconomy through the lens of IoTHDs. We discuss the components of IoTHDs, vulnerabilities and threats leading to security risks, and control suggestions to address the security risks in IoTHDs. We propose and apply a multi-layer approach to IoTHD security risk management as a beneficial method to facilitate end-to-end security in IoTHDs.

Lastly, we discuss the purpose of modern and emerging IoTHDs. Understanding this allows for an enhanced understanding of emerging and future vulnerabilities and threats, i.e., theoretical threat classification due to emerging IoTHD issues (in terms of novel attack/defense topologies, emerging social dynamics around devices, neuro-link adjacent devices, brain–computer interfaces, and wearable and minimally invasive device vulnerabilities) and practical examples with a case report in the literature. Following this, we discuss future IoTHD controls/countermeasures considerations in terms of device and culture design, practices and training, and innovations to introduce as relating to 4th industrial revolution (4IR) technologies (relating to AI, blockchain, and others that assist toward automation), applications of state defense in the vein of defend forward, and business opportunities that can be capitalized upon by enterprising minds. Overall, this condensed survey and exploration paper will be a valuable tool for anyone concerned with the security of IoTHDs and their potential impact on healthcare and other sectors. We believe that our paper can contribute to navigating the complexities and potential risks of IoTHDs and those that emerge from them.

2. IoT Healthcare Components

IoTHDs are gaining popularity in healthcare. Some are legacy devices that do not immediately have IoTHD features that can be retrofitted, but many are newly manufactured devices that automatically have IoT functionality that can be embedded. Covering important common assets they produce in processing patient phenomena is also important. According to the literature, over half of the IoTHDs have critical security vulnerabilities [20,21]. Before enumerating the vulnerabilities of these devices and the future directions of IoTHDs, we define the different types of IoTHDs that we focus on in this paper.

2.1. IoT System High-Level Architecture

In the literature, the extent of the reference architecture used for IoT systems in healthcare examines layered models. The architecture of the IoT in healthcare essentially consists of three (3) basic layers consisting of the perception, network, and application layers [22,23]. Fundamentally, medical information is collected from networked medical devices and wearable or implanted sensors and is transmitted through communication infrastructures to relevant end-users through software applications for monitoring and taking appropriate action. We summarize the high-level architecture of IoT components in healthcare. This is visualized in Figure 1.

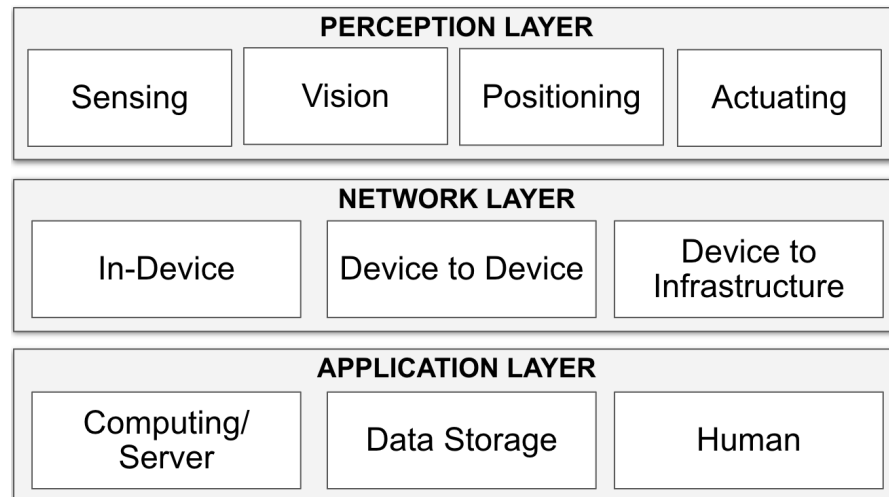


Figure 1. IoT architecture layers and their components, adapted from [24].

2.1.1. Perception Layer

This layer comprises devices with sensing capabilities where medical devices and wearable and implanted sensors are used to obtain real-time patient or end-user medical information to facilitate diagnosis and high-quality medical treatments. Such devices include Radio Frequency Identification (RFID) tags, infrared sensors, imaging equipment, GPS, other medical sensors, and smart device sensors [22,25]. These devices allow for comprehensive perception through object identification, image recognition, location recognition, and actuation and can convert this information to digital signals for transmission [25]. We discuss more regarding perception-layer devices in Section 2.2.

2.1.2. Network Layer

The network layer constitutes wired and wireless networks, which connect perception devices, application-layer devices, and other network devices to transmit medical information collected at the perception layer to the application layer. Communication between things can occur using short-range communication technologies, such as RFID (Radio Frequency Identification) and NFC (Near-Field Communication), and medium-range communication technologies, such as Bluetooth, Zigbee, WiFi, and the global system for mobile (GSM) communications [22]. However, high-frequency fourth-generation (4G) and fifth-generation (5G) cellular networks are becoming more readily available and providing a reliable connection for up to thousands of devices at the same time [25].

2.1.3. Application Layer

The application layer interprets and applies data generated at the perception layer and transmitted through the network layer. The layer is also responsible for providing usability to the end-user, delivering application-specific computing services, and data storage.

The end-users could be a doctor monitoring their patient's data in real time on a hospital computer, a specialist monitoring their patient's record on a smart device, and a

family member of the patient or even the patient themselves monitoring vital signs on their smart device. We discuss more regarding relevant end-users in Section 2.4.

Most promising IoT medical applications are facilitated using artificial intelligence (AI) for image analysis in radiology, pathology, and dermatology, electronic medical records (EMRs) text recognition with natural language processing, and drug activity design, as well as illness trajectories, medical outcomes and interventions, and re-admissions predictions [26].

Data storage and manipulation are critical aspects of IoT healthcare applications. Cloud infrastructures support data-intensive electronic medical records (EMRs), patient portals, medical IoT smartphone applications, and big data analytics driving decision support systems and therapeutic strategies [27].

2.2. IoT Healthcare Devices

Our analysis focuses on IoTHDs, ranging from networked medical devices to wirelessly reprogrammable implantable devices and software applications. In this paper, we refer to medical devices as any instrument, machine, implant, in vitro reagent, or related components intended for the diagnosis or in the cure, mitigation, treatment, or prevention of diseases [28].

We discuss examples of these IoTHDs and their application to healthcare.

2.2.1. Medical Imaging

Medical images are becoming even more important due to the advancements in telemedicine. Magnetic Resonance Imaging (MRI) and CT (Computed Tomography) are volumetric medical imaging methods commonly used for medical diagnosis. X-rays are a more elementary mode of medical imagery. Because these images contain important information about one's health concerns, they are usually considered key components that the healthcare sector needs to protect in the field of cyberbiosecurity [29–31]. One of the many forms of medical images is Digital Imaging and Communications in Medicine (DICOM). DICOM is a standard for storing and transmitting medical images, which gives the biomedical details of the organ that is being examined [32]. DICOM and PACS (picture archiving and communication systems) are well-known for medical imaging transmission and storage protocols [33]. Typically, CT and MRI images can be acquired in the DICOM format and stored in PACS servers where the PACS clients, such as doctors and medical staff, can access the stored files through the DICOM protocol. However, these medical imaging systems have been exposed to malicious attacks because of the lack of critical network security [34,35]. For example, DICOM provides encryption options but has also been exposed to malicious attacks [36].

Although Generative Adversarial Networks (GANs) are mostly used in image fabrication, they can also be used in sensing data. Some studies have already shown the feasibility of using GANs in ubiquitous sensing data other than images. For example, Erol et al. [37] utilized GANs to generate realistic radar data for human activity recognition [37]. While these are not relevant for medical procedures, they can be when adapted to specific surgical or other medical techniques that are machine guided. For example, deep learning was utilized to attempt noise reduction in ultrasound images [38]. This demonstrates the potential for adversaries to build means that mimic medical devices' behavior in time. Beyond the radar data, inertial measurement unit (IMU) sensing data or biometric data can always be replayed using GANs [39].

In addition, other forms of imaging include smart cameras to assist healthcare delivery, including wound analysis in patients with diabetes [40], monitoring dermatitis and skin conditions [41] and heart rates, and monitoring tear film buildup in dry eye disease [42].

2.2.2. Medical Sensors

Besides medical imaging equipment, biometric medical sensors can directly retrieve digital output readings from human beings [43]. Medical images are predominantly created at a specialized medical facility, but medical sensing data can be collected at a hospital or

in daily life [44,45]. This is made possible because IoT technologies have grown rapidly, and thus ubiquitous sensing is available by wearable devices worn by the user that interconnect wearable sensors through wireless connections [46,47]. For example, vital sign patches to wirelessly track and monitor heart rate, respiration rate, temperature, step count, sleep cycle, stress levels, and falls or incapacitation; wireless electrocardiogram monitors [48]; smartwatches and Fitbits (to track activity, heart rate, and sleep patterns); fall detectors, such as iFall (a wearable accelerometer that communicates with a smartphone and the cloud), to detect and respond to patient falls [49]; wearable blood pressure monitors [50]; neural sensors to read and understand neural brain signals and to infer the state of the brain [51]; and finger pulse oximeters to measure oxygen saturation levels in the blood [52]. With the criticality of these devices to patient diagnosis, injecting or removing sensing data can also cause a significant misdiagnosis. However, a lot of these devices have notably poor signal quality already. For instance, wrist-mounted pulse oximeter devices are regularly off by a large margin when addressing patients with darker skin tones [52]. Devices like these require additional reevaluation on top of their potential to leak data. This presents a possible compound disruption to the quality of care in analogously deficient devices. As a result, disruptions can further impede the reliability of healthcare operations. Thus, future healthcare sectors must ensure that medical sensing data are secure.

2.2.3. Implanted Medical Devices

As micro-electromechanical systems (MEMS) have grown significantly, researchers have made inroads to propose medical devices that can be implanted into human bodies—yet popular acceptance of these devices may be many years away. This is to say nothing of the current reliability of these devices, which may be low. Numerous brain–machine interfaces aim to communicate with neural signals of human brains to treat disease conditions that are currently difficult to treat reliably [53–56]. Likewise, implanted medical devices not only stay in human bodies but will eventually be parts of live devices that can transmit data outside the body [57]. For example, for digital (smart) medications, an ingestible sensor (a microfabricated sensor made from copper, magnesium, and silicon, in minute quantities) can communicate with an external body sensor, such as a wearable sensor patch [23].

In this regard, there are multiple vulnerabilities in using such implanted medical devices [58]. For example, authentication methods on implanted medical devices are an especially pertinent topic [59]. It is also important to consume battery power more efficiently [58]. Implanted devices can be hacked to consume inefficiently and reduce user life quality. In addition, data availability, integrity, and confidentiality should always be available to the users [60]. By doing this, healthcare professionals can better manage the implanted devices.

2.2.4. Virtual Medical Home Assistants

As discussed earlier, advanced IoT technologies can enable patients to be treated at home. Virtual medical home assistants could be part of healthcare [16,61–63]. For example, continuous glucose monitors and smart insulin pens (which track dose and time and recommend the correct type of insulin to use) [64]; sleep trackers; home security cameras; and voice assistants can also be part of healthcare components because they generate medical information, e.g., fall events, and transmit them to off-site data storage facilities [65,66]. These devices can be used at home for remotely monitoring patients' biomedical status remotely [16].

Specifically, smart voice assistants (also known as conversation agents) installed in the home setting can support users through conversations, answer specific health-related questions without human contact, and collect data for screening and remote patient monitoring [67]. Product designers, security experts, human factors engineers, and regulators might benefit from considering how the lexicon might affect voice assistants. For example, they might want to consider how people of different backgrounds/incomes would talk to a doctor and (presumably) a voice assistant differently. Considerations within this space might help expose additional vulnerabilities in device operation.

Additionally, health robots can be applied to support the detection of unhealthy behaviors, manage medication use, and assist in rehabilitation therapies [68].

Overall, the definition of healthcare input data has expanded substantially. Accordingly, healthcare should protect these wide scopes of input data from malicious adversaries [14,69–72]. As healthcare organizations become more distributed in treating and observing patients, they represent wider attack surfaces.

2.3. IoT Healthcare Supporting Technologies

Various software components and infrastructure technologies support IoTHDs to function effectively.

2.3.1. IoTHD Software Components

Software components are crucial in enabling various functionalities and facilitating communication among different devices and systems, and they need to be designed, developed, and tested with security in mind. Healthcare facilities can choose from a wide variety of healthcare software programs. Each choice requires high-quality security implementations to secure patient data and medical facilities. IT solutions in healthcare support medical professionals by automating manual workflow or supporting medical workers wherever they work. Most software gathers patient information to coordinate the best care among qualified healthcare providers. The Electronic Health Record Software (EHR) and Electronic Medical Record Software (EMR) are the most used healthcare software. These are the gateways for both patients and providers. Other medical software currently available includes Medical Diagnosis Software, which enables the real-time transmission of information between providers, medical databases, visualization and imaging, medical research, tele-health and telemedicine, and patient engagement software [73]. Software for the healthcare industry is not currently standardized. Even at its best, some of the current healthcare software is cumbersome. The user experience was not prioritized in the design of the system interface. Although EHR is intended to simplify the process, it can be compromised. As a result, hackers are free to take patient data and hold it hostage while exploiting it to make money. Some hospitals still use paper medical records because they have not fully migrated to EHR. Teaching hospital employees the best ways to secure patient data throughout these changes is crucial. As secure as any software is, medical professionals will continue making human errors in healthcare. The medical software should be a backup to the provider to provide the best possible care.

Healthcare systems have also used outdated legacy software that is still in use due to its critical functionality but is often no longer supported by the manufacturers, making them vulnerable to security risks and compatibility issues. One major challenge with legacy software in IoT healthcare device systems is the potential for security vulnerabilities. These software components no longer receive updates and patches, making them susceptible to cyberattacks that exploit known vulnerabilities. This could result in compromised sensitive patient data or the device, potentially harming patients [34,74,75]. Another issue with legacy software is compatibility. As new technologies and systems are developed, legacy software may no longer be compatible with newer hardware or software. This can create issues when integrating older devices into new systems or upgrading existing ones. It is also important to note that in some cases, healthcare organizations may be required to continue using legacy software due to regulatory or compliance requirements.

AI-based software also benefits IoTHDs. AI can read available EMR data, including medical history, physicals, laboratory reports, imaging, and medications, and contextualize these data to generate treatment and/or diagnosis decisions and/or possibilities. Further, it can interpret data from various sources. For example, IBM Watson uses AI to read both structured and unstructured text in EMR, to read images to highlight primary and incidental findings, and to compile relevant medical literature in response to clinical queries [39]. IoT-based healthcare and deep machine learning can assist health professionals in seeing the unseeable and providing new and enhanced diagnostic capabilities. Although diagnostic

confidence may never reach 100%, combining machines and clinician expertise reliably enhances system performance. For example, compared with the diagnostic evaluation by 54 ophthalmologists and senior residents, applying AI to retinal images improved the detection and grading of diabetic retinopathy and macular edema, achieving high specificity (98%) and sensitivity (90%) [76]. AI and deep learning can also optimize disease management, provide big data and analysis generated from mHealth apps and IoT devices, and are seeing adoption in healthcare [77]. Some examples of this include predicting risk, future medical outcomes, and care decisions in diabetes and mental health [78] and predicting the progression of congestive heart failure [79,80], bone disease [81], Alzheimer disease [82], and benign and malignant tumor classification [83]. However, AI-based threats are new and emerging. These threats used machine learning techniques to rapidly and comprehensively learn new vulnerabilities and attack routes. A recent survey [84] listed actual and possible frameworks that can attack devices, software, and other assets in health security.

2.3.2. IoTHD Supporting Infrastructure

Backbone infrastructures are critical in ensuring IoTHDs function effectively, securely, and reliably.

IoTHDs generate massive amounts of data that need to be processed and analyzed in real time, where cloud computing infrastructure provides the necessary processing power and storage capacity to handle this data. However, with more cloud apps entering the health market, it is just as important that an evidence base supports its effectiveness and safety and can deal with the security of health data and the reliability and transparency of that data by third parties. Furthermore, it has been suggested that centralized cloud storage will present issues in the future to users, such as excessive data accumulation and latency, because of the distance between IoT devices and data centers.

IoTHDs require a reliable and secure communication infrastructure to transmit data between devices, servers, and other systems. This infrastructure includes wired and wireless networks, protocols, and communication standards. Communicated healthcare data are often stored on a local machine (often decentralized) or turned over to a central hospital repository. Cloud-based computing to support the delivery of health services has many benefits, as it is ubiquitous, flexible, and scalable in terms of data acquisition, storage, and transmission between devices connected to the cloud [66]. The use of the cloud can be foreseen to support data-intensive electronic medical records (EMRs), patient portals, medical IoT devices (which can include smartphone apps), and the big data analytics driving decision support systems and therapeutic strategies [85].

Decentralized data processing and networking approaches may improve the scalability of the IoT in healthcare. Edge cloud is a newer cloud computing concept that allows IoT sensors and network gateways to process and analyze data themselves (i.e., at the edge) in a decentralized fashion, reducing the amount of data required to be communicated and managed at a centralized location [31,86]. Similarly, blockchain storage uses a decentralized approach to data storage, creating independent blocks containing individual sets of information, forming a dependent link in a collective block, and creating a network regulated by patients rather than a third party [87]. However, the usage of blockchain is minimal for now. There are examples of platforms engineering blockchain for medical practice already [20,87]; however, research on edge clouds and blockchains in healthcare is still limited and is an important area for future research.

2.4. IoT Healthcare Stakeholders

Individuals must interface with IoTHDs on the front end (usually the Graphical User Interface (GUI)) and back end (usually through medical infrastructure). We focus on patients and patient family members, healthcare personnel, and IoTHD developers as they have security impacts on IoTHDs and their related assets.

2.4.1. Patients and Related Family Members

Patients and their related family members have a tremendous role in accessing and advocating for quality care. It is important to consider the modes of care and the communication platforms (smartphone vs. hospital-owned medical device(s)). Healthcare security professionals should consider wide scenarios at play with the transmission of hospital information. For example, upon obtaining acceptance from the patient, or even the patient themselves on their smartphone, family members will communicate healthcare details differently.

2.4.2. Healthcare Personnel

We discuss healthcare personnel in degrees of contact with patients. First-degree personnel commonly include physicians, nurses, students, receptionists, phlebotomists, technicians, surgeons, scribes, emergency response doctors, janitors, security workers, and administrators. Contract workers who may be involved with security, the transportation of materials, information technology staff, and guest scientists or collaborators make up second-degree personnel. Third-degree personnel can work with or associate with second-degree personnel or are unpaid, such as students, volunteers, patient visitors, and police officers, in limited cases of needed operation, participation, and agency.

2.4.3. IoTHD Manufacturers

IoTHD manufacturers cover all those in charge of building, configuring, and maintaining IoTHDs. IoTHD manufacturers can introduce security issues during device manufacturing cycles and should similarly sharpen the protection of their most critical manufactured assets. These include tighter protocols, vetting, and minimization of interactions with core IP assets, offline backups, networking segmentation, web filtering, etc. [88]. Additionally, IoTHD manufacturers should assume they are already targets and be aware of phishing attacks [88].

2.5. Security Risk Management

To study the security aspects and possible risks with IoTHDs, we apply information systems security risk management (ISSRM) concepts, defined by Dubois et al. [89], that define the asset, risk, and risk treatment-related concepts to guide security risk management. We selected the ISSRM method because it supported systematic asset identification and functional decomposition of the system [90,91] when compared to other risk management methods used for IoT systems, such as NIST (National Institute of Standards and Technology) [92], OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation Method) [93], and TARA (Threat Assessment and Remediation Analysis) [94]. Affia et al. [95] provides a more detailed comparison of these methods. We also follow a threat-driven approach to security risk management [96], developed in line with the ISSRM method, to provide security threat analysis support benefits, including threat and risk treatment coverage, by leveraging the STRIDE method. We explore major concepts of the ISSRM method below:

- Asset-related concepts—identify relevant assets for security risk analysis. It describes the business assets—that represent information, data, and processes that bring value to an organization—and system assets—that support business assets to protect. Asset-related concepts also describe the security criteria (in terms of confidentiality, integrity, and availability) that define the security needs of the assets [89].
- Risk-related concepts—illustrate the vulnerability, threat agent, threats, and risk impact analysis of the assets in scope. A security risk is a combination of a security event and its impact (negation of the security criterion), harming business and system assets. A vulnerability is a characteristic of system assets, constituting its flaws—an implementation defect that can lead to a vulnerability [89]. A threat agent refers to an entity that has the potential to cause damage to information system assets, thereby initiating a threat and becoming the origin of a risk. Typically, a threat agent is identified by their motivation, skills, capability, knowledge, available resources, and opportunity to carry

out an attack [89,97]. A threat event is a component of security risk that occurs when a threat targets system assets and exploits their vulnerability. The STRIDE method [98] can then be used for security threat analysis [96]. The abbreviation STRIDE stands for spoofing (S)—pretending to be someone else to gain access to sensitive data or resources, tampering (T)—altering data or code to manipulate the application’s behavior or cause it to malfunction, repudiation (R)—denying ones actions or the actions of others and making it difficult to track down the source of an action, information disclosure (I)—exposing or gaining access to information one should not be able to access, denial of service (D)—preventing a system from providing its intended service by crashing it, slowing it down, or filling its storage, and elevation of privilege (E)—gaining access to functionality without authorization [98]. Further in this study, we use STRIDE to guide a security threat analysis due to its industrial usage, maturity, high research concentration within the security community, and applicability for guiding risk treatment.

- Risk treatment-related concepts—tackle mitigating the identified security risks, guiding risk mitigation decisions, security requirements, and controls to treat the risks. Security requirements aim to define conditions to be reached by mitigating identified security risks and are prerequisites to controls that implement the specified security requirements [89]. The STRIDE security requirements can thus guide requirements elicitation for risk treatment [96].

In this study, we apply these security risk management concepts in a multi-layer approach to understand the security risks within the IoTHD ecosystem.

3. Security Risks in IoT Health Devices

The examination of security risk management in IoT layers through the related work [24] has brought to light certain issues that may not have been discovered if the IoT system’s architecture was not considered. These issues include research gaps arising from an unequal focus on security research on some IoT architecture layers to the detriment of others, the effect of risk on one layer cascading to other layers, and the necessity of implementing multi-layer risk analysis and defence strategies. Thus, we seek to apply a multi-layer approach to IoTHD security management as a beneficial method to facilitate end-to-end security in IoTHDs. In this section, we summarize our multi-layer IoTHD asset findings in Table 1, discuss the vulnerabilities of these IoTHD system assets, highlight relevant threat agents with the motivation and expertise to attack IoTHDs, and then formalize threats to IoTHDs in Table 2. We also provide a multi-layer risk analysis based on real-world scenarios to instantiate our approach.

3.1. IoTHD Assets

Table 1 summarizes the IoTHD assets (system and business assets) based on the discussed IoTHDs and classifies these assets into functional areas of each layer.

Table 1. IoTHD Architecture-layer assets.

| Layer | System Assets | Business Assets | |
|--------------------|-----------------------------|---|---|
| Perception [23,25] | Sensing | Neural sensors, infrared sensors, RFID (Radio Frequency Identification) tags, light sensors, magnetometer, thermometers, smartwatches, monitoring patches, finger pulse oximeters | Patient biomedical status: patient activity, heart rate, sleep patterns, neural activity/brain signal, oxygen saturation levels, body temperature, glucose level in blood |
| | Positioning | Location sensor, movement sensor, gyroscope, accelerometer | Pseudo-range measurements |
| | Visioning | Smart cameras, medical imaging systems (MRI and CT) | Surveillance (audio, picture, video) data, MRI and CT images |
| | Actuating | Medical device control unit, social robot actuators | Medical device commands |
| Network [23,25,99] | In-device | DICOM, Bluetooth, WiFi, Zigbee, RFID, wireless sensor networks, NFC (Near-Field Communication), Z-wave, MQTT, LoRa and ultra-wide bandwidth (UWB), wireless body area networks (WBAN) | Transmitted perception data |
| | Device-to- device | | |
| | Device-to- infrastructure | | |
| Application [23] | Computing/ Personal Servers | Web application platform, mobile application, PACS server | Application process, application data, perception data |
| | Data Storage | Virtualized storage at edge computing, local database, PACS storage | Perception and application data |
| | End-user | Patients and related family members, healthcare personnel, IoTHD manufacturers | Application process, PII, patient biomedical status |

3.2. IoTHD Vulnerabilities

A vulnerability is a weakness in a system asset, group of system assets, or security control that a threat agent could exploit to cause harm to the system. As such, medical devices, specifically when they are connected to networks, are just as vulnerable as any other networked security systems and are subject to security breaches because they are all interconnected [100]. As the medical world expands in networking and information technology, there are increased opportunities for threat incidents initiated by malicious

agents that target IoTHD system assets by exploiting their vulnerabilities. IoTHDs have become more vulnerable to cybersecurity vulnerabilities due to the rapid growth, prioritized role in aiding healthcare diagnosis, and greater connectivity between the devices, leading to high-impact clinical treatment and patient safety [100]. This section discusses the vulnerabilities of IoTHD system assets within their respective IoT layers.

3.2.1. Perception-Layer Vulnerabilities

IoTHDs, including legacy devices, are vulnerable to physical attacks that render devices unusable. Those medical devices are usually expensive and mostly managed by RFID in hospitals [101]. Despite the efforts of the protocol-level approaches, medical devices are often targeted by physical thefts, which is harder to protect through software solutions. Additionally, the potential for smart pills to be a target of theft exists as well [102], alongside medical identity theft by stealing fobs, cards, and other physical means of accessing healthcare assets. According to Mancini et al. [103], medical identity is used to access certain medical benefits by adversaries. IoT health devices are also limited in the power and resources they possess [100]. Thus, encrypting data transmitted by these devices, for instance, can significantly slow down their operation, reducing their usable battery life. This is a critical issue as some medical devices rely on prolonged battery life, and any reduction in it could affect their effectiveness and even pose risks to patients.

Data authentication is crucial to medical device security because these factors are related to one's medical history and data privacy. IoTHDs may suffer from an elevation of privilege attacks (EoP) when device authentication is missing [104]. Implanted devices that enable communication between brains, brain-stems, and other parts of the central nervous system are vulnerable to unethical access to consumer/patient neural information. Although these devices are designed to help mitigate patients' diseases, adversaries can potentially exploit the IoTHDs to extract information from our brains. Several researchers have pointed out that this could be a new ethical threat to humans in the coming decades [105,106].

3.2.2. Network-Layer Vulnerabilities

Data integrity is a key security criterion for securing data generated and transmitted by IoTHDs. However, the data integrity of the remotely collected data in communication is not always easy. Vulnerabilities in communication are likely to persist. For accessibility, any data generated by IoTHDs are usually always available. While adversaries may block transmission channels by using jamming or flooding attacks, medical devices should be able to provide ceaseless data monitoring [107,108]. The lack of accessibility may also cause data integrity, which can be used for altering data stored on IoTHDs [78,106]. Automation has boosted medical device manufacturing, providing many advantages in improving productivity while reducing unnecessary costs [109,110]. However, in medical device manufacturing, every component created with network capability or means of amplifying, dampening, or re-routing network communications creates new avenues of attacks [111]. For example, ransomware can cause massive supply-chain disruptions [111].

3.2.3. Application-Layer Vulnerabilities

Many computer vision technologies have been proposed to alter images [1,112]. Thus, it threatens healthcare sectors that adversaries could apply techniques such as modification, swapping, and obscuring toward vulnerable medical images [113,114]. For example, injecting or removing medical evidence to and from those medical images can cause a major misdiagnosis [115,116]. Medical images with insufficient security guidelines updates can also often suffer from various malicious manipulation attacks [33]. Additionally, adversaries and researchers have proposed more complicated attacking models and defense requirements as deep learning techniques evolve. For example, CT-GANs (Computed Tomography—Generative Adversarial Networks) [117] train GANs to generate fake CT images by having AI learn real medical images [117].

At the application layer, web services have become a popular means of interfacing with existing (and somewhat legacy) systems. However, when it comes to ensuring greater interoperability, some implementations can be insecure due to weak authentication and the absence of encryption. As a result, there is a risk of information being tampered with during transmission. Given the growing importance of IoTHDs, preserving data integrity is of utmost importance [100]. The human factor is also a component of the application layer. A lack of awareness of cybersecurity issues, poor security practices, and the consistent education and training of healthcare personnel, patients, and end-users of IoTHDs on cybersecurity risks and their impact contributes to the persistent cybersecurity vulnerabilities [100]. Some examples of these insecure practices include the insecure disposal of devices containing sensitive information or data, sharing passwords, and distributing passwords for device access, especially in cases where password protection is required [100].

3.3. Relevant Threat Agents

A threat agent can be a person, group, or organization that intends to exploit a vulnerability to cause harm to a system intentionally. A threat agent is characterized by motivation, available resources, and expertise to use an attack method sufficient to trigger a threat. The threat agent is, thus, the source of risk. This section highlights relevant threat agents with the motivation and expertise to attack IoTHDs.

3.3.1. Nation and State Actors

Nation and state actors are parties that operate on behalf of governments—with or without that government's public support. These tend to be well-funded entities collaborating with other allied countries and often work with "private enterprise" or criminal associations [118–120]. However, governments can fund operations that are often seen as independent. They have been known to be the main parties perpetrating cyber warfare largely through APTs contributing sustained operations [13,121]. For example, various APTs have been noted for interfering in politics, assisting in IP theft, participating in extortion attempts, or shoring up military imbalances in capacity between nations. A yet unknown source has been behind the "Tardigrade" APT targeting biomanufacturing facilities [122]. So far, Tardigrade has been suspected of gathering intelligence on vaccine production data [88] to disrupt it. Even more unusual is the metamorphic ability of Tardigrade to learn the systems it is in, change its signatures when detected, and then act anew. Thus, meaningful concerns can be had about new Tardigrade-like and Tardigrade derivatives in development or deployed elsewhere, perhaps even other industries. Limited actions can be performed while Tardigrade is under examination, but key insights can be gleaned:

- State actors continue to have the means to produce sophisticated works.
- APTs produced are likely to prioritize and maintain autonomy, allowing damages delivered to be sustained. Interference can be run through these to disrupt the operations of critical healthcare [122].
- If APTs can securely deliver hostile software into organizations with enough IoTHDs, and those devices are distributed widely enough and sufficiently evade patching, they can be a significant means of surveillance.
- The most relevant APTs toward IoTHDs appear to be those that would target both IP and operations of such IP. Such could deliver strategic technological gains to nation-states while offering positioning to control companies of rival nation-states and or their alliances.
- IoTHD developers should assume they are already targets and sharpen the protection of their most critical assets, including tighter protocols, vetting, and minimization of interactions with core IP assets. Further, as per BIO-ISAC's reported recommendation for bio manufacturers, all IoTHD developers should similarly consider reviewing the degree of backups, networking segmentation, and product lead times [88].

- Owing to automation in APTs and other means of automated attacks, we may see increased automation in defense.

3.3.2. Healthcare Facilities and Related Personnel

Conversations about healthcare facilities and personnel commonly include physicians, nurses, students, receptionists, phlebotomists, technicians, surgeons, scribes, emergency response doctors, janitors, security workers, and administrators. These are first-degree personnel. The many contract workers who may be involved with security, the transportation of materials, information technology staff, and guest scientists or collaborators are important to include, which can make up the second degree. One more degree can be removed for those who work with or associate with workers at the second degree or are unpaid, such as students, volunteers, patient visitors, and police officers, in limited cases of needed operation, participation, and agency. From the first to the third degree, there is a gradient of access to IoTHDs, from higher to lower. Still, all must be considered to a degree depending on the tasks at hand and the value of the IoTHD assets, for they can all provide an input that can determine a valuable output. Each of these degrees of separation entails different trees of attacks on healthcare assets. Healthcare personnel need to consider how the IoT either shortens the degree of separation or removes barriers entirely.

3.3.3. Independent and Unorthodox Communities

Unorthodox communities include many diverse actors of different funding groups and sizes. Independent actors can include from hobbyists and lone actors to organized groups either looking to exploit for intrigue, the repurposing of devices, or exploitation or harm. From the ethical hacker end of the spectrum, spaces such as those within Community Bio and Makerspaces and groups such as “I Am The Calvary” and the “Grinder [Implant] Community” would be those among whom IoHTDs may find beneficent uses. These individuals improve technology through identifying vulnerabilities and alerting manufacturers, addressing the vulnerabilities directly, positively advertising the proper use of the devices, or repurposing the devices within accepted frameworks. Toward the other end, lone exhibitors, criminals, and criminal groups can be expected to pose considerable, irregular threats to IoTHD users.

3.4. IoTHD Security Threats

Medical devices, specifically when they are connected to networks, are just as vulnerable as any other networked security systems and are subject to security breaches because they are all interconnected. IoT devices have increasingly become prevalent in healthcare and have improved patient care, remote monitoring, and medical research. However, these devices pose security threats that malicious actors (see Section 3.3) can exploit. Security threats to IoT devices in healthcare can occur at different layers, including the perception, network, and application layers.

We aggregate the results of the security threats to IoTHDs [123–126] following the STRIDE method [24,96] in Table 2.

Table 2. IoTHD security threats [24,123–126].

| System Asset | Security Threats | | | | | |
|---|---|--|---------------|---------------|---|--|
| | S | T | R | I | D | E |
| Perception Layer: Sensing, Positioning, and Vision Technologies | Sensor spoofing, Sybil, node impersonation, sending deceptive messages, cloning, weak authentication scheme | Forgery, data/image manipulation, replay, falsification of device readings, data injection, device tampering | Bogus message | Eavesdropping | Message saturation, jamming, DoS, battery depletion | Backdoor, weak authentication scheme, malware, remote update of device control unit, hardware trojan, compromised node, password intrusion, physical theft |

Table 2. Cont.

| System Asset | Security Threats | | | | | |
|---|---|--|---|--|---|---|
| | S | T | R | I | D | E |
| Network Layer: Device-to-Device, Device-to-Infrastructure | Routing attacks, In-replay attack, masquerading, fingerprinting, impersonation attack, eavesdropping, position faking | Firmware modification, injection (RF packet), manipulation/alteration/fabrication of event trace tampering, malicious update (software/firmware) | Bogus messages, (message modification, code, manipulation, loss of event trace ability) | Eavesdropping, man-in-the-middle, location tracking, sniffing, message interception, information disclosure, traffic analysis, Grayhole, Sink-side-channel, ARP Tab. Poisoning | DoS/DDoS, battery depletion, flooding, message suppression, Blackhole, Wormhole, MIMO attacks | Malware, Brute Force, gaining control, social engineering, logical attacks, unauthorized access, session hijack |
| Application Layer: Human, Computing, Data Storage | Spoofing, impersonation, weak authentication scheme | Firmware/software modification, malicious update, SQL injection | Audit log tampering, forgery | Eavesdropping, location tracking, privacy leakage, SQL injection, data breach, message disclosure | DoS, DDoS, buffer overflows | Outdated OSs, social engineering/phishing, unauthorized access, malware, software hijacking, Dropbear SSH Server, IaaS cloud attack, password intrusion, ransomware |

3.5. IoTHD Countermeasures

As the medical world expands in networking and information technology, security threats in IoTHDs will continue to impact the future of clinical treatment and patient safety directly. Technical controls, governance, resilience measures, unified reporting, context expertise, regulation, and standards are general suggestions for the remediation of security risks due to IoTHD threats [100]. We discuss countermeasures to IoTHD security threats (see Section 3.4) at the perception, network, and application layers [124,126,127].

3.5.1. Perception/Device-Level Controls

In the era of Healthcare 4.0, all the sensing data from IoTHDs will be transmitted to remote servers and stored in cloud databases [128–130]. In addition, due to the nature of IoT devices, various sensing capabilities are used. Especially in implanted medical devices and sensors, if the data protocols or message formats vary, data protection against a wide range of malicious attacks can be more difficult [83]. Thus, more unified networks can be built with unified data encryption and transmission schemes to bring more protection capabilities against future adversaries [131]. Perception-layer components are prone to physical attacks, such as tampering or theft. Physical-layer security schemes [124,132] including RFID-based secure algorithms [101] have been suggested to protect against physical attacks (i.e., eavesdropping, sniffing, data breach, compromised node and device cloning attacks).

Researchers have also proposed secure data management protocols for medical identity protection [133,134] against medical identity theft that allow for privileged attacks. Mashima et al. [135] pioneered to secure medical systems against physical theft [135] that creates a trusted domain and an online monitoring system. However, medical identity threats cannot only be resolved by engineering efforts but also require holistic efforts. Halstead et al. [136] emphasized the importance of educating healthcare workers to become aware of these physical threats [136]. Medical professionals are not trained to deal with security threats, so device manufacturers should provide some security on their devices, release patches, and ensure secure products. While medical staff have little to do with the security of their devices, the owner of the healthcare facility can maintain (buy) strong device security and hire capable cybersecurity teams [137].

IoTHD perception-layer components become a more beneficial target as they collect patient medical data and control the device. Data hygiene entails the removal or limited persistence of data created on or entered into the device to reduce the impact of device data breaches and limit how much sensitive data can be transmitted to other IoT layers.

Developers must consider protocols that limit the data taken and the data deciphered to limit thefts, as the ability to decode human biosignatures improves [105]. Additionally, data authentication schemes (i.e., biometric-based, mutual authentication, etc.) are crucial to medical device security because these factors are related to the privacy of one's medical history and data [124]. Such schemes can help remediate impersonation, password intrusion, reply, weak authentication, and side-channel attacks.

3.5.2. Network/Communication-Level Controls

Vulnerabilities in IoTHD communication can be addressed through key management schemes (using symmetric or asymmetric approaches) to protect the information exchanges between IoTHD system components [124]. With key management, the messages to be transmitted are protected with a key, which allows the packets to be encrypted. However, with the traditional approaches, there is a possibility of high power consumption and complexity [138]. There is also a need to adapt to newer technologies such as 5G technology and the emergence of more complex smart applications [124]. Proxy-based mechanisms can introduce additional security by adding an entity, layer, or process to secure the data generated in medical devices and transmitted between medical devices and the healthcare platform at the application layer. Wu et al. [139] created a proxy-based approach with ciphertext-policy attribute-based encryption (CP-ABE) to protect the communications and provide fine-grained access control in devices and WBANs. Similarly, Marwan et al. [140] proposed the CloudSec framework for data sharing and processing with two cryptosystems (AES and Paillier cryptosystems) for data encryption and key management.

Secure routing mechanisms such as SDN technology [141] protect IoTHDs from attacks such as Wormhole, routing attacks, DoS, battery depletion, flooding, Grayhole, etc., that take advantage of the high power consumption or low processing capabilities of the transmission mechanisms. Thus, deploying secure gathering and routing strategies to incur the least communication overheads and transmission costs mitigate these attacks [141,142]. Intrusion detection techniques are also beneficial for discovering attacks or malicious actions in the network or system [124].

Lastly, as with limiting the data collected through data hygiene methods, limiting the data transmitted from IoTHDs remains important. Despite implicit agreements upon the IoTHDs' vulnerabilities in communication, several studies [143,144] have reviewed the literature on how to build reliable data communication protocols or systems.

3.5.3. Application-Level Controls

Security at this layer is critical because it manages the exchange of sensitive data between the device and the user or external systems. Developers of IoT health applications should follow secure coding practices, such as input validation, output encoding, and data sanitization, to prevent common application-layer attacks, such as SQL injection and buffer overflows. While key management schemes protect data in transit between the IoT device and the user's mobile device or external systems [100,124], sensitive data should be encrypted at rest in the user's mobile device or external systems. Strong encryption algorithms such as AES symmetric key based-schemes and RSA should be used [124]. IoT health devices must also ensure data integrity of the data transmitted and received, as incorrect data can lead to life-threatening situations. Mechanisms such as check-sums, digital signatures, and hash functions can be used to ensure that data have not been tampered with. Access control mechanisms can also be implemented to limit authorized users' access to sensitive data and device functionality. Authentication mechanisms such as username/password, biometrics, or smart cards can be used to authenticate users.

Secure data aggregation techniques protect the patient's sensitive information aggregated from distributed medical devices (medical sensors) by applying an aggregation technique to secure and privatize the information. Tang et al. [145] applied different characteristics to implement secure data aggregation techniques, such as differential privacy preservation, obliviousness security, patient fair incentives, and data aggregation source

identification. Chen et al. [146] proposed the federated learning paradigm using trained models to implement secure data aggregation.

4. Practical Examples Inspired by Real-World Concerns

We have followed a high-level layered architecture perspective to IoT systems, allowing for a more in-depth asset-oriented security risk analysis of IoTHDs within their perception, network, and application layers. We applied a suitable security risk management method—the ISSRM method—and its domain model [89] to guide our analysis. Our analysis in Section 3 shows that a multi-layer security risk management analysis benefits securing IoT health devices. By identifying and mitigating potential risks at each layer, IoT health devices can be made more secure, protecting user privacy and safety. In this section, we summarize this analysis at each layer.

4.1. Risk 1: Medical Image Modification

Medical imaging systems can comprise sensor equipment to collect CT and MRI images in various formats and store, transmit, or share them using the picture archiving and communication system (PACS). PACS is networked medical imaging technology that facilitates the storage, retrieval, and sharing of medical images.

4.1.1. Perception-Layer Risk Analysis

In the case of medical imaging using PACS, the perception layer includes devices used to capture and configure the CT and MRI imagery, as well as the software used. These include the CT scanners, MRI, DR device, ultrasound to capture medical imagery, and the modality workstation configuring and sending all the imagery in the DICOM format to the PACS server [117]. Vulnerabilities in the perception layer may arise from inadequate security measures, such as weak passwords, unpatched software, or default settings that have not been changed, which can increase the risk of unauthorized access to these assets. The attacker with physical access to the perception-layer assets, i.e., the modality workstation, can plant the malware by accessing the unlocked workstation. To secure against this threat, anti-virus software can be used on modality workstations and should be kept up to date [117]. Additionally, digital signatures [147] and digital watermarking [148] with each scan and machine learning techniques [149] can be used to detect tampered images and, thus, prevent their use for medical diagnosis.

4.1.2. Network-Layer Risk Analysis

The network layer in this scenario refers to the PACS network infrastructure used to transmit and store the medical images, typically in the DICOM format. The network layer comprises internal networks, WiFi access points connected to the internal network, and an internet connection. PACS which are not directly connected to the internet can be indirectly connected via the facility's internal network [150] and are thus vulnerable to attacks. PACS servers exposed to the internet pose a high risk of security threats that could compromise the confidentiality, integrity, and availability of the medical images stored on the server. Threats in this layer could include social engineering attacks, physical access, network intrusions, denial-of-service attacks, and other types of attacks that target the network infrastructure [151]. The risk of these threats increases when the medical images are transmitted over unsecured networks or stored in an unencrypted form. For example, an attacker can access the internal network by hacking WiFi access points with critical vulnerabilities, such as "Krack" [152] and "BleedingBit" [153], where Bluetooth and WiFi electronics are integrated into a single chip. To address such threats, healthcare facilities should enable encryption between the hosts in their PACS network using proper SSL certificates [117] and remain up to date with patches to vulnerable network software.

4.1.3. Application-Layer Risk Analysis

In the application layer, the risk of unauthorized access to the medical images stored on the PACS server can lead to malicious image modification. Although most healthcare facilities use local servers, a few have transitioned to cloud storage [154], increasing the potential attack surface. When a PACS server is exposed to the internet, there is a risk of various security threats that could compromise the confidentiality, integrity, and availability of the medical images stored on the server. Thus, a threat agent with motivation, expertise, and resources to gain unauthorized access to the PACS server can use the CT-GAN technique on medical imaging systems, posing a high risk of malicious image modification, leading to the loss of integrity of MRI/CT images, misdiagnosis of a severe disease, delayed treatment for the affected patients, and a loss of trust in the medical system. Vulnerabilities in medical imaging systems, such as inadequate encryption and security measures, increase the likelihood and severity of this risk.

Mirsky et al. [117] also demonstrated how an attacker could compromise medical images on PACS servers by designing two conditional GAN models. One injects medical evidence into healthy images, while the other removes medical evidence from images with detectable tumors [117]. This approach is critical because it can cause a misdiagnosis of severe diseases. Pathologies requiring high-resolution scanning would become a higher risk of CT-GAN-related attacks [117]. To mitigate this risk, organizations should implement adequate security controls, such as encryption (of data in motion (DiM) and data at rest (DaR)) and access controls, and limit the exposure the PACS server has to the internet [117]. Additionally, organizations should reduce the sensitive data collected (e.g., pathologies that do not need a CT scan should be discouraged), prioritize pathologies that require high-resolution scanning for further security measures, and consider alternatives to CT scanning for pathologies that do not require it. Finally, organizations should use risk management methodologies, such as the STRIDE method, to identify and address specific threats posed by the CT-GAN technique.

4.1.4. Summary

Malicious image modification by malicious actors can have severe consequences for the affected patients and the medical system. Attacker motivations comprise ideological, political, money, fame, and revenge motivations; attacker goals vary according to motivations, including to affect elections (political), hold data hostage (money), insurance fraud (money), terrorism (revenge), etc.; and the impact includes physical (injury and death), mental (trauma and life course), and monetary (loss and payouts). These point to nation/state actors and unorthodox communities, although independent actors (i.e., hobbyists and ethical hackers) may seek to explore such evolving uses of CT-GANs [117]. Therefore, it is essential to implement appropriate security measures, such as strong authentication and access control, data encryption, and regular security assessments, to mitigate the risks at each IoT layer. We illustrate a scenario of malicious image manipulation in Table 3.

4.2. Risk 2: Malicious Synthesis and Camouflage of Genetic Sequences

DNA synthesis has become more common [155]. It now is a non-trivial threat [156] where genetic sequences being synthesized and analyzed for various purposes, such as medical research, drug development, and forensic analysis, can be leaked to unauthorized parties or corrupted.

4.2.1. Perception-Layer Risk Analysis

The perception-layer security risk analysis of the DNA synthesis IoT health device system involves identifying risks associated with the user's interaction with the system. In this case, the risk involves the attack on the synthesizer through sound waves produced during the operation of the synthesizer. The acoustic side-channel attack is a type of "sonic malware" or "bioacoustic hacking" that can infer information about the synthesizer's operation and the synthesized DNA sequence [157,158]. This attack requires close physi-

cal proximity to the DNA synthesizer, which means that healthcare or related personnel could be likely threat agents. Alternatively, an attacker can breach systems in proximity to the DNA synthesizer (e.g., remote monitoring systems, employee phone/laptop, etc.) and record the information leaked in the acoustic side-channel of the DNA synthesizer through an existing microphone(s) of those systems [157]. To mitigate acoustic side-channel risks, Faezi et al. [157] suggested using physically identical components placed in a geometrically uniform manner to remove any variations in acoustic emissions. Additionally, preventing unauthorized personnel from accessing any room containing a DNA synthesizer helps to maintain confidentiality of the synthesized DNA sequences. Any unapproved devices discovered in the same room as a DNA synthesizer should be reported as a security threat [157].

4.2.2. Network-Layer Risk Analysis

DNA synthesizers can connect to computers, external drives, and Ethernet cables. However, operators generally keep the machine disconnected from the internet and local networks or use secured protocols to eliminate the possibility of cyberattacks [157]. Although the possibility of network-layer attacks is limited, security risks target the communication between the DNA synthesizer and any integrated external system posing a significant risk to the confidentiality of the synthesized DNA sequences. Appropriate security measures, such as encryption, access controls, and monitoring for suspicious activity in any room containing a DNA synthesizer, can mitigate network-layer risks [157].

4.2.3. Application-Layer Risk Analysis

The application-layer security risk analysis of the DNA synthesis IoT health device system involves risk impacts stemming from perception-layer threats. When genetic sequences are manipulated, these corrupted sequences will be used in various medical applications, posing significant risks to genetic research and development [157]. Routine risk assessments can help identify corrupted sequences and prevent malicious actors from exploiting them.

4.2.4. Summary

DNA synthesis in medical research, drug development, and forensic analysis poses a significant security risk to genetic research and development integrity. The risk of malicious DNA synthesis and camouflage, particularly through acoustic side-channel attacks, can compromise genetic data and misdiagnose severe diseases. Faezi et al. [157] discuss attacker intent, such as industrial espionage and bioterrorism; however, because most attacks require close physical proximity to the DNA synthesizer, the healthcare or related personnel are the likely threat agent (although they can be recruited by a nation/state actor or an unorthodox group). To mitigate these risks, appropriate security measures must be implemented at the perception, network, and application layers, including removing variations in acoustic emissions, encryption, access controls, and monitoring for suspicious activity. We illustrate a scenario of a genetic sequences attack in Table 3.

4.3. Risk 3: Transport of Critical Materials and Unintentional Advertising

IoT health devices often use expensive and potentially dangerous materials such as radioactive isotopes to function properly, such as in medical devices used in radiation therapy or medical imaging. These devices may have communication protocols that could be vulnerable to malicious attacks or unintentional exposure, leading to serious health risks for the public. For example, in the Goiânia accident, numerous people were exposed to radioactive material stolen from a hospital, and this could easily happen again [159]. Therefore, assessing the security risks at the perception, network, and application layers of these IoT health systems and implementing appropriate security measures to protect against such risks is important. We illustrate a scenario of attacks exploiting the unintentional advertising of critical materials in Table 3.

4.3.1. Perception-Layer Risk Analysis

This IoT health device system's perception layer involves medical materials containing high-activity radioactive materials. The lack of comprehensive security protocols to protect them can result in unintentional advertising, making them a target for theft. The theft of these materials can pose severe health risks to the public and lead to legal consequences, damaging the reputation of medical device manufacturers [160]. Therefore, marking these materials discreetly among professionals is crucial to avoid unnecessary exposure to unprepared populations and to implement appropriate security measures to protect against malicious attacks [161]. For instance, the International Atomic Energy Agency (IAEA) has established guidelines for the security of radioactive sources, including physical protection, control and accounting requirements, and detection and response to unauthorized access [162].

4.3.2. Network-Layer Risk Analysis

The network layer of this IoT health device system involves assessing vulnerabilities in the communication protocols of IoTHDs. Network-layer security risks may involve the possibility of a malicious actor gaining access to IoTHD communication protocols and using them to identify and target medical materials containing radioactive isotopes. This could involve network scanning or malware to gain unauthorized access to the device or network.

Implementing appropriate security measures to protect against such attacks, such as encryption and access controls, and conducting routine vulnerability testing is necessary. Novel engineering efforts are also required to develop more specified security protocols to protect against theft and the unintentional exposure of these materials and revised education and law enforcement for medical professionals and peripheral agencies [163,164].

4.3.3. Application-Layer Risk Analysis

Application-layer security risks could include a malicious actor exploiting vulnerabilities in the software or firmware of medical devices to gain unauthorized access to sensitive information or materials. This could include tactics such as exploiting software vulnerabilities or using malware to gain access to device settings or data. Implementing appropriate security measures, such as revising education and law enforcement for medical professionals and peripheral agencies to ensure the safe handling and disposal of radioactive materials, can significantly reduce the risk of malicious attacks and unintentional exposure.

4.3.4. Summary

Overall, the security risks associated with medical devices that use expensive and potentially dangerous materials require careful consideration and appropriate measures to ensure the safety of the public and the reputation of medical device manufacturers. Healthcare facilities housing high-risk radioactive materials and devices become easy targets for theft or sabotage. Attackers can be highly motivated and well-resourced unorthodox communities or state-sponsored threat actors with specific agendas, such as economic or political gain, terrorism, or activism. This could include insiders with privileged access to the medical device manufacturer's systems or facilities. Due to the high value of the medical materials involved, the attackers may be highly skilled and sophisticated and able to leverage a variety of attack vectors and techniques to achieve their objectives [165]. Thus, medical device manufacturers must keep abreast of potential malicious actors and implement appropriate security measures to protect against malicious attacks and unintentional exposure. This may require novel engineering efforts such as blockchain technology to enhance security and traceability in managing radioactive sources in medical facilities [164], and revised education and law enforcement for medical professionals and peripheral agencies [163].

Table 3. Practical Security Risk Examples Inspired by Real-World Concerns.

| Risk Scenario | Image Modification Using CT-GAN [117] | Genetic Attack [157] | Sequences | Unintentional Advertising of Critical Materials [160] |
|-------------------|---|--|-------------|--|
| Business Asset | Medical diagnoses, MRI/CT images | Patient sequences | genetic se- | Critical material advertisement |
| Security Criteria | Integrity of medical diagnoses and MRI/CT images | Integrity of sequences | genetic se- | Confidentiality of presence of radioactive isotopes communication protocols |
| System Asset | PACS medical imaging servers | DNA synthesizers | | Medical devices using radioactive isotopes, medical materials, communication protocol |
| Vulnerability | PACS server accidentally exposed to the internet via web access solutions | Sound waves produced during the operation of the synthesizer can infer operational information | | Improper development and application of communication protocols unintentionally advertise the availability of radioactive materials, making them a potential target for theft |
| Threat Agent | Attacker with knowledge of using the CT-GAN technique with interest in manipulating a patient’s MRI/CT images | Attackers with the capability and opportunity to record acoustic signals produced by the synthesizer and interest in manipulating genetic sequences for financial gain | | Attacker seeking to steal radioactive materials for malicious purposes |
| Threat | An attacker gains unauthorized access to the PACS server and manipulates a patient’s MRI/CT image using the CT-GAN technique to cause a wrong diagnosis | Attacker records the acoustic signals produced by the synthesizer’s pumps to infer information about the synthesizer’s operation, including the synthesized DNA sequence | | Attacker seeking to exploit the vulnerabilities to gain access to valuable materials through theft could lead to exposure and harm to unprepared and unshielded populations |
| Impact | Loss of integrity of MRI/CT images, misdiagnosis of a severe disease, delayed treatment, loss of trust in the medical system | Loss of integrity of genetic information, medical research disruption, and intellectual property theft | | Leak of the presence of radioactive isotopes, severe health risks for the public, damage to the reputation of medical device manufacturers, legal consequences |
| Risk Treatment | (i) Encryption and secure storage of MRI/CT PACS servers and medical images (ii) Reduce sensitive data collection (iii) Authentication and authorization controls on PACS servers | (i) Encryption, access controls, monitoring for suspicious activity (ii) Routine risk assessments and vulnerability testing | | (i) Specified security protocols to protect against theft (ii) Improved logistical efforts to ensure proper handling and disposal of the materials (iii) Revised education for law enforcement and peripheral agencies |

4.4. Lessons Learned

A multi-layer approach to security risk management is essential for IoT health device systems because it helps identify potential risks and threats across different system layers. IoT health devices involve interconnected components that operate at different levels, including perception, network, and application layers. Each of these layers has

unique vulnerabilities and threats requiring different security measures. At the perception layer, the physical sensors and actuators that gather and control data are vulnerable to tampering, eavesdropping, and spoofing attacks. Network-layer vulnerabilities can result from unsecured wireless communications, weak authentication, and unencrypted data transmission. The application-layer vulnerabilities arise from the software and applications used to process and store data, including outdated software, unpatched vulnerabilities, and weak password policies.

IoT health device manufacturers and healthcare organizations can identify and assess these vulnerabilities and threats across different system layers by taking a multi-layer approach to security risk management. This approach enables relevant stakeholders to implement appropriate security measures that address the specific risks at each layer. It also helps to ensure that security controls are integrated across all layers to provide end-to-end security. Furthermore, as we have seen from the scenarios discussed, a multi-layer approach can help identify risks across different layers. For instance, in the DNA synthesizers scenario, attacks may require physical proximity to the device (at the perception layer) and the ability to analyze acoustic signals (at the application layer). This highlights the importance of considering security risks spanning different IoT system layers and implementing security measures that address these risks.

5. The Future of IoTHD Security

Many new medical technologies are increasingly accepted and trusted by medical professionals [166–168]. Specifically, we will briefly address several innovations of the 4th industrial revolution, including artificial intelligence [169], blockchain [170,171], genetic engineering, quantum computing, and intersectional/combinatorial use. Innovations with these technologies can be expected to set the stage for novel exploits leading into the middle and latter parts of the 21st century.

5.1. Administrative (Laws and Policy Changes)

As discussed above, modern medical devices vary in many aspects, such as software, operating systems, and communication protocols. More administrative efforts are needed to achieve cybersecurity in various medical devices, especially at the law and policy levels.

First, governmental health agencies must specifically define their roles in cybersecurity administration toward devices [86]. Formulating a policy/framework and having vendors follow the guidelines is required. That said, a single reliable network that supports heterogeneous medical devices can be newly defined, and vendors could promptly integrate existing/new medical devices into the secure network. Depending on laws and policy, governments may decide whether they utilize existing networks or redesign a network for future IoTHDs [77]. For example, current MRI/CT images are connected to centralized pictures archiving and communication system (PACS) networks. Building a new framework should consider those existing networks [172]. In the new form of medical network frameworks, migrating legacy devices effectively is necessary. These gateway designs can include but are not limited to data transformation, network protocol design, and encryption/decryption schemes. Some medical devices do not have network capabilities; thus, a form of data transformation and secure uploading scheme will be needed. Otherwise, adversaries could conduct physical data theft attacks or man-in-the-middle attacks.

Vendors are expected to abide by laws/policy changes at any level of cybersecurity. This can be developing security programs or adding two-factor authentication. Both administrations and vendors should collaboratively inspect the quality of security fulfillment. During the inspection periods, the government may define standardized action items as validated and deliverable tests. It is recommended that government health agencies define fine-grained requirements with expected outcomes, eventually decreasing overall timelines. Vendors can then provide corresponding item results in their lab settings. That way, health agencies can assess the risk management abilities of the manufacturers. This process should be performed seamlessly; existing users would not face denial-of-service

experiences. Overall, being aware of cybersecurity for medical devices in laws and policies is important. When building a future framework/network, governmental and industrial efforts can expedite smoother transitions [173].

5.2. *Defending Forward*

A small but significant amount of the literature on the intersections of biosecurity and cybersecurity discusses the national security implications at risk. George (2020) speaks about this at length with the health of citizens and the status of bioeconomies [174]. Palmer and Karahan [13] discuss how intersectional research is important to consider in light of cybersecurity defense initiatives under the term “Defend Forward”, given how integral health infrastructure is. The careless integration of IoTHDs can threaten military operations if they can be widely and acutely exploited. It, therefore, appears sensible that further scrutiny be given to IoTHDs as they are considered for purchase and use in proximity to military and policing forces, regardless of the country. Further, such scrutiny is reasonable to be heightened as 4IR technologies, especially that of artificial intelligence, are employed [175]. Several AI-based studies [76,81,82,176,177] discuss this at length wherein AI can meaningfully present further hurdles if misused or taken advantage of. Future considerations toward defend forward applications should be mindful of health infrastructure that is accessible at these intersections.

5.3. *AI Innovations and New Directions*

According to Kruk et al. [178], about 3.6 million people die annually due to poor quality healthcare [178]. There is also an employment gap of 5.9 million nurses globally [179]. This is alarming and has triggered a lot of technological innovations within the space of artificial intelligence (AI), machine learning, and the Internet of Things (IoT) to solve these challenges. Machine learning techniques have proven to learn complex representations and patterns to automate some clinical responsibilities. Internet of Things devices, on the other hand, have provided the capabilities to collect high-throughput heterogeneous rich data from patients and individuals for training and improving AI algorithms. Healthcare workers and patients expect AI to play an important role in diagnosis and treatment more effectively and accurately than the current methods [180–183]. For example, as AI in computer vision improves image analysis, patients can obtain better image quality from medical devices with AI. Likewise, AI characteristics can improve the diagnosis and disease management process. This is not to say that the applications are not without hurdles, but there exists evidence for optimism over time as practitioners improve their integration of artificial intelligence-based modalities [184]. We can expect artificial intelligence to improve applications in resource-strapped areas.

AI and machine learning have permeated every aspect of healthcare delivery—identifying and discovering new therapeutics, diagnosing diseases and infections, or aiding in treatment decision making. Toward the discovery of novel therapeutics and drugs, AI has been used to speed up the virtual screening of compounds to narrow the search space for lead compounds or potentially viable drugs [185]. This decreases the cost and time it will take to bring new drugs to market by pharmaceutical companies. Within disease diagnosis, AI has been used to diagnose disease and medical abnormalities from data collected with IoT devices (such as wearable fitness devices), medical imaging devices, and blood chemistry analyzers [186]. In terms of administering treatments, ML algorithms have been used to inform how limited clinical resources should be allocated [187]. For example, machine learning algorithms have been used to prioritize patients to maximize how clinical resources are used to treat patients. Moreover, ML algorithms have aided in determining the optimal time for administering certain treatments. AI and ML have shown incredible performance in the past and have demonstrated a lot of potential for the future. Despite these, AI in healthcare poses major drawbacks that must be addressed as the field evolves. One of these drawbacks is the lack of ethnic diversity in some datasets used in training these AI systems [188]. An AI system is as good as the dataset it was built on. Thus, if certain groups of people are not represented in

these training datasets, AI systems built on these datasets will perform terribly when used on underrepresented groups. Notable authors who have discussed issues and potential pathways to solutions regarding representation in data and the algorithms handling them can be found among [189–195].

Moreover, many AI systems and IoT applications require good infrastructure, such as reliable internet and electricity. In resource-constrained environments where such amenities are a challenge, it will be almost impossible to deploy these technological innovations fully. Thus, more work is needed to investigate ways to deploy these technologies in resource-constrained settings. With access to medical data, generative AI can generate fake medical information, including MRI/CT images, for which new security means have been suggested [117,196,197]. Thus, data generated by IoTTHDs must be validated by experts or high-performing discriminator models. Building a good discriminator model for data protection can help healthcare sectors to protect from malicious data fabrication attacks. This approach is needed given the data generated. The same aspects can be applied to other types of medical data resources. To extrapolate, future cyberbiosecurity models may apply more complicated discriminative techniques to detect generic sequences of DNA synthesis or other important biological outputs or signatures. In terms of biomolecules, biosystems, biomachine interfaces, and biocomputing, there exist many new and dynamic targets [155,198]. A single organization or academic institute cannot make this approach. Thus, region-wide or nation-wide data collection and research collaborations are needed and can expedite more complicated AI solutions [199–203].

5.4. Innovations of Blockchain Technology

Blockchain technology refers to cryptography-linked records in chained blocks. It is an emerging technology that may prove essential in shoring-up privacy concerns and adding needed avenues of automation in record processing [204]. With an eye on privacy, several groups have put forth security solutions at this intersection. For example, Kumar and Chand [205] revealed a model for using blockchain with the IoT in medical privacy contexts; this builds on efforts of protocols which aimed to cover the privacy of PII on the blockchain. Those concerned with regulation would be pleased to note that conversation at the intersection of blockchain, regulation, and hospital device application is alive. Sneha et al. [206] introduced a model that “emphasizes distribution and encryption of data, smart contracts, and permissioned blockchain-based architecture” within the scope of the FDA review process. Alblooshi et al. [171] developed a protocol specifically for medical devices. All in all, blockchain efforts exist and are growing. Testing, time, and adoption will tell if the efforts take root. They present novel avenues for managing medical data. These reflect just some of the innovations taking place with blockchain technology.

5.5. Genetic Engineering

Genetic engineering is a 4IR technology that has been pacing rapidly [207–210]. It allows skilled technicians to change fundamental aspects of organism DNA and make profound biomaterials. Of the latter, DNA is being investigated as a programmable 4D scaffold that may improve wearable technology and offer further bio-digital functionality [211–213]; in fact, IoT functionality with DNA is already a matter of investigation. In the former case, genetic engineering has immediate healthcare implications as, for example, this can translate to effective gene therapies and allows for crafting tissue and organ grafts that have a much lower rejection from those these are implanted into. Sequencing, the decoding of one’s genome, is required for this. Thankfully, the cost to sequence genomes per base pair has fallen drastically, and the speed to do so on a population basis for analyzing a community is here. The advent of COVID-19 provided an important basis and means to implement effective genetic surveillance to study population susceptibility [214,215]. The means can be minimized significantly. For example, researchers demonstrated that Oxford Nanopore sequencing technology could be utilized via a gaming laptop, allowing for sequencing on the go [216].

From the individual to the corporate entity to the nation-state, there are many reasons to be interested in sequencing. The same goes for information about genetic editing. Cheap gene engineering kits and exploration stations, via companies such as The Odin or Amino Labs, can be obtained cheaply, allowing for the potential of biomedical exploration and prototyping by larger swaths of individuals [207,208]. IoTHDs that utilize either gene editing or sequencing may find themselves targets. Companies might consider adding these products to their labs and sandboxes to test intermediate attacks between connected systems. Reverse engineering and purchasing more advanced units, especially industrial and hospital-grade sequencing and diagnostic units, may heighten preparedness.

5.6. Quantum Computing

Quantum computing conducts complex computations by harnessing quantum states. Instead of calculations based on binary architecture, quantum computing can hold more information, significantly reducing computation times and energy usage. This concept of quantum bit computation could eventually lead to accurate diagnosis and precision medicine in healthcare [85]. Although the advanced processing ability of quantum computing may threaten legacy encryption schemes, it can also be used to reinforce the current encryption systems with quantum computing power. There is ample opportunity for business opportunities in exploring both sides of these uses.

5.7. Intersectional Fusions of 4th IR Technologies

One potential innovation to be mindful of is the intersection of multiple 4IR technologies in the future. An example can be found in a recent avant-garde project that fuses biotechnology and blockchain in a decentralized autonomous organization (or DAO for short) called BitMouseDAO, sought to encode cryptocurrency into a mouse [217]. This would involve genetically engineering the mouse's DNA to hold the key to access an amount of Bitcoin. Fifty (50) years ago, this idea would have been considered poor science fiction, but the means of technology exist. However, less than twenty (20) years ago, considerable amounts of digital data were converted into DNA reliably stored and played back in text or video format. In the last decade, a researcher and his team managed to encode malware in DNA and use it to perform a remote attack on a DNA sequencer, which spelled immediate implications for future healthcare operations [155]. The takeaway is the value of pondering what creative teams may produce in their goal to produce novel attacks on IoTHDs.

It is not out of the question that institutions may one day see novel attacks that act on the synchronized actions of patients who seek medical services that access their genetic information under the right combination of spiked and submitted samples. It is possible from here that complex bio-digital DDOS attacks can be made functional for more devastating malware, perhaps in the form of a condensed but dynamic machine learning algorithm that eventually winds its way through a facility. This scenario is wonderfully contrived for the time being. Thankfully, this is not a practical attack in the next few years, but with time, testing, and a large enough value target, it very well could be in ten (10) years by an enterprising group. Underestimation is an ever-present vulnerability that must be frequently assessed.

6. Concluding Remarks

The world of medical devices is diverse, and varieties that utilize internet connectivity add to this diversity and increase use. IoT health devices have become increasingly prevalent in the healthcare sector, offering a range of benefits, such as remote monitoring, real-time tracking, and improved patient outcomes. Thus, when rapid technological advancements outpaced the gradual advancement of healthcare cybersecurity, security concerns became difficult to manage. Each interconnected medical device has unique security risks, and there is not a one-size-fits-all approach to securing IoTHDs. In this paper, we have provided a survey and mapping of IoTHDs, regarding healthcare components and the communities that use them, a multi-layer security risk management analysis, and future

and evolving considerations. Each device presents risks that we have classified into the STRIDE threat categories, showing the need to consider the security risks of IoTTHDs in their environment and focus on security risk management. We introduced the multi-layer approach to conducting security risk management for these IoTTHD systems as it provides a comprehensive view of the system's security posture and enables the implementation of appropriate security measures that address vulnerabilities and threats at each layer while ensuring end-to-end security. We do not cover all of the forms of IoTTHDs but provide a useful introduction to thinking about the threat landscape of IoTTHDs, proposing that all adoption of IoTTHDs is done carefully and with the utmost consideration for security risk management.

Author Contributions: Conceptualization, A.-a.O.A., H.F., W.J., I.A.S., L.P., X.-L.P.; Methodology, A.-a.O.A., H.F., W.J., L.P., X.-L.P.; Formal analysis, A.-a.O.A., X.-L.P., L.P.; Investigation, A.-a.O.A., H.F., W.J., X.-L.P.; writing—original draft preparation, A.-a.O.A., H.F., W.J., L.P., X.-L.P.; Visualization, A.-a.O.A. and W.J.; Validation/Verification, A.-a.O.A., H.F., W.J., I.A.S., L.P., X.-L.P.; Supervision, A.-a.O.A., X.-L.P. and L.P.; Project administration, A.-a.O.A., X.-L.P.; Funding acquisition, X.-L.P.; Review and Editing, A.-a.O.A., H.F., W.J., I.A.S., L.P., X.-L.P. All authors have read and agreed to the published version of the manuscript.

Funding: Publication costs were funded by CYBER Solutions Academy. The work itself was a volunteer effort.

Data Availability Statement: This is a review paper and as such no data is available to review. All data used in this review was obtained through academic publications or through open-access sources.

Conflicts of Interest: This work was pursued without aim of commercial gain and its completion was pursued as a volunteer, educational pursuit drawing from the domain understandings of each author. The majority of this work was completed by the time most of the authors were still in school or having recently graduated. That said, Issah Abubakari Samori is employed as an Artificial Intelligence Engineer with MinoHealth AI Labs. Xavier-Lewis Palmer volunteers through educational initiatives separately held by CYBER Solutions Academy and MinoHealth AI Labs.

References

1. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the internet of medical things. *Health Policy Technol.* **2021**, *10*, 100549. [[CrossRef](#)]
2. Sadoughi, F.; Behmanesh, A.; Sayfour, N. Internet of things in medicine: A systematic mapping study. *J. Biomed. Inform.* **2020**, *103*, 103383. [[CrossRef](#)] [[PubMed](#)]
3. Annamalai, M.; Jesintha, D. Smart IoT system based patient monitoring and medicine reminder based on registry service selection scheme. *Eur. J. Mol. Clin. Med.* **2021**, *7*, 2710–2721.
4. Martin, R. The Internet of Things (IoT)—Removing the Human Element. *Infosec Writ.* **2015**, *28*, 12.
5. Richardson, L.C.; Lewis, S.M.; Burnette, R.N. Building capacity for cyberbiosecurity training. *Front. Bioeng. Biotechnol.* **2019**, *7*, 112. [[CrossRef](#)]
6. Greenbaum, D. Cyberbiosecurity: An Emerging Field that has Ethical Implications for Clinical Neuroscience. *Camb. Q. Healthc. Ethics* **2021**, *30*, 662–668. [[CrossRef](#)] [[PubMed](#)]
7. Adler, A.; Beal, J.; Lancaster, M.; Wyschogrod, D. Cyberbiosecurity and Public Health in the Age of COVID-19. In *Emerging Threats of Synthetic Biology and Biotechnology*; Springer: Dordrecht, The Netherlands, 2021; pp. 103–115.
8. Perakslis, C. Cyberbiosecurity, Ecopsychology, and Beyond: Our Formidable PIT Community [Last Word]. *IEEE Technol. Soc. Mag.* **2020**, *39*, 84. [[CrossRef](#)]
9. Potter, L.; Palmer, X.L. Human Factors in Biocybersecurity Wargames. In Proceedings of the Future of Information and Communication Conference, San Francisco, CA, USA, 29–30 April 2021; Springer: Berlin, Germany, 2021; pp. 666–673.
10. Hester, R.J. Bioveillance: A Techno-security Infrastructure to Preempt the Dangers of Informationalised Biology. *Sci. Cult.* **2020**, *29*, 153–176. [[CrossRef](#)]
11. Mazurczyk, W.; Drobnik, S.; Moore, S. Towards a systematic view on cybersecurity ecology. In *Combating Cybercrime and Cyberterrorism*; Springer: Berlin, Germany, 2016; pp. 17–37.
12. Potter, L.; Ayala, O.; Palmer, X.L. Biocybersecurity: A Converging Threat as an Auxiliary to War. In Proceedings of the ICCWS 2021 16th International Conference on Cyber Warfare and Security, Online, 25–26 February 2021; Academic Conferences Limited: Reading, UK, 2021; p. 291.
13. Palmer, X.; Potter, L.N.; Karahan, S. COVID-19 and biocybersecurity's increasing role on defending forward. *Int. J. Cyber Warf. Terror. (IJCWT)* **2021**, *11*, 15–29. [[CrossRef](#)]

14. Amiri, A.; Shekarchizadeh, M.; Esfahani, A.R.S.; Masoud, G.H. Bio-Cyber Threats and Crimes, the Challenges of the Fourth Industrial Revolution. *Bioethics* **2021**, *81*, 97.
15. Strielkina, A.; Illiashenko, O.; Zhydenko, M.; Uzun, D. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 24–27 May 2018; IEEE: New York, NY, USA, 2018; pp. 67–73.
16. Karthick, R.; Ramkumar, R.; Akram, M.; Kumar, M.V. Overcome the challenges in bio-medical instruments using IOT—A review. *Mater. Today Proc.* **2021**, *45*, 1614–1619. [[CrossRef](#)]
17. Gui, Y.; Siddiqui, A.S.; Tamore, S.M.; Saqib, F. Investigation of vulnerabilities on smart grid end devices. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS), Knoxville, TN, USA, 29 April–1 May 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.
18. Guttieres, D.; Stewart, S.; Wolfrum, J.; Springs, S.L. Cyberbiosecurity in advanced manufacturing models. *Front. Bioeng. Biotechnol.* **2019**, *7*, 210. [[CrossRef](#)] [[PubMed](#)]
19. Schabacker, D.S.; Levy, L.A.; Evans, N.J.; Fowler, J.M.; Dickey, E.A. Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Front. Bioeng. Biotechnol.* **2019**, *7*, 61. [[CrossRef](#)] [[PubMed](#)]
20. Norman, I.; Aikins, M.; Binka, F.; Nyarko, K. Hospital all-risk emergency preparedness in Ghana. *Ghana Med. J.* **2012**, *46*, 1–6.
21. Costa, L.; Barros, J.P.; Tavares, M. Vulnerabilities in IoT devices for smart home environment. In Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISPP, Prague, Czech Republic, 23–25 February 2019; SciTePress: Vienna, Austria, 2019; Volume 1, pp. 615–622.
22. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future internet: The internet of things architecture, possible applications and key challenges. In Proceedings of the 2012 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17–19 December 2012; IEEE: New York, NY, USA, 2012; pp. 257–260.
23. Kelly, J.T.; Campbell, K.L.; Gong, E.; Scuffham, P. The Internet of Things: Impact and implications for health care delivery. *J. Med. Internet Res.* **2020**, *22*, e20135. [[CrossRef](#)] [[PubMed](#)]
24. Affia, A.A.O.; Matulevičius, R.; Nolte, A. Security risk management in cooperative intelligent transportation systems: A systematic literature review. In *Proceedings of the OTM Confederated International Conferences on the Move to Meaningful Internet Systems*, Rhodes, Greece, 21–25 October 2019; Springer: Berlin, Germany, 2019; pp. 282–300.
25. Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035. [[CrossRef](#)]
26. Miller, D.D.; Brown, E.W. Artificial intelligence in medical practice: The question to the answer? *Am. J. Med.* **2018**, *131*, 129–133. [[CrossRef](#)]
27. Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A survey on internet of things and cloud computing for healthcare. *Electronics* **2019**, *8*, 768. [[CrossRef](#)]
28. US Food and Drug Administration. *Is the Product a Medical Device*; US Food and Drug Administration: Silver Spring, MD, USA, 2018; Volume 17.
29. Mahler, T.; Nissim, N.; Shalom, E.; Goldenberg, I.; Hassman, G.; Makori, A.; Kochav, I.; Elovici, Y.; Shahrar, Y. Know your enemy: Characteristics of cyber-attacks on medical imaging devices. *arXiv* **2018**, arXiv:1801.05583.
30. Jesudoss, A.; Daniel, M.J.; Richard, J.J. Intelligent medicine management system and surveillance in IoT environment. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Kazimierz Dolny, Poland, 21–23 November 2019; IOP Publishing: Bristol, UK, 2019; Volume 590, p. 012005.
31. Peccoud, J.; Gallegos, J.E.; Murch, R.; Buchholz, W.G.; Raman, S. Cyberbiosecurity: From naive trust to risk awareness. *Trends Biotechnol.* **2018**, *36*, 4–7. [[CrossRef](#)]
32. Larobina, M.; Murino, L. Medical image file formats. *J. Digit. Imaging* **2014**, *27*, 200–206. [[CrossRef](#)] [[PubMed](#)]
33. Eichelberg, M.; Kleber, K.; Kämmerer, M. Cybersecurity challenges for PACS and medical imaging. *Acad. Radiol.* **2020**, *27*, 1126–1139. [[CrossRef](#)] [[PubMed](#)]
34. Singh, A.K.; Anand, A.; Lv, Z.; Ko, H.; Mohan, A. A survey on healthcare data: A security perspective. *ACM Trans. Multim. Comput. Commun. Appl.* **2021**, *17*, 1–26. [[CrossRef](#)]
35. Zarour, M.; Alenezi, M.; Ansari, M.T.J.; Pandey, A.K.; Ahmad, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Ensuring data integrity of healthcare information in the era of digital health. *Healthc. Technol. Lett.* **2021**, *8*, 66–77. [[CrossRef](#)]
36. Wang, Z.; Li, Q.; Wang, Y.; Liu, B.; Zhang, J.; Liu, Q. Medical protocol security: DICOM vulnerability mining based on fuzzing technology. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2549–2551.
37. Erol, B.; Gurbuz, S.Z.; Amin, M.G. GAN-based synthetic radar micro-Doppler augmentations for improved human activity recognition. In Proceedings of the 2019 IEEE Radar Conference (RadarConf), Boston, MA, USA, 22–26 April 2019; IEEE: New York, NY, USA, 2019; pp. 1–5.
38. Shen, Z.; Li, W.; Han, H. Deep Learning-Based Wavelet Threshold Function Optimization on Noise Reduction in Ultrasound Images. *Sci. Program.* **2021**, *2021*, 3471327. [[CrossRef](#)]
39. Thiel, A. Biometric identification technologies and the Ghanaian ‘data revolution’. *J. Mod. Afr. Stud.* **2020**, *58*, 115–136. [[CrossRef](#)]
40. Bhelonde, A.; Didolkar, N.; Jangale, S.; Kulkarni, N.L. Flexible wound assessment system for diabetic patient using android smartphone. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015; IEEE: New York, NY, USA, 2015; pp. 466–469.

41. Połap, D.; Winnicka, A.; Serwata, K.; Keşik, K.; Woźniak, M. An intelligent system for monitoring skin diseases. *Sensors* **2018**, *18*, 2552. [CrossRef]
42. Shimizu, E.; Ogawa, Y.; Yazu, H.; Aketa, N.; Yang, F.; Yamane, M.; Sato, Y.; Kawakami, Y.; Tsubota, K. “Smart Eye Camera”: An innovative technique to evaluate tear film breakup time in a murine dry eye disease model. *PLoS ONE* **2019**, *14*, e0215130. [CrossRef]
43. Ernst, T.; Guillemaud, R.; Mailley, P.; Polizzi, J.; Koenig, A.; Boisseau, S.; Pauliac-Vaujour, E.; Plantier, C.; Delapierre, G.; Saoutieff, E.; et al. Sensors and related devices for IoT, medicine and smart-living. In Proceedings of the 2018 IEEE Symposium on VLSI Technology, Honolulu, HI, USA, 18–22 June 2018; IEEE: New York, NY, USA, 2018; pp. 35–36.
44. Hameed, S.S.; Hassan, W.H.; Latiff, L.A.; Ghabban, F. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Comput. Sci.* **2021**, *7*, e414. [CrossRef]
45. Debar, H.; Beuran, R.; Tan, Y. A Quantitative Study of Vulnerabilities in the Internet of Medical Things. In Proceedings of the ICISSP, Floriana, Malta, 25–27 February 2020; pp. 164–175.
46. Hudson, F.; Clark, C. Wearables and medical interoperability: The evolving frontier. *Computer* **2018**, *51*, 86–90. [CrossRef]
47. Valanarasu, M.R. Smart and secure IoT and AI integration framework for hospital environment. *J. ISMAC* **2019**, *1*, 172–179.
48. Majumder, S.; Chen, L.; Marinov, O.; Chen, C.H.; Mondal, T.; Deen, M.J. Noncontact wearable wireless ECG systems for long-term monitoring. *IEEE Rev. Biomed. Eng.* **2018**, *11*, 306–321. [CrossRef] [PubMed]
49. Sposaro, F.; Tyson, G. iFall: An Android application for fall monitoring and response. In Proceedings of the 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Minneapolis, MN, USA, 3–5 September 2009; IEEE: New York, NY, USA, 2009; pp. 6119–6122.
50. Kakria, P.; Tripathi, N.; Kitipawang, P. A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors. *Int. J. Telemed. Appl.* **2015**, *2015*, 8. [CrossRef] [PubMed]
51. Gruzelier, J.H. EEG-neurofeedback for optimising performance. I: A review of cognitive and affective outcome in healthy participants. *Neurosci. Biobehav. Rev.* **2014**, *44*, 124–141. [CrossRef] [PubMed]
52. Tedesco, S.; Sica, M.; Ancillao, A.; Timmons, S.; Barton, J.; O’Flynn, B. Accuracy of consumer-level and research-grade activity trackers in ambulatory settings in older adults. *PLoS ONE* **2019**, *14*, e0216891. [CrossRef] [PubMed]
53. Armstrong, W.; Michael, K. The Implications of Neuralink and Brain Machine Interface Technologies. In Proceedings of the 2020 IEEE International Symposium on Technology and Society (ISTAS), Tempe, AZ, USA, 12–15 November 2020; IEEE: New York, NY, USA, 2020; pp. 201–203.
54. Zhu, D.; Bieger, J.; Garcia Molina, G.; Aarts, R.M. A survey of stimulation methods used in SSVEP-based BCIs. *Comput. Intell. Neurosci.* **2010**, *2010*, 1–12. [CrossRef]
55. Liu, Q.; Chen, K.; Ai, Q.; Xie, S.Q. Recent development of signal processing algorithms for SSVEP-based brain computer interfaces. *J. Med. Biol. Eng.* **2014**, *34*, 299–309. [CrossRef]
56. Chevallier, S.; Kalunga, E.K.; Barthélemy, Q.; Monacelli, E. Review of Riemannian distances and divergences, applied to SSVEP-based BCI. *Neuroinformatics* **2021**, *19*, 93–106. [CrossRef]
57. Moutinho, S. Scientists Entered People’s Dreams and Got Them ‘Talking’. 2021. Available online: <https://www.science.org/content/article/scientists-entered-peoples-dreams-and-got-them-talking?> (accessed on 3 January 2023).
58. Leavitt, N. Researchers fight to keep implanted medical devices safe from hackers. *Computer* **2010**, *43*, 11–14. [CrossRef]
59. Rostami, M.; Juels, A.; Koushanfar, F. Heart-to-heart (H2H) authentication for implanted medical devices. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 1099–1112.
60. Tabasum, A.; Safi, Z.; AlKhater, W.; Shikfa, A. Cybersecurity issues in implanted medical devices. In Proceedings of the 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 25–26 August 2018; IEEE: New York, NY, USA, 2018; pp. 1–9.
61. Zanjali, S.V.; Talmale, G.R. Medicine reminder and monitoring system for secure health using IOT. *Procedia Comput. Sci.* **2016**, *78*, 471–476. [CrossRef]
62. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
63. Aman, A.H.M.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *J. Netw. Comput. Appl.* **2021**, *174*, 102886. [CrossRef] [PubMed]
64. Sangave, N.A.; Aungst, T.D.; Patel, D.K. Smart connected insulin pens, caps, and attachments: A review of the future of diabetes technology. *Diabetes Spectr.* **2019**, *32*, 378–384. [CrossRef] [PubMed]
65. Thamilarasu, G.; Odesile, A.; Hoang, A. An intrusion detection system for internet of medical things. *IEEE Access* **2020**, *8*, 181560–181576. [CrossRef]
66. Onik, M.F.A.; Anam, K.; Rashid, N. A secured cloud based health care data management system. *Int. J. Comput. Appl.* **2012**, *49*, 1–7.
67. Iliovski, A.; Dojchinovski, D.; Gusev, M. Interactive voice assisted home healthcare systems. In Proceedings of the 9th Balkan Conference on Informatics, Sofia, Bulgaria, 26–28 September 2019; pp. 1–5.
68. Tao, V.; Moy, K.; Amirfar, V.A. A little robot with big promise may be future of personalized health care. *Pharm. Today* **2016**, *22*, 38. [CrossRef]
69. Vanhove, M.P.; Rochette, A.J.; de Bisthoven, L.J. Joining science and policy in capacity development for monitoring progress towards the Aichi Biodiversity Targets in the global South. *Ecol. Indic.* **2017**, *73*, 694–697. [CrossRef]

70. Wall, P.; Saxena, D.; Brown, S. Artificial Intelligence in the Global South (AI4D): Potential and Risks. *arXiv* **2021**, arXiv:2108.10093.
71. Davies, M. Biometrics, surveillance technologies and the rise of the 'security state' in South Africa. *Africa LSE*. 2017. Available online: <https://blogs.lse.ac.uk/africaatlse/2017/03/22/biometrics-surveillance-technologies-and-the-rise-of-the-security-state-in-south-africa/> (accessed on 1 July 2022).
72. Gong, T.; Huang, H.; Li, P.; Zhang, K.; Jiang, H. A medical healthcare system for privacy protection based on IoT. In Proceedings of the 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, China, 12–14 December 2015; IEEE: New York, NY, USA, 2015; pp. 217–222.
73. Subramoniam, S.; Sadi, S. Healthcare 2.0. *IT Prof.* **2010**, *12*, 46–51. [[CrossRef](#)]
74. Drake, R.; Ridder, E. Healthcare Cybersecurity Vulnerabilities. In Proceedings of the International Conference on Cybersecurity and Cybercrime, Boston, MA, USA, 16–18 November 2022; Volume 9, pp. 49–56.
75. Alkinoon, M.; Choi, S.J.; Mohaisen, D. Measuring healthcare data breaches. In Proceedings of the Information Security Applications: 22nd International Conference, WISA 2021, Jeju Island, Republic of Korea, 11–13 August 2021; Revised Selected Papers 22; Springer: Berlin, Germany, 2021; pp. 265–277.
76. Wang, W.; Kiik, M.; Peek, N.; Curcin, V.; Marshall, I.J.; Rudd, A.G.; Wang, Y.; Douiri, A.; Wolfe, C.D.; Bray, B. A systematic review of machine learning models for predicting outcomes of stroke with structured data. *PLoS ONE* **2020**, *15*, e0234722.
77. Zuiderwijk, A.; Chen, Y.C.; Salem, F. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Gov. Inf. Q.* **2021**, *38*, 101577. [[CrossRef](#)]
78. Cuningkin, V.; Riley, E.; Rainey, L. Preventing Medjacking. *AJN Am. J. Nurs.* **2021**, *121*, 46–50. [[CrossRef](#)] [[PubMed](#)]
79. Food and Drug Administration. Draft Guidance for Industry and Food and Drug Administration Staff: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. 2014. Available online: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices> (accessed on 1 July 2022).
80. Food and Drug Administration. Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health. 2019. Available online: <https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health> (accessed on 1 July 2022).
81. Akogo, D.A.; Appiah, V.; Palmer, X.L. CellLineNet: End-to-end learning and transfer learning for multiclass epithelial breast cell line classification via a convolutional neural network. *arXiv* **2018**, arXiv:1808.06041.
82. van der Wal, D.; Jhun, I.; Laklout, I.; Nirschl, J.; Richer, L.; Rojansky, R.; Theparee, T.; Wheeler, J.; Sander, J.; Feng, F.; et al. Biological data annotation via a human-augmenting AI-based labeling system. *NPJ Digit. Med.* **2021**, *4*, 145. [[CrossRef](#)] [[PubMed](#)]
83. Zhang, H.T.; Park, T.J.; Islam, A.N.; Tran, D.S.; Manna, S.; Wang, Q.; Mondal, S.; Yu, H.; Banik, S.; Cheng, S.; et al. Reconfigurable perovskite nickelate electronics for artificial intelligence. *Science* **2022**, *375*, 533–539. [[CrossRef](#)]
84. Sibi Chakkaravarthy, S.; Sangeetha, D.; Venkata Rathnam, M.; Srinithi, K.; Vaidehi, V. Futuristic cyber-attacks. *Int. J. Knowl.-Based Intell. Eng. Syst.* **2018**, *22*, 195–204. [[CrossRef](#)]
85. Srinivas, M.; Durgaprasadarao, P.; Raj, V.N.P. Intelligent medicine box for medication management using IoT. In Proceedings of the 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; IEEE: New York, NY, USA, 2018; pp. 32–34.
86. Gehl Sampath, P. Governing artificial intelligence in an age of inequality. *Glob. Policy* **2021**, *12*, 21–31. [[CrossRef](#)]
87. Hooker, S. Moving beyond “algorithmic bias is a data problem”. *Patterns* **2021**, *2*, 100241. [[CrossRef](#)]
88. Web Titan. Tardigrade Malware Used in Targeted Attacks on Vaccine Manufacturers and Biomedical Firms. 2021. Available online: <https://www.webtitan.com/blog/tardigrade-malware-vaccine-manufacturers-biomedical-firms/> (accessed on 3 January 2023).
89. Dubois, É.; Heymans, P.; Mayer, N.; Matulevičius, R. A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering*; Springer: Berlin, Germany, 2010; pp. 289–306.
90. Affia, A.A.O.; Matulevičius, R. Securing an MQTT-based Traffic Light Perception System for Autonomous Driving. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; IEEE: New York, NY, USA, 2021; pp. 255–260.
91. Abasi-amefon, O.A.; Matulevičius, R.; Tönisson, R. Security Risk Estimation and Management in Autonomous Driving Vehicles. In Proceedings of the International Conference on Advanced Information Systems Engineering, Melbourne, VIC, Australia, 28 June–2 July 2021; Springer: Berlin, Germany, 2021; pp. 11–19.
92. NIST, N. Risk management guide for information technology systems. *NIST Spec. Publ.* **2002**, *800*, 800–830.
93. Caralli, R.A.; Stevens, J.F.; Young, L.R.; Wilson, W.R. *Introducing Octave Allegro: Improving the Information Security Risk Assessment Process*; Technical report; Carnegie-Mellon University, Software Engineering Institute: Pittsburgh, PA, USA, 2007.
94. Wynn, J.; Whitmore, J.; Upton, G.; Spriggs, L.; McKinnon, D.; McInnes, R.; Graubart, R.; Clausen, L. *Threat Assessment & Remediation Analysis (TARA): Methodology Description Version 1.0*; Technical report; The MITRE Corporation: Bedford, MA, USA, 2011.
95. Affia, A.A.O.; Nolte, A.; Matulevičius, R. IoT Security Risk Management: A Framework and Teaching Approach. *Informatics Educ.* **2023**, *22*. [[CrossRef](#)]
96. Affia, A.a.O.; Matulevičius, R.; Nolte, A. Security Risk Management in E-commerce Systems: A Threat-driven Approach. *Balt. J. Mod. Comput.* **2020**, *8*, 213–240.
97. Matulevičius, R. *Fundamentals of Secure System Modelling*; Springer: Berlin, Germany, 2017.
98. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.

99. Jabeen, T.; Ashraf, H.; Ullah, A. A survey on healthcare data security in wireless body area networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 9841–9854. [CrossRef] [PubMed]
100. Williams, P.A.; Woodward, A.J. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Med. Devices* **2015**, *8*, 305. [CrossRef] [PubMed]
101. Aghili, S.F.; Mala, H.; Kaliyar, P.; Conti, M. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. *Future Gener. Comput. Syst.* **2019**, *101*, 621–634. [CrossRef]
102. Cummins, G. Smart pills for gastrointestinal diagnostics and therapy. *Adv. Drug Deliv. Rev.* **2021**, *177*, 113931. [CrossRef]
103. Mancini, M. Medical identity theft in the emergency department: Awareness is crucial. *West. J. Emerg. Med.* **2014**, *15*, 899. [CrossRef]
104. Stine, I.; Rice, M.; Dunlap, S.; Pecarina, J. A cyber risk scoring system for medical devices. *Int. J. Crit. Infrastruct. Prot.* **2017**, *19*, 32–46. [CrossRef]
105. Lesaja, S.; Palmer, X.L. Brain-Computer Interfaces and the Dangers of Neurocapitalism. *arXiv* **2020**, arXiv:2009.07951.
106. Pycroft, L.; Boccard, S.G.; Owen, S.L.; Stein, J.F.; Fitzgerald, J.J.; Green, A.L.; Aziz, T.Z. Brainjacking: Implant security issues in invasive neuromodulation. *World Neurosurg.* **2016**, *92*, 454–462. [CrossRef]
107. Wood, D.; Apthorpe, N.; Feamster, N. Cleartext data transmissions in consumer iot medical devices. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas, TX, USA, 3 November 2017; pp. 7–12.
108. Kim, J. Energy-efficient dynamic packet downloading for medical IoT platforms. *IEEE Trans. Ind. Inform.* **2015**, *11*, 1653–1659. [CrossRef]
109. Chauhan, A. Robotics and automation: The rescuers of COVID era. In *Artificial Intelligence for COVID-19*; Springer: Berlin, Germany, 2021; pp. 119–151.
110. Lepasepp, T.K.; Hurst, W. A systematic literature review of industry 4.0 technologies within medical device manufacturing. *Future Internet* **2021**, *13*, 264. [CrossRef]
111. Richmond, S. Stopping The Attacks: Cybersecurity In Healthcare Manufacturing, 2021. Available online: <https://www.forbes.com/sites/forbestechcouncil/2021/08/17/stopping-the-attacks-cybersecurity-in-healthcare-manufacturing/?sh=4db312231a8d> (accessed on 3 January 2023).
112. Shen, M.; Deng, Y.; Zhu, L.; Du, X.; Guizani, N. Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach. *IEEE Netw.* **2019**, *33*, 27–33. [CrossRef]
113. Sun, Y.; Lo, F.P.W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
114. Hatzivasilis, G.; Soutatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of security and privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th international conference on distributed computing in sensor systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; IEEE: New York, NY, USA, 2019; pp. 457–464.
115. Arpaia, P.; Bonavolontà, F.; Cioffi, A.; Moccaldi, N. Power Measurement-based Vulnerability Assessment of IoT medical devices at varying countermeasures for cybersecurity. *IEEE Trans. Instrum. Meas.* **2021**, *70*, 1–9. [CrossRef]
116. Jackson, G.W., Jr.; Rahman, S. Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications Related To The Medical Internet Of Things (MIoT). *arXiv* **2019**, arXiv:1908.00666.
117. Mirsky, Y.; Mahler, T.; Shelef, I.; Elovici, Y. {CT-GAN}: Malicious Tampering of 3D Medical Imagery using Deep Learning. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 461–478.
118. Chen, P.; Desmet, L.; Huygens, C. A study on advanced persistent threats. In Proceedings of the Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, 25–26 September 2014; Proceedings 15; Springer: Berlin, Germany, 2014; pp. 63–72.
119. Moore, T. The economics of cybersecurity: Principles and policy options. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 103–117. [CrossRef]
120. Hu, P.; Li, H.; Fu, H.; Cansever, D.; Mohapatra, P. Dynamic defense strategy against advanced persistent threat with insiders. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Hong Kong, China, 26 April–1 May 2015; IEEE: New York, NY, USA, 2015; pp. 747–755.
121. Palmer, X.L.; Potter, L.; Karahan, S. An Exploration on APTs in Biocybersecurity and Cyberbiosecurity. In Proceedings of the International Conference on Cyber Warfare and Security, Albany, NY, USA, 17–18 March 2022; Volume 17, pp. 532–535.
122. BIO-ISAC Media. BIO-ISAC Releases Advisory to Biomanufacturers. 2021. Available online: <https://www.isac.bio/post/tardigrade> (accessed on 3 January 2023).
123. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]
124. Martínez, A.L.; Pérez, M.G.; Ruiz-Martínez, A. A comprehensive review of the state of the art on security and privacy issues in Healthcare. *ACM Comput. Surv.* **2022**, *55*, 1–38. [CrossRef]
125. Zubair, M.; Unal, D.; Al-Ali, A.; Shikfa, A. Exploiting bluetooth vulnerabilities in e-health IoT devices. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, Paris, France, 1–2 July 2019; pp. 1–7.
126. Perez, A.J.; Zeadally, S. Recent advances in wearable sensing technologies. *Sensors* **2021**, *21*, 6828. [CrossRef]
127. Choi, J.; Choi, C.; Kim, S.; Ko, H. Medical information protection frameworks for smart healthcare based on IoT. In Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics, Seoul, Republic of Korea, 26–28 June 2019; pp. 1–5.

128. Mohanthy, S.B. Real time internet application with distributed flow environment for medical IoT. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015; IEEE: New York, NY, USA, 2015; pp. 832–837.
129. Roy, M.; Chowdhury, C.; Aslam, N. Designing transmission strategies for enhancing communications in medical IoT using Markov decision process. *Sensors* **2018**, *18*, 4450. [CrossRef]
130. Xu, B.; Da Xu, L.; Cai, H.; Xie, C.; Hu, J.; Bu, F. Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Trans. Ind. Infom.* **2014**, *10*, 1578–1586.
131. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* **2018**, *6*, 20596–20608. [CrossRef]
132. Atat, R.; Liu, L.; Ashdown, J.; Medley, M.J.; Matyjas, J.D.; Yi, Y. A physical layer security scheme for mobile health cyber-physical systems. *IEEE Internet Things J.* **2017**, *5*, 295–309. [CrossRef]
133. Mashima, D.; Ahamad, M. Enabling Robust Information Accountability in E-healthcare Systems. In Proceedings of the HealthSec, Bellevue, WA, USA, 8–10 August 2012.
134. Blough, D.M.; Liu, L.; Sainfort, F.; Ahamad, M. *CT-T: MedVault-Ensuring Security and Privacy for Electronic Medical Records*; Technical report; Georgia Institute of Technology: Atlanta, GA, USA, 2011.
135. Mashima, D.; Srivastava, A.; Giffin, J.T.; Ahamad, M. Protecting E-healthcare Client Devices against Malware and Physical Theft. In Proceedings of the HealthSec, Washington, DC, USA, 11–13 August 2010.
136. Halstead, S. Educating Health Organization on Cyber Threats. Ph.D. Thesis, Utica College, Utica, NY, USA, 2021.
137. McMahan, E.; Williams, R.; El, M.; Samtani, S.; Patton, M.; Chen, H. Assessing medical device vulnerabilities on the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; IEEE: New York, NY, USA, 2017; pp. 176–178.
138. Lee, Y.S.; Alasaarela, E.; Lee, H. Secure key management scheme based on ECC algorithm for patient’s medical information in healthcare system. In Proceedings of the The International Conference on Information Networking 2014 (ICOIN2014), Phuket, Thailand, 10–12 February 2014; IEEE: New York, NY, USA, 2014; pp. 453–457.
139. Wu, L.; Chi, H.; Du, X. A Secure Proxy-based Access Control Scheme for Implantable Medical Devices. *arXiv* **2018**, arXiv:1803.07751.
140. Marwan, M.; Karti, A.; Ouahmane, H. Proposal for a secure data sharing and processing in cloud applications for healthcare domain. *Int. J. Inf. Technol. Appl. Sci.* **2021**, *3*, 10–17. [CrossRef]
141. Ren, J.; Li, J.; Liu, H.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2021**, *27*, 760–776. [CrossRef]
142. Mehta, R.; Parmar, M. Trust based mechanism for securing iot routing protocol rpl against wormhole & grayhole attacks. In Proceedings of the 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 6–8 April 2018; IEEE: New York, NY, USA, 2018; pp. 1–6.
143. Rizvi, S.; Kurtz, A.; Pfeffer, J.; Rizvi, M. Securing the internet of things (IoT): A security taxonomy for IoT. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; IEEE: New York, NY, USA, 2018; pp. 163–168.
144. Dinculeană, D.; Cheng, X. Vulnerabilities and limitations of MQTT protocol used between IoT devices. *Appl. Sci.* **2019**, *9*, 848. [CrossRef]
145. Tang, W.; Ren, J.; Deng, K.; Zhang, Y. Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. *IEEE Internet Things J.* **2019**, *6*, 8714–8726. [CrossRef]
146. Chen, Y.; Qin, X.; Wang, J.; Yu, C.; Gao, W. Fedhealth: A federated transfer learning framework for wearable healthcare. *IEEE Intell. Syst.* **2020**, *35*, 83–93. [CrossRef]
147. Cao, F.; Huang, H.K.; Zhou, X. Medical image security in a HIPAA mandated PACS environment. *Comput. Med. Imaging Graph.* **2003**, *27*, 185–196. [CrossRef]
148. Singh, A.K.; Kumar, B.; Singh, G.; Mohan, A. Medical image watermarking techniques: A technical survey and potential challenges. in *Medical Image Watermarking: Techniques and Applications*; Springer: Berlin Germany, 2017; pp. 13–41.
149. Ghoneim, A.; Muhammad, G.; Amin, S.U.; Gupta, B. Medical image forgery detection for smart healthcare. *IEEE Commun. Mag.* **2018**, *56*, 33–37. [CrossRef]
150. Huang, H. *Pacs-Based Multimedia Imaging Informatics: Basic Principles and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2019.
151. Widup, S.; Bassett, G.; Hylender, D.; Rudis, B.; Spittler, M. 2015 Verizon Protected Health Information Data Breach Report. 2015. Available online: https://www.researchgate.net/publication/289254312_2015_Verizon_Protected_Health_Information_Data_Breach_Report (accessed on 1 July 2022).
152. Epia Realpe, L.F.; Parra, O.J.S.; Velandia, J.B. Use of KRACK Attack to Obtain Sensitive Information. In Proceedings of the Mobile, Secure, and Programmable Networking: 4th International Conference, MSPN 2018, Paris, France, 18–20 June 2018; Revised Selected Papers 4; Springer: Berlin, Germany, 2019; pp. 270–276.
153. Seri, B.; Vishnepolsky, G.; Zusman, D. BLEEDINGBIT: The Hidden Attack Surface within BLE Chips. 2019. Available online: <https://info.armis.com/rs/645-PDC-047/images/Armis-BLEEDINGBIT-Technical-White-Paper-WP.pdf> (accessed on 1 July 2022).

154. Siwicki, B. Cloud-Based Pacs System Cuts Imaging Costs by Half for Rural Hospital | Healthcare IT News. Available online: <https://www.healthcareitnews.com/news/cloud-based-pacs-system-cuts-imaging-costs-half-rural-hospital> (accessed on 3 January 2023).
155. Ney, P.; Koscher, K.; Organick, L.; Ceze, L.; Kohno, T. Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More. In Proceedings of the USENIX Security Symposium, Vancouver, BC, Canada, 16–18 August 2017; Volume 26, pp. 765–779.
156. Puzis, R.; Farbiash, D.; Brodt, O.; Elovici, Y.; Greenbaum, D. Increased cyber-biosecurity for DNA synthesis. *Nat. Biotechnol.* **2020**, *38*, 1379–1381. [[CrossRef](#)] [[PubMed](#)]
157. Faezi, S.; Chhetri, S.R.; Malawade, A.V.; Chaput, J.C.; Grover, W.; Brisk, P.; Al Faruque, M.A. Oligo-snoop: A non-invasive side channel attack against DNA synthesis machines. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium, San Diego, CA, USA, 24–27 February 2019.
158. Faezi, S.; Chhetri, S.R.; Malawade, A.V.; Chaput, J.C.; Grover, W.; Brisk, P.; Al Faruque, M.A. Acoustic Side Channel Attack Against DNA Synthesis Machines. In Proceedings of the 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCP), Sydney, NSW, Australia, 21–25 April 2020; IEEE: New York, NY, USA, 2020; pp. 186–187.
159. Oliveira, A.R.d.; Hunt, J.; Valverde, N.; Brandao-Mello, C.; Farina, R. Medical and related aspects of the Goiania accident: An overview. *Health Phys.* **1991**, *60*, 17–24. [[CrossRef](#)] [[PubMed](#)]
160. Kurnot, J.; Kuca, M.; Neidigk, S. Case Study on the Effectiveness of Mechanical Attack Testing to Help Determine Vulnerabilities of a Device that Contains Radiological Material and Proven Methods of Addressing such Vulnerabilities. In Proceedings of the International Conference on the Security of Radioactive Material: The Way Forward for Prevention and Detection, Vienna, Austria, 3–7 December 2018.
161. Choo, K.K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Comput. Secur.* **2021**, *102*, 102136. [[CrossRef](#)]
162. International Atomic Energy Agency. *Security of Radioactive Material in Use and Storage and of Associated Facilities*; Number 11-G (Rev.1) in Implementing Guides; International Atomic Energy Agency (IAEA): Vienna, Austria, 2019.
163. Darwish, S.; Nouretdinov, I.; Wolthusen, S.D. Towards composable threat assessment for medical IoT (MIoT). *Procedia Comput. Sci.* **2017**, *113*, 627–632. [[CrossRef](#)]
164. Umayam, M.L. Possibilities of Blockchain Technology for Nuclear Security. In *Blockchain for International Security: The Potential of Distributed Ledger Technology for Nonproliferation and Export Controls*; Springer: Berlin, Germany, 2021; pp. 55–73.
165. Rane, S.; Harris, J.T. A Game Theoretical Model of Radiological Terrorism Defense. *Int. J. Nucl. Secur.* **2021**, *7*, 7. [[CrossRef](#)]
166. Mueller, S. Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? *Biosaf. Health* **2021**, *3*, 11–21. [[CrossRef](#)]
167. Mantle, J.L.; Rammohan, J.; Romantseva, E.F.; Welch, J.T.; Kauffman, L.R.; McCarthy, J.; Schiel, J.; Baker, J.C.; Strychalski, E.A.; Rogers, K.C.; et al. Cyberbiosecurity for biopharmaceutical products. *Front. Bioeng. Biotechnol.* **2019**, *7*, 116. [[CrossRef](#)]
168. Millett, K.; Dos Santos, E.; Millett, P.D. Cyber-biosecurity risk perceptions in the biotech sector. *Front. Bioeng. Biotechnol.* **2019**, *7*, 136. [[CrossRef](#)]
169. Lee, K.F.; Qiufan, C. *AI 2041: Ten Visions for Our Future*; Currency: Sydney, NSW, Australia, 2021.
170. Schlatt, V.; Guggenberger, T.; Schmid, J.; Urbach, N. Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *Int. J. Inf. Manag.* **2022**, *68*, 102470. [[CrossRef](#)]
171. Alblooshi, M.; Salah, K.; Alhammadi, Y. Blockchain-based ownership management for medical IoT (MIoT) devices. In Proceedings of the 2018 International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 18–19 November 2018; IEEE: New York, NY, USA, 2018; pp. 151–156.
172. Chandrasekaran, S.; Subramaniam, R. Why IoT Sensors Need Standards—They Could Improve Performance and Spur Development of New Applications. 2022. Available online: <https://spectrum.ieee.org/why-iot-sensors-need-standards> (accessed on 3 January 2023).
173. Hardman, A.; Martin, W. Risk Management Framework for DoD Medical Devices. In Proceedings of the HIMSS'18, Las Vegas, NV, USA, 5–9 March 2019.
174. George, A.M. The national security implications of cyberbiosecurity. *Front. Bioeng. Biotechnol.* **2019**, *7*, 51. [[CrossRef](#)] [[PubMed](#)]
175. Shaw, J.; Rudzicz, F.; Jamieson, T.; Goldfarb, A. Artificial intelligence and the implementation challenge. *J. Med. Internet Res.* **2019**, *21*, e13659. [[CrossRef](#)]
176. Jia, Z.; Wang, Z.; Hong, F.; Ping, L.; Shi, Y.; Hu, J. Personalized deep learning for ventricular arrhythmias detection on medical IoT systems. In Proceedings of the 39th International Conference on Computer-Aided Design, Online, 2–5 November 2020; pp. 1–9.
177. Fang, L.; Li, Y.; Liu, Z.; Yin, C.; Li, M.; Cao, Z.J. A practical model based on anomaly detection for protecting medical IoT control services against external attacks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 4260–4269. [[CrossRef](#)]
178. Kruk, M.E.; Gage, A.D.; Joseph, N.T.; Danaei, G.; García-Saisó, S.; Salomon, J.A. Mortality due to low-quality health systems in the universal health coverage era: A systematic analysis of amenable deaths in 137 countries. *Lancet* **2018**, *392*, 2203–2212. [[CrossRef](#)] [[PubMed](#)]
179. Lu, Z.x.; Qian, P.; Bi, D.; Ye, Z.w.; He, X.; Zhao, Y.h.; Su, L.; Li, S.l.; Zhu, Z.l. Application of AI and IoT in clinical medicine: Summary and challenges. *Curr. Med. Sci.* **2021**, *41*, 1134–1150. [[CrossRef](#)]

180. Isgut, M.; Gloster, L.; Choi, K.; Venugopalan, J.; Wang, M.D. Systematic Review of Advanced AI Methods for Improving Healthcare Data Quality In Post COVID-19 Era. *IEEE Rev. Biomed. Eng.* **2022**, *16*, 53–69. [CrossRef]
181. Wahl, B.; Cossy-Gantner, A.; Germann, S.; Schwalbe, N.R. Artificial intelligence (AI) and global health: How can AI contribute to health in resource-poor settings? *BMJ Glob. Health* **2018**, *3*, e000798. [CrossRef] [PubMed]
182. Jiang, F.; Jiang, Y.; Zhi, H.; Dong, Y.; Li, H.; Ma, S.; Wang, Y.; Dong, Q.; Shen, H.; Wang, Y. Artificial intelligence in healthcare: Past, present and future. *Stroke Vasc. Neurol.* **2017**, *2*, 230–243. [CrossRef] [PubMed]
183. Antwi, W.K.; Akudjedu, T.N.; Botwe, B.O. Artificial intelligence in medical imaging practice in Africa: A qualitative content analysis study of radiographers' perspectives. *Insights Imaging* **2021**, *12*, 80. [CrossRef]
184. Ali, O.; Abdelbaki, W.; Shrestha, A.; Elbasi, E.; Alryalat, M.A.A.; Dwivedi, Y.K. A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities. *J. Innov. Knowl.* **2023**, *8*, 100333. [CrossRef]
185. Urbina, F.; Lentzos, F.; Invernizzi, C.; Ekins, S. Dual use of artificial-intelligence-powered drug discovery. *Nat. Mach. Intell.* **2022**, *4*, 189–191. [CrossRef] [PubMed]
186. Kumar, Y.; Koul, A.; Singla, R.; Ijaz, M.F. Artificial intelligence in disease diagnosis: A systematic literature review, synthesizing framework and future research agenda. *J. Ambient. Intell. Humaniz. Comput.* **2022**, 1–28. [CrossRef] [PubMed]
187. Bajgain, B.; Lorenzetti, D.; Lee, J.; Sauro, K. Determinants of implementing artificial intelligence-based clinical decision support tools in healthcare: A scoping review protocol. *BMJ Open* **2023**, *13*, e068373. [CrossRef] [PubMed]
188. Kleinberg, G.; Diaz, M.J.; Batchu, S.; Lucke-Wold, B. Racial underrepresentation in dermatological datasets leads to biased machine learning models and inequitable healthcare. *J. Biomed Res.* **2022**, *3*, 42–47.
189. Gebru, T. Race and gender. In *The Oxford Handbook of Ethics of AI*; Oxford University Press: Oxford, UK, 2020; pp. 251–269.
190. Buolamwini, J.; Gebru, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In Proceedings of the Conference on Fairness, Accountability and Transparency, PMLR, New York, NY, USA, 23–24 February 2018; pp. 77–91.
191. Hoffmann, A.L. Where fairness fails: Data, algorithms, and the limits of antidiscrimination discourse. *Inform. Commun. Soc.* **2019**, *22*, 900–915. [CrossRef]
192. John-Mathews, J.M.; Cardon, D.; Balagué, C. From reality to world. A critical perspective on AI fairness. *J. Bus. Ethics* **2022**, *178*, 945–959. [CrossRef]
193. Jo, E.S.; Gebru, T. Lessons from archives: Strategies for collecting sociocultural data in machine learning. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Barcelona, Spain, 27–30 July 2020; pp. 306–316.
194. Manyika, J. Getting AI right: Introductory notes on AI & society. *Daedalus* **2022**, *151*, 5–27.
195. Zhou, J.; Chen, F.; Holzinger, A. Towards explainability for AI fairness. In Proceedings of the xxAI-Beyond Explainable AI: International Workshop, Held in Conjunction with ICML 2020, Vienna, Austria, 18 July 2020; Revised and Extended Papers; Springer: Berlin, Germany, 2022; pp. 375–386.
196. Gull, S.; Mansour, R.F.; Aljehane, N.O.; Parah, S.A. A self-embedding technique for tamper detection and localization of medical images for smart-health. *Multimed. Tools Appl.* **2021**, *80*, 29939–29964. [CrossRef]
197. Levy, M.; Amit, G.; Elovici, Y.; Mirsky, Y. The security of deep learning defences for medical imaging. *arXiv* **2022**, arXiv:2201.08661.
198. Chui, M.; Evers, M.; Manyika, J.; Zheng, A.; Nisbet, T. The bio revolution: Innovations transforming economies, societies, and our lives. In *Augmented Education in the Global Age*; Routledge: Abingdon, UK, 2023; pp. 48–74.
199. Albahri, A.; Duhaïm, A.M.; Fadhel, M.A.; Alnoor, A.; Baqer, N.S.; Alzubaidi, L.; Albahri, O.; Alamoodi, A.; Bai, J.; Salhi, A.; et al. A systematic review of trustworthy and explainable artificial intelligence in healthcare: Assessment of quality, bias risk, and data fusion. *Inf. Fusion* **2023**, *96*, 156–191. [CrossRef]
200. Arshad, S.; Arshad, J.; Khan, M.M.; Parkinson, S. Analysis of security and privacy challenges for DNA-genomics applications and databases. *J. Biomed. Inform.* **2021**, *119*, 103815. [CrossRef] [PubMed]
201. Mahajan, A.; Vaidya, T.; Gupta, A.; Rane, S.; Gupta, S. Artificial intelligence in healthcare in developing nations: The beginning of a transformative journey. *Cancer Res. Stat. Treat.* **2019**, *2*, 182–189. [CrossRef]
202. Samori, I.A.; Palmer, X.L.; Potter, L.; Karahan, S. Commentary on Biological Assets Cataloging and AI in the Global South. In Proceedings of the Intelligent Systems and Applications: Proceedings of the 2022 Intelligent Systems Conference (IntelliSys), Amsterdam, The Netherlands, 1–2 September 2022; Springer: Berlin, Germany, 2022; Volume 3, pp. 734–744.
203. Powell, E.; Akogo, D.; Potter, L.; Palmer, X.L. Co-leadership and Cross-pollination of University and DIY Bio Spaces: An Exploration in Consideration of Biocybersecurity. In Proceedings of the Future Technologies Conference (FTC), Vancouver, BC, Canada, 28–29 November 2021; Springer: Berlin, Germany, 2022; Volume 3, pp. 610–621.
204. 247 Crypto. JPMorgan becomes First Bank to enter Metaverse Launching Virtual Lounge in Decentraland. 2022. Available online: <https://247-crypto.com/jpmorgan-enter-metaverse-onyx-lounge-decentraland/> (accessed on 3 January 2023).
205. Kumar, M.; Chand, S. MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic. *J. Netw. Comput. Appl.* **2021**, *179*, 102975. [CrossRef] [PubMed]
206. Sneha, S.; Panjwani, A.; Lade, B.; Randolph, J.; Vickery, M. Alleviating challenges related to FDA-approved medical wearables using blockchain technology. *IT Prof.* **2021**, *23*, 21–27. [CrossRef]
207. West, R.M.; Gronvall, G.K. CRISPR Cautions: Biosecurity implications of gene editing. *Perspect. Biol. Med.* **2020**, *63*, 73–92. [CrossRef] [PubMed]

208. Bao, J.; Ma, Y.; Ding, M.; Wang, C.; Du, G.; Zhou, Y.; Guo, L.; Kang, H.; Wang, C.; Gu, B. Preliminary exploration on the serum biomarkers of bloodstream infection with carbapenem-resistant *Klebsiella pneumoniae* based on mass spectrometry. *J. Clin. Lab. Anal.* **2021**, *35*, e23915. [[CrossRef](#)]
209. Bush, J.; Hu, C.H.; Veneziano, R. Mechanical properties of DNA hydrogels: Towards highly programmable biomaterials. *Appl. Sci.* **2021**, *11*, 1885. [[CrossRef](#)]
210. Al-Husainy, M.A.F.; Al-Shargabi, B.; Aljawarneh, S. Lightweight cryptography system for IoT devices using DNA. *Comput. Electr. Eng.* **2021**, *95*, 107418. [[CrossRef](#)]
211. Dey, S.; Fan, C.; Gothelf, K.V.; Li, J.; Lin, C.; Liu, L.; Liu, N.; Nijenhuis, M.A.; Saccà, B.; Simmel, F.C.; et al. DNA origami. *Nat. Rev. Methods Prim.* **2021**, *1*, 13. [[CrossRef](#)]
212. Liu, A.P.; Appel, E.A.; Ashby, P.D.; Baker, B.M.; Franco, E.; Gu, L.; Haynes, K.; Joshi, N.S.; Kloxin, A.M.; Kouwer, P.H.; et al. The living interface between synthetic biology and biomaterial design. *Nat. Mater.* **2022**, *21*, 390–397. [[CrossRef](#)]
213. Li, Y.C.; Zhang, Y.S.; Akpek, A.; Shin, S.R.; Khademhosseini, A. 4D bioprinting: The next-generation technology for biofabrication enabled by stimuli-responsive materials. *Biofabrication* **2016**, *9*, 012001. [[CrossRef](#)] [[PubMed](#)]
214. Bilooei, S.F.; Jovicevic, D.; Iranzadeh, A.; Thomas, A.; Muscat, I.; Mpofu, C.; Steiner, H.; Meany, T. Rapid genome surveillance of SARS-CoV-2 and study of risk factors using shipping container laboratories and portable DNA sequencing technology. *medRxiv* **2022**, medRxiv:2022-02.
215. Rahman, A.; Hossain, M.S.; Alrajeh, N.A.; Alsolami, F. Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices. *IEEE Internet Things J.* **2020**, *8*, 9603–9610. [[CrossRef](#)] [[PubMed](#)]
216. Girgis, S.T.; Adika, E.; Nenyewodey, F.E.; Senoo Jnr, D.K.; Ngoi, J.M.; Bandoh, K.; Lorenz, O.; van de Steeg, G.; Nsoh, S.; Judge, K.; et al. Nanopore sequencing for real-time genomic surveillance of *Plasmodium falciparum*. *bioRxiv* **2022**, bioRxiv:2022-12.
217. Gault, M. The Plan to Put Bitcoin in Mouse DNA with a Genetically Engineered Virus. 2022. Available online: <https://www.vice.com/en/article/5dg5az/the-quest-to-put-bitcoin-in-mouse-dna-with-a-genetically-engineered-virus> (accessed on 3 January 2023).

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