electronics

MDPI

Review

An Overview of Medical Electronic Hardware Security and Emerging Solutions

Shayan Taheri * and Navid Asadizanjani

Electrical and Computer Engineering Department, University of Florida, Gainesville, FL 32611, USA; nasadi@ece.ufl.edu

* Correspondence: shayan.taheri@ufl.edu

Abstract: Electronic healthcare technology is widespread around the world and creates massive potential to improve clinical outcomes and transform care delivery. However, there are increasing concerns with respect to the cyber vulnerabilities of medical tools, malicious medical errors, and security attacks on healthcare data and devices. Increased connectivity to existing computer networks has exposed the medical devices/systems and their communicating data to new cybersecurity vulnerabilities. Adversaries leverage the state-of-the-art technologies, in particular artificial intelligence and computer vision-based techniques, in order to launch stronger and more detrimental attacks on the medical targets. The medical domain is an attractive area for cybercrimes for two fundamental reasons: (a) it is rich resource of valuable and sensitive data; and (b) its protection and defensive mechanisms are weak and ineffective. The attacks aim to steal health information from the patients, manipulate the medical information and queries, maliciously change the medical diagnosis, decisions, and prescriptions, etc. A successful attack in the medical domain causes serious damage to the patient's health and even death. Therefore, cybersecurity is critical to patient safety and every aspect of the medical domain, while it has not been studied sufficiently. To tackle this problem, new human- and computer-based countermeasures are researched and proposed for medical attacks using the most effective software and hardware technologies, such as artificial intelligence and computer vision. This review provides insights to the novel and existing solutions in the literature that mitigate cyber risks, errors, damage, and threats in the medical domain. We have performed a scoping review analyzing the four major elements in this area (in order from a medical perspective): (1) medical errors; (2) security weaknesses of medical devices at software- and hardware-level; (3) artificial intelligence and/or computer vision in medical applications; and (4) cyber attacks and defenses in the medical domain. Meanwhile, artificial intelligence and computer vision are key topics in this review and their usage in all these four elements are discussed. The review outcome delivers the solutions through building and evaluating the connections among these elements in order to serve as a beneficial guideline for medical electronic hardware security.

Keywords: medical domain; medical errors; medical security; medical hardware; IoMT devices; artificial intelligence; computer vision

Citation: Taheri, S.; Asadizanjani, N. An Overview of Medical Electronic Hardware Security and Emerging Solutions. *Electronics* **2022**, *11*, 610. https://doi.org/10.3390/electronics11040610

Academic Editor: Kenji Suzuki

Received: 13 October 2021
Accepted: 23 December 2021
Published: 16 February 2022

1. Introduction

Recent advancements and progress in computer science along with the demands for great computing performance makes artificial intelligence (AI) a promising candidate for engaging in different applications and benefitting modern society [1–6]. AI includes various methods from statistics to computational complexity. AI is used in a diverse set of applications, namely weather forecasts, face recognition, fraud detection, deciphering genomics, and medical domain [7–12]. AI combined with biostatistics helps in improving many medical processes and computations. In fact, medical AI is able to understand the patterns and features of data in this domain and perform related predictive and corrective tasks [13–19].

Medical AI includes leveraging AI algorithms in radiology, pathology, dermatology, etc. with the purpose of enhancing the diagnostic speed, accuracy, and knowledge, as well as increasing the diagnostic confidence to close to 100%. Different areas associated to and within AI, such as computer vision (CV), machine learning, autonomous systems, natural language processing, intelligent agents, deep neural networks, and automated reasoning are utilized to learn the medical background and analyze the medical records more effectively [20–23]. Overall, AI and CV contributions are key players in the medical field:

1. Medical operations including monitoring, prediction, diagnosis, treatment, and prognosis become intelligence with higher performance.
2. Reduction in the medical errors along with improvements in medical operations in terms of execution time, quality of diagnosis, quantity of diagnosis, etc. Many problems in conventional human clinical practices are eliminated.
3. Easier and faster medical access is extremely important and valuable. The lengthy processes of getting doctor visits, diagnosis, prescription, treatment results are improved, leading to the provision of a service to more patients.
4. Improving the reliability, quality, and quantity of processing and transmitting information in the medical domain.
5. Enhancing major computations within these systems including segmentation, classification, detection, registration, and medical information processing.
6. The major growth in machine learning, more specifically deep learning, provide high-performance algorithms and systems that understand and model medical data through multiple layers of transformations. These algorithms help in extracting and learning features from data automatically at different abstract levels. Better classifications by the deep learning systems enables better diagnosis and medical decisions. There are many deep neural network architectures, especially convolutional neural networks (i.e., automatic and adaptive learning of spatial hierarchies of features from medical data/image through backpropagation using multiple building blocks, such as convolution layers, pooling layers, and fully connected layers). They are critical elements in the classification and recognition systems and each of them suits a specific type of data and application well. When the predictive model accuracy, the confidence of learning performance, is increased, the medical operations become more successful.
7. Underpinned by the ability to learn from salient features from large volumes of healthcare data, an AI system assists clinicians through interpreting diagnostic, prognostic, and therapeutic data from very large patient populations. This provides real-time guidance on risk, clinical care options, and outcome, but in addition provide up-to-date medical information from journals, textbooks, and clinical practices to inform proper patient care.
8. The systems have unique characteristics: (a) plasticity, causing changes in system performance through learning and need of creating new concepts about the timing of learning and assignment of responsibilities for risk management; (b) unpredictability of system behavior, in response to unknown inputs due to the black box characteristics precluding deductive output prediction; and (c) need to assure the characteristics of datasets to be used for learning and evaluation.

Due to this merit of AI/CV-based medical applications, all aspects of this research direction should be studied comprehensively. These aspects are categorized as requirements, opportunities, and challenges. The requirements help in preparing a better working environment for these systems, the opportunities show us the areas of novel contributions and ideas for new systems, and the challenges are very critical due to the nature of this domain and how a limitation can become a life threat, so resolving them is mandatory.

Utilizing AI/CV in the medical domain has its requirements, such as strong computational resources (e.g., graphical processing unit), multimedia processing, and large data storages [24–28]. The large data repositories need advanced managing and querying systems for finding, retrieving, and transmitting data. Without such systems, it is extremely

difficult to access, manage, and extract the relevant data from the databases. These medical data come from various sensing setups in the medical field, such as the diagnostic and investigative imaging facilities in hospitals. Additionally, the systems should be able to properly correct and adjust their learned knowledge based on the differences available on the input data.

There are many opportunities to explore for these systems [29–31]. One example is understanding their underlying operations with respect to each medical task. The medical AI system should be self-explanatory so that we can gain enough knowledge from the input data, computations, and the output data. In the medical domain, there are complex challenges particularly in the integration, fusion, and mapping of various distributed and heterogeneous data in arbitrarily high dimensional spaces [29–31]. The explainable AI helps in addressing these challenges through understanding why a set of diverse data contribute to a certain result and medical decision [32]. As a result, the trust and reliability of current and future medical AI systems are analyzed and boosted using the self-explanatory property.

The limitations of these systems are critical due to their connection to human life. Any failure in the system or any error in computations lead to catastrophic short- or long-term consequences, and even death. The result of a failure or an error is a wrong diagnosis, assessment, decision, prescription, surgical operation, etc. One of the limitations in this area is the shortage of data. The medical datasets are hard to develop considering the challenging acquisition and preprocessing processes (e.g., labeling). There are different ways of overcoming this issue, such as transfer learning and synthetic data generation.

This subject requires a detailed study in order to make sure that the systems have sufficient knowledge, provided from the training phase. Another limitation is the security threats targeting these systems. Recently, security aspects of AI and CV-based systems have received remarkable attention from the community and a number of works have been proposed. However, the connection between the medical dangers and the security threats on these systems has not been analyzed sufficiently [33–39] and a comprehensive review is required.

Alongside the high-level overview of AI/CV-based systems, physical/hardware realization of these systems also requires a comprehensive review and analysis [5]. The medical devices in the form of implantable and wearable must have the resources and capabilities to execute and complete the AI/CV-based medical computations according to the designated specifications. Smart insulin pumps are an example of these devices. They require novel technologies in their hardware. The security of hardware is an important topic for these devices [40–44]. There is an urgent need for researchers in academia, industry, and government to address these issues.

Many hardware-related security issues of medical devices stem from the globalization of the semiconductor supply chain. It creates opportunities for adversarial parties in IC supply chain to perform attacks causing purposeful damages in the medical devices and consequently malicious medical errors. Recently, major attention has been given to leveraging physical inspection, AI, and CV for hardware trust and assurance [45–48]. In fact, both AI and CV can play a crucial role in design and development of both stronger threats and defenses.

Novel attack and defense models are developed in this multi-disciplinary research and effective methods are examined to make the models fully operational targeting computing systems. Both non-AI/CV and AI/CV computations run by the systems are subject to attacks. Therefore, we define three directions in the intersection of AI/CV and hardware security for medical devices: (a) AI/CV-based attacks; (b) AI/CV-based defenses; and (c) security of AI/CV elements. The novel AI/CV-based defenses in the medical devices should be protected in order to make sure that all the non-security and security elements in the device can resist in the face of different attacks.

In this review paper, we focus on: the emerging security weaknesses and threats in medical applications based on the known medical errors; the application of artificial intelli-

gence and computer vision in the medical field; and the security aspects of medical devices at software and hardware levels. The paper contributions are stated as: (a) identification of the errors in the medical domain, refer to Section 2; (b) analysis of the security weaknesses in the software, imaging, and electronics used in medical applications, refer to Section 3; (c) utilization of AI/CV-based electronic components in medical applications (e.g., smart remote surgery and medical image analytics), refer to Section 4; (d) review of the attack and defense models for software and hardware in the medical domain based on the identified errors, refer to Section 5; and (e) evaluations of the challenges and opportunities for IoMTs, refer to Section 6. The paper is concluded in Section 7.

The four major contributing elements of this review (in order from the medical perspective) is graphically shown in Figure 1. As shown in the figure, "medical errors" is the foundation for the other elements in the review. According to these errors, we detect the weaknesses of medical entities in different layers of computations that can be exploited by adversaries for performing malicious purposes (refer to Section 3). In the element presented in Section 4, applicability and usefulness of AI and CV technologies in optimizing quantity, quality, and accuracy of medical processes are studied. Lastly, we survey and analyze the cyber attacks capable of creating malicious medical errors along with their countermeasures. It is important to mention that both artificial intelligence and computer vision are key subjects in this review and their employment in all these four elements are discussed. Overall, this review is considered as an instruction manual for medical security from the hardware perspective.

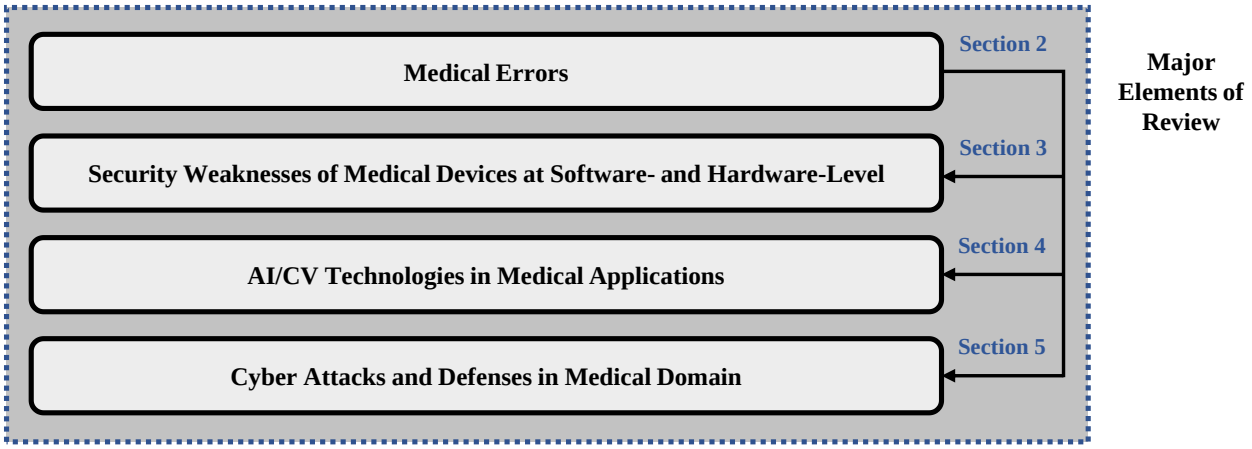

Figure 1. The four major contributing elements of this review on threats and vulnerabilities in medical domain.

2. Medical Errors

In this section, the errors in the medical domain are discussed. These medical errors are among the top three causes of death in the United States according to the recent research [49]. Unsafe healthcare treatments are at the core of incidents in hospital settings, such as patients' injuries, falls, infections, and longer hospital stays. Having more strength in the medical field is really important due to their roles in every society in terms of helping people to have satisfactory health, treating ill patients, saving lives, and preventing deaths.

A failure/error in these tasks results in serious adverse consequences and even death [50–56]. Therefore, it is critical to monitor and conduct medical processes for prevention, reduction, and elimination of all possible errors in the field. Alongside the detrimental effects of medical errors on humans, they cause added costs to both patients and healthcare personnel. Figure 2 shows an example of costs associated with medical errors [57]. The data from the figure are from two studies accomplished by the Betsy Lehman Center: (a) measuring the annual incidence, types, and system costs of medical errors throughout the commonwealth. (b) measuring the physical, emotional, behavioral, and financial impacts of preventable medical harm on Massachusetts residents.

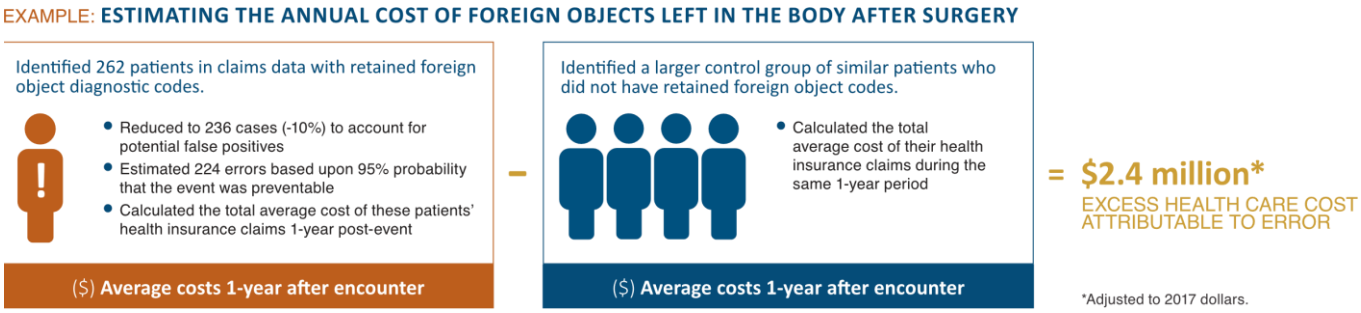

Figure 2. An estimation of the annual cost of foreign objects left in the body after surgery [57].

With respect to case (a), certain parameters were considered in the study, such as preventable medical harm events that occurred in one year, the most common and costly types of errors, and the budget spent on excess health insurance claims resulting from these errors. The national cost of medical error was estimated using the Massachusetts All-Payer Claims Database (APCD), which includes both commercial health insurance and Medicaid claims, and Medicare claims data (i.e., both databases from 2013 because of a subsequent change in the diagnostic coding system) encompassing most reimbursable procedures or treatments.

For the case of (b), the public experience in Massachusetts on medical error is analyzed. A large randomized cross-section of residents was involved in the analysis. This experience-based analysis includes multiple cases for investigation: (1) the incidence and types of medical errors; (2) the healthcare settings; (3) the physical, emotional, and financial consequences of error to patients and families over time; (4) the provider response after an error; and (5) the impact of open communication about errors on patient and family wellbeing. The residents were identified and interviewed in two statewide telephone-based health insurance surveys (initial in 2017 and follow up in 2018) conducted by Center for Health Information and Analysis. From the study, we understand that patients and families are excellent observers of medical error.

One in seven Medicare patients in hospitals experience a medical error. Medical errors are silent in terms of exposing themselves immediately and are largely unseen tragedies. Beyond the obvious emotional complications, unexpected adverse effects related to medical error increase personal and institutional financial responsibilities, which increases estimated billions of dollars to health care costs annually. A medical error is defined as failure of a planned medical action to be completed as intended or the use of a wrong medical plan to achieve an aim. Research shows that a high percentage of medical errors are not reported. This leads to a dangerous environment for patients. Additionally, having an experience with medical error causes dissatisfaction, loss of trust, financial failures, and long-lasting health and emotional issues for the patient victims.

More specifically, the medical errors are stated as: (a) a safety problem: a lack of freedom from accidental injury; (b) an adverse drug event: an adverse drug event is injury resulting from the use of a drug. An adverse drug event may be caused by an adverse drug reaction, a medication error, or an overdose. An adverse drug event frequently necessitates discontinuation of the drug use; (c) an adverse drug reaction: an adverse drug reaction is an unavoidable, remarkably detrimental, or unpleasant reaction that occurs during the normal and correct use of a medical product. A number of drug reactions may be minor and temporary, while others have the potential to be permanent and serious; (d) medication errors: medication errors are defined as errors that happen due to the mistakes made in the processes of the drug's prescription, transcription, dispensing, administration, or monitoring; (e) near miss: an error that is detected and corrected before the occurrence of harm; (f) sentinel event: an unexpected occurrence involving the risk or complete occurrence of serious physical or psychological injury and even death; (g) diagnostic errors: diagnosis errors are errors that occur when a diagnosis is missed, wrongly performed, or

delayed. As an example, a categorization of medical errors related to medications with the respective impacts and definitions are shown in Table 1 [58].

Table 1. The definition of levels of harm. National Coordinating Council for Medication Error Reporting and Prevention Index for categorizing of medication errors, with added definitions for the current study [58]. Abbreviations used: NCC MERP, National Coordinating Council for Medication Error Reporting and Prevention. Reprinted with permission from Ref. [58]. 2004 Wiley Online Library.

Medical Status	Category	NCC MERP Definition	Additional Definitions for the Current Study
No error	A	Circumstances or events that have the capacity to cause error	
No harm	B	An error occurred but did not reach the patient ("an error of omission" does reach the patient)	
	C	An error occurred that reached the patient but did not cause harm	
	D	Error reached the patient, and required monitoring to confirm that no harm resulted and/or required intervention to preclude harm	
Harm	E	Error occurred that may have contributed to or resulted in temporary harm to the patient and required intervention	
	F	Error occurred that may have contributed to or resulted in temporary harm to the patient and required initial or prolonged hospitalization	F1. An error reached the patient that required additional surgery or an unnecessary general anesthetic F2. Unnecessary incision during a necessary operation
	G	Error occurred that may have contributed to or resulted in permanent patient harm	G1. Delayed cancer diagnosis that is likely to affect prognosis (when final outcome is not yet known)
	H	Error occurred that required intervention necessary to sustain life	
Death	I	Error occurred that may have contributed to or resulted in the patient's death	

The table is a modified version of the National Coordinating Council for Medication Error Reporting and Prevention harm index, developed to assess harm caused by medication errors. In this alphabetic system, harm is assigned a letter category from "A" (no harm, but circumstances predisposing to error) to "I" (death). Modifications were made to accommodate some non-medication errors that do not fit well into this system.

(h) Systems or process errors: systems or process errors involve predictable human mistakes in the context of poorly designed system. (i) active errors: active errors usually involve the most active staff members and occur at the connection point between a human and certain parts of a larger system; (j) latent errors: hidden errors involve failures of organization or design (e.g., systems and processes) that allow active errors to cause harm. A sample of medical errors and their associated processes are displayed in Table 2 [58]. This table shows a classification system based on the "care flow" guided by the reported events.

This classification: (1) maximizes the interrater agreement; and (2) gives the most helpful information to practicing otolaryngologists. The table includes a conceptualization of an idealized patient encounter beginning with history and physical examination, continuing through either medical or surgical therapy and postoperative care. The errors are classified by where they occurred in the care flow. The classification table can foster agreements and provide useful information in the practicing otolaryngologist. Using this information, errors can be categorized according to whether they occurred during evaluation and diagnosis, surgical management, or medical (non-surgical) management.

Table 2. The idealized care flow and potential errors [58]. Reprinted with permission from Ref. [58]. 2004 Wiley Online Library.

Care Flow Process	Potential Errors	
Work-up and diagnosis	Obtain history and perform examination	Errors in history or examination
	Construct a differential diagnosis	Errors in differential diagnosis
	Order testing to reduce differential	Testing errors
	Reach definitive diagnosis	Errors in final diagnosis
Surgical management	Choose a surgical therapy	Choose wrong procedure
	Surgical planning (facility, personnel, preop tests)	Errors in surgical planning
	Correct site surgery	Wrong site surgery
	Anesthetic administered	Anesthesia errors
	Drugs administered from field	Wrong drug/dilution from surgical field
	Intraoperative patient management	Errors in management (e.g., failure to call consult intraoperatively)
	Perform surgery correctly	Technical surgical errors
	Remove all instruments and sponges	Retained foreign body
	Surgical equipment available and functional	Equipment-related errors
	Postoperative care	Errors in postoperative care
Medical management	Choose correct therapy	Choose incorrect therapy
	Administer medical therapy	Medication errors
Miscellaneous	Nursing and ancillary care	Nursing/ancillary errors
	Administrative	Administrative errors
	Communication	Communication errors
	Miscellaneous	All others

In addition, the top 10 frequent medical errors are observable in Figure 3 [57]. The findings about the most frequent types of errors follow a pattern similar to the earlier national study on which it was based, with seven of the most frequent errors making it into the top 10 lists in both studies.

Medical errors occur anywhere in the health care system: hospitals, clinics, surgery centers, doctors' offices, nursing homes, pharmacies, and patients' homes. Medical errors are issues that are prevented with better planning, adequate knowledge, and/or a higher level of attention and communication. Planning failures and knowledge insufficiencies encompass virtually every aspect of the delivery of care, and they create many errors of different types.

Therefore, it is required that nurses and other health care professionals work together to establish the most effective plan of care for each patient, to ensure that all members of the health care team have the necessary knowledge and skills to implement the plan of care, and to evaluate the effectiveness and safety of the implemented plan. We can see the statistics from different healthcare settings that medical errors can happen, and the range of ages of patient victims, in Figure 4 [57].

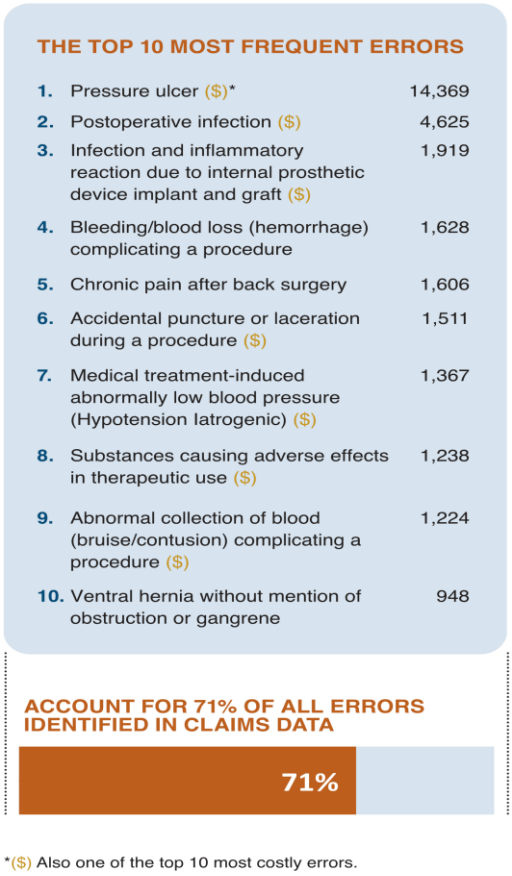

Figure 3. The top 10 of the most frequent errors [57].

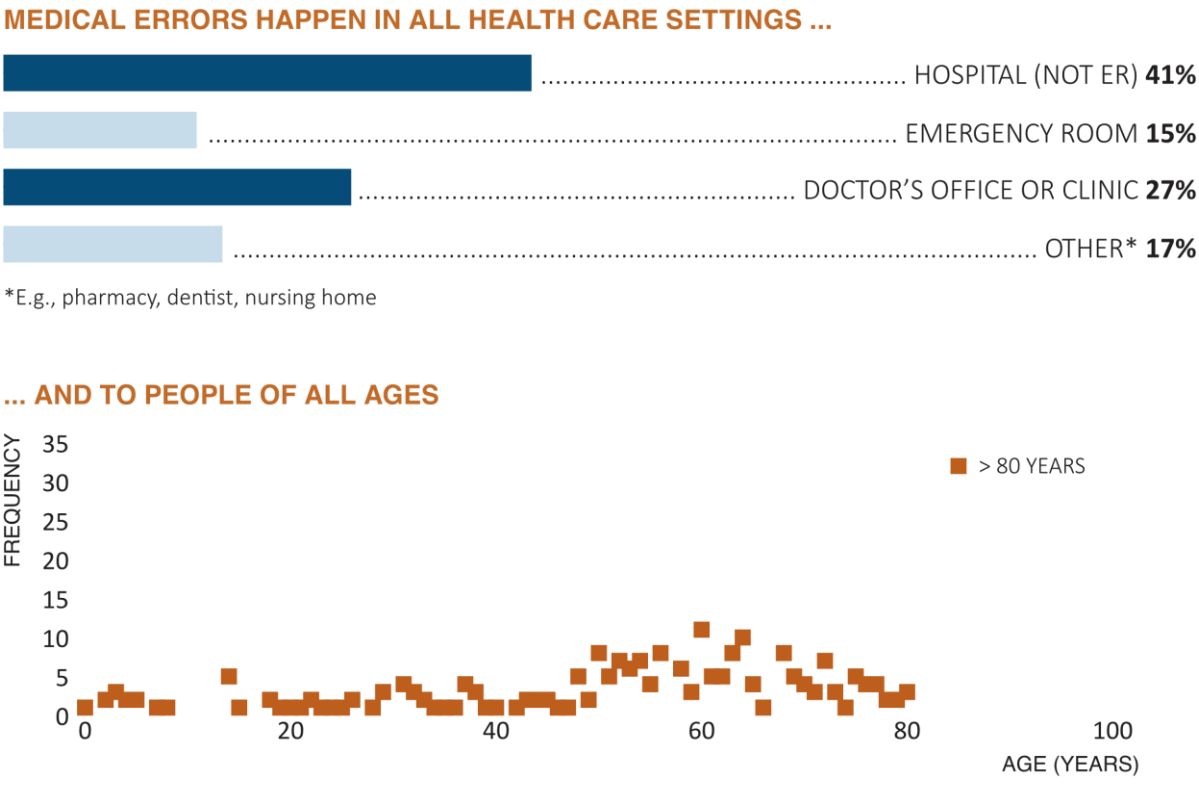

Figure 4. Graphical illustration of the occurrence of medical errors in different healthcare settings along with the people of all ages [57]. Abbreviations used: ER, Emergency Room.

The bar chart from this figure shows that errors happen in all health care settings, including nursing homes, dental offices, emergency rooms, hospitals, urgent care, prison infirmaries, primary care practices, and retail pharmacies. Also, people who reported medical errors live in every part of the state. The bottom plot of figure displays the age of the patient to whom the medical error happened ranged from less than one to over 90. Although median age at the time of the error was 53 years old, 15% of the errors described occurred to patients less than 18 years old and 18% of the errors occurred to respondents 75 or older. In another comparison, the changes on the number of medical errors over time and for different ages are shown in Figure 5 [59].

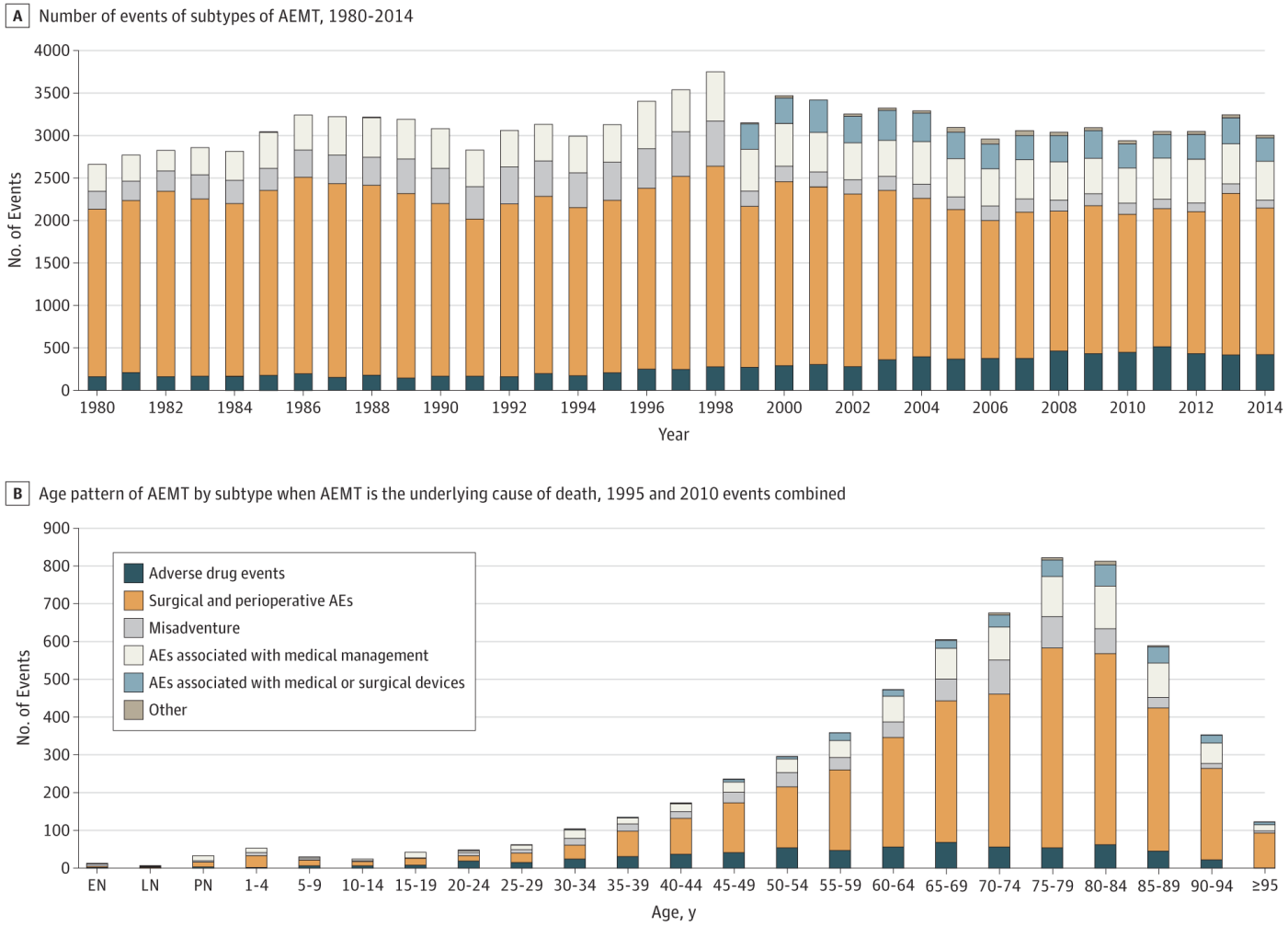

Figure 5. The changes on the number of medical errors over time and for different ages [59]. Abbreviations used: AEMT, Adverse Effects of Medical Treatment; and AE, Adverse Effects.

Lack of knowledge and considerations involves poor planning and execution, inappropriate or absent policies and procedures, failure to get and maintain equipment, failure to hire and retain staff, failure to maintain safe staffing levels, failure to monitor care, and failure to recognize errors, and correct the conditions that caused the errors. Accurate communication is fundamental for: (a) diagnosing, treating, dispensing, and administering medications; (b) maintaining patient safety; (c) following policies and procedures; and (d) ensuring treatment instructions are carefully followed. Communication errors can be verbal or written and occur in every part of the process of delivery of care. It is necessary to find the sources of errors (i.e., security weaknesses) before doing any actions (i.e., defense mechanisms). Doing survey is one of the established methods for finding the possible nodes in the healthcare domain in which different parties and scenarios are considered.

Open communication between healthcare professionals about care concerns, also known as "speaking up" is essential to patient safety. It is important to compare interns' and residents' experiences, attitudes, and factors associated with speaking up about traditional versus professionalism 'related safety threats. The comparisons are usually provided in anonymous and cross-sectional surveys. The measurements for them include (but not limited to) attitudes about, barriers and facilitators for, likelihood of, and self-reported experience with speaking up. Many interns and residents commonly observe unprofessional behavior, but it is less likely that they speak up about it compared with their observations of traditional safety threats, so continuous studies in this domain are needed to keep patients safe and prevent the existing and emerging errors. Related to the discussed matters, we can observe the material of a national survey about "speaking up" in [60] (especially see all of the tables in the reference).

The items in survey include: (a) respondents' self-reported exposure to and speaking up about traditional patient safety breaches and unprofessional behavior; (b) barriers, facilitators and attitudes towards speaking up about patient safety breaches and unprofessional behavior; (c) new and validated measures of patient safety culture; (d) respondent characteristics and (e) two patient safety vignettes: traditional safety threat versus professionalism-related safety threat (refer to "[60], table number one"). The survey was developed by certain physicians and researchers with expertise in patient safety, professionalism, ethics and psychometrics.

"Unprofessional behavior" in the survey was defined as conduct of a health professional that demonstrates disrespect or lack of compassion, commitment to ethical principles, integrity or accountability towards patients or coworkers. "Patient safety breach" was defined as an act or omission that unnecessarily increases the risk of accidental or preventable injuries produced by medical care.

The vignettes were based on actual cases and designed using review of the literature, personal experience, and consultation with medical and surgical residents, nursing leadership and experts in patient safety. They help to determine whether respondents' perceived likelihood of speaking up differed between a traditional patient safety threat and a professionalism related safety threat while accounting for any differences in the perceived potential for harm.

Throughout the survey, descriptive statistics were used to report responses. For comparing the demographics of respondents to the total population, χ^2 goodness-of-fit test was used. The McNemar's test was used to analyses within-respondent differences in (a) self-reported speaking up behavior; (b) barriers and facilitators to speaking up; (c) and attitudes regarding speaking up between traditional and professionalism-related patient safety threats.

Multivariate logistic regression was used to explore factors independently associated with speaking up in the traditional and professionalism-related safety vignettes. Factors potentially associated with speaking up were identified from the literature and assessed via scales and individual survey items. All hypothesized factors were included in each regression model. Covariates included level of hierarchy, perceived potential for harm to patients, perceived patient safety-related climates, gender, level of postgraduate training, specialty, moral courage, self-reported patient safety training, and study site.

Consistent with analysis of factorial survey data, the unit of analysis was the vignette, rather than individual respondents (sample size equals to number of respondents multiplied by number of speaking up judgements made in response to a vignette). It was estimated that a sample size of 2131 speaking up judgements for each vignette would provide 80% power to detect an effect size (OR 1.5) assuming moderate correlation (R = 0.5) between covariates. This number translates to 533 respondents with four speaking up judgements per vignette (i.e., likelihood of speaking up to a nurse, intern, resident and attending). To account for multiple comparisons, two-tailed statistical significance was set at an alpha level of 0.01. Analyses were performed using SAS V.9.4.

Of the 1800 interns and residents surveyed, 837 (47%) completed the questionnaire. The "table number two from [60]" illustrates the characteristics of the respondents and the total population surveyed. During their most recent inpatient month, 49% (410/837) of respondents reported observing a patient safety breach and 75% (628/837) of respondents reported observing unprofessional behavior ($p < 0.001$). However, respondents reported speaking up about the unprofessional behavior they observed less commonly than speaking up about a patient safety breach (46%, 287/628 vs 71%, 291/410; $p < 0.001$).

The majority of respondents (82%, 683/837) agreed that speaking up about unprofessional behavior was important for patient safety. Greater than double the proportion of respondents agreed that it is difficult to speak up in their clinical area about unprofessional behavior compared with patient safety concerns (38%, 322/837 vs 16%, 133/837; $p < 0.001$, in "reference [60], table number three") and substantially fewer forecasted meaningful change after speaking up in each setting (40%, 332/837 versus 60%, 504/837; $p < 0.001$, respectively).

While 65% (541/837) reported encouragement from colleagues to speak up about patient safety concerns, only 36% (305/837) reported the same for unprofessional behavior; $p < 0.001$. Respondents were least likely to report observing others speaking up about both patient safety concerns and unprofessional behavior as a bystander (i.e., when observing threats that did not directly involve themselves or their patients) (43%, 362/837 and 27%, 224/837, respectively).

The "table number five from [60]" shows respondents' likelihood of speaking up in traditional versus professionalism-related patient safety vignettes across levels of hierarchy (i.e., speaking up to a nurse, intern, resident or attending). Significantly fewer respondents reported that they would likely speak up in the professionalism-related patient safety vignette than the traditional patient safety vignette across all hierarchy positions, and these differences persisted even among respondents who perceived a high potential for harm to the patient in both vignettes (see "reference [60], the fifth table" in which $p < 0.001$ for all comparisons). The fewest number of respondents reported that they would likely speak up to an attending physician for both the traditional patient safety and professionalism-related vignettes (64%, 537/836 and 9%, 78/836, respectively). Meanwhile, we can see the impact of open communication on lowering the patient harm in Figure 6 [57].

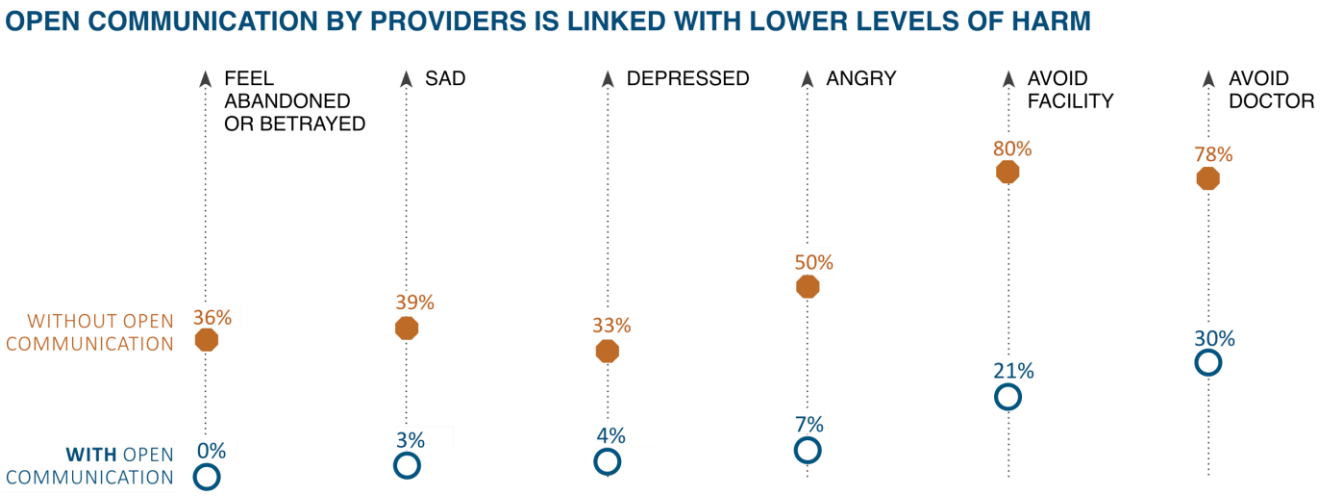

Figure 6. The connection between the open communication by providers and the lower levels of harm [57].

These errors involve medicines and drugs, surgery, procedures, diagnosis, equipment and devices, or lab reports. Each of these cases have their own issues such as having expired, being counterfeit, unsafe, unapproved, untrusted, ineffective, etc. They can happen during even the most routine tasks. Most errors result from problems created by today's complex health care system. The errors also happen when doctors and patients have problems in

their communications. Table 3 shows important signs of counterfeit prescription drugs that physicians should be aware of [61]. The physicians should be assured that the medical products are Food and Drug Administration (FDA)-approved.

Table 3. The signs of counterfeiting [61]. Abbreviations used: Rx, Prescription.

1. Product packaging and label are not in English.
2. Words are misspelled on the bottle.
3. "Rx Only" designation is absent.
4. Expiration date is missing or has passed.
5. Lot number is omitted.
6. Generic name or active ingredient is not printed with brand name.
7. Product appearance, packaging, prescribing information, labeling or indications for use are unfamiliar.
8. Physician and/or patient package label and product information are absent.

The medical errors are reduced and prevented through protecting and improving the operations performed by "humans", "software", and "hardware". Certain technologies including artificial intelligence and computer vision are able to make the operations more accurate and successful, causing a reduction in the errors. Using AI and CV, humans provide stronger information for the operations to make better decisions. Also, software along with hardware function more intelligently with higher performance.

Overall, health professionals and patients should employ all their knowledge and skills through their natural abilities and emerging technologies to make sure that protection against the errors is provided in all stages of the medical processes. When errors are detected and reported, it is important that the information is spread in a manner that would alert most individuals about preventing future errors. Methods for providing information about errors is outlined in Table 4 [62].

Table 4. The dissemination of medication errors [62]. Reprinted with permission from Ref. [62]. 2009 Wiley Online Library.

Medium	Contribution (%)
Email	10.3
In-services and Lectures	57.1
Memorandums and Letters	64.7
Newsletters	54.5
Orientation for New Employees	48.1
Other or not disseminated	41

There are a number of tips that "humans" should consider for making the medical domain safer with less errors. They need to become an active member of the healthcare agencies for joining in every action and decision with respect to healthcare. Studies show that patients who are more involved with their care tend to get better results. Such involvement includes: (a) making health professionals aware of the consumption of medicines and supplements; (b) providing a comprehensive medical record to all the needed individuals and parties; (c) informing any update on the health status; (d) caring about cleanliness from all health professionals and parties in any medical process; (e) choosing the best places for treatments and surgeries; (f) asking about any news on the health status; (g) requesting complete medical instructions; (h) acquire a proper understanding of any medical process needed; (i) establishment of medical standards by a full medical expert testimony; and (j) demanding criminal responsibility and persecution for individuals related to certain medical errors; etc.

Ten common recommendations for reducing/eliminating medical errors are provided in Table 5 [58]. Meanwhile, the errors should be disclosed without considering the consequences from blaming, negative emotions, expectations, and so forth in order to perform better management of these cases, refer to Figure 7 [63].

Table 5. The top 10 safety recommendations [58]. Abbreviations used: ESS, Endoscopic Sinus Surgery; and OSA, Obstructive Sleep Apnea. Reprinted with permission from Ref. [58]. 2004 Wiley Online Library.

1. ESS is a potentially high-risk surgery. The use of image-guidance has not been proven to reduce injury but may be considered.
2. Cranial and other major nerves are potential high-risk structures. Nerve monitoring has not been proven to reduce injury but may be considered.
3. Check cautery meticulously for intact insulation. Consider using a disposable cautery.
4. Ensure that allergy sera are clearly labeled and checked before administration. Have a second staff member or the patient confirm that the correct vial is used.
5. Develop and maintain a tracking system to ensure that the correct test is ordered, completed, and the results reviewed.
6. Have all consults, tests, and personnel in place prior to surgery. If there are relative contraindications to elective surgery, consider carefully before going forward.
7. When sophisticated equipment fails, it may be difficult to fix immediately. Have appropriate support for equipment and if possible test equipment prior to induction.
8. The perioperative and postoperative period is a high-risk interval. Risk factors for postoperative death may include narcotic use, developmental delay, and OSA.
9. Be aware of the potential for wrong site/wrong patient surgery, particularly in busy settings. Initial the surgical site and have a "time out" at the beginning of each procedure.
10. Eliminate concentrated epinephrine from the surgical field.

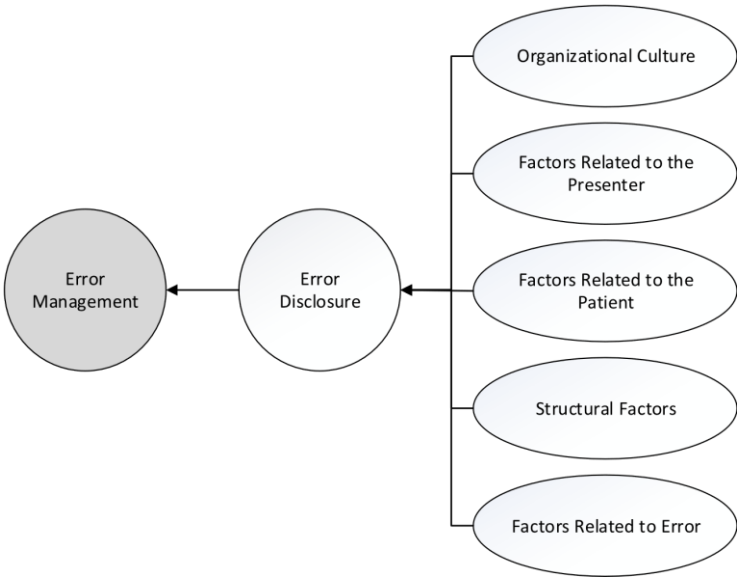

Figure 7. Managing errors and the factors and indexes comprising it [63].

Specific methods from AI and CV are applicable on human-related data, including hospital-based incident reports, exhaustive chart reviews, documented focused interviews, and surveys in order to comprehensively evaluate and summarize the possible errors at this level. The errors in this human-level are classified according to the location of the event (e.g., in the operating room), the professional involved (e.g., a physician or a pharmacist), the agent involved (e.g., intravenous drugs or oral drugs), the cognitive error (e.g., an error in vigilance or an error of judgment), and also by contributing system factors (e.g., poor

hand-offs, excessive workload, or poor equipment). These classification systems deliver important information but may be somewhat broad for the practical study of errors in a particular area of the field.

To analyze and plan to remediate the medical problems and errors in more detail and from the "software" and "hardware" perspective, it is first necessary to collect (and produce) diverse sufficient data related to the problems/errors. Next, the data needs to be analyzed, understood, learned, processed, and summarized based on the medical objectives. Various imaging techniques are employed for obtaining data: X-ray radiography, computed tomography (CT) scans, magnetic resonance imaging, ultrasound, bone scan, endoscopy, elastography, tactile imaging, thermography, medical photography, nuclear medicine functional imaging. For one-dimensional/signal types of data, the techniques are sensing systems that measure and deliver information, such as electroencephalography, magnetoencephalography, and electrocardiography. A typology of commonly used medical imaging modalities is illustrated in Figure 8 [64].

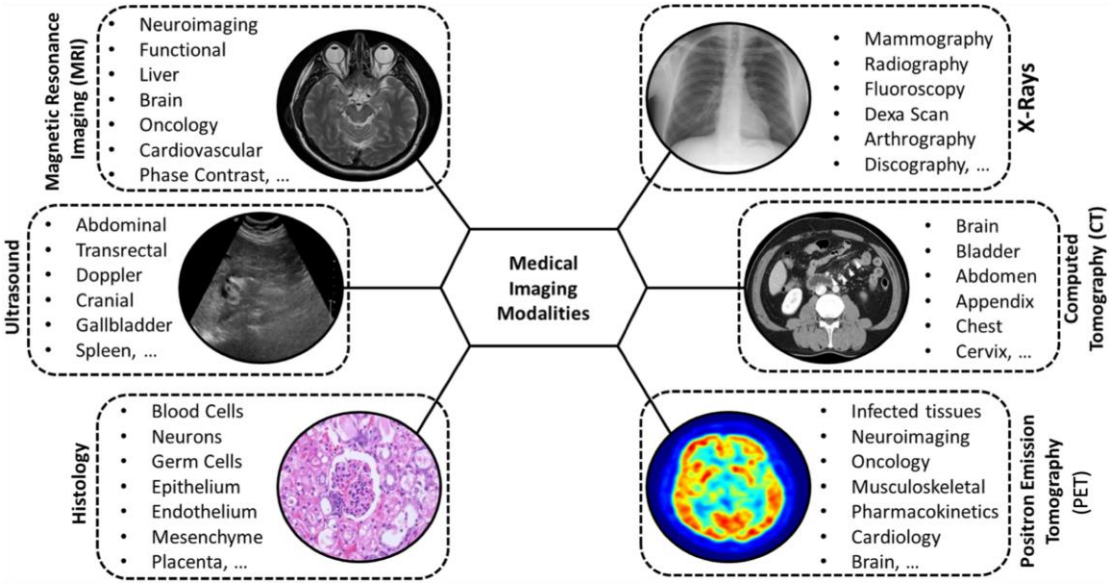

Figure 8. A typology of commonly used medical imaging modalities [64].

These data are presented with respect to time, location, etc. Strong classification systems enhanced with the state-of-the-art computing elements from AI/CV are required to perceive the medical data and specify their status with respect to errors. These systems should be capable of identifying the scopes of practice where errors happen. The "human-, software-, or hardware-level" detection and recognition systems in this context should be computationally strong (i.e., in terms of the computing resources, such as convolutional neural network) and knowledgeable (i.e., in terms of being trained on enough diverse data) to be able to find different kinds of medical errors and determine their impacts on the healthcare system.

In summary, medical errors are a part of the medical field with great importance and disastrous consequences. Screening and managing medical processes using the state-of-the-art technologies are critical for prevention, reduction, and elimination of all possible errors. Different kinds of entities in the medical domain, including "humans", "software", and "hardware" can have the role of reducing and preventing these errors as well as enhancing the respective operations.

3. Security Weaknesses of Medical Devices at Software and Hardware Levels

Over the last few years, healthcare administrations have been computerizing their provision of care that led to an increased number of networked medical devices and remotely data acquisition [37,65–70]. Due to such computerization, medical devices have

made excellent progress since five decades ago. These networked medical devices have enhanced the quality and accessibility of health treatments (leading to less medical errors) through ubiquitous computing. Moreover, these devices have transformed medical treatments and improved the lives of the masses through different innovations. The innovations include new areas of therapeutic and diagnostic treatments that help in achieving reliable healthcare facilities. Nowadays, medical devices are portable/wearable, networked, and capable of being employed for different medical operations. The quantity, quality, and diversity of medical devices create a great and promising environment for the future of medical field. Different classes of medical devices are shown in Table 6 [71].

Table 6. The medical device classes [71]. Abbreviations used: BGM, Blood Glucose Meters; and CGM, Continuous Glucose Monitoring. Reprinted with permission from Ref. [71]. 2017 Institute of Electrical and Electronics Engineers.

Medical Device Class	Attributes	Example Devices
Class 1	Common, low risk, and low complexity	Lancet and Dental Floss.
Class 2	More complex, greater risk to patient, and partially implanted	Syringe, Insulin Pump, and BGM.
Class 3	Fully implanted, greater risk, and regulate body function.	Artificial Pancreas, CGM, Replacement Heart Valves.

The connectivity of these devices to the Internet network has created the Internet of Medical Things (IoMT), which is the most demanding technology in the healthcare sector [72]. The medical type of Internet of Things (IoT) has made an excellent opportunity for the medical devices (with embedded computing engines) to interact with each other, the users (e.g., patients and physicians), and any other medical-related entity in the worldwide network. Through IoMT, many benefits are given to the devices and the users including, wireless communication, remote monitoring, high-speed transmission of clinical information from patients to clinicians (and vice versa), real-time diagnosis and therapy management, which are all aimed at improving patient care.

The overview of an exemplary healthcare system is delivered in Figure 9 [73], an example architecture for IoMT is given in Figure 10 [74], and samples of medical devices are shown in Figure 11 [75]. In "reference [37], the table number two" provides the information about a number of medical devices in the field. The devices covered are wearables (e.g., tracking with Bluetooth Low Energy or Wi-Fi communication medium), implantable devices (e.g., devices with Radio Frequency, Bluetooth Low Energy, Wi-Fi communication medium), and on-site equipment (e.g., using Wireless Local-Area Network communication medium).

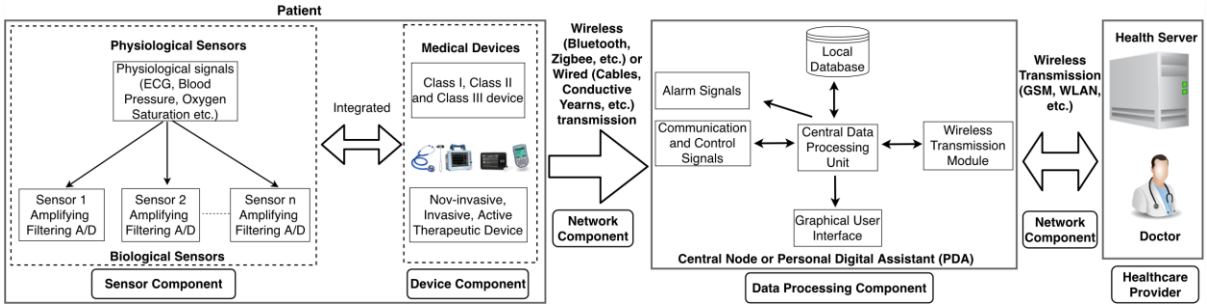

Figure 9. Overview of an example healthcare system [73]. Abbreviations used: ECG, Electrocardiogram; GSM, Global System for Mobile Communications; WLAN, Wireless Local Area Network; and A/D, Analog-to-Digital Converter. Reprinted with permission from Ref. [73]. 2021 Association for Computing Machinery.

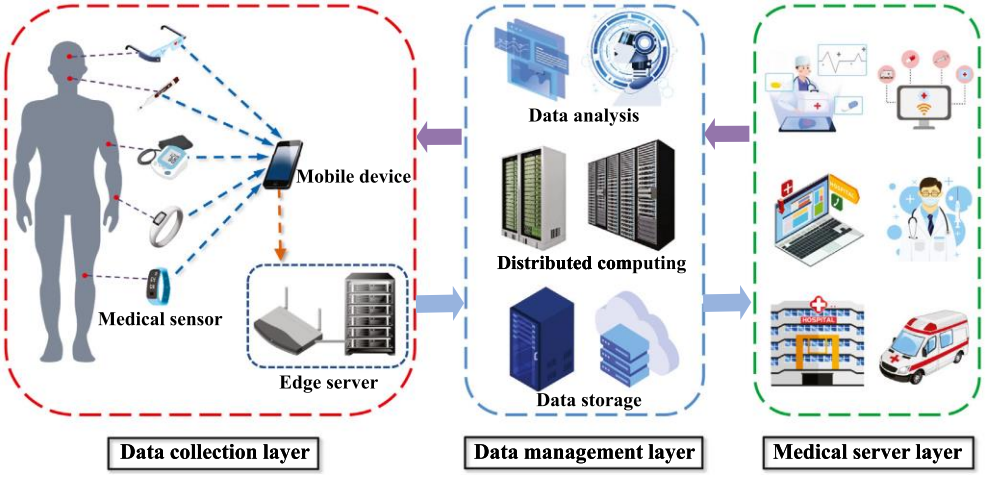

Figure 10. System architecture of the Internet of Medical Things (IoMT) [74]. Reprinted with permission from Ref. [74]. 2021 Association for Computing Machinery.

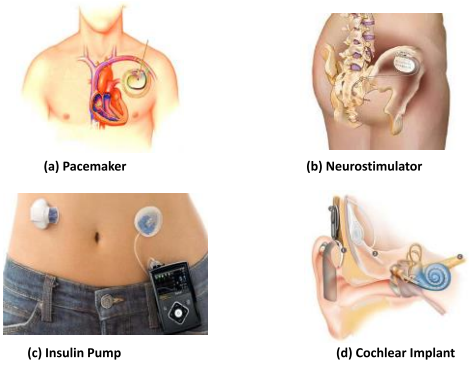

Figure 11. Implantable medical devices: (**a**) An artificial pacemaker implanted in a patient's chest with electrodes contacting heart muscles. (**b**) A Medtronic InterStimneuro-stimulation device for sacral nerve stimulation therapies. (**c**) A semi-implanted insulin pump monitors current glucose levels and delivers proper amount of insulins continuously. (**d**) A cochlear implant helps patients suffering hearing loss [75]. Reprinted with permission from Ref. [75]. 2016 Institute of Electrical and Electronics Engineers.

The devices in IoMT are managed in order to provide the appropriate services for various patients with as few medical errors as possible. In this network, health records/data are acquired from, generated by, and delivered to the respective authorized entities in the healthcare system via portals, medical servers, and health databases. The data are the most valued resource for any organization and for any application, especially in the medical field. With the help of IoMT devices, the medical information is exchanged between all possible entities in the network while considering energy efficiency and satisfactory performance. Different technologies are leveraged in these communications, such as WiFi, Bluetooth, Zigbee, Z-wave, radio-frequency identification, near-field communication, and ultra-wide bandwidth [76]. These medical devices include (but not limited to) glucometers, smart pen, blood pressure and heart rate monitors, implantable cardiac devices (pacemakers and insulin pumps), and wireless vital monitors.

The IoMT platform is not only beneficial to the patients but also to the facilitates of different departments in healthcare environment. As a result of this benefit, the budget for healthcare management and handling are reduced and it is used for other medical processes. However, alongside the advantages of IoMT, there are vulnerabilities, risks, and security issues behind every IoMT device that need to be considered [34,39,77–79].

The IoMT is disruptively shifting the paradigm of cybersecurity, privacy, and data protection toward new territories [80]. With ever increasing connection of new devices,

information gathering is becoming ubiquitous and deeply pervasive. Simultaneously, networks are becoming exposed to new threats with an unprecedented surface of risks. The implementation of IoMT systems comes with security and privacy challenges because of: (a) their highly dynamic nature; (b) the heterogeneous nature of hardware; (c) global connectivity; (d) changeable properties; (e) wide accessibility; and (f) the existing traditional and less effective security protocols are not suitable for the current and next generation of the devices used in these networks and systems [80,81].

These factors often result in IoMT ecosystems being physically unprotected and susceptible to manipulation by external parties. Therefore, there are a number of threats that can negatively affect IoMT devices. The possible threats can be mentioned as: manipulating communication channels, denial of service, physical threats, eavesdropping, and identity fabrication. During the IoMT system implementation, the primary security issue in three parameters of confidentiality, integrity, and availability as well as the layer-wise issues should be identified and resolved. Meanwhile, the security complications with respect to three primary technologies, namely machine learning, artificial intelligence, and blockchain should be addressed in the implementation processes.

One of the critical processes in the security of IoMT devices is anomaly detection [82]. It is about identifying data patterns that deviate remarkably from the expected behavior. Identifying an anomaly can determine the parameters of predictive maintenance, fault prevention, automation within this context. There are certain challenges for this process that need to be resolved, including data fusion, data volumes, data speed, and network/energy efficiency.

Anomaly detection in IoMT security is considered as a hard problem since it is required to find computation-accuracy-energy in a constrained environment. Various techniques from statistical analysis, time-series analysis, signal processing, supervised learning, reinforcement learning, deep learning, and so forth are employed to detect possible anomalies more effectively. Different data-based architectural environments (i.e., cloud, fog, and edge) should be studies due to their impacts on the detection process.

The software, hardware, and the transmitting/processing information by the IoMT devices are all at risk by different kinds of threats and have security weaknesses that can damage the function of devices and/or the transmitting/processing data, causing intentional (malicious) medical errors. Any vulnerable system operation or outdated software causes different sorts of security breaches in the network. Certain devices and systems in the network, such as pacemakers, X-ray machines and CT scanners are highly vulnerable for these matters. In other words, the healthcare system is in a thoroughly critical and concerning condition, refer to Table 7 [83].

Table 7. Status of healthcare system based on vulnerabilities [83].

Healthcare-Cybersecurity Condition	Description
Known Vulnerabilities Epidemic	Single legacy and medical technology can have over 1400 vulnerabilities
Vulnerabilities Impact Patient Care	One security compromise shutdowns patient care process
Premature/Over-Connectivity	Meaningful use of healthcare drives hyperconnectivity without secure design and implementation
Legacy Equipment	Equipment is running on old, unsupported, and vulnerable operating systems
Severe Lack of Security Talent	The majority of health delivery organizations lack full-time and qualified security personnel

As a practical example, the medical devices in the United States follow a process that integrates FDA guidance, regulatory decision making, post-market surveillance, and oversight with a typical product development life cycle. This life cycle is used as a framework for contextualizing the possible challenges and opportunities, especially with a particular focus on the development, deployment, operations, and maintenance phases. Manufac-

turers typically own the bulk of the device development phase, whereas the healthcare delivery organizations (HDOs) lead the procurement phase. Manufacturers and HDOs often share a responsibility for the remaining phases. The normal product life cycle, along with the challenges and the opportunities for the cybersecurity life cycle of medical devices are shown in Figures 12–14 [84].

The IoMT devices are constantly collecting and storing huge amounts of personal and sensitive information, which makes them very appealing targets for cyber criminals and it is the one of the easiest entry points for adversaries to attack due to presence of less defense mechanisms for them. The adversaries can steal medical records during their transmissions. Other attacks to launch on them are fooling user authentication, account harvesting, and poodle attacks. The databases in the network that contain the medical information of patients and the employment information of physicians are also in danger.

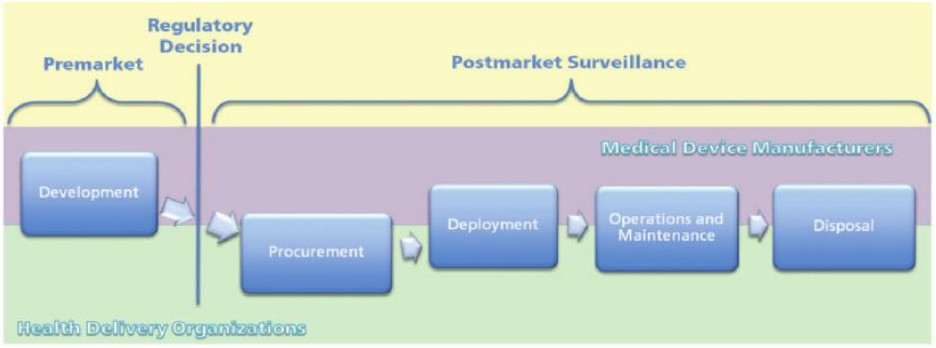

Figure 12. Medical device product life cycle [84].

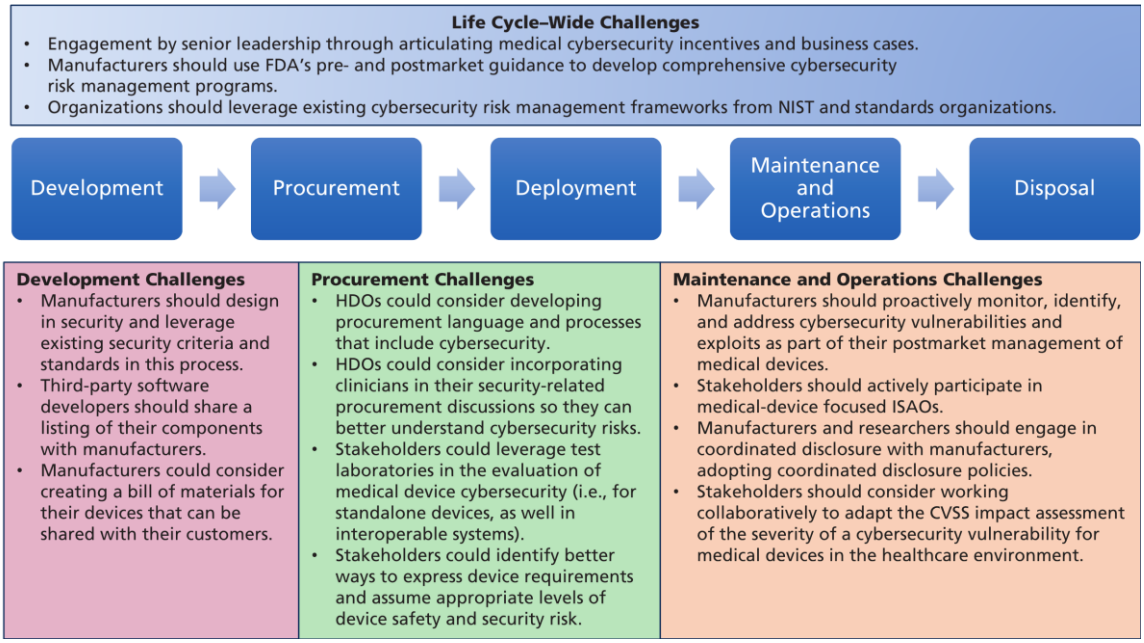

Figure 13. Summary of medical device cybersecurity life cycle challenges. Abbreviations used: CVSS, Common Vulnerability Scoring System; FDA, Food and Drug Administration; HDO, Healthcare Delivery Organization; ISAO, Information Sharing and Analysis Organizations; and NIST, National Institute of Standards and Technology [84].

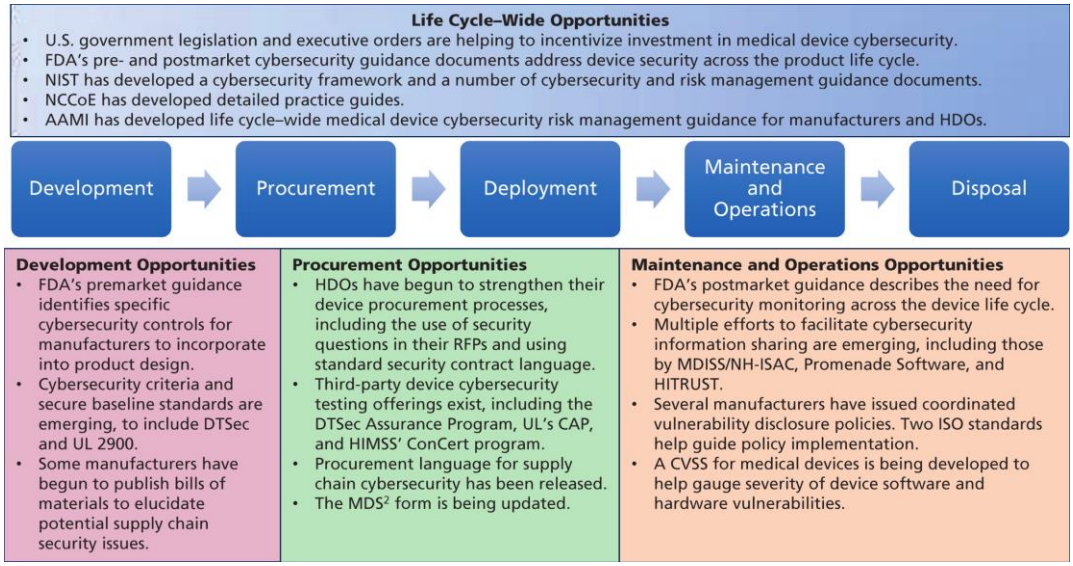

Figure 14. Summary of medical device cybersecurity life cycle opportunities. Abbreviations used: AAMI, Association for the Advancement of Medical Instrumentation; CVSS, Common Vulnerability Scoring System; DTSec, Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices; FDA, Food and Drug Administration; HDO, Healthcare Delivery Organization; HIMSS, Healthcare Information and Management Systems Society; HITRUST, Health Information Trust Alliance; ISO, International Organization for Standardization; MDISS, Medical Device Innovation, Safety and Security Consortium; MDS2, Manufacturer Disclosure Statement for Medical Device Security; NCCoE. National Cybersecurity Center of Excellence; NH-ISAC, National Health Information Sharing and Analysis Center; NIST, National Institute of Standards and Technology; and RFP, Request for Proposal [84].

In another threat strategy, the network is threatened by the Distributed Denial of Service (DDoS) attack from exploitation of a backdoor that causes jeopardizing both the devices and the data in the network. This attack is among the fastest growing and simple to conduct threats especially for IoMT, and it is really challenging to get tackled. In the IoMT networks, most of the devices are connected to the Internet and consequently they are exposed to various attacks from this channel.

Detection and overcoming problems in network traffic caused by the distributed denial of service attack have been researched more from angle of conventional terminal devices (e.g., personal computers, laptops, mobile devices, tablets, and servers). The mentioned situation is different from the IoMT environment in which there are numerous devices with lower levels of security and protection, leading to extreme growth in the generated DDoS traffic. So, it is required to study the IoMT security with focus on the DDoS attacks in more detail and introduce different sorts of respective attacks and countermeasures to the community. In this regard, a number of studies have already been completed. The authors in [85] proposed a conceptual network anomaly detection model based on the device classes that are dependent on individual device traffic characteristics.

The authors in [86] presented a DDoS traffic detection model that uses a boosting method of logistic model trees for different classes of IoT devices. Specifically, a different version of the model will be generated and applied for each device class, since the characteristics of the network traffic from each device class may have subtle variation(s). The IoMT devices can be categorized into four different classes in this context: Class 1—very high level of traffic predictability; Class 2—high level of traffic predictability; Class 3—medium level of traffic predictability; and Class 4—low level of traffic predictability. They show that device classes are helpful in more effective detection of DDoS traffic.

It has already been realized that botnets (such as Mirai) have used insecure devices from these networks to conduct DDoS attacks, especially for critical Internet infrastruc-

ture. This shows the importance of developing new defensive methods that can detect the malicious traffic in the networks. The authors in [87] demonstrated that leveraging different machine learning techniques (i.e., neural networks) for using IoT-specific network behaviors (e.g., limited number of endpoints and regular time intervals between packets) to inform feature selection can result in high accuracy DDoS detection in the network traffic. Practically, they showed that enhancing home gateway routers or other network middle boxes with low-cost machine learning algorithms to analyze their respective traffic data (i.e., flow-based and protocol-agnostic) is useful in automatic detection of sources of DDoS attacks from the IoT devices. Figure 15 displays an attack surface for medical devices in the Internet of Things [88]. The main elements related cyber vulnerabilities in the medical domain can be observed in Figure 16 [89].

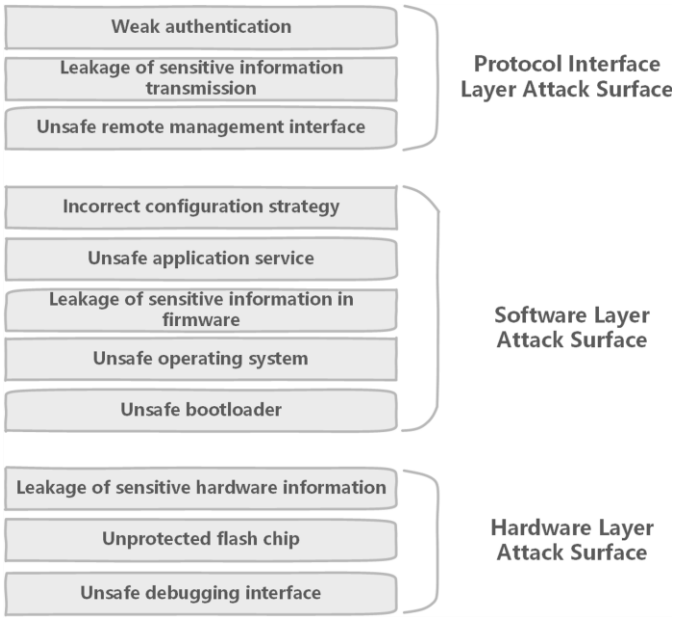

Figure 15. Attack surface of IoT device [88].

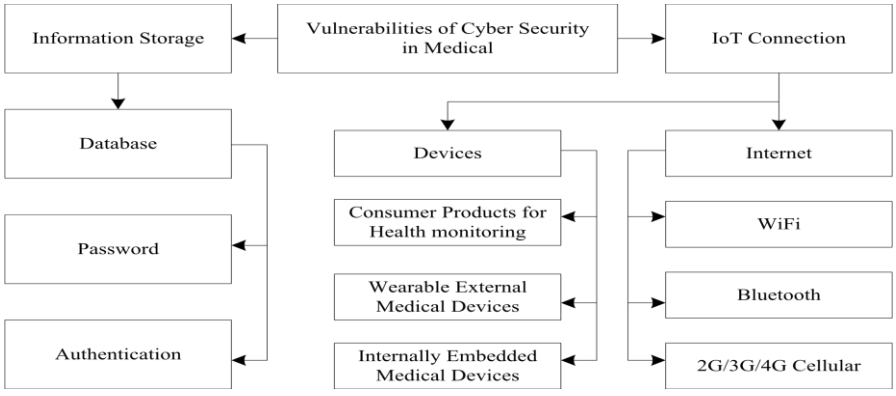

Figure 16. Main vulnerabilities of cybersecurity in the medical domain [89]. Abbreviations used: IoT, Internet of Things; and "N"G, Nth-Generation cellular network.

As it was mentioned earlier, the medical devices can be threatened by confidentiality, integrity, or availability. The confidentiality-based threats usually occur when an attacker obtains unauthorized access to certain sensitive information. With respect to the integrity-based threats, an adversary tampers sensitive information without having authorized access. In availability-based threats, the services to valid users are denied. In overall, the demonstrated cyber-attacks on the medical devices are mentioned as: (1) firmware

modification attack; (2) eavesdropping attack; (3) sniffing attack; (4) information disclosure attack; (5) man-in-the-middle attack; (6) unauthorized access and spoofing attack; (7) replay attack; (8) tampering and modification attack; (9) denial of service, resource depletion, and jamming attack; (9) side-channel analysis attack; and (10) hardware Trojan (i.e., malicious hardware modification), buffer overflow, brute force, grey-hole, sybil, masquerading, and other emerging attacks. A summary of these attacks are in "reference [37], tables three to fourteen along with eighteen to twenty-one".

In a IoMT platform, prevention of cybersecurity threats should have the same importance as medical treatments. Regardless of the quality, effectiveness, and strengths of medical processes, if an attack is executed successfully on the platform, a malicious (intentional) medical error is produced, and then most (or even all) processes become useless. As a result, manufacturers and health care providers should consider identification, detection, and prevention mechanisms for different kinds of attacks at multiple computing layers of the entities in the network. Despite the presence of any defense mechanism, all users should practice the necessary cyber defenses to mitigate security weaknesses. Therefore, a comprehensive collaboration across all stakeholders (including patients and other end users, health care facilities, independent health care providers, and manufacturers of medical devices) is extremely required to ensure the IoMT is secured.

In summary, we have a greater number of networked medical devices, especially to the Internet, and remotely data acquisition due to the great demand for computerization of medical processes. Excellent benefits are provided to the patient care through this transformation, such as high speed and quality transmission and assessment of medical information. Besides this positive aspect, there comes various security weaknesses related to the devices and their data that should be corrected.

4. Artificial Intelligence/Computer Vision (AI/CV) Technologies in Medical Applications

The research areas of computer science, specifically artificial intelligence, have made continuous progress and enhancements in computation speed and performance. AI broadly and clearly benefits modern society for various applications, such as forecasting weather, recognizing faces, detecting fraud, and deciphering genomics [90]. However, AI's future role in medical practice remains less clear, especially how AI can reduce/eliminate non-intentional and intentional (malicious) medical errors. Any classic medical device (e.g., prosthetics, stents, and implants) becomes smart using a computing/processing element, creates an IoMT by connection to the Internet, and contains knowledge through having an AI module. AI enables and enhances four main features in medical devices, Prediction, Prevention, Personalization, and Participation [4,91–93], that significantly strengthen the medical operations and possibly reduce/eliminate medical errors.

Machines (computers) learn to detect and compute undiscoverable patterns from massive datasets (i.e., big data) using layered mathematical and statistical models (i.e., algorithms). Recently, the algorithms from AI have been applied in various applications, through a variety of shallow and deep artificial neural network configurations, to solve complex problems. The deep neural networks from the area of deep learning, especially convolutional neural networks (CNNs), have received significant interest from research and funding agencies in academia and industry [94]. Deep Learning is a state-of-the-art technique to make an inference on extensive or complex data. The major progresses in the field of AI are graphically displayed in Figure 17 [95]. The difference between usage of neural networks and the other AI approaches is graphically shown in Figure 18 [96]. We can see a simple architecture for a neural network in Figure 19 [97].

These AI elements have certain requirements: the availability of powerful and cost-effective computing (processing) hardware and software, advancements in personal and mobile devices, the prevalence of large datasets (with a number of them in the cloud), registration of wearable and IoT devices, the expansion of open source coding resources, inclusion of novel human-machine interfaces, and the combination of different methods. Possessing large and diverse dataset(s) is extremely critical for training a deep neural

network. Without comprehensive training, the neural network is not able to analyze and recognize different kinds of data.

Since data acquisition may not provide all the data that are needed, defined data augmentation techniques are used to generate synthetic data, such as applying generative adversarial network (GAN) [98,99]. GANs have been of interest to the computer vision community for the past few years. Their most remarkable impacts are on plausible image generation, image-to-image translation, and facial attribute manipulation. It is important to have a stabilized training for GANs that they can generate high-quality and diverse images. The block diagram for a GAN is displayed in Figure 20 [100].

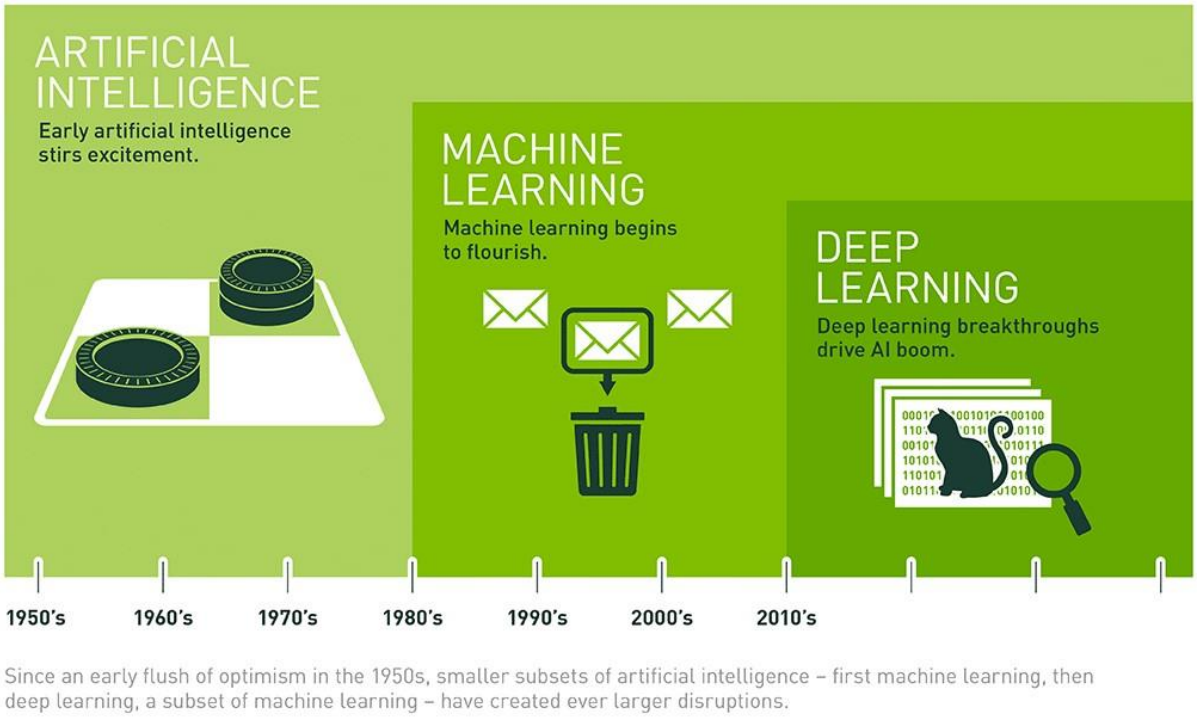

Figure 17. The major progresses in the field of artificial intelligence AI [95].

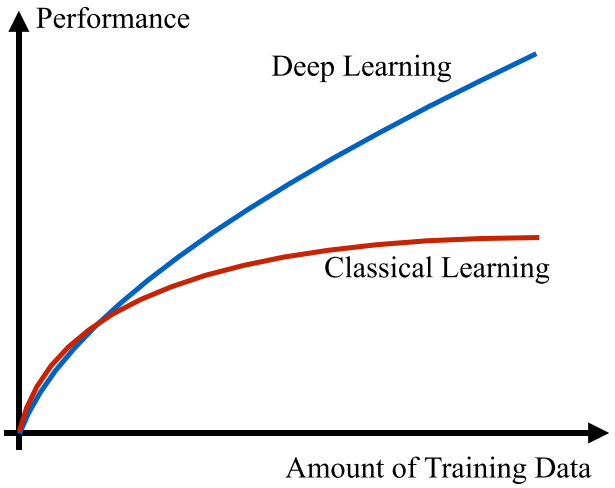

Figure 18. Classical and deep learning comparison [96]. Reprinted with permission from Ref. [96]. 2019 Institute of Electrical and Electronics Engineers.

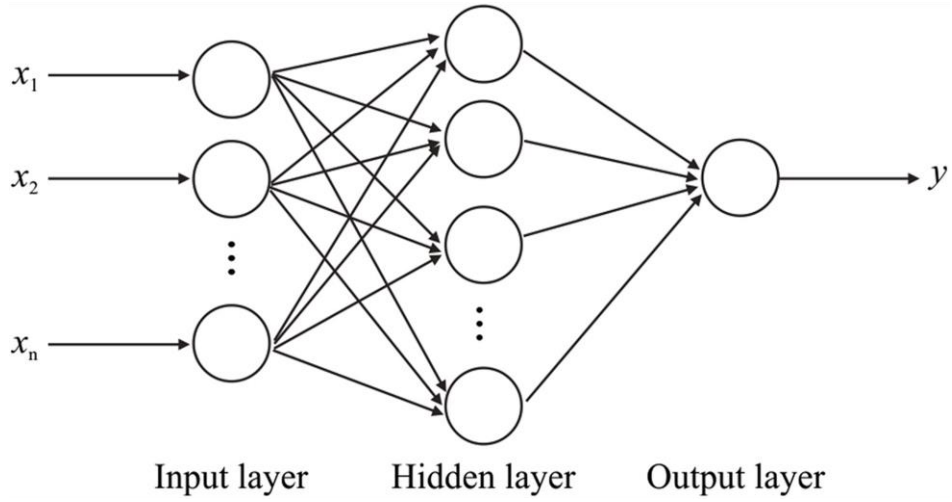

Figure 19. A simple artificial neural network architecture [97].

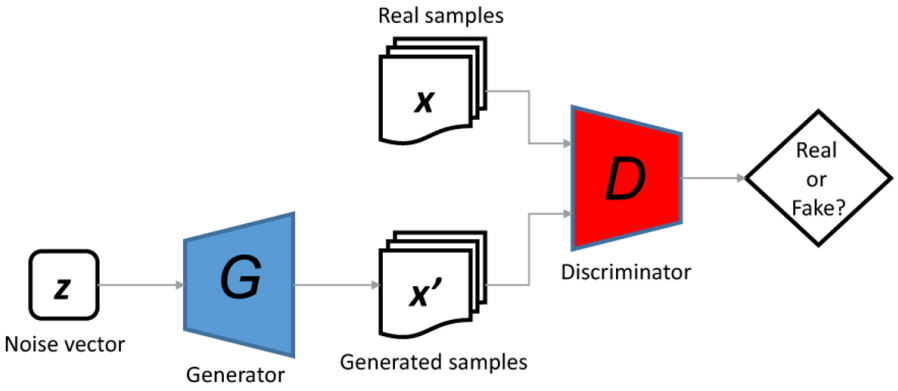

Figure 20. The general structure of generative adversarial networks [100].

CNNs help to strengthen and create a connection between the processes of feature extraction and classification. They aim to transform the high-dimension input image into low-dimension, yet highly abstracted semantic output. The enhancements in their number of layers, architectures, and complex computations have brought near-human accuracy in many classification and recognition applications.

Meanwhile, the deep neural networks have been made (self)-explanatory in emerging applications in order to overcome their non-transparency, non-traceable predictions (by humans), and possible biases in their functionalities (caused by less diverse and artificial training data). The (self)-explainable property points out the connection between input and output and represent (in a simplified way) the inner structure of neural network as a black box.

Running these networks on capable computing hardware resources deliver high-performance recognition and classification. These advanced neural networks have the strength of delivering perfect results with sufficient training and tuning. The deep neural networks have made prominent achievements in computer vision, specifically for image classification, object detection, and image segmentation.

In more detail, the AI-based computer vision methods provide: (i) object recognition in order to determine whether image data contains a specific object; (ii) object detection in order to localize instances of semantic objects of a given class; and (iii) scene understanding to parse an image into meaningful segments for analysis. These CV algorithms can perform automated extraction of information from images, including three-dimensional models, camera positions, object locations, group contents, and so forth. An example of different

tasks completed by CV is shown in Figure 21 [101]. Correcting the mistakes of AI/CV algorithms during training enhances the confidence of the respective predictive models.

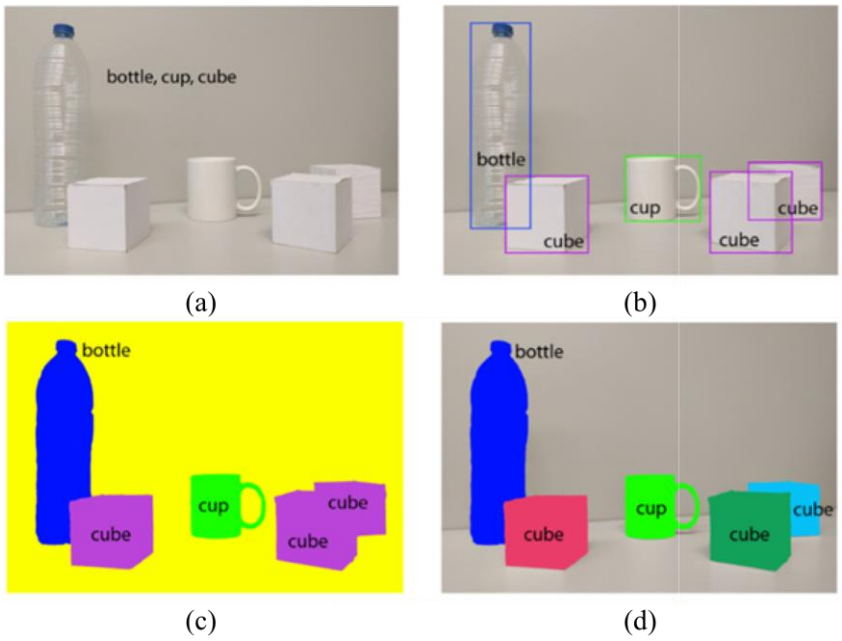

Figure 21. An example of different visual perception problems: (**a**) image classification, (**b**) object detection, (**c**) semantic segmentation, and (**d**) instance segmentation [101].

AI/CV have been successfully applied for detection of atrial fibrillation, epilepsy seizures, and hypoglycemia, as well as diagnosis of diseases based on histopathological examination or medical imaging (i.e., image analysis in radiology, pathology, and dermatology) with having improved speed, accuracy, and assessment. This demonstrates the efficiency of AI/CV in reducing/eliminating medical errors. Therefore, there is an established foundation for applying AI/CV on all areas in the medical field. A sample trend for applying AI on medical tasks is displayed in Figure 22 [102]. Major phases for introducing AI in a medical workflow are shown in Figure 23 [64].

The AI/CV-based medical systems have the abilities to identify different sorts of medical data, with even more accuracy and intelligence than humans, for various medical processes (in different specializations) and reduce/eliminate their possible errors. Enough knowledge and large diverse data are important factors for their desirable operations. Having AI/CV medical software, with their reasoning, understanding, learning/experiencing, and decision-making abilities, helps doctors to complete medical procedures successfully, even without requiring direct assistance from specialists. The structure and the computing elements (e.g., data acquisition and classification system) of an AI/CV system for combatting coronavirus disease 2019 (COVID-19) are shown in Figures 24–26 [103–105].

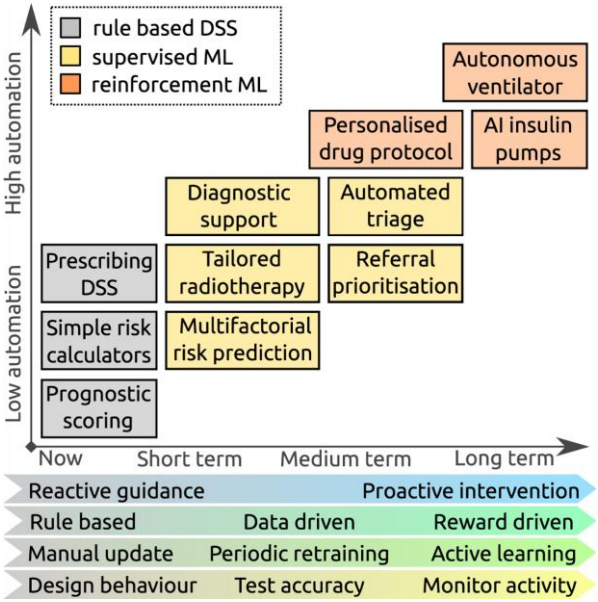

Figure 22. Expected trends in machine learning research: boxes show representative examples of decision support tasks that are currently offered by rule-based systems (grey), and hypothetical applications of ML systems in the future (yellow and orange), demonstrating increasing automation. The characteristics of the ML systems that support these tasks are anticipated to evolve, with systems becoming more proactive and reward driven, continuously learning to meet more complex applications, but potentially requiring more monitoring to ensure they are working as expected. Abbreviations used: ML, Machine Learning; AI, Artificial Intelligence; and DSS, Decision Support Systems [102].

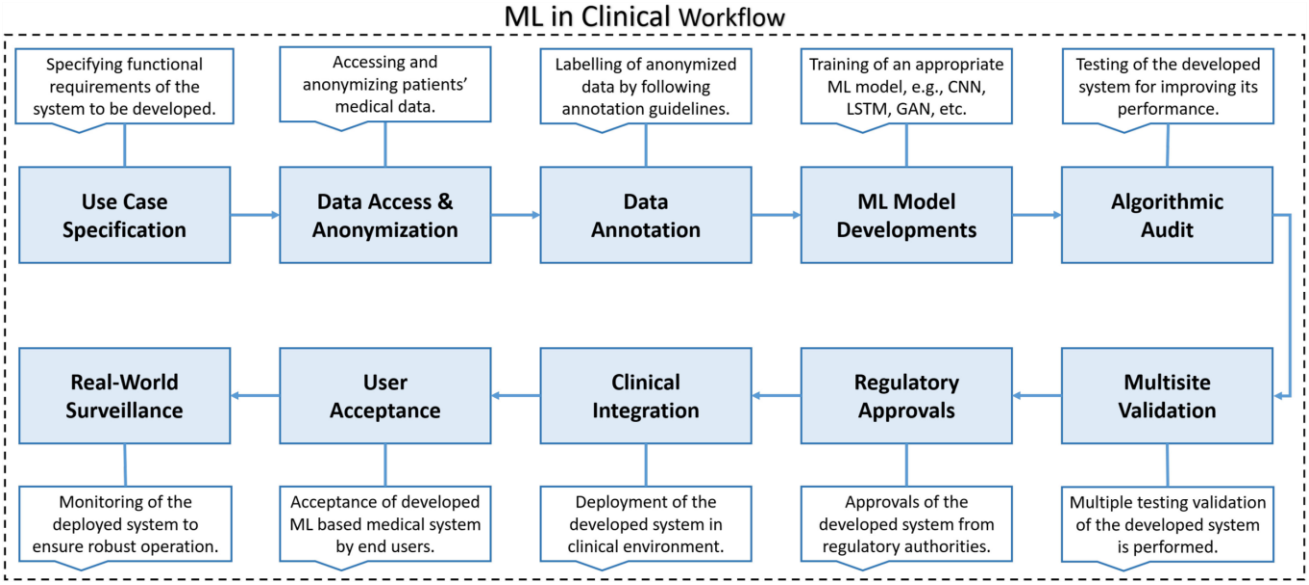

Figure 23. The illustration of major phases for development of machine learning based healthcare systems. Abbreviations used: ML, Machine Learning; CNN, Convolutional Neural Network; LSTM, Long Short Term Memory networks; and GAN, Generative Adversarial Network [64].

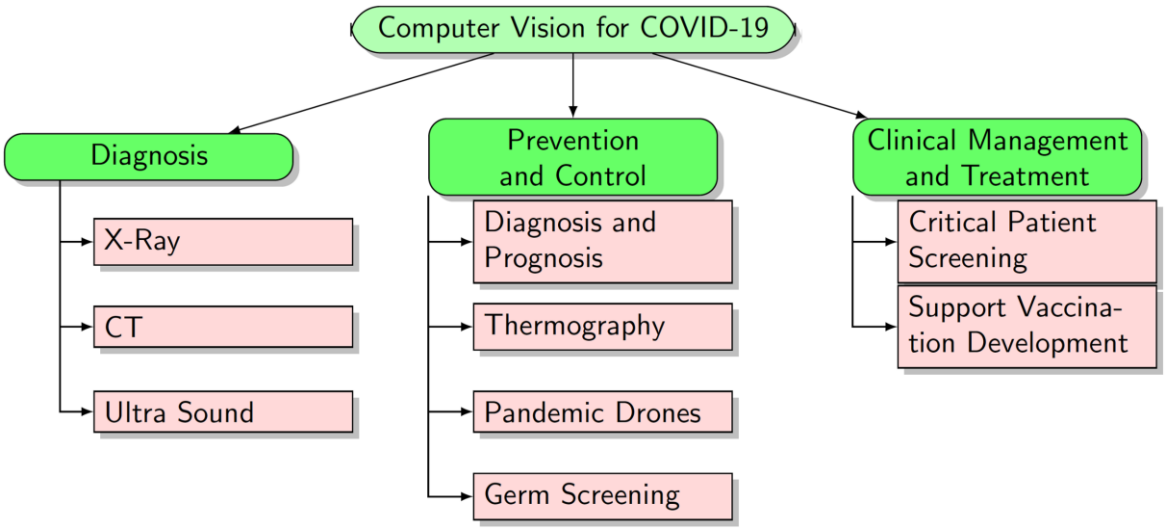

Figure 24. Classification of computer vision approaches for COVID-19. Our survey classifies COVID-19 related computer vision methods into three broad categories [103]. Abbreviations used: COVID-19, Coronavirus disease 2019; and CT, Computed Tomography.

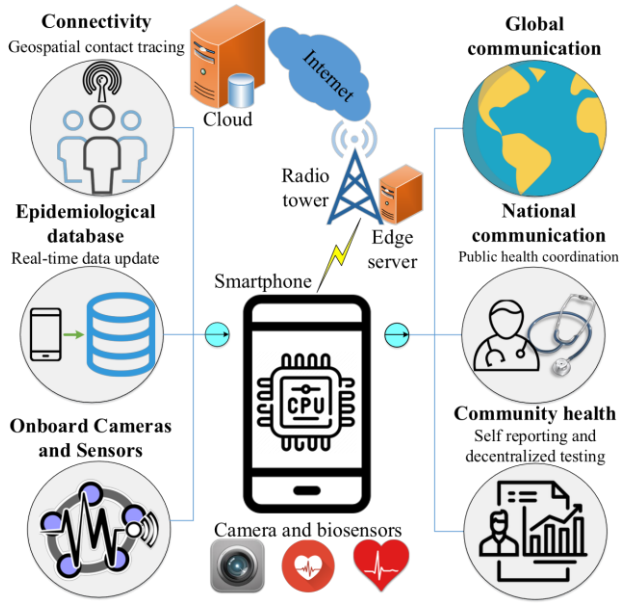

Figure 25. An AI-based framework using mobile phones for COVID-19 diagnosis and surveillance [104].

A combination of AI/CV medical systems and physicians can noticeably reinforce the quality, quantity, and performance of medical tasks and reduce/eliminate their errors. This opportunity tackles many of the issues related to the shortage or lack of doctors and specialists with acceptable expertise and experience in different medical areas. It also reduces the waiting time and the execution time of medical tasks. Other benefits from this combination are the decrease in the medical costs and the medical inaccuracies, reduced complications, a faster registration process of patients, a preserved history of patients for referral, and easier and more efficient communications between the medical entities (e.g., hospital and dispensary). An overview of how AI can contribute into the medical field is illustrated in Figure 27 [105]. Different potential roles of AI-based technologies in healthcare are shown in Figure 28 [5].

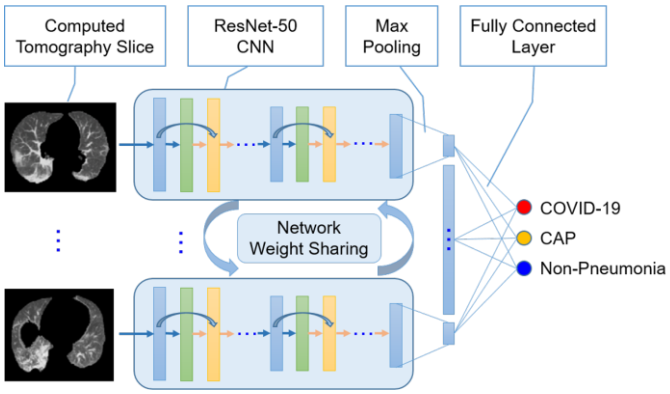

Figure 26. Illustrative architecture of the COVNet model for COVID-19 detection using CT images. Max pooling operation is used to combine features extracted by ResNet-50 CNNs whose inputs are CT slices. The combined features are fed into a fully connected layer to compute probabilities for three classes, i.e., non-pneumonia, community acquired pneumonia, and COVID-19. The predicted class is the one that has highest probability among the three classes [105]. Abbreviations used: ResNet-50, Residual Network with 50 deep layers; CNN, Convolutional Neural Network; COVID-19, Coronavirus disease 2019; and CAP, Community Acquired Pneumonia.

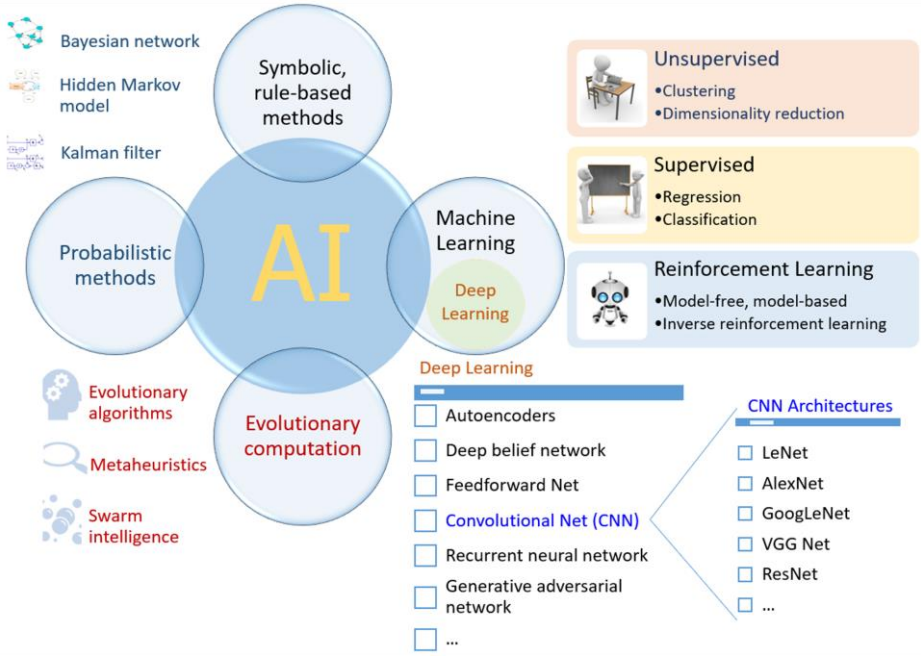

Figure 27. An overview of common AI methods where machine learning constitutes a key ingredient. The development of deep learning, a subset of machine learning, has contributed significantly to improving the power and capability of recent AI applications. A number of deep learning-based convolutional neural network (CNN) architectures, e.g., LeNet, AlexNet, GoogLeNet, Visual Geometry Group (VGG) Net and ResNet, have been proposed and applied successfully in different domain, especially in the computer vision. Other techniques such as autoencoders and recurrent neural networks are crucial components of many prominent natural language processing tools. The deep learning methods in particular, and AI in general, may thus be employed to create useful applications to deal with various aspects of the COVID-19 pandemic [105]. Abbreviations used: AI, Artificial Intelligence.

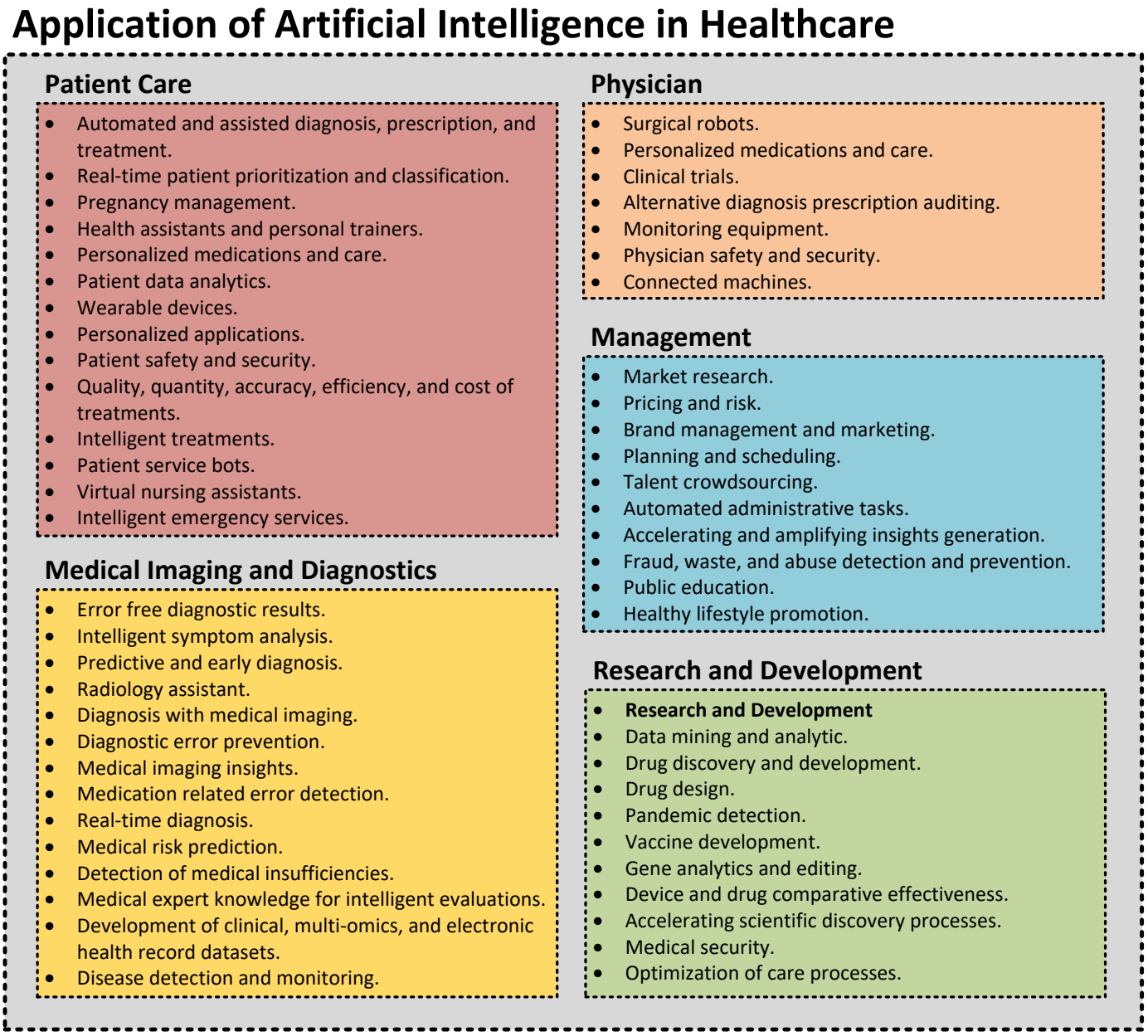

Figure 28. Application of artificial intelligence in healthcare.

In addition to AI/CV, the electronic medical systems employ wireless technologies, information technologies, human–machine interface technology, and medical care-specific technologies for greater functioning. While diagnostic confidence never reaches the maximum, combining AI/CV machines with physicians reliably and significantly enhances system performance and reduces/eliminates errors. The AI/CV medical systems are implemented and/or executed in different hardware environments, including graphical processing unit, application specific integrated circuit, field programmable gate array, and the new generations of hardware accelerators [101,106–110].

In summary, AI/CV optimizes quantity, quality, and accuracy of medical diagnoses and testing, enhances correctness of medical decisions and prescriptions, strengthens care trajectory of chronic disease patients, suggests precision therapies for complex illnesses, reduces medical errors, improves subject enrollment into clinical trials, etc. Despite the advantages provided by AI/CV for medical systems, it is possible to observe challenges in certain parts, including medical ethics issues (i.e., threatening patients' preferences, safety,

and privacy), responsibility for medical errors, and risks of system failures that demand novel and effective solutions.

5. Cyber Attacks and Defenses in Medical Domain

Medical devices are one of the widely adopted elements in the healthcare industry aiming to improve the quality of service for both patients and healthcare personnel [111,112] and reduce/eliminate medical errors. These devices can monitor and manage different health conditions of patients automatically without any manual intervention from the medical professionals. In fact, instead of keeping patients in hospitals, these devices are capable of constantly monitoring the patient's health in real-time, while offering them better physical flexibility and mobility.

A number of these devices are medical robots (i.e., surgical robots, nursing robots, etc.). Also, they can be used for assistance in recording patient's medical conditions and organizing patient's records in real-time. These diverse devices can connect with each other as well as the organization's network. With increasing communication capabilities, they are able to speed up the transfer of medical information.

Connecting these devices to a network constructs a novel medical cyber–physical system (MCPS) [111,113]. An MCPS integrates many entities for performing medical-based computational, networking, and physical processes. The MCPS can satisfy the needs associated with the increasing number of patients, including accuracy, reliability, efficiency, and effectiveness of the health-care domain. The medical CPS should have unique characteristics in terms of the running applications, the networking capabilities, and the complex physical dynamics of human body suitable for the designated medical processes.

In simple words, the major goal of MCPS is to enhance the efficiency, quantity, quality, and accuracy of patient care by ensuring personalized treatment in a safe way. It is important to note that the traditional medical equipment and the novel medical devices have compatibility in terms of accuracy, speed, communication, and the other interactive parameters to make sure that the medical processes are completed as timely and operatively planned. The Internet connectivity of the medical devices provides even more efficiency to the requirements associated with the increase in the number of patients. The mechanism for connection of a medical device to the Internet is displayed in Figure 29 [114], an example of an Internet-of-Things system is shown in Figure 30 [114], and the security and privacy taxonomy of IoMT is provided in Figure 31 [33].

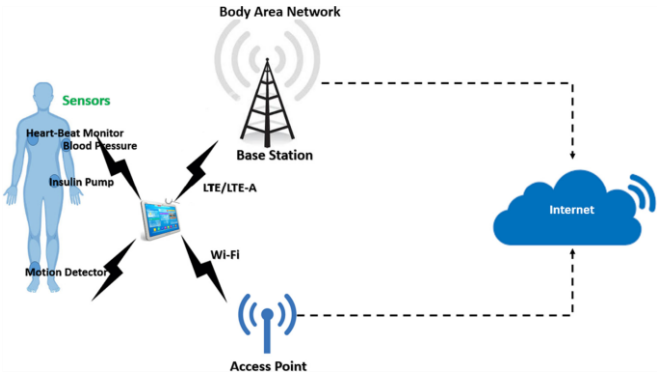

Figure 29. Body area network [114]. Reprinted with permission from Ref. [114]. 2020 Elsevier. Abbreviations used: LTE, Long Term Evolution; and LTE-A, Long Term Evolution-Advanced.

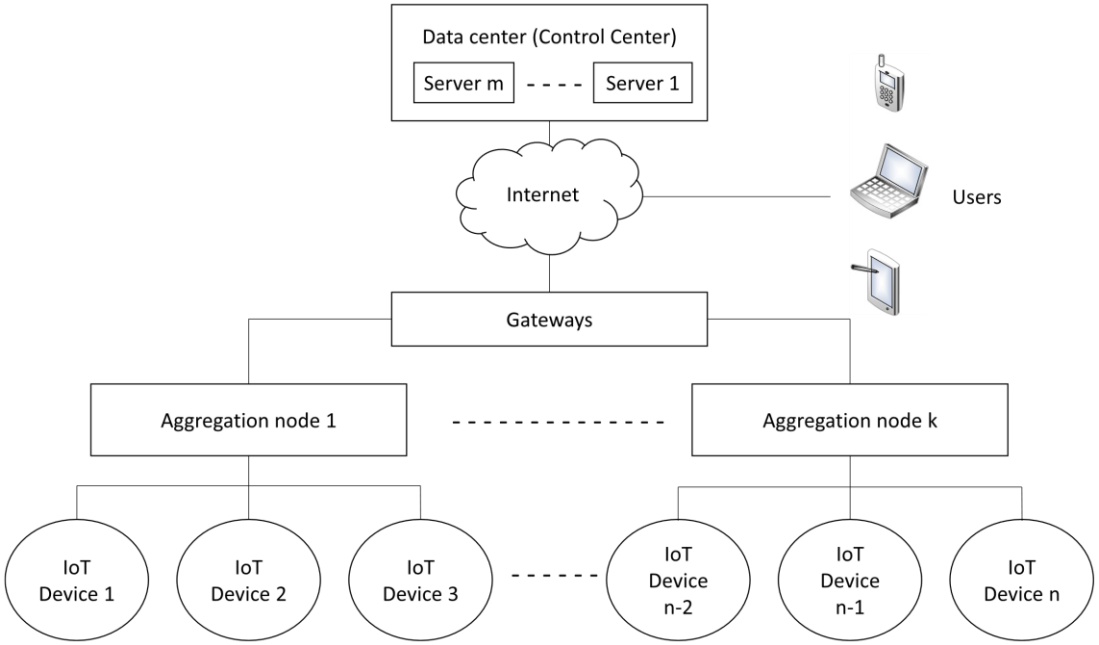

Figure 30. An example of an Internet-of-Things system with "n" IoT devices, "k" aggregation nodes, and "m" servers [114]. Abbreviations used: IoT, Internet of Things. Reprinted with permission from Ref. [114]. 2020 Elsevier.

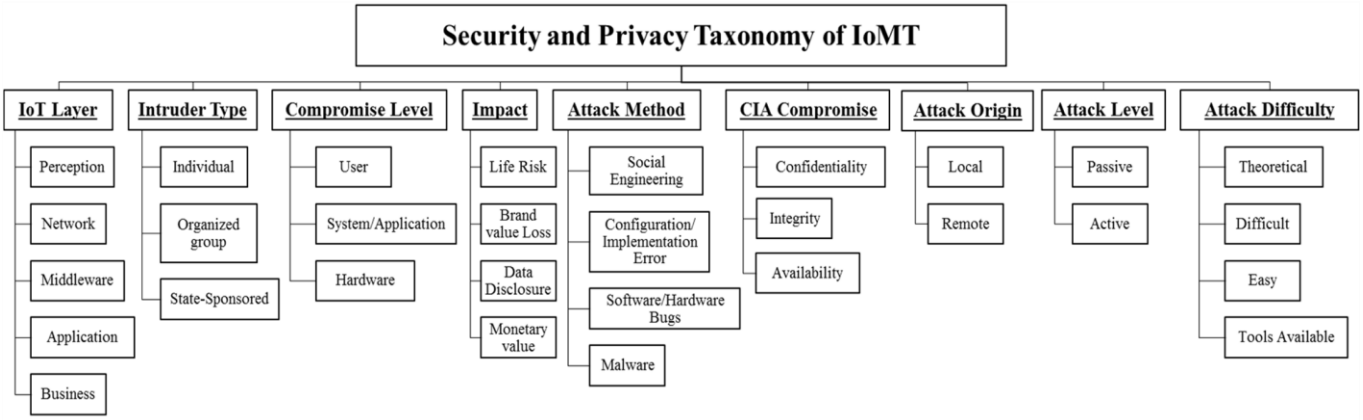

Figure 31. Security and privacy taxonomy of IoMT [33]. Abbreviations used: IoMT, Internet of Medical Things; IoT, Internet of Things; and CIA, Confidentiality, Integrity, and Availability. Reprinted with permission from Ref. [33]. 2017 Institute of Electrical and Electronics Engineers.

With more medical devices being connected to each other and to the other medical entities, the security of this Internet-based MCPS (i.e., IoMT) requires noticeable attentions. Any technology incorporated in the medical system and related to the growth of network connectivity requires more considerations from the security perspective. In fact, the more medical devices there are in the network, the more opportunities are available for the adversaries, and the more malicious (intentional) the medical errors that are created. The attacks at the computing-level cause changing the functionality and the data, or stealing the information, while their impacts at the medical application level are medical errors with severe and life-threatening effects. Due to the catastrophic health consequences, any security issue concerning healthcare systems should be addressed aggressively and proactively.

In recent years, several healthcare-based security issues have been reported both in the media and the academic community. For the advancements in cyber attacks further exacerbated this situation, refer to Figure 32 [115]. A story popularized in the media held

that doctors disabled the wireless connectivity of a former U.S. Vice President's pacemaker to protect it from being hacked. Adding to this story, researchers demonstrated several cyber-attacks on commercial products, including attack scenarios of remotely disabling and reprogramming the therapies performed by an implantable cardiac defibrillator. More advancements involved in the MCPS/IoMT demands more attention to the security of devices in the network. Any defect stems from adaptation of new techniques (from different areas) leads to a malicious attack, an intentional medical error, with life-threatening outcomes. Moreover, the requirements of updating these techniques make the protection mechanism even more challenging.

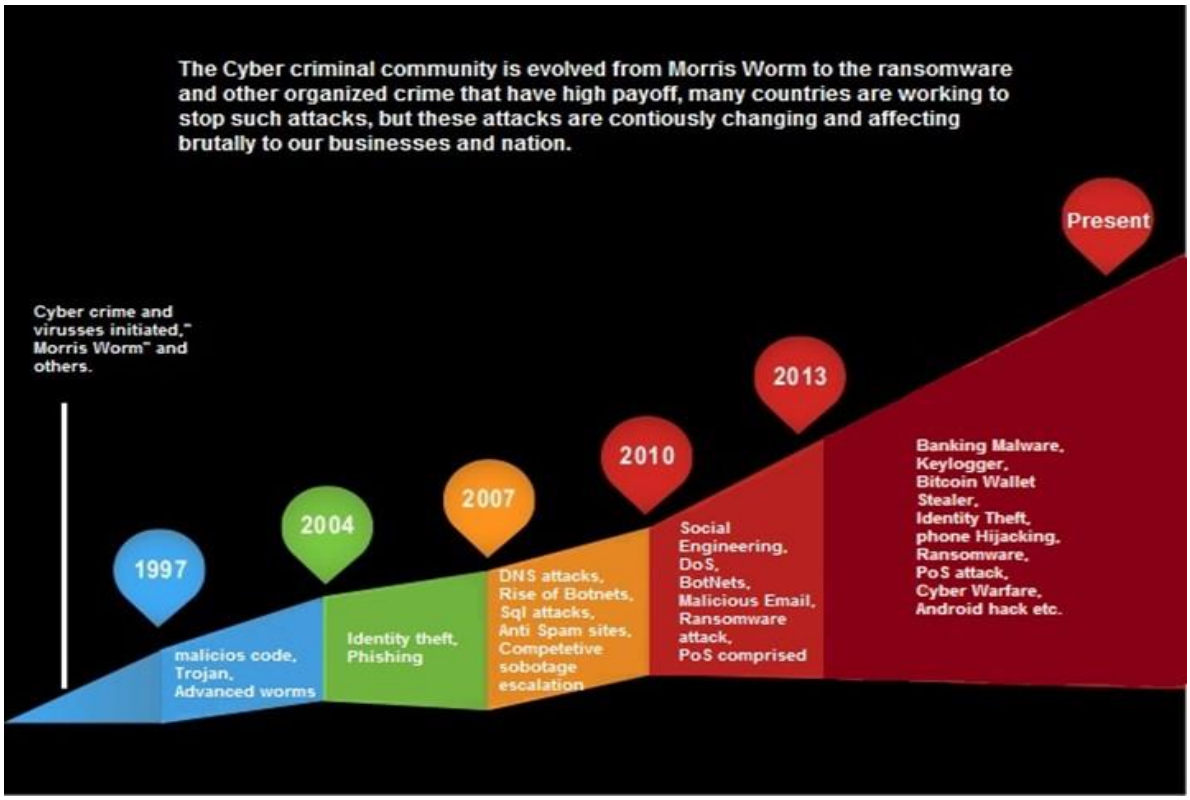

Figure 32. The advancements in cyber attacks over time [115]. Abbreviations used: DNS, Domain Name System; SQL, Structured Query Language; DOS, Denial of Service; Botnet, Bot Network; and POS, Point-of-Sale.

There are two main reasons for the vulnerability of connectivity: (1) the information communicated among medical devices is highly sensitive and private to both medical organizations and patient. For this sake, such sensitive data is a valuable target for cyber-criminals. (2) the infrastructure of MCPS/IoMT is often complicated due to the large number and diversity of medical devices, especially Internet-enabled devices, which are vulnerable to a broader range of cyber threats. Both passive attacks (eavesdropping of the wireless communication) and active attacks (impersonation and control of the medical devices to alter the intended therapy) can be successfully launched using public domain information and widely available off-the-shelf hardware.

Alongside the networking and software attacks, the medical devices can also be the target of hardware attacks (i.e., hardware-based intentional medical errors). Different layers of hardware platforms (i.e., from device technology to architecture) and various entities in the integrated circuit (IC) supply chain are targeted for launching the hardware attacks. In addition, there are diverse threat models for this purpose, such as reverse engineering, hardware Trojan, side-channel attack, and intellectual property privacy [43,116]. Figure 33 shows the entities in the IC supply chain to be selected for intrusion and executing malicious

operations [117]. The crafted attacks from these entities can cause different payloads, such as leakage of information, malfunctioning, performance degradation, energy waste, etc.

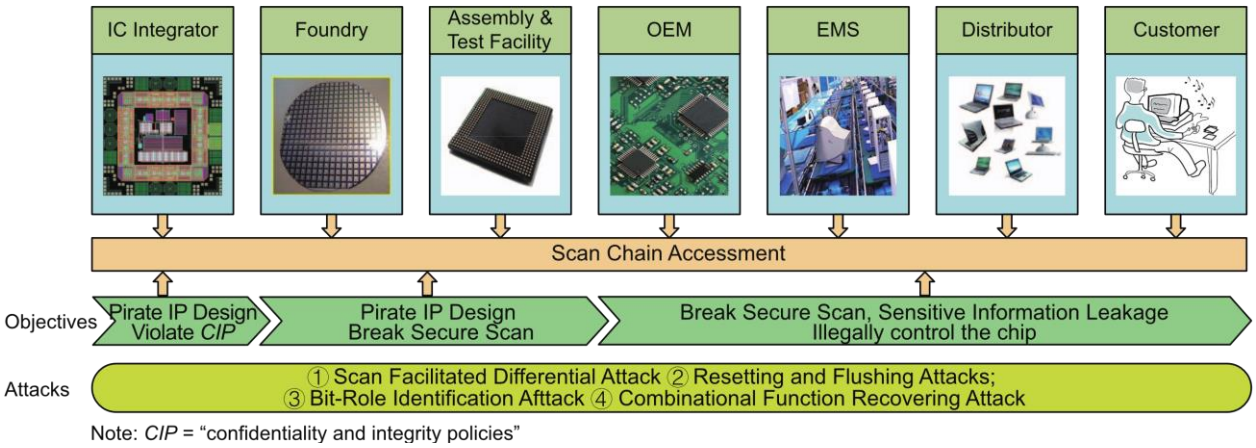

Figure 33. Attacker's objectives throughout integrated circuit (IC) supply chain [117]. Abbreviations used: IC, Integrated Circuit; OEM, Original Equipment Manufacturer; EMS, Electronics Manufacturing Services; and IP, Intellectual Property. Reprinted with permission from Ref. [117]. 2017 Institute of Electrical and Electronics Engineers.

The medical devices are remotely exploitable through the communication media (e.g., Wi-Fi, Bluetooth, and Zigbee) and attackers can easily eavesdrop on the communication channel to access the transmitted information. The medical data can be stolen from hospital websites, electronic medical recording systems, communication systems, and picture archives. This wide attack surface is the root of interest for adversaries to intrude and create malicious medical errors. The data are subject to use for patient information leakage, misdiagnosis, and mistreatment, leading serious danger to the physical and mental health of patients. The characteristics of possible attacks are delivered in Figure 34.

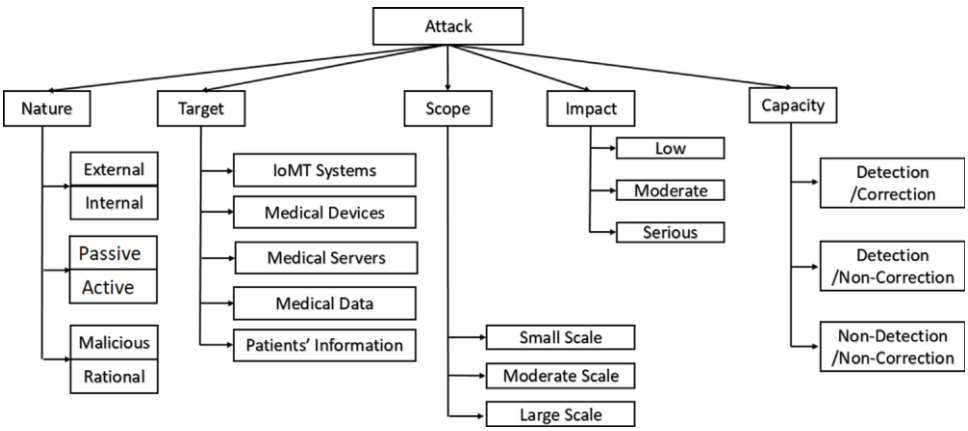

Figure 34. Characteristics and profiles of attackers and its corresponding impact [114]. Abbreviations used: IoMT, Internet of Medical Things. Reprinted with permission from Ref. [114]. 2020 Elsevier.

Similar to other distributed networks, MCPS/IoMT also suffer from insider attacks, where the intruders have authorized access to the network resources, resulting in the leakage of patient information. Without timely detection, insider attacks cause a network to be paralyzed. So, there is a necessitation for defending MCPS/IoMT against various attacks, especially insider threats (i.e., each medical device can be considered as a network node).

Unfortunately, there is no comprehensive security solution available in the industry and research community to mitigate the emerging cyber-attacks on healthcare systems. The healthcare domain is increasingly facing security challenges and threats due to numerous

design flaws and the lack of proper security measures in healthcare devices and applications. The IoMT devices have insufficient or even no protection and defense against different kinds of software and hardware attacks. The medical field requires the immediate attention of the security research community to develop the respective countermeasures. The researchers in the field have proposed a few countermeasures (e.g., privacy-preserving communication protocols, encrypted databases, etc.), but they cannot address the overall attack surface in healthcare systems. The characteristics of possible defenses are shown in Figure 35.

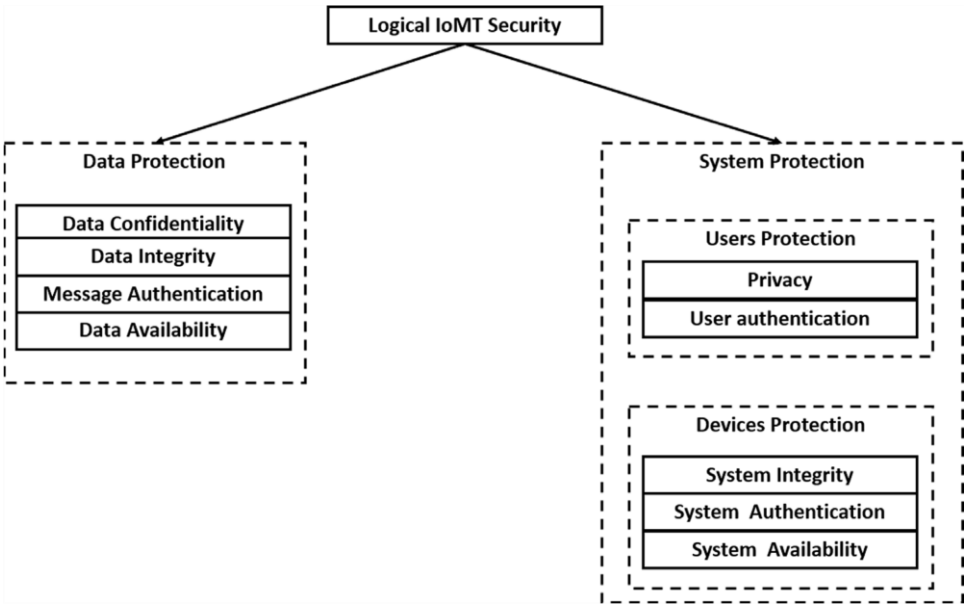

Figure 35. IoMT security goals [114]. Abbreviations used: IoMT, Internet of Medical Things. Reprinted with permission from Ref. [114]. 2020 Elsevier.

The demanding defense solutions should provide a high-level of privacy and security, without affecting computation and usage of resources (performance) significantly. The defenses should be able to detect and prevent attacks, reduce/correct the damage of executed attacks, and preserve the patients' privacy. In detection-based defensive approaches, the MCPS/IoMT can also be made resilient in confronting the threats. A resilient MCPS/IoMT is designed to endure disruptions and it remains functional despite the malign operations from adversaries. Enhancing the medical devices with AI/CV computing elements help them to predict and confront different behaviors and actions from the attacks launched. A modern intrusion detection system (IDS) suitable for this application is provided in Figure 36.

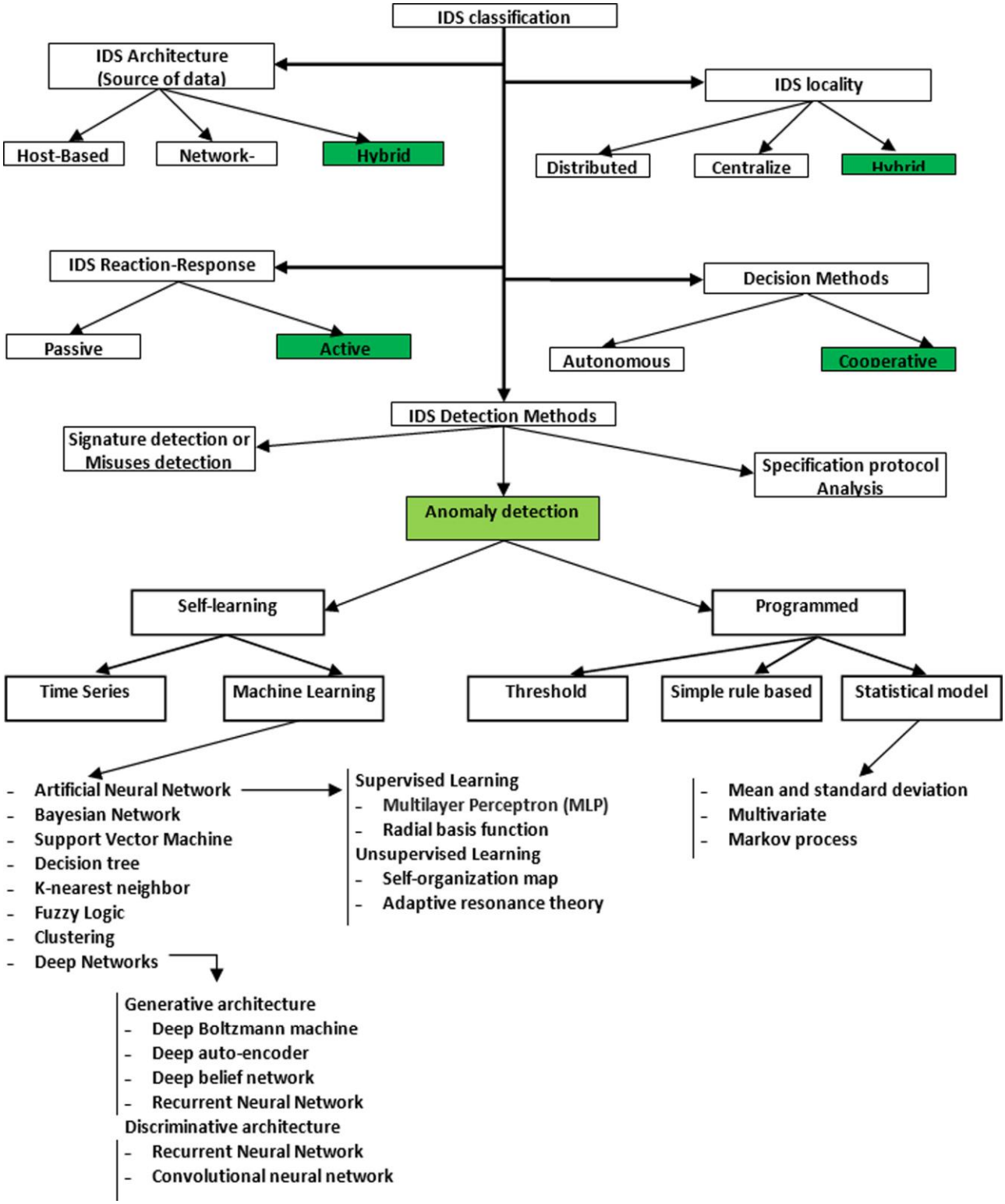

Figure 36. Modern intrusion detection system (IDS) classification based on five factors: architecture, locality, reaction–response, decision class, and detection methods [114]. Abbreviations used: IDS, intrusion detection system. Reprinted with permission from Ref. [114]. 2020 Elsevier.

Similar to the attacks, the defense solutions can be designed for networking communications, device software, and/or device hardware. With respect to hardware-based defensive solutions, reverse engineering is one of the effective methods for hardware trust

and assurance [118–120]. Although originally used for negative purposes (e.g., disclosing sensitive information to a competitor/adversary), it can detect malicious alteration and/or tampering (applied by semiconductor foundries) with high accuracy.

Reverse engineering of electronic chips and systems refers to the process of retrieving an electronic design layout and/or netlist, stored information (memory contents, firmware, software, etc.), and functionality/specification through electrical testing and/or physical inspection. The systematic overview of a reverse engineering process is shown in Figure 37 [119]. Possible data samples for a reverse engineering-based detection and recognition system are provided in Figure 38 [121]. Figure 39 displays a component detection system using deep learning for reverse engineering [121].

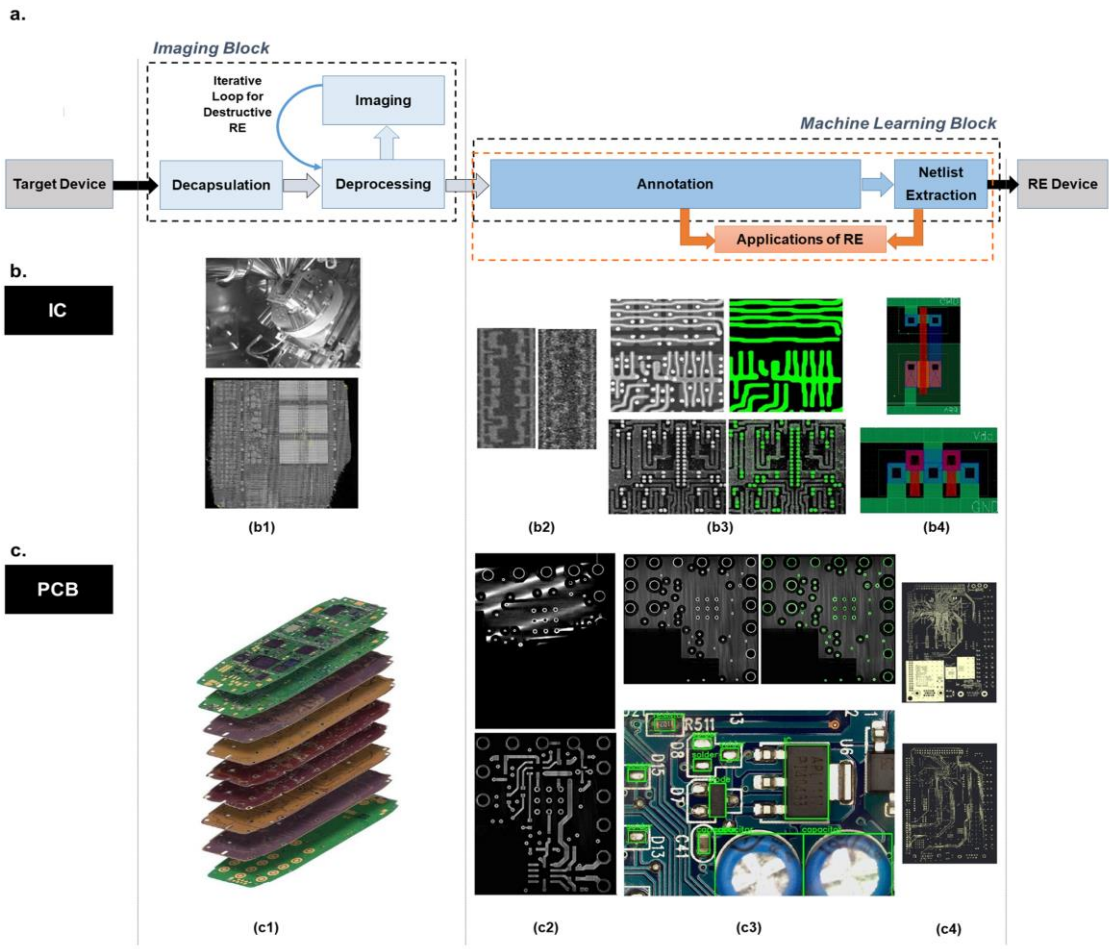

Figure 37. The systematic overview of a reverse engineering (RE) process, which can be performed on ICs and printed circuit boards (PCBs), its challenges and possibilities. (**a**) A typical workflow of RE encompassing various stages. Two main blocks of such a workflow are: Image Analysis and Machine Learning. The outputs of the machine learning-related block can enable us to provide hardware-based trust and assurance, as an application of reverse engineering. (**b**) reverse engineering workflow for IC: (**b1**) deprocessing of the IC, (**b2**) example of noise removal in the active region using different imaging parameters, (**b3**) segmentation and extraction of polysilicon structures and vias in an IC, (**b4**) netlist of extracted logic cells. (**c**) Reverse engineering workflow for PCB: (**c1**) image depicting a multi-layered PCB. Depending on the number of the layers in a PCB, different types of reverse engineering techniques should be considered. Irrespective of this, these challenges are inevitable, (**c2**) example for misaligned layer and reconstructed image, (**c3**) segmentation and extraction of vias for X-rayed PCB and labelled components on the surface of an optically imaged PCB, (**c4**) segmented layout of PCB layers with connected and not-connected vias [119]. Abbreviations used: RE, Reverse Engineering. Reprinted with permission from Ref. [119]. 2021 Association for Computing Machinery.

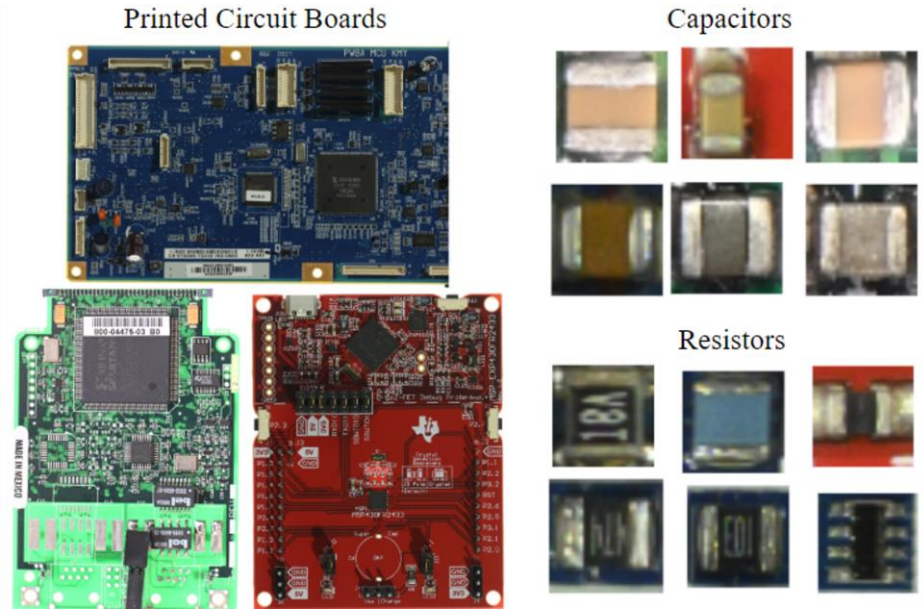

Figure 38. Sample data from the Florida Institute for Cybersecurity (FICS)-PCB dataset [121].

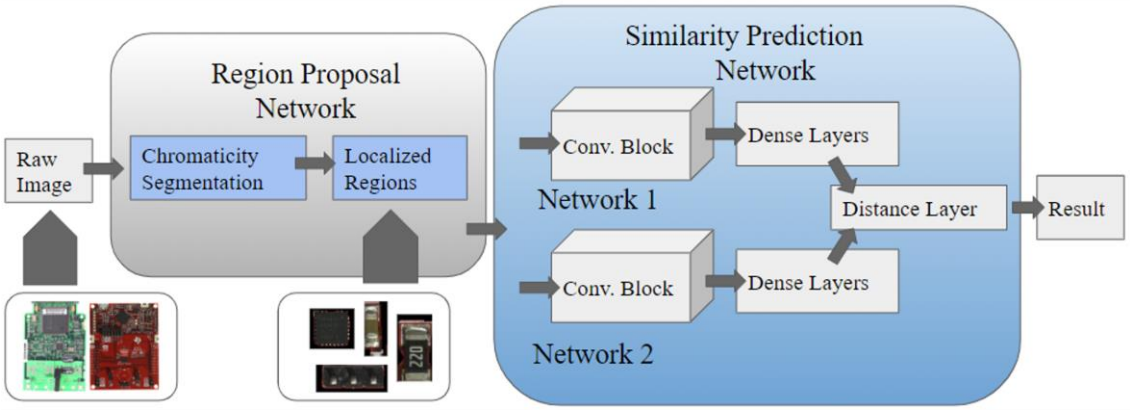

Figure 39. The Electronic Component Localization and Detection Network (ECLAD-Net) architecture for PCB component detection [121]. Abbreviations used: Conv Block, Convolutional Block.

In summary, The Internet connectivity of medical devices and inclusion of more computing elements in the network introduces various security issues that can produce malicious medical errors. Different layers of these computing devices as well as their processing data can be the victims for different kinds of attacks. Additionally, the running software on these devices along with the network infrastructure are subject to exploitation by adversaries. With respect to hardware-based attacks, there are multiple parties in the IC supply chain that can serve as malicious entities. Also, the victim of attacks for the medical hardware can be the device technology, the circuit, the architecture, or all of them in a cross-layer threat model. Unfortunately, there are limited studies on security analysis of medical devices and very few solutions have been proposed. The defense solutions for overcoming the medical security problems can be introduced for networking communications, device software, device hardware, or be in a cross-layer form.

6. Challenges and Opportunities

With the internet, wireless technology, and increased connectivity of IoMT technologies along with incorporation of state-of-the-art methods from AI/CV, the new generation of medical devices is facing advanced security and privacy challenges as discussed in this review study. It is really important to investigate the vulnerabilities of technologies of

IoMT in depth and how they can produce intentional (malicious) medical errors. In the evaluation, certain factors including attack surface, technical requirement, architecture flaws, and operating system weaknesses need to be considered.

Instead of (electronic) medical equipment being well installed in hospitals along with medical agencies with physical accessibility for experts, the new generation of IoMT devices are worn by or implanted in patients. The traditional medical equipment in IoMT can be remotely accessed and managed to perform the medical tasks. As the majority of the IoMT devices have to handle personal and physiological data, the impact of security attacks on the users could be more direct and severe compare to other IoT systems. For example, wireless connected implantable devices are designed to manage cardiac functions, insulin functions, nerve stimulation, etc., and they are equipped with electrodes, pumps, and other actuators. Malicious attacks on such devices make serious medical errors and can have life-threatening effects. With minimal security protection on these medical devices, they can easily be hacked to perform malicious operations.

The security issues for IoMT are not limited to attacks on the medical devices, because the network, all its associated entities, communication means, and the transmitting data are other points of interest for staging malicious actions. Due to the fact that there are ever new techniques for attacking networks, administrators have to be constantly aware of the emerging problems, and they need to update the medical systems with fixing patches and anti-virus libraries in order to protect them against the malicious attacks.

This feature is not available for the wearable and implantable medical devices, which means it is not straightforward to inject patches and anti-viruses into them. Because of less or no physical accessibility to these devices after their installation, they cannot be shut down on time when an issue occurs, and the situation continues until security experts can get access and recover them to the normal operation. These shortcomings can easily put a patient's life in danger.

Introducing other interesting and novel technologies in studying IoMT security and privacy provide many research opportunities, such as blockchain that can be applied in the healthcare domain for keeping medical records in a decentralized/distributed fashion, so that the blocks in the blockchain depend on one another. There are a number of security concerns and challenges for IoMT, including key management, communication protocols, technical heterogeneity and complexity of devices and systems (e.g., in terms of processing elements and operating systems), availability of computing resources, authentication mechanisms, behavioral profile for medical devices using informative features, unavailability of source code or binary programs, data confidentiality and protection, malicious/non-malicious error-tolerant design, intrusion detection mechanism, security of access control, trade-off between security, energy efficiency, and performance, security-aware computing mechanism, general and standard architectures for IoMT, privacy-preserving mechanisms, employment of AI/CV and Big Data, shortage of data for training and analysis purposes, and temporal and spatial considerations of network security (e.g., number, location, and timing of patients). Tackling these problems are in fact new interesting research directions to study.

Therefore, security in the medical domain is an important and critical factor that can endanger the medical processes at application/human, software, and hardware levels. Through the respective attacks, the functionality and/or information of devices and systems are damaged leading to medical errors. The errors in the medical field are extremely serious and life-threatening with the high possibility of causing death.

Alongside the subjects mentioned, there are many security benefits and opportunities for IoMT to explore:

(a) AI and CV for IoMT: Two technological waves of AI and CV are great candidates for creating significant novelties in the IoMT and its entities. These technologies are able to improve the performance and functionality of the elements in the network and make them intelligent. They also can be used in developing more effective security solutions in terms of detecting, recognizing, and predicting the attacks. Meanwhile, it

should not be neglected that the methods from AI/CV are great tools for adversaries to create smart and unpredictable attacks.

(b) The dependency of the third-party and open-source code: the firmware on medical devices relies heavily on third-party and open-source codes. The manufacturers usually take new features, high performance, and low power consumption as the main targets of their products and shorten the development cycle as much as possible to enhance market competitiveness. This means adoption of agile development models in the medical domain. They directly reuse open source code, refer to public code implementation, cross-compile platform code, and rely on third-party libraries. Many of the resources have vulnerabilities that are transmitted into the medical devices that can create medical errors. However, this adoption of resources can also provide opportunities for detection and discover of vulnerabilities among the existing and future resources through similarity evaluations.

(c) Development of peripheral systems: as IoMT devices become more interactive, the need for development of novel and strong peripheral systems increases. There are a number of opportunities in this development for improving software and hardware of peripheral systems in terms of firmware acquisition and analysis, terminal points, cloud endpoints, etc. However, the new attacks that emerge from this process should be taken into account with the respective countermeasures.

In summary, there are many challenges and opportunities in IoMT to research, especially from the security perspective. These new directions are further broadened considering the today's desirable technologies, such as AI and CV. The novel methods from these technologies can serve both the attack and defense parties in the network. Meanwhile, most of the existing security studies for IoMT rely on computer simulations, and practical assessments of both attacks and defenses are missing. Therefore, the real-world implementations of existing and future studies are needed and they introduce more challenges and opportunities to the field.

7. Conclusions

While medical and computer technologies play key roles in our population's health, they are vulnerable to cyber threats and medical errors due to the presence of interconnected medical devices and systems, easily accessible access points, outdated medical products, and a lack of emphasis upon emerging cybersecurity attacks for the medical field. The available studies in the medical domain mostly focus on patient care and treatments, however healthcare technologies hold vast amounts of valuable and sensitive data, without the presence of strong and effective defense systems. In many cases, financial gains and national interests are extremely important motivations for the attacks, as medical identity is more critical than other identity credentials.

Other attacks may be motivated by political and military benefits, leading to creation of cyberwarfare in the field. With having vulnerable health systems, human lives are in danger regardless of the social/economic importance of an individual. The attacks target different medical processes, such as malfunctioning in critical and surgical equipment within hospitals or even at home where interventions rely on a power supply. The introduction of more dangerous and stronger threats in the medical domain jeopardizes all the entities in this field, including humans and computing devices, resulting in serious harm to humans and finance.

This review shows that cybersecurity is an essential part of maintaining the safety, privacy, and trust of patients along with any entity in the medical field. There are great opportunities at different system layers for research and investment to ensure the security and protection of healthcare technologies and patient information. In fact, security must be considered for the medical domain from conception to realization considering all the entities and elements in the procedures. In short, cybersecurity must become part of the medical culture and the area of medical security, especially from the hardware perspective, has substantial, sophisticated, and appropriate topics to explore.

Author Contributions: Conceptualization, S.T.; methodology, S.T.; validation, S.T.; formal analysis, S.T.; investigation, S.T.; resources, S.T.; writing—original draft preparation, S.T.; writing—review and editing, S.T. and N.A.; visualization, S.T.; supervision, N.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Haenlein, M.; Kaplan, A. A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *Calif. Manag. Rev.* **2019**, *61*, 5–14. [CrossRef]
2. Müller, V.C.; Bostrom, N. Future progress in artificial intelligence. *AI Matters* **2014**, *1*, 9–11. [CrossRef]
3. Schwabacher, M.; Goebel, K. A survey of artificial intelligence for prognostics. In Proceedings of the AAAI Fall Symposium: Artificial Intelligence for Prognostics, Arlington, VA, USA, 9–11 November 2007; pp. 107–114.
4. Rong, G.; Mendez, A.; Assi, E.B.; Zhao, B.; Sawan, M. Artificial Intelligence in Healthcare: Review and Prediction Case Studies. *Engineering* **2020**, *6*, 291–301. [CrossRef]
5. He, J.; Baxter, S.L.; Xu, J.; Xu, J.; Zhou, X.; Zhang, K. The practical implementation of artificial intelligence technologies in medicine. *Nat. Med.* **2019**, *25*, 30–36. [CrossRef]
6. Brynjolfsson, B.Y.E.; McAfee, A. *Artificial Intelligence for Real*; Harvard Business School Publishing Corporation: Boston, MA, USA, 2017; pp. 1–31.
7. Chassagnon, G.; Vakalopoulou, M.; Paragios, N.; Revel, M.-P. Artificial intelligence applications for thoracic imaging. *Eur. J. Radiol.* **2020**, *123*, 108774. [CrossRef]
8. Zawacki-Richter, O.; Marín, V.I.; Bond, M.; Gouverneur, F. Systematic review of research on artificial intelligence applications in higher education—Where are the educators? *Int. J. Educ. Technol. High. Educ.* **2019**, *16*, 39. [CrossRef]
9. Kyamakya, K. Artificial intelligence in Transportation Telematics. *OGAI J. (Oesterreichische Gesellschaft Artif. Intell.)* **2006**, *25*, 2–4.
10. Bahrammirzaee, A. A comparative survey of artificial intelligence applications in finance: Artificial neural networks, expert system and hybrid intelligent systems. *Neural Comput. Appl.* **2010**, *19*, 1165–1195. [CrossRef]
11. Nichols, J.; Chan, H.W.H.; Baker, M.A.B. Machine learning: Applications of artificial intelligence to imaging and diagnosis. *Biophys. Rev.* **2018**, *11*, 111–118. [CrossRef]
12. Wu, H.; Han, H.; Wang, X.; Sun, S. Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. *IEEE Access* **2020**, *8*, 153826–153848. [CrossRef]
13. Miller, D.D.; Brown, E.W. Artificial Intelligence in Medical Practice: The Question to the Answer? *Am. J. Med.* **2018**, *131*, 129–133. [CrossRef]
14. Chan, Y.-K.; Chen, Y.-F.; Pham, T.; Chang, W.; Hsieh, M.-Y. Artificial Intelligence in Medical Applications. *J. Healthc. Eng.* **2018**, *2018*, 4827875. [CrossRef]
15. Chan, H.-P.; Samala, R.K.; Hadjiiski, L.M.; Zhou, C. Deep Learning in Medical Image Analysis. *Adv. Exp. Med. Biol.* **2020**, *1213*, 3–21. [CrossRef]
16. Gore, J.C. Artificial intelligence in medical imaging. *Magn. Reson. Imaging* **2019**, *68*, A1–A4. [CrossRef]
17. Meskó, B.; Görög, M. A short guide for medical professionals in the era of artificial intelligence. *NPJ Digit. Med.* **2020**, *3*, 126. [CrossRef]
18. Hamamoto, R. Application of Artificial Intelligence for Medical Research. *Biomolecules* **2021**, *11*, 90. [CrossRef]
19. Lewis, S.J.; Gandomkar, Z.; Brennan, P.C. Artificial Intelligence in medical imaging practice: Looking to the future. *J. Med. Radiat. Sci.* **2019**, *66*, 292–295. [CrossRef]
20. Esteva, A.; Chou, K.; Yeung, S.; Naik, N.; Madani, A.; Mottaghi, A.; Liu, Y.; Topol, E.; Dean, J.; Socher, R. Deep learning-enabled medical computer vision. *NPJ Digit. Med.* **2021**, *4*, 5. [CrossRef]
21. Khemasuwan, D.; Sorensen, J.S.; Colt, H.G. Artificial intelligence in pulmonary medicine: Computer vision, predictive model and COVID-19. *Eur. Respir. Rev.* **2020**, *29*, 200181. [CrossRef]
22. Ward, T.M.; Mascagni, P.; Ban, Y.; Rosman, G.; Padoy, N.; Meireles, O.; Hashimoto, D.A. Computer vision in surgery. *Surgery* **2020**, *169*, 1253–1256. [CrossRef]
23. Chadebecq, F.; Vasconcelos, F.; Mazomenos, E.; Stoyanov, D. Computer Vision in the Surgical Operating Room. *Visc. Med.* **2020**, *36*, 456–462. [CrossRef]
24. Wallace, S.; Laird, J.; Coulter, K. Examining the Resource Requirements of Artificial Intelligence Architectures. *Ann. Arbor.* 2000. Available online: http://ai.vancouver.wsu.edu/~{}wallaces/professional/downloads/wallace-2000-cgf.pdf (accessed on 1 December 2021).
25. Li, R.; Zhao, Z.; Zhou, X.; Ding, G.; Chen, Y.; Wang, Z.; Zhang, H. Intelligent 5G: When Cellular Networks Meet Artificial Intelligence. *IEEE Wirel. Commun.* **2017**, *24*, 175–183. [CrossRef]
26. van Lent, M.; Laird, J.; van Lent, M.; Laird, J.; van Lent, M.; Laird, J. Developing an Artificial Intelligence Engine. Available online: https://www.researchgate.net/profile/John-Laird-6/publication/243763189_Developing_an_artificial_intelligence_engine/links/56dedfe908aec8c022cf2ea2/Developing-an-artificial-intelligence-engine.pdf (accessed on 1 December 2021).

27. Dalpiaz, F.; Niu, N. Requirements Engineering in the Days of Artificial Intelligence. *IEEE Softw.* **2020**, *37*, 7–10. [CrossRef]
28. Fung, J.; Mann, S. Computer vision signal processing on graphics processing units. In Proceedings of the 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, Montreal, QC, Canada, 17–21 May 2004. [CrossRef]
29. Cath, C. Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2018**, *376*, 20180080. [CrossRef]
30. Zhou, L.; Pan, S.; Wang, J.; Vasilakos, A.V. Machine learning on big data: Opportunities and challenges. *Neurocomputing* **2017**, *237*, 350–361. [CrossRef]
31. Susar, D.; Aquaro, V. Artificial Intelligence. In Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, Melbourne, VIC, Australia, 3–5 April 2019. [CrossRef]
32. Arrieta, A.B.; Díaz-Rodríguez, N.; Del Ser, J.; Bennetot, A.; Tabik, S.; Barbado, A.; Garcia, S.; Gil-Lopez, S.; Molina, D.; Benjamins, R.; et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Inf. Fusion* **2019**, *58*, 82–115. [CrossRef]
33. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9–12 October 2017; pp. 112–120. [CrossRef]
34. Hatzivasilis, G.; Soultatos, 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; pp. 457–464. [CrossRef]
35. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and Privacy in the Medical Internet of Things: A Review. *Secur. Commun. Netw.* **2018**, *2018*, 5978636. [CrossRef]
36. Burleson, W.; Carrara, S. *Security and Privacy for Implantable Medical Devices*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–205. [CrossRef]
37. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. [CrossRef]
38. Camara, C.; Peris-Lopez, P.; Tapiador, J.E. Security and privacy issues in implantable medical devices: A comprehensive survey. *J. Biomed. Inform.* **2015**, *55*, 272–289. [CrossRef]
39. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet Things* **2019**, *8*, 100123. [CrossRef]
40. Vashistha, N.; Lu, H.; Shi, Q.; Rahman, M.T.; Shen, H.; Woodard, D.L.; Asadizanjani, N.; Tehranipoor, M. Trojan Scanner: Detecting Hardware Trojans with Rapid SEM Imaging Combined with Image Processing and Machine Learning. In Proceedings of the ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis, Phoenix, AZ, USA, 28 October–1 November 2018; pp. 256–265. [CrossRef]
41. Xiao, K.; Forte, D.; Jin, Y.; Karri, R.; Bhunia, S.; Tehranipoor, M.M. Hardware Trojans. *ACM Trans. Des. Autom. Electron. Syst.* **2016**, *22*, 1–23. [CrossRef]
42. Rahman, M.T.; Shi, Q.; Tajik, S.; Shen, H.; Woodard, D.L.; Tehranipoor, M.; Asadizanjani, N. Physical Inspection & Attacks: New Frontier in Hardware Security. In Proceedings of the 2018 IEEE 3rd International Verification and Security Workshop (IVSW), Girona, Spain, 2–4 July 2018; pp. 93–102. [CrossRef]
43. Rostami, M.; Koushanfar, F.; Rajendran, J.; Karri, R. Hardware security: Threat models and metrics. In Proceedings of the 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, 18–21 November 2013; pp. 819–823. [CrossRef]
44. Behnam, P. Validation of Hardware Security and Trust: A Survey. *arXiv* **2018**, arXiv:1801.00649.
45. Tan, B.; Karri, R. Challenges and New Directions for AI and Hardware Security. In Proceedings of the 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, 9–12 August 2020; IEEE: New York, NY, USA, 2020; pp. 277–280. [CrossRef]
46. Facon, A.; Guilley, S.; Ngo, X.-T.; Perianin, T. Hardware-enabled AI for Embedded Security: A New Paradigm. In Proceedings of the 2019 3rd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), Hanoi, Vietnam, 21–22 March 2019; pp. 80–84. [CrossRef]
47. Brundage, M.; Avin, S.; Wang, J.; Belfield, H.; Krueger, G.; Hadfield, G.; Khlaaf, H.; Yang, J.; Toner, H.; Fong, R.; et al. Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims. 2020. Available online: http://arxiv.org/abs/2004.07213 (accessed on 1 December 2021).
48. Mittal, S.; Gupta, H.; Srivastava, S. A survey on hardware security of DNN models and accelerators. *J. Syst. Arch.* **2021**, *117*, 102163. [CrossRef]
49. A Makary, M.; Daniel, M. Medical error—the third leading cause of death in the US. *BMJ* **2016**, *353*, i2139. [CrossRef]
50. Berlin, L. Medical errors, malpractice, and defensive medicine: An ill-fated triad. *Diagnosis* **2017**, *4*, 133–139. [CrossRef] [PubMed]
51. Ahmed, Z.; Saada, M.; Jones, A.M.; Al-Hamid, A.M. Medical errors: Healthcare professionals' perspective at a tertiary hospital in Kuwait. *PLoS ONE* **2019**, *14*, e0217023. [CrossRef]
52. Parks-Savage, A.; Archer, L.; Newton, H.; Wheeler, E.; Huband, S.R. Prevention of medical errors and malpractice: Is creating resilience in physicians part of the answer? *Int. J. Law Psychiatry* **2018**, *60*, 35–39. [CrossRef]

53. Levi, B.H.; Rosenthal, G.E.; Kaldjian, L.C.; Jones, E.; Wu, B.J.; Forman-Hoffman, V.L. Reporting Medical Errors to Improve Patient Safety. *Arch. Intern. Med.* **2008**, *168*, 40–46.
54. Hobgood, C.; Peck, C.R.; Gilbert, B.; Chappell, K.; Zou, B. Medical Errors-What and When: What Do Patients Want to Know? *Acad. Emerg. Med.* **2002**, *9*, 1156–1161. [CrossRef]
55. Elwahab, S.A.; Doherty, E. What about doctors? The impact of medical errors. *Surgeon* **2014**, *12*, 297–300. [CrossRef]
56. Blendon, R.J.; DesRoches, C.M.; Brodie, M.; Benson, J.M.; Rosen, A.B.; Schneider, E.; Altman, D.E.; Zapert, K.; Herrmann, M.J.; Steffenson, A.E. Views of practicing physicians and the public on medical errors. *NEJM* **2002**, *347*, 1933–1940. [CrossRef] [PubMed]
57. Fain, R.; Healey, B.; Sudders, M.; Palleschi, M.; Campbell, E. *The Financial and Human Cost of Medical Error*; Betsy Lehman Center for Patient Safety: Boston, MA, USA, 2019.
58. Shah, R.K.; Kentala, E.; Healy, G.B.; Roberson, D.W. Classification and Consequences of Errors in Otolaryngology. *Laryngoscope* **2004**, *114*, 1322–1335. [CrossRef] [PubMed]
59. Gorski, D. Are Medical Errors Really the Third Most Common Cause of Death in the U.S.? 2019 Edition. 2019. Available online: https://sciencebasedmedicine.org/are-medical-errors-really-the-third-most-common-cause-of-death-in-the-u-s-2019-edition/ (accessed on 1 December 2021).
60. Martinez, W.; Lehmann, L.S.; Thomas, E.J.; Etchegaray, J.M.; Shelburne, J.T.; Hickson, G.B.; Brady, D.W.; Schleyer, A.M.; Best, J.A.; May, N.B.; et al. Speaking up about traditional and professionalism-related patient safety threats: A national survey of interns and residents. *BMJ Qual. Saf.* **2017**, *26*, 869–880. [CrossRef] [PubMed]
61. Anagnostiadis, E.; Chatterjee, S.V. The Dangers of Buying Prescription Drugs from Rogue Wholesale Distributors. *J. Med. Regul.* **2018**, *104*, 13–16. [CrossRef]
62. Cohen, M.R.; Proulx, S.M.; Crawford, S.Y. Survey of hospital systems and common serious medication errors. *J. Healthc. Risk Manag.* **1998**, *18*, 16–27. [CrossRef]
63. Nasiripour, A.; Raiessi, P.; Jafari, M. Medical Errors Disclosure: Is It Good or Bad? *Hosp. Pr. Res.* **2018**, *3*, 16–21. [CrossRef]
64. Qayyum, A.; Qadir, J.; Bilal, M.; Al-Fuqaha, A. Secure and Robust Machine Learning for Healthcare: A Survey. *IEEE Rev. Biomed. Eng.* **2020**, *14*, 156–180. [CrossRef]
65. Rakitin, S.R. Networked Medical Devices: Essential Collaboration for Improved Safety. *Biomed. Instrum. Technol.* **2009**, *43*, 332–338. [CrossRef]
66. Williams, P.; Woodward, A. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Med. Devices Evid. Res.* **2015**, *8*, 305–316. [CrossRef]
67. Rushanan, M.; Rubin, A.D.; Kune, D.F.; Swanson, C.M. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; IEEE: New York, NY, USA; pp. 524–539. [CrossRef]
68. 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]
69. Pycroft, L.; Aziz, T.Z. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Rev. Med. Devices* **2018**, *15*, 403–406. [CrossRef] [PubMed]
70. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the Internet of Medical Things. *Healthc. Policy Technol.* **2021**, *10*, 100549. [CrossRef]
71. McMahon, E.; Williams, R.; El, M.; Samtani, S.; Patton, M.; Chen, H. Assessing medical device vulnerabilities on the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; IEEE: New York, NY, USA; pp. 176–178. [CrossRef]
72. Suvarna, R.; Kawatkar, S.; Jagli, D. Internet of Medical Things (IoMT)—An overview. *Int. J. Adv. Res. Comput. Sci. Manag. Stud.* **2016**, *4*, 173–178.
73. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A Survey on Security and Privacy Issues in Modern Healthcare Systems. *ACM Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]
74. Li, X.; Dai, H.-N.; Wang, Q.; Imran, M.A.; Li, D. Securing Internet of Medical Things with Friendly-jamming schemes. *Comput. Commun.* **2020**, *160*, 431–442. [CrossRef]
75. Zheng, G.; Shankaran, R.; Orgun, M.A.; Qiao, L.; Saleem, K. Ideas and Challenges for Securing Wireless Implantable Medical Devices: A Review. *IEEE Sensors J.* **2016**, *17*, 562–576. [CrossRef]
76. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. *Sensors* **2020**, *20*, 4828. [CrossRef]
77. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
78. Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
79. 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.* **2020**, *174*, 102886. [CrossRef]
80. Ziegler, S. *Internet of Things Security and Data Protection*; Springer: Berlin/Heidelberg, Germany, 2019.

81. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
82. Erhan, L.; Ndubuaku, M.; Di Mauro, M.; Song, W.; Chen, M.; Fortino, G.; Bagdasar, O.; Liotta, A. Smart anomaly detection in sensor systems: A multi-perspective review. *Inf. Fusion* **2021**, *67*, 64–79. [CrossRef]
83. Roberts, P. Update: Cash for Medical Device Clunkers? Task Force Calls for Healthcare Security Overhaul. 2017. Available online: https://securityledger.com/2017/06/cash-for-medical-device-clunkers-task-force-calls-for-healthcare-security-overhaul/ (accessed on 1 December 2021).
84. Schwartz, S.; Ross, A.; Carmody, S.; Chase, P.; Coley, S.C.; Connolly, J.; Petrozzino, C.; Zuk, M. The Evolving State of Medical Device Cybersecurity. *Biomed. Instrum. Technol.* **2018**, *52*, 103–111. [CrossRef]
85. Cvitić, I.; Peraković, D.; Periša, M.; Botica, M. Novel approach for detection of IoT generated DDoS traffic. *Wirel. Netw.* **2019**, *27*, 1573–1586. [CrossRef]
86. Cvitic, I.; Perakovic, D.; Gupta, B.; Choo, K.-K.R. Boosting-based DDoS Detection in Internet of Things Systems. *IEEE Internet Things J.* **2022**, *9*, 2109–2123. [CrossRef]
87. Doshi, R.; Apthorpe, N.; Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35. [CrossRef]
88. Yu, M.; Zhuge, J.; Cao, M.; Shi, Z.; Jiang, L. A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. *Futur. Internet* **2020**, *12*, 27. [CrossRef]
89. Razaque, A.; Amsaad, F.; Khan, M.J.; Hariri, S.; Chen, S.; Siting, C.; Ji, X. Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. *IEEE Access* **2019**, *7*, 168774–168797. [CrossRef]
90. Zhang, Y.; Balochian, S.; Agarwal, P.; Bhatnagar, V.; Housheya, O.J. Artificial Intelligence and Its Applications 2014. *Math. Probl. Eng.* **2016**, *2016*, 3871575. [CrossRef]
91. Shi, F.; Wang, J.; Shi, J.; Wu, Z.; Wang, Q.; Tang, Z.; He, K.; Shi, Y.; Shen, D. Review of Artificial Intelligence Techniques in Imaging Data Acquisition, Segmentation, and Diagnosis for COVID-19. *IEEE Rev. Biomed. Eng.* **2020**, *14*, 4–15. [CrossRef]
92. Fan, X.; Wu, J.; Tian, L. A Review of Artificial Intelligence for Games. *Artif. Intell. China* **2020**, 298–303. [CrossRef]
93. Oke, S.A. A literature review on artificial intelligence. *Int. J. Inf. Manag. Sci.* **2008**, *19*, 535–570.
94. Li, Z.; Liu, F.; Yang, W.; Peng, S.; Zhou, J. A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, 1–21. [CrossRef] [PubMed]
95. Copeland, M. What's the Difference Between Artificial Intelligence, Machine Learning and Deep Learning? 2016. Available online: https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/ (accessed on 1 December 2021).
96. Zappone, A.; Di Renzo, M.; Debbah, M. Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both? *IEEE Trans. Commun.* **2019**, *67*, 7331–7376. [CrossRef]
97. Real, M.M.; Salvador, R. Physical Side-Channel Attacks on Embedded Neural Networks: A Survey. *Appl. Sci.* **2021**, *11*, 6790. [CrossRef]
98. Luo, J.; Huang, J. Generative adversarial network: An overview. *Yi Qi Yi Biao Xue Bao/Chin. J. Sci. Instrum.* **2019**, *40*, 74–84. [CrossRef]
99. Kumar, M.R.P.; Jayagopal, P. Generative adversarial networks: A survey on applications and challenges. *Int. J. Multimed. Inf. Retr.* **2020**, *10*, 1–24. [CrossRef]
100. Wu, X.; Xu, K.; Hall, P. A survey of image synthesis and editing with generative adversarial networks. *Tsinghua Sci. Technol.* **2017**, *22*, 660–674. [CrossRef]
101. Feng, X.; Jiang, Y.; Yang, X.; Du, M.; Li, X. Computer vision algorithms and hardware implementations: A survey. *Integration* **2019**, *69*, 309–320. [CrossRef]
102. Challen, R.; Denny, J.; Pitt, M.; Gompels, L.; Edwards, T.; Tsaneva-Atanasova, K. Artificial intelligence, bias and clinical safety. *BMJ Qual. Saf.* **2019**, *28*, 231–237. [CrossRef]
103. Ulhaq, A.; Born, J.; Khan, A.; Gomes, D.P.S.; Chakraborty, S.; Paul, M. COVID-19 Control by Computer Vision Approaches: A Survey. *IEEE Access* **2020**, *8*, 179437–179456. [CrossRef]
104. Pham, Q.-V.; Nguyen, D.C.; Huynh-The, T.; Hwang, W.-J.; Pathirana, P.N. Artificial Intelligence (AI) and Big Data for Coronavirus (COVID-19) Pandemic: A Survey on the State-of-the-Arts. *IEEE Access* **2020**, *8*, 130820–130839. [CrossRef] [PubMed]
105. Nguyen, T.T.; Nguyen, Q.V.H.; Nguyen, D.T.; Hsu, E.B.; Yang, S.; Eklund, P. Artificial Intelligence in the Battle against Coronavirus (COVID-19): A Survey and Future Research Directions. *arXiv* **2020**, arXiv:2008.07343.
106. Talib, M.A.; Majzoub, S.; Nasir, Q.; Jamal, D. *A Systematic Literature Review on Hardware Implementation of Artificial In-Telligence Algorithms*; Springer: New York, NY, USA, 2021; Volume 77.
107. Xu, Q.; Arafin, T.; Qu, G. Security of Neural Networks from Hardware Perspective. In Proceedings of the 2021 26th Asia and South Pacific Design Automation Conference (ASP-DAC), Tokyo, Japan, 18–21 January 2021. [CrossRef]
108. Schuman, C.D.; Potok, T.E.; Patton, R.M.; Birdwell, J.D.; Dean, M.E.; Rose, G.S.; Plank, J.S. A Survey of Neuromorphic Computing and Neural Networks in Hardware. *arXiv* **2017**, arXiv:1705.06963.
109. HajiRassouliha, A.; Taberner, A.J.; Nash, M.; Nielsen, P.M. Suitability of recent hardware accelerators (DSPs, FPGAs, and GPUs) for computer vision and image processing algorithms. *Signal Process. Image Commun.* **2018**, *68*, 101–119. [CrossRef]

110. Batra, G.; Jacobson, Z.; Madhav, S.; Queirolo, A.; Santhanam, N. Artificial-Intelligence Hardware: New Opportunities for Semiconductor Companies. McKinsey Co. December 2018. Available online: https://www.mckinsey.com/~{}/media/McKinsey/Industries/Semiconductors/OurInsights/ArtificialintelligencehardwareNewopportunitiesforsemiconductorcompanies/Artificial-intelligence-hardware.pdf (accessed on 1 December 2021).
111. Dey, N.; Ashour, A.S.; Shi, F.; Fong, S.J.; Tavares, J. Medical cyber-physical systems: A survey. *J. Med. Syst.* **2018**, *42*, 74. [CrossRef] [PubMed]
112. Pandey, G.; Vora, A. Vora Open Electronics for Medical Devices: State-of-Art and Unique Advantages. *Electronics* **2019**, *8*, 1256. [CrossRef]
113. Lee, I.; Sokolsky, O. Medical cyber physical systems. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; pp. 743–748. [CrossRef]
114. 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. *Futur. Gener. Comput. Syst.* **2019**, *105*, 581–606. [CrossRef]
115. Shakeel, I. Evolution in the World of Cyber Crime. 2016. Available online: https://resources.infosecinstitute.com/topic/evolution-in-the-world-of-cyber-crime/ (accessed on 1 December 2021).
116. Tehranipoor, M.; Wang, C. (Eds.) *Introduction to Hardware Security and Trust*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012. [CrossRef]
117. Wang, X.; Zhang, D.; He, M.; Su, D.; Tehranipoor, M. Secure Scan and Test Using Obfuscation Throughout Supply Chain. *IEEE Trans. Comput. Des. Integr. Circuits Syst.* **2017**, *37*, 1867–1880. [CrossRef]
118. Fyrbiak, M.; Strauss, S.; Kison, C.; Wallat, S.; Elson, M.; Rummel, N.; Paar, C. Hardware reverse engineering: Overview and open challenges. In Proceedings of the 2017 IEEE 2nd International Verification and Security Workshop (IVSW), Thessaloniki Greece, 3–5 July 2017; pp. 88–94. [CrossRef]
119. Botero, U.J.; Wilson, R.; Lu, H.; Rahman, M.T.; Mallaiyan, M.A.; Ganji, F.; Asadizanjani, N.; Tehranipoor, M.M.; Woodard, D.L.; Forte, D. Hardware Trust and Assurance through Reverse Engineering: A Tutorial and Outlook from Image Analysis and Machine Learning Perspectives. *ACM J. Emerg. Technol. Comput. Syst.* **2021**, *17*, 1–53. [CrossRef]
120. Azriel, L.; Speith, J.; Albartus, N.; Ginosar, R.; Mendelson, A.; Paar, C. A survey of algorithmic methods in IC reverse engineering. *J. Cryptogr. Eng.* **2021**, *11*, 299–315. [CrossRef]
121. Sathiaseelan, M.M.; Paradis, O.; Taheri, S.; Asadizanjani, N. Why Is Deep Learning Challenging for Printed Circuit Board (PCB) Component Recognition and How Can We Address It? *Cryptography* **2021**, *5*, 9. [CrossRef]