Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review

Tahreem Yaqoob, Haider Abbas, *Senior Member, IEEE*, and Mohammed Atiquzzaman, *Senior Member, IEEE*

***Abstract*—Over the last few years, healthcare administrations have been digitizing their provision of care that led to an increased number of networked medical devices and medical telemetry. Due to such digitization, medical devices have made phenomenal strides in the course of the last half-century. These networked medical devices have enhanced the quality and accessibility of health treatments by achieving pervasive healthcare vision. Moreover, these devices have transformed the canvas of medical treatments and improved the lives of the masses. Such innovation, as a result, assisted in paving the way for reliable healthcare facilities through the introduction of new areas of therapeutic and diagnostic treatments. Medical devices, nowadays, are portable, networked, and capable enough to facilitate human lives. The refined quality and variety of these devices put forward a promising future. However, on the other hand, the healthcare sector is experiencing the greatest amount of security breaches due to the presence of security flaws in medical devices. As these devices are no longer standalone systems and are network-connected, the attack surface has increased profoundly. Actually, devices in practice were designed, developed, and disseminated long ago. Therefore, they were not developed from the ground up with security as a vital design constraint. The flaws present in these devices have acquired the consideration of researchers from both industry and academia. In this paper, we studied security vulnerabilities present in state-of-the-art medical devices by studying security tests and the attacks demonstrated by the researchers on more than a hundred devices. Finally, some state-of-the-art solutions and countermeasures along with applicable regulations in literature were also studied and analyzed. Since these devices are life-critical and can even cause the death of a patient, therefore, this survey is significant as it can assist researchers to get an overview of loopholes present in medical devices and existing countermeasures. We concluded this survey paper with some open research areas that should be properly considered in order to secure these life-critical medical devices.**

***Index Terms*—Medical devices, security vulnerabilities, wearables, implantable devices, on-site medical equipment, FDA, HIPAA.**

Manuscript received May 31, 2018; revised December 12, 2018 and February 27, 2019; accepted April 15, 2019. Date of publication April 30, 2019; date of current version November 25, 2019. This work was supported by the Higher Education Commission, Pakistan, through its initiative of National Center for Cyber Security for the affiliated laboratory National Cyber Security Auditing and Evaluation Lab under Grant 2(1078)/HEC/M&E/2018/707. *(Corresponding author: Haider Abbas.)*

T. Yaqoob and H. Abbas are with the National University of Sciences and Technology, Islamabad 440000, Pakistan (e-mail: tahreem.ncsael@mcs.edu.pk; haider@mcs.edu.pk).

M. Atiquzzaman is with the University of Oklahoma, Norman, OK 73019 USA (e-mail: atiq@ou.edu).

Digital Object Identifier 10.1109/COMST.2019.2914094

I. Introduction

MODERN technical innovations with the introduction of networked medical devices have transformed the canvas of healthcare operations. Such a revolution brings the potential of next-generation integrated medical systems that improved the delivery of healthcare facilities by refining the capability and capacity of medical devices [1]. The medical device industry is extremely diverse. The life cycle of each of the devices can be considerably different from others in terms of design, implementation, and application. A medical device, according to the World Health Organization (WHO), is an instrument, machine, article, or an apparatus that can be used for diagnosis, treatment, monitoring, and prevention of disease or illness [2]. These innovative devices can be classified into three important types depending upon their functionality and usage. They can be software only, hardware-based or both [3]. The majority of the medical devices uses both hardware and software in order to perform critical operations. Further, they are no longer isolated and use communication technologies to provide quality health facilities. Networked medical devices have enabled better opportunities for diagnosing, treating and monitoring a wide range of chronic diseases. The prompt proliferation in the interconnectivity of medical devices with other related systems has improved patient care profoundly. The advent of wearable and implantable medical devices has empowered innovative opportunities for diagnosis, treatment, and monitoring of medical conditions. These devices have augmented life expectancy in the United States by almost 10 years since the 1950s [4]. The popularity of Internet-connectivity in healthcare has fueled the market for developing implantable devices, wearables, and connected on-site medical equipment. A plethora of such devices are present in the market that range between vital sign monitoring, glucose monitoring, wristbands, second skin [5], electrocardiograms (ECG), implantable pacemakers, insulin pumps, blood pressure monitors, radiology equipment, ventilator machines embedded sensors, ECG sensors, acidometers, ICU equipment, and many more. Since these devices share, process, analyze, measure, and transfer biological signals in the real-time; therefore, their application in healthcare and medicine is tremendous. These devices have improved the quality of healthcare facilities as they have a major impact on diagnosis, monitoring, and treatment of chronic disease. Connected devices deliver

healthcare services by overcoming temporal, organizational, and geographical barriers. Moreover, networked medical devices address emerging problems regarding health facilities, which include need to entitle patients to self-care and manage their medications, the high cost of existing healthcare services, direct access to healthcare facilities irrespective of place and time, and increasing a number of chronic diseases. Therefore, they are estimated to increase to 100.35 million in 2018 and will reach 200 million by 2019 [6], [7]. According to Evaluate Ltd. [8], medical devices sales will increase at a rate of 5% annually, touching $530 billion by 2022. Transparency Market Research [9] claims that medical devices, particularly implantable devices are anticipated to increase at a rate of 300 to 500 percent in 2018. In addition, the technology is forecasted to touch a market value of almost 57,653 million dollars by 2020 that is three times more of 2016 [10]. In addition, a recent report forecasts that the implantable medical device industry would grow at the rate of 8 percent and will reach 73.9 billion dollars by 2018 [11]. Similarly, according to Sudip [12], the wearable devices market will expand at the rate of 16 percent and will earn 5.8 billion dollars by 2019.

Such medical innovations generally present a double-edged sword. On the one hand, they have improved the quality of healthcare treatments while on the other hand, they have opened ground for the adverse security breaches that affected the lives of individuals negatively. For instance, in the case of an intelligent treatment, implantable insulin pump collects and analyzes physiological values from adjacent sensor nodes to get an accurate value of dose. However, in case these sensor nodes are malicious, then the decision based on the physiological signals derived from these sensors would be faulty and even puts human life in danger [13]. Healthcare is an attractive target for hackers to exploit due to its huge attack surface. A recent technical report states that almost 10 to 15 networked medical devices are present with a single bed in a hospital [14]. Researchers from academia and industry and public announcements have frequently reported the presence of security vulnerabilities in the firmware of connected medical devices and their underlying causes. The common theme is the absence of security measures in the design of electronic systems (software) that is integrated within these devices. Software used in medical devices is of extreme importance since it is responsible for critical functions. The vulnerabilities present in the software of medical devices are mostly responsible for successful cyber-attacks in healthcare. During the last decade, almost 1,527,311 medical devices were affected by breaches [15] due to software vulnerabilities. Furthermore, the proliferation of wireless technology in these medical devices leads to a greater number of cyber-attacks. Majority of the medical devices use Bluetooth, Wi-Fi, radio frequency, and ZigBee channels to communicate. In the same way, medical devices making use of wired communication technology also become a victim of cyber-attacks. Adversaries can misuse these channels to launch targeted and sophisticated attacks on medical devices as discussed in this survey. Therefore, cyber-security experts should look beyond wireless vector in order to address all security vulnerabilities while maintaining the availability and usability of these devices. The value proposition of implantable devices, wearables, and on-site equipment in terms of monitoring has some intersection with Wireless Body Area Network (WBAN) as it provides a system for inclusive monitoring by incorporating wearable and implantable sensors.

During the last few years, several survey papers have been published that target security issues in WBANs and IMDs [16], [17], [18], [19], [20] but none of those comprehensively considered security vulnerabilities of implants, wearables, and on-site medical equipment requiring FDA approval. The survey presented by Seneviratne *et al.* [21] discussed state-of-the-art wearables that do not require FDA approval and are not in the scope of WBAN. To the best of our knowledge, this is the first exhaustive study that not only reviews security vulnerabilities present in all medical devices but also studies security-related attacks demonstrated by researchers from academia and industry. Moreover, the research highlights policy and regulatory weaknesses that serve these issues in the first place. Finally, it discusses countermeasures available for these problems and concludes the paper with some open research areas. The major contributions of this paper are listed below.

- Identification of possible attack vectors with the help of network model for medical devices.
- Discussion of security vulnerabilities present in state-of-the-art medical devices, including implantable devices, wearables, and on-site equipment.
- Description of applicable attacks on medical devices and the attacks which the researchers actually demonstrated from industry and academia to highlight the need for security.
- A comprehensive review of the United States and European Union regulations for marketing medical devices and their underlying limitations.
- Comprehensive analysis of policy weaknesses that lead to a great number of security weaknesses present in medical devices.
- A discussion and analysis of existing countermeasures to resolve problems associated with medical devices.
- Open research areas are presented based on the literature reviewed.

The rest of this research is organized into five different sections that discuss all major contributions of the paper. In Section II, we present an overview of network model of medical devices in order to understand their security issues followed by attack vectors and features of communication technologies. Section III surveys security weaknesses present in state-of-the-art medical devices and their communication technologies with an emphasis on demonstrated and applicable cyber-attacks. Further, it reviews policy weaknesses that increase security issues in medical devices. Section IV reviews and analyzes leading edge countermeasures available in the market to overcome security issues of medical devices. Section V discusses some potential open research areas and Section VI concludes the paper.

II. Overview of Networked Medical Devices

Ubiquitous healthcare is an evolving technology, which ensures an increase in availability, veracity, and efficiency

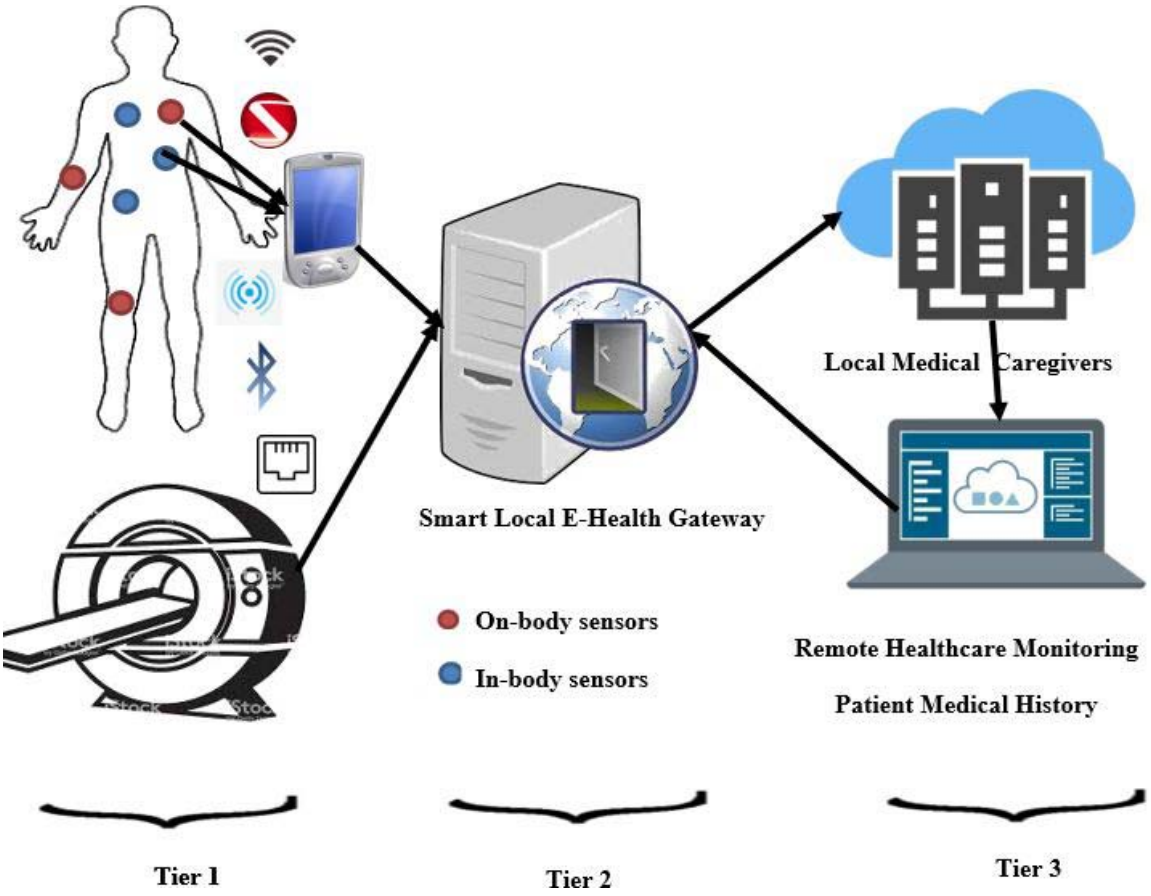

Fig. 1. Network Model.

of medical cure through recent innovations in electronics, wired and wireless communication. In the case of wireless communication, medical devices incorporate intelligent and small sensors to be used in, around, on, or embedded in the human body. In this perspective, WBAN establishes a prominent arena of research and development since it proposes the perspective of remarkable improvement in the monitoring and delivery of quality health-related facilities [22]. WBAN comprises several heterogeneous biological sensors that are placed in different parts of the human body and can be implanted in human skin or wearable. Based on the placement of sensors, WBAN can be referred to as implantable WBAN and wearable WBAN. WBAN nodes can be in the form of implanted node, external node, or body surface node. Implant node is placed inside the human body just underneath the skin. External node does not have a direct connection with the human skin while the body surface node is positioned on the surface of the human body [23]. The sensor-based medical devices can be used for monitoring human movements, measuring variations in vital signs of the patient, diagnosing specific disease and identifying human statuses or emotions including stress, happiness or fear. In general, these devices communicate with the distinct coordinator node that possesses additional processing capabilities and is less energy constrained. These are actually accountable for transmitting biological signals of patients to physician for real-time monitoring of patient's vital signs as it helps in the timely diagnosis of acute diseases [24]. Similarly, a huge amount of medical devices make use of wired technology to provide quality healthcare facilities. In general, wired networks are used to connect hospitals, data center, and medical devices. Their application in transferring large image files from radiology and cardiac devices is tremendous. HIMSS in their report states that the wired network is the sole method of connecting medical devices and health information systems [25].

A. Medical Devices' Communication Architecture

To comprehend security challenges of medical devices, it is significant to comprehend the structure of communication that devices follow to interact with physicians, cloud-assisted data center, hospital management system [26], and data analytics systems. The network model is shown in Fig. 1 to comprehend communication flow and possible attack vectors.

Tier 1 presents wireless medical devices that integrate a set of intelligent, small-sized, and resource-constrained wireless on-body sensors and in-body sensors that are positioned in different parts of the human body to store, process, and monitor different psychological parameters required for diagnosis. This tier also includes on-site medical devices, including radiology and ICU equipment, ventilator, anesthesia, dialysis machines, etc. and is connected to the Internet for providing accurate health treatments. The majority of these devices contain sensors as well. Furthermore, short distance technology

comprising Bluetooth Low Energy (BLE), ZigBee, low power WPAN, Wi-Fi, Bluetooth, Ethernet, etc., are used to transfer sensed information to the gateway (tier 2). Wireless medical devices share physiological data through PDA/smartphone or device programmer commonly known as Body Control Unit (BCU).

Tier 2 depicts the transmission of sensed data from mobile devices or medical equipment to a smart local gateway via wired or wireless communication protocols. Several e-health gateways are distributed geographically developing the fog to perform health-related tasks at the local layer [27]. Each gateway behaves like the dynamic touching point between Internet/local switch and WBAN as it supports different protocols. It performs sophisticated services including protocol conversion, filtering, data aggregation, and security. Health providers can access sensed patient information through the gateway.

Tier 3 presents cloud computing which is utilized to store and analyze relevant data gathered in tier 1 and processed in tier 2. This tier implements data analytics, epidemical, and statistical medical research, broadcasting, machine learning tasks and data warehouse. Finally, it delivers a graphical interface for feedback and final visualization. Service providers and caregivers can use this cloud infrastructure to access trends of diseases, medical history, epidemics, and remote healthcare monitoring.

B. Attack Vectors

With the help of network model depicted in Fig. 1, it can be analyzed that network connectivity to wearables, IMDs and on-site medical equipment open attack surface. These devices are open to security breaches at different stages. Seven possible attack vectors are identified by analyzing the network model that are listed below.

- *Software/Firmware/Hardware vulnerabilities:* Attacks are possible on this vector due to the use of insecure practices to develop software, inadequate integrity, and authenticity checks to update firmware and use of malicious ICs or embedded hardware Trojans.
- *BLE/ZigBee/Wi-Fi/RF/Ethernet communication protocol:* This channel could be vulnerable to targeted and sophisticated attacks due to improper configuration of protocol, use of obsolete proprietary protocol and inefficient existing security solutions.
- *A personal computer or smartphone app:* Smartphone apps used along with sensory devices are prone to different attacks due to non-compliance with regulations and their over-privileged nature.
- *App connection to the gateway through Wi-Fi:* The transmission of health data directly from sensors, devices or via a smartphone app is open to different attacks due to lack of security mechanisms.
- *Storage of data at the gateway:* In case of inadequate security mechanisms such as robust encryption, authentication, access control, and inappropriate policy framework, the health data might be at risk.
- *Gateway connection to the cloud:* It is another important area, which is exposed to security breaches in case inappropriate security mechanisms. Secure data transmission to the cloud is challenging.
- *Data stored in the cloud for further analysis:* Due to inadequate security mechanisms such as robust encryption, authentication, access control of data stored in the cloud, several attacks are applicable.

These seven fragments sketch the major possible areas for security breaches. This research investigates general security flaws, along with the discussion of demonstrated and applicable attacks applicable to attack vectors of tier 1 with help of existing IMDs, wearables, and on-site medical equipment.

C. Medical Devices' Communication Technologies, Standards, and Security Challenges

Networked medical devices require both wireless short-range standards and wired technologies to perform their respective tasks efficiently. Medical devices, therefore, use BLE, Wi-Fi, ZigBee, Radio Frequency (RF), and Ethernet to communicate [23], [28], [29]. The review of security features present in these standards is discussed in Table I.

1) ZigBee: ZigBee is an important technology used by the majority of the sensor based devices. It is an efficient technology, which is extensively used in a low power setting. It is directed at applications that use radio frequency, and entail long battery life, secure networking, low throughput, and low data rate. The ZigBee-enabled sensors normally have long battery lives since with the help of sleep mode feature these devices could remain operational for quite a lot of years before their batteries' depletion. The significant ZigBee network devices include end devices, router, and coordinator. The essential functionality is dependent on the coordinator that works as a full-function device and is installed primarily [30]. This component is responsible for the management and establishment of the overall network. The router also has major responsibility, i.e., to prolong network coverage with the help of routing function. However, it is incapable of creating a network by itself. End devices normally have limited functionality and are responsible for sensing and transmitting data over the network with the help of router and coordinator. ZigBee networks could be managed in the star, mesh, and cluster topologies containing two significant components. The main component is the ZigBee alliance that actually entitles application layers, network description, security, and software application layers. The second important component is the IEEE 802.15.14 standard that describes medium and physical layers regarding access control. According to the aforementioned standard, access to the wireless channel is through slotted Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). It also assists in handling the allocation and management of a guaranteed time slot (GTS) and channel access. ZigBee enabled medical devices normally operates in frequency bands of 868 MHz, 915 MHz, and 2.4 GHz. The typical range of ZigBee communication is 10 to 100 meters that entirely depends on environmental conditions and output power. However, for long-distance communication, mesh topology can also be used [30]. Advanced Encryption Standard (AES) algorithm along with a 128-bit key is used

TABLE I
COMMUNICATION TECHNOLOGIES USED BY MEDICAL DEVICES

Wireless technology	**Standard adopted**	**Frequency**	**Network topology**	**Transmission range**	**Bitrate**	**Encryption**	**Authentication**
Bluetooth	802.15.1	13.56 MHz and 2.4 GHz ISM band	Piconet	10 to 30m	2.1 Mbit/s	E0 stream cipher	Shared key
BLE	802.15.1	2.4 and 2.5 GHz ISM band	Star	50m	2.1 Mbit/s	AES block cipher	CBC−MAC
ZigBee	802.15.4	8 MHz, 915 MHz, and 2.4 GHz	Mesh, cluster tree, star	10 to 20 m	250 Kbit/s	AES block cipher	CBC−MAC
IEEE 802.15.6	802.15.6	HBC, UWB, NB	Star	$<$ 100m	75.9 Kbit/s to 15.6 Mbit/s	Elliptic curve public key cryptography	AES−CCM
UWB	802.15.4a	3.1 and 10.6 GHz	Peer to Peer, piconet	10m	480 Mbit/s	AES cipher CTR counter mode	CBC−MAC
Wi-fi	802.11	2.4 GHz	Mesh	100m	54 Mbit/s	RC4 stream cipher	WPA2
Low Power Wi-Fi	802.11ah	950, 915, 868, and 780 MHz	Single hop	100 − 1000m	150 Kbit/s	128 bit AES	CBC−MAC
Ethernet	802.3/u/z/ab/an	—	Point-to-Point, coaxial bus, and star network	100m copper, 100m copper, 5000m fiber, 100m copper, and 100m copper	10 Mbps, 100 Mbps, 1000 Mbps, 1000 Mbps and 10 Gbps	Medium Access Control Security (MACSec)	Extensible Authentication Protocol (EAP)

in this standard to provide security. To enhance the security mechanism, ZigBee uses three entirely different keys, including master key, link key, and network key. The link key is used for secure data exchange by ensuring confidentiality between nodes. Each node pair possesses the unique key that is handled at the application layer whereas network key is created by a trust center and is utilized by all devices. The master key is responsible for the secure exchange of link keys among different nodes and is preconfigured before deployment. To connect ZigBee network, each of the nodes should request current network key by using the preconfigured master key. However, such standard is vulnerable for energy depletion attack, DOS, replay attack, and sniffing [31]. Moreover, AES is not suitable for resource-constrained sensory devices as it is a complex cryptographic algorithm and demands a great amount of battery power and processing capabilities.

2) Bluetooth: It was specifically planned for short-range wireless communication. This technology enables devices to communicate up to seven other devices simultaneously through single piconet. It basically forms an ad hoc network in which one device acts as master and the others as slaves. For communication, slaves actually have to synchronize with master device clock by following a pattern directed by the master. Apart from that, these devices can even belong to different piconets concurrently since they move in the proximity to some other master devices [40]. An important characteristic of such technology is that it provides an opportunity to connect and communicate with a range of devices from almost all over the world. Another important characteristic is the capability of these devices to communicate without any requirement of the unobstructed positioning of gadgets. It is therefore widely used for connecting personal devices. These devices operate in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band by consuming frequency hopping. It stipulates three categories of devices, based on their transmission power and coverage that varies between 1 to 100 m and generally lies within 10 to 30 m. Moreover, the maximum rate of data is 3 Mbps. To provide security, Bluetooth technology incorporates stream cipher entitled E0 that requires re-synchronization for all payloads [41]. The major components of such cipher include encryption/decryption routines, stream and payload key generator. Key size normally varies between 8 to 128 bits in this scheme depending upon the communication devices. Although some security mechanisms are present in this system, it is

still vulnerable to viruses, Man-in-the-Middle (MITM) and blue-snarfing [42].

3) Bluetooth Low Energy (BLE): BLE is a derived standard of Bluetooth and is an appropriate approach for sensor-based medical devices due to low power consumption. BLE is specifically designed for connecting small sensor-based devices to portable stations. They are very minute to hold power consumption and cost of traditional Bluetooth radio. However, in health monitoring, their application is tremendous. This standard could even provide 1 Mbps data rate. Synchronization of devices could take a few milliseconds as it uses few channels for pairing devices [41]. Such characteristic of BLE enables it an ideal choice for latency critical sensory devices. Its features including low energy consumption, low latency, and nominal data rate make it appropriate for communication between an access point (AP) and sensor nodes. Furthermore, robust frequency hop spread spectrum permits BLE to coincide with Wi-Fi. On the other hand, intervention with other devices might be a concern in this standard since the BLE functions in the 2.4 to 2.5 GHz ISM band. Security in BLE is present in three different modes ranging between no security, pass key and numeric comparison but is still vulnerable to MITM, tracking, and sniffing [40].

4) IEEE 802.11: It is a set of standards that are explicitly planned for wireless local area network (WLAN). In general, this technology has four important standards including 802.11 a/b/g/n. The standard operates in 2.4 and 5 GHz ISM band with coverage of almost 100 m [43]. According to this standard, Wi-Fi lets users surf Internet once connected to AP or in ad-hoc mode at broadband speeds. It is normally appropriate for the large rate of data transfer by contributing high-speed wireless connectivity and permitting video streaming and conferencing. The most important benefit of such a standard is that all devices, laptops, tablets, and smartphones are Wi-Fi integrated while high-energy consumption emerges as an important drawback [28].

5) IEEE 802.11ah: This standard was developed in 2014 specifically for Wireless Local Area Network (WLAN) that functions in almost 900 MHz [36]. The major objective behind the development of such standard is to enhance the capabilities of IEEE 802.11ac in the light of low power devices [37]. Apart from that, another important consideration during the development of this standard is to use lower frequencies since it possesses lower power consumption and helps in extending range.

6) IEEE 802.3: Ethernet is one of the most widely used standards put forth by the IEEE for wired connectivity. It is also known as the CSMA/CD protocol, which specifies networking and physical characteristics of wired network. This standard consists of two different components including interconnecting media and network nodes.

- Interconnecting media can be defined as the media through which the signals propagate within the network. Its basic objective is to determine the rate at which data transfers. It can be coaxial cable, twisted pair cables, and Fiber Optics Cable.
- Network nodes are the points from which communication takes place, which include Data Terminal Equipment (DTE) and Data Communications Equipment (DCE).

Ethernet makes use of several network topologies including point to point, coaxial bus, and star network for communication. The transmission rate of this standard varies between 10 Mbps, 100 Mbps, 1000 Mbps, 1000 Mbps and 10 Gbps. Such standard provides the provision of connectionless user data integrity, origin authenticity, and data confidentiality, data confidentiality through MACsec and EAP.

III. State of the Art Medical Equipment and Associated Security Vulnerabilities

Medical devices generally transmit sensed data to the nearby smartphone, local gateway and cloud for further real-time analysis. The sensed data is confidential in nature as it presents unique personal data. Therefore, secure transmission of such data emerges as an important issue. Due to resource-constrained nature of wearable and implantable medical devices, it is not possible to incorporate traditional security mechanisms [38]. On the other hand, in case of on-site medical equipment, security was not considered while manufacturing these devices and for this reason, they are using insecure proprietary protocols [39]. It, therefore, increases the attack surface in the context of medical devices. This section comes up with a survey of state of the art medical devices with an emphasis on security vulnerabilities and cyber-attacks. Table II presents a list of devices that are reviewed in this paper. The devices include wearables, implantable devices, and on-site medical equipment. It studies important security vulnerabilities present in existing devices along with demonstrated or possible attacks and their consequences. The wearable devices surveyed in this paper include tracking devices with a smartphone app or smartphone app with built-in smartphone sensors that used BLE or Wi-Fi as a communication medium [29]. On the other side, the majority of the reviewed implantable devices use RF, BLE, and Wi-Fi as a communication medium while on-site medical equipment uses WLAN or Wi-Fi.

Threats to medical devices can be of confidentiality, integrity, or availability. Threats related to confidentiality include situations in which adversary gets unauthorized access to some sensitive information. In integrity related threats, attacker tampers sensitive information without authorization. However, attacks related to availability include cases in which adversary acts to deny services to legitimate users. Table III demonstrate that attacks on medical devices are due to vulnerabilities in communication protocols, design flaws in software and absence of appropriate security mechanisms during development [40]–[42]. Majority of the researchers exploited the communication protocol used by implantable devices in order to gain access to the device. Moreover, encryption, integrity check, and authentication mechanisms in these devices are weak or lacking due to which eavesdropping, firmware modification, spoofing, and tampering attacks are possible and demonstrated by researchers. In addition to this, to attack some devices like cardioverter defibrillator there is no need to be in close proximity as an implementation flaw in device keeps it

TABLE II
STATE OF THE ART MEDICAL DEVICES

Type	Devices
Implantable	Cardioverter-Defibrillator, Insulin pump, Automated external defibrillator, St Jude Promote, Boston Scientific Cognis, Medtronic Adapta and Medtronic InSync Sentry, Brain-Computer Interfaces (BCI), Cardiac monitor, pacemakers, Oximeter, Accelerometer, Hermes medical shoe platform, Syringe Infusion Pump, Gastric electrical stimulator, Infusion pumps, Cardiac Science G3 Plus, Pacemakers, St. Jude cardiac device, OneTouch Ping Pump, and Prosthetic Limb
Wearables	Withings Activite, Apple watch, Basis Peak, Microsoft band 2, Mobile Action Q-band, Pebble Time, Runtastic Moment Elite, Strivv Fusion, Xiaomi MiBand, Acer Liquid Leap, Fitbit Charge, Aria, Alta, Surge Iconic, Flex, Garmin Vivosmart, Huawei Talkband B1, LG Lifeband Touch FB84, Withings Plus Ox/WS30, Nike+ Fuelband SE, Codoon band, Jawbone, Basis watch, Xiaomi Huami, Samsung Gear 3, Google glass, Samsung smart watch, Activ8rLives, Thomson TBS705, iChoice S1, Withings Cardio, Bong 3 HR smart band, MiBand 2, TW64 and Mambo HR, Dexcomrx glucose monitor, Gear Fit, OTbeat, Forerunner 920, Up Move, Pebble steel smart watch, 1301 Android smart watch apps, 512 Apple smart watch apps and 129 Samsung smart watch apps
On-site equipment	Siemens Healthcare, GE Healthcare, Canon, Philips Healthcare, Toshiba Medical Systems, RainbowFish, Samsung, Medical Imaging Devices (MID), Computed Tomography (CT) and Medical Resonance Imaging (MRI), ReliOn Xray and MRI machines, CareFusion Xray and MRI machines, Positron Emission Tomography (PET) scanner, CT scanner, Medical ventilator, Anesthetic machine, Heart-lung machine, Dialysis machine, Fluoroscopy workstation and radiation oncology system

in standby mode after it has been activated [43]. This, in turn, brings it to interrogation mode once it receives some message.

A. Demonstrated Cyber Attacks on Medical Devices

Some of the demonstrated attacks on medical devices are discussed in Tables XVIII, XIX, XX, and XXI.

1) Firmware Modification Attack: In the firmware modification attack, an adversary tries to modify program stored in non-volatile memory that controls hardware of devices. The firmware update is an important feature present in modern devices to improve the user experience. However, attackers exploit such feature by injecting custom firmware due to inefficient security mechanisms. Rieck [65] performed firmware modification attack on Withings Activite fitness tracker by reverse engineering the firmware code using IDA pro. The checksum Cyclic Redundancy Check (CRC) 32 is used here to authenticate updates. However, the adversary can easily replace such checksum by altering the original firmware to evade all checks as demonstrated in [65]. Another group of study [19], [40], [67], [69], [70], [77] also demonstrated a similar attack on wearables as described in Table XIX and Table XX. In the case of implantable devices, firmware modification attack is studied periodically in literature. Hei *et al.* [51] demonstrated this attack on Automated External Defibrillator (AED) by exploiting inadequate procedure of CRC as a digital signature. Researchers reverse engineered the firmware code and overwrote recent exception handler in order to execute own code. Similarly, [45], [59], [60] discussed this attack on ICD and Cardiac Science G3 Plus AED that are further elaborated in Table XVIII. Summary of these type of attacks is given in Table III.

2) Eavesdropping: It is the real-time interception of users personal information by an unauthorized entity. This attack is critical, as it becomes an entry point for the majority of other attacks as well. Existing literature shows that BLE and RF technology is vulnerable to an eavesdropping [43], [45]. Cusack *et al.* [72] in their research demonstrated an eavesdropping on a wearable device, i.e., Fitbit Charge tracker, due to fixed MAC address in advertisement packets. They analyzed BLE traffic using Ubertooth, Adafruit, and HCI snoop log to exploit the public device address. Another group of literature [71], [76], [79] demonstrated this attack on wearables by exploiting the vulnerability of static MAC address as described in Table XIX and Table XX. Likewise, eavesdropping is possible on implantable medical devices. Marin *et al.* [43] demonstrated eavesdropping attack by reverse engineering communication protocol. Due to the lack of suitable encryption mechanism, an adversary could intercept the packets. Moreover, signal processing techniques also help in extracting secret keys used in implantable devices [43]. In the same way, [16], [43], [44], [45], [47], [48], [49], [50], [51], [53], [56], and [90] also discussed eavesdropping in commercially available implants and on-site medical equipment as discussed in Table XVIII and Table XXI. The brief summary of eavesdropping applicable to medical devices is discussed in Table IV.

3) Sniffing: Another frequently occurring attack upon medical devices is sniffing. Hardware and software sniffers are widely used in literature to sniff traffic and perform the analysis. Kim *et al.* [40] demonstrated sniffing by analyzing static MAC addresses in advertisement packets through ubertooth on three commercially available trackers including A-fit, B-fit, and C-fit. Similarly, [196] performed traffic analysis using blueberry pi scanning device and extracted sensitive health information in plain text due to lack of encryption mechanism. In addition, [70] also intercepted credentials in plain

TABLE III
FIRMWARE MODIFICATION ATTACK

Medical device	Type	Attack methodology	Vulnerability
Automated external defibrillator [45]	Implantable	Reverse engineering (overwrite recent exception handler in order to execute own code)	Input validation checks are missing. The inadequate use of CRC as a digital signature does not ensure integrity. Weak authentication mechanisms as passwords are obfuscated with simple XOR mechanism that can easily be compromised. Passwords in plaintext are stored on the local drive and can be easily extracted.
ICD [59]	Implantable	Reverse Engineer communication protocol	Lack of encryption and authentication
Cardiac Science G3 Plus Automatic External Defibrillator (AED) [60]	Implantable	Transferring malicious commands to device	Lack of secure key exchange and authentication mechanisms
Withings Activite fitness tracker [65]	Wearable	Reverse engineer firmware Health Mate version 2	Design flaws and weak authentication mechanism to verify updates
Huawei Talkband [67], [19]	Wearable	Reverse engineer application code	Lack of encryption and integrity check mechanism
Fitness tracker [69]	Wearable	Reverse engineer gateway application and create fake gateway by exploiting authentication related vulnerabilities	Lack of authentication for a firmware update
Fitbit trackers including flex, Ionic, and Alta [70]	Wearable	Reverse engineer firmware tracker and official application	Credentials in plaintext are just secured by HTTPS that does not prevent MITM, Weak encryption and verification mechanisms, On activating live mode, after authentication all traffic goes unencrypted, hardcoded private name
Nike+ Fuelband [77]	Wearable	Reverse engineer the band	The absence of read and write protection on the device. Checksum value can easily be modified
Codoon band [65]	Apps tracking physiological data	Reverse engineer application	The robust authentication mechanism is not present
A-fit, B-fit and C-fit apps [40]	Apps tracking physiological data	Reverse engineer gateway and android application. Further, BLE traffic is analyzed through ubertooth	Encryption mechanism is not present. Authentication and integrity check mechanisms are not incorporated

text form by reverse engineering the firmware and official application of Fitbit trackers including flex, Ionic, and Alta as described in Table XIX and Table XX. Likewise, [40], [53], [69], [70], [72], [73], [74], [76], and [78] also sniffed the traffic of commercially available wearables. In implantable devices and on-site equipment, the attack is possible as [53] sniffed signal of the implanted accelerometer to extract the secret key and [90] sniffed traffic of 52 different medical devices as described in Table XVIII and Table XXI. A summary of such attack is given in Table V.

TABLE IV
EAVESDROPPING

Medical device	Type	Attack methodology	Vulnerability
Cardioverter Defibrillator [43]	Implantable	The reverse engineering of proprietary communication protocol	Lack of authentication, encryption, and integrity mechanism. An implementation flaw keeps the device in standby mode due to which there is no need to be in close proximity in order to attack device.
Insulin pump [16][44]	Implantable	Universal Software Radio Peripheral	Lack of encryption mechanism due to which messages were transmitted in plain text. Moreover, the prevention mechanism against DOS is also missing.
Automated external defibrillator [45]	Implantable	Reverse engineering (overwrite recent exception handler in order to execute own code)	Input validation checks are missing. The inadequate use of CRC as a digital signature does not ensure integrity. Weak authentication mechanisms. Passwords are in plaintext
Brain-Computer Interfaces (BCI) [47][48]	Implantable	Brain spyware	Intercept signals by using malicious software i.e. spyware to extract sensitive information
Cardiac monitor [49]	Implantable	Communication channel exploitation	Lack of encryption, Hardware/software flaws
Pacemakers [50]	Implantable	Communication channel exploitation	Lack of encryption and access control, Hardware/software flaws
Insulin pump system [51]	Implantable	Exploit wireless communication channel	Lack of encryption
Accelerometer [53]	Implantable	Communication channel exploitation (Captures sound produced by vibration motor to extract key with help of signal processing techniques)	Lack of security mechanisms in the communication protocol
Gastric electrical stimulator [56]	Implantable	Wireless channel exploitation	Lack of encryption and authentication mechanism, Hardware/Software error
Insulin delivery alarm system [156]	Implantable	Lack of information, signal reduction, and noise addition techniques	Initialization-based method, confirmation-based technique, and duration-based methods are used to determine medical condition, injected insulin and device's battery status
Fitbit charge and surge [71][72]	Wearable	Traffic analysis using ubertooth, adafruit, and HCI snoop log	Fixed MAC address
Xiaomi Huami [72]	Wearable	Traffic analysis using ubertooth, adafruit, and HCI snoop log	Fixed MAC address
Google glass [76]	Wearable	Traffic analysis	Weak authentication and encryption mechanism
Dexcomrx glucose monitor, Gear Fit, OTbeat, Forerunner, UpMove [79]	Wearable	Traffic analysis	Lack of MAC address randomization
52 medical devices, including X-ray machines, PACS, and MRI [90]	On-site hospital equipment	Map radiology department subnet with nmap and analyzed through OpenVas and Wireshark	Unpatched OS (XP, Service Pack 2 and Service Pack 3, Enabled Server Messenger Block (SMB) protocol, Lack of authentication mechanism or default passwords, Unencrypted data during rest and transit

4) Information Disclosure: This attack is related to information exposure by an unauthorized entity due to weaknesses in device or communication medium. Such an attack is common in all devices. Rahman *et al.* [66] in their research demonstrated an information disclosure attack on Fitbit fitness tracker by reverse engineering the communication

TABLE V
SNIFFING

Medical device	Type	Attack methodology	Vulnerability
Pebble steel watch [13]	Wearable	Traffic analysis	Lack of robust authentication mechanism
Fitbit trackers including flex, Ionic, and Alta [70]	Wearable	Reverse engineer firmware tracker and official application	Credentials in plaintext are just secured by HTTPS that does not prevent MITM, Weak encryption and verification mechanisms, On activating live mode, after authentication all traffic goes unencrypted, hardcoded private name
Samsung gear 2 3 live [72]- [74]	Wearable	Injecting counterfeit message to forget the previous key and generate a new key	Weak encryption and authentication mechanism
Google glass [76]	Wearable	Traffic analysis	Weak authentication and encryption mechanism
TW64 Bong 3 HR band [78]	Wearable	Traffic analysis using TI SmartRF, and BLETestTool	Lack of encryption mechanism
A-fit, B-fit and C-fit apps [40]	Apps tracking physiological information	Reverse engineer gateway and android application. Further, BLE traffic is analyzed through ubertooth	Encryption mechanism is not present. Authentication and integrity check mechanisms are not incorporated
Fitness trackers (with the app) [69]	Apps tracking physiological information	Reverse engineering the application code	Single MAC address is used to advertise device for connection establishment, Lack of encryption (passwords in plaintext), Absence of privacy policies and security mechanisms

protocol. Researchers extracted sensitive health information due to lack of authentication, consistency check, and encryption mechanism. Other group of literature [19], [32], [40], [67], [69], [72], [73], [74], [83], [84], [85], [88] and [89] extracted sensitive information from wearables due to policy and permission weaknesses, lack of security mechanisms, BLE weaknesses and design flaws of devices as discussed in Table XIX and Table XX. The summary of this attack is given in Table VII. In the same way, literature reported that adversaries could disclose information in implantable and on-site devices. Marin *et al.* [43] extracted sensitive health-related information by reverse engineering communication protocol. Due to the lack of suitable encryption mechanism, an adversary could intercept the packets. Likewise, researchers [16], [43], [44], [45], [47], [48], [49], [50], [51], [53], [55], [56], [58], [59], [60], [61], [64], [90] and [91] successfully extracted sensitive information from commercial implantable devices and on-site equipment through Universal Software Radio Peripheral, reverse engineering, spying, traffic analysis, and side channel attacks due to lack of encryption, authentication, host certificate validation mechanism, and OS vulnerabilities as discussed in Table XVIII and Table XXI. This attack is also applicable on-site medical equipment as researchers [106]–[117] and [118]–[129] due to lack of input validation, authentication, encryption, and access control mechanisms. The details of security vulnerabilities and attack methodologies are discussed in Table XXI. Similarly, researcher [161] performed acoustic and EM signal-based attack to capture physiological information from BP monitoring device. Moreover, wireless radio, i.e., oscilloscope and some open-source tools can send false signals. The summary of this attack is given in Table VI and Table XV.

5) MITM: Such an attack happens when an adversary intercepts the communication between two legitimate parties, and is prevalent in all medical devices. Rieck [65] demonstrated MITM attacks on Withings Activite fitness tracker by reverse engineering the firmware Health Mate version 2 due to design flaws and weak authentication mechanism to verify updates. Similarly, [13], [42], [65], [70] and [76] accessed health-related information from wearables through reverse engineering communication protocol and Android application, MITM proxy and traffic analysis and are discussed in Table XIX and Table XX. Ellouze *et al.* [44] demonstrated such attack on insulin pump through Universal Software Radio Peripheral by exploiting lack of encryption mechanism. Other researchers [45], [51], [52], [55], [59], [90] and [92] also reported similar attack on implants and on-site equipment by exploiting communication channel and host certificate validation and are discussed in Table XVIII and Table XXI. The summary of this attack is described in Tables VI, VII, and XV.

TABLE VI
INFORMATION DISCLOSURE, UNAUTHORIZED ACCESS AND MITM ON IMPLANTABLE DEVICES

Medical device	**Attack methodology**	**Vulnerability**
Cardioverter Defibrillator [43]	Reverse engineering of proprietary communication protocol	Lack of authentication, encryption, and integrity mechanism. An implementation flaw keeps the device in standby mode due to which there is no need to be in close proximity in order to attack device.
Insulin pump [16], [44]	Universal Software Radio Peripheral	Lack of encryption mechanism due to which messages were transmitted in plain text. Moreover, the prevention mechanism against DOS is also missing.
Automated external defibrillator [45]	Reverse engineering (overwrite recent exception handler in order to execute own code)	Input validation checks are missing. The inadequate use of CRC as a digital signature does not ensure integrity. Weak authentication mechanisms as passwords are obfuscated with simple XOR mechanism that can easily be compromised. Passwords in plaintext are stored on the local drive and can be easily extracted.
Brain-Computer Interfaces (BCI) [47], [48]	Brain spyware	Intercept signals by using malicious software i.e. spyware to extract sensitive information
Cardiac monitor [49]	Communication channel exploitation	Lack of encryption, Hardware/software flaws
Pacemakers [50]	Communication channel exploitation	Lack of encryption and access control, Hardware/software flaws
Insulin pump system [51]	Exploit wireless communication channel	Lack of encryption
Oximeter [52]	Communication channel exploitation	Lack of security PIN required for pairing
Accelerometer [53]	Communication channel exploitation (Captures sound produced by vibration motor to extract key with help of signal processing techniques)	Lack of security mechanisms in the communication protocol
Syringe Infusion Pump [55]	File Transfer Protocol (FTP) server exploitation	Lack of authentication mechanism in the FTP server while allowing FTP connections, Lack of validation of host certificates
Gastric electrical stimulator [56]	Wireless channel exploitation	Lack of encryption and authentication mechanism, Hardware/Software error
Infusion pumps [58]	Embedded system vulnerabilities exploitation	Lack of encryption, authentication and access control mechanism, Default hardcoded administration passwords
ICD [59]	Reverse Engineering of the communication protocol	Lack of encryption and authentication
Pacemakers [61]	Operating system (XP) vulnerabilities exploitation	Windows XP vulnerabilities

6) Unauthorized Access and Spoofing: Due to security vulnerabilities present in medical devices, an adversary can access sensitive health-related information by unfair means and can even spoof health service providers. These attacks are reported frequently in literature in the context of all devices. Researchers [40], [41], [42], [66], [69], [70], [72], [75], [76], [85], [86] and [87] and obtained sensitive health information from wearables by reverse engineering communication protocol and brute force to obtain pin used for pairing and traffic analysis as described in Table XIX and Table XX. In case of the implantable and on-site medical devices, these attacks are applicable as [14],

TABLE VII
INFORMATION DISCLOSURE, UNAUTHORIZED ACCESS, AND MITM ON WEARABLES

Medical device	Attack methodology	Vulnerability
Withings Activite fitness tracker [65]	Reverse engineering the firmware Health Mate version 2	Design flaws and weak authentication mechanism to verify updates
Fitbit tracker [66]	Reverse engineer communication protocol	Lack of encryption, authentication and consistency check mechanism
Mobile action Qband [42]	Exploitation of communication protocol and app	Lack of authentication and encryption mechanism
Runtastic Moment Elite [42]	Communication channel and app exploitation	Lack of authentication mechanism and communication protocol's privacy is not incorporated
Strivv Fusion [42]	Communication channel and app exploitation	Lack of authentication mechanism
Xiaomi MiBand [42]	Communication channel and app exploitation	Lack of authentication mechanism
Acer liquid leap [67]	Communication channel and app exploitation	Lack of authentication mechanism
Huawei Talkband [67], [19]	Reverse engineer application code	Lack of encryption and integrity check mechanism
Nike+ Fuelband SE [67], [19]	Reverse engineer application code	Lack of robust authentication mechanism
Pebble steel watch [13]	Traffic analysis	Lack of robust authentication mechanism
Fitness tracker [69]	Reverse engineer gateway application and create fake gateway by exploiting authentication related vulnerabilities	Lack of authentication
Fitbit trackers including flex, Ionic, and Alta [70]	Reverse engineer firmware tracker and official application	Credentials in plaintext are just secured by HTTPS that does not prevent MITM
Samsung gear 2 3 live [72]- [74]	Injecting counterfeit message to forget the previous key and generate a new key	Weak encryption and authentication mechanism
Fitbit mobile app [83], [84]	Commercial use of patient sensitive data due to policy weaknesses	The vendor can use and exploit personal health data
Basis watch [85]	Policy weakness regarding data usage, collection, transfer, and storage	The vendor can use and exploit personal health data
A-fit, B-fit and Cfit apps [40]	Reverse engineer gateway and android application. Further, BLE traffic is analyzed through ubertooth	Encryption mechanism is not present. Authentication and integrity check mechanisms are not incorporated
Fitness trackers (with the app) [69]	Reverse engineer application code	Lack of encryption
Android and Apple apps [88]	Static and dynamic analysis using MITM proxy	Unencrypted credentials and sensitive information

[18], [43], [44], [45], [51], [53], [58], [60], [61], [62], [90] and [93] discussed and demonstrated those as listed in Table XVIII and Table XXI. The brief description of tampering and spoofing upon all medical devices is given in Tables VII, XV, IX, and X.

7) Replay Attack: Replay attack in the context of medical devices is about obtaining valid packet data transmitted by these devices with an intention to corrupt or impersonate it. Researchers [70] and [73] demonstrated this attack on wearable fitness trackers by exploiting weaknesses of

TABLE VIII
INFORMATION DISCLOSURE, UNAUTHORIZED ACCESS, AND MITM ON ON-SITE EQUIPMENT

Medical device	Vulnerability	Attack Methodology
52 medical devices, including X-ray and MRI [90]	Obsolete OS, Enable SMB protocol, and lack of authentication	Mapped radiology department subnet with nmap and analyzed through OpenVas and Wireshark
Medical Imaging Devices (MID), Computed Tomography (CT) and Medical Resonance Imaging (MRI)[91]	Lack of authentication mechanism	Security analysis
Phillips IntelliSpace Cardiovascular (ISCV) [105],[106],[107]	Improper privilege management, plaintext credentials, and inadequate session expiration	Malware to access ISCV server
Philips Xcelera Cardiology Information Management [106],[108]	Improper privilege management, and plaintext credentials	Malware to access ISCV server
Philips iSite/IntelliSpace PACS [109]	Insufficient encryption, and authentication, poor authorization, and hard-coded weak credentials	PACS server and memory addressing exploitation
Philips Alice 6 Polysomnography System (PSG) [110]	An improper authentication, encryption and integrity check scheme	Analysis of network packets
General Electronics (GE) optima medical imaging system [111]	Hardcoded or default credentials	Network analysis
GE digital radiographic imaging systems [111]	Hardcoded or default credentials	Traffic analysis
Revolution medical imaging systems [111]	Hardcoded or default credentials	Traffic analysis
Centricity PACS imaging systems [112]	Hardcoded or default credentials	Network analysis
Thunis stationary fluoroscopic and radiographic X-ray system [112]	Traffic analysis	
Entegra nuclear medicine workstation [112]	Hardcoded or default credentials	Network analysis
CADstream medical imaging software [112]	Hardcoded or default credentials	Network analysis
Image vault medical imaging software [112]	Hardcoded or default credentials	Network analysis
Millennium medical imaging system [112]	Hardcoded or default credentials	Network analysis
The precision medical imaging system [112]	Hardcoded or default credentials	Network analysis
Xeleris medical imaging workstations [113]	Hardcoded or default credentials	Network analysis
Withings wireless blood pressure monitor [114]	Insufficient encryption mechanisms	Traffic analysis through Wireshark
Mayo clinic 20,000 networked medical equipment [115]	Hardcoded passwords, Old OS and transfer and communication protocols, unencrypted communication	Traffic analysis, reverse engineering, vulnerability scanning, and fuzz testing
Philips e-Alert unit [117]	Hardcoded credentials, Lack of encryption, and input validation	Traffic analysis and known exploits
Blood gas analyzer [113]	Lack of encryption and authentication mechanism	Zeus and catidel malware to create the backdoor
PACS [114]	Lack of encryption and input sanitization	Malicious code injection
X-ray systems [114]	Lack of encryption and input validation	Malicious code injection
Neurostimulator/Implantable Pulse Generator (IPG) [123]	Lack of encryption	Traffic analysis

authentication, encryption mechanism and hardcoded MAC address for pairing. Similarly, [18] demonstrated replay attack on smartphone apps due to improper certificate validation and privilege escalation that is listed in Table XIX and Table XX. In implantable devices, [43] demonstrated replay attack on cardioverter defibrillator by reverse engineering

TABLE IX
SPOOFING AND REPLAY ATTACK

Medical device	Type	Attack methodology	Vulnerability
Cardioverter Defibrillator [43]	Implantable	Reverse engineering of proprietary communication protocol	Lack of authentication, encryption, and integrity mechanism
Insulin pump [16], [44]	Implantable	Universal Software Radio Peripheral	Lack of encryption mechanism
Automated external defibrillator [45]	Implantable	Reverse engineering (overwrite recent exception handler in order to execute own code)	Input validation checks and authentication mechanisms are missing
Oximeter [52]	Implantable	Communication channel exploitation	Lack of security PIN required for pairing
ICD [59]	Implantable	Reverse Engineering the communication protocol	Lack of encryption and authentication
Mobile action Qband [42]	Wearable	Exploitation of communication protocol and app	Lack of authentication and encryption mechanism
Pebble time [42]	Wearable	Communication channel exploitation	BLE privacy policy is not properly considered and incorporated
Strivv Fusion [42]	Wearable	Communication channel and app exploitation	Lack of authentication mechanism and communication protocol privacy is not incorporated
A-fit, B-fit and Cfit apps [40]	Wearable	Reverse engineer gateway and android application. Further, BLE traffic is analyzed through ubertooth	Encryption mechanism is not present. Authentication and integrity check mechanisms are not incorporated
Fitbit Aria (apps) [72]	Apps tracking physiological data	Static and dynamic analysis using open-source tools	Privileged app and pinning mechanism for SSL is absent
Withings WS-30 app [73]	Apps tracking physiological data	Static and dynamic analysis using open-source tools	Privileged app and pinning mechanism for SSL is absent
Activ8rLives /Body Analyser [73]	Apps tracking physiological data	Static and dynamic analysis using open-source tools	No password policy, Over-privileged and trust manager issue due to improper certificate validation
Thomson TBS705 app [73]	Apps tracking physiological data	Static and dynamic analysis using open-source tools	Lack of encryption
Withings Cardio app [73]	Apps tracking physiological data	Reverse engineer and traffic analysis	Privileged app and pinning mechanism for SSL is absent

proprietary communication protocol and exploiting its limitations in terms of integrity and authentication mechanism. Likewise, [52] and [59] also performed such attack on an insulin pump and ICD due to inherent weaknesses of devices as discussed in Table XVIII. A brief description of such attack is given in Table IX.

8) Tampering and Modification Attack: These attacks are related to alteration in data without proper authorization. Researchers [60] reported such attack on wearable Fitbit tracker due to lack of authentication, encryption, and consistency check mechanism. Similarly, due to lack of MAC address randomization, tampering is possible in Apple watch [42]. In addition, [14], [40], [42], [66], [67], [69], [70], [72], [73], [78] and [86] demonstrated such attack on wearables by exploiting their vulnerabilities as discussed in Table XIX and Table XX. Both attacks are also prevalent in implanted devices and are discussed by the researchers multiple times. Researchers [16], [43], [47], [48], [49], [50],

TABLE X
TAMPERING AND MODIFICATION ATTACK ON IMPLANTABLE DEVICES

Medical device	Attack methodology	Vulnerability
Cardioverter Defibrillator [43]	Reverse engineering of proprietary communication protocol	Lack of authentication, encryption, and integrity mechanism. An implementation flaw keeps the device in standby mode due to which there is no need to be in close proximity in order to attack device.
Cardiac monitor [49]	Communication channel exploitation	Lack of encryption, Hardware/software flaws
Pacemakers [50]	Communication channel exploitation	Lack of encryption and access control, Hardware/software flaws
Hermes medical shoe platform [54]	Communication channel exploitation (Alter values of pressure sensor)	Weak encryption techniques
Syringe Infusion Pump [55]	FTP server exploitation	Lack of authentication mechanism in the FTP server while allowing FTP connections, Lack of validation of host certificates
Gastric electrical stimulator [56]	Wireless channel exploitation	Lack of encryption and authentication mechanism, Hardware/Software error
Cardiac Science G3 Plus Automatic External Defibrillator (AED) [60]	Transferring malicious commands to device	Lack of secure key exchange and authentication mechanisms
Pacemakers [61]	Operating system (XP) vulnerabilities exploitation	Windows XP vulnerabilities
Prosthetic limb [64]	Traffic analysis	Weak encryption and authentication mechanism

[51], [52], [53], [54], [55], [56], [60], [61], [62], [63] and [64] demonstrated this attack on commercially available implants by exploiting communication channel, FTP server, encryption, and authentication mechanism as described in Table XVIII. These attacks are also applicable to stationary hospital equipment since researchers [90]–[93] studied the feasibility of cyberattack on such devices through vulnerability scanning and traffic analysis as shown in Table XXI. Since on-site medical equipment lacks security configurations and at-least 70% of such devices have enabled Server Message Block (SMB) and other vulnerable ports. Further, robust authentication and encryption mechanisms are also missing. Due to these factors, an unauthenticated remote attacker can easily hijack these devices and can tamper with patient's sensitive data. Similarly, the physiological information from implants and wearables can be tampered through wireless radio, i.e., oscilloscope, radio frequency electromagnetic waves, and some open-source tools as they can send false signals [129] and [161]. The summary of this attack is given in Tables X, XI, and XII.

9) DOS, Resource Depletion, and Jamming Attack: These attacks are associated with disabling the device by exhausting its energy rapidly. Due to resource-constrained nature, a battery of such devices could be drained easily by launching these attacks. The basic objective of adversary behind such attacks is to make the device or service unavailable for legitimate users. In the case of wearable devices, [60] demonstrated resource depletion attack on commercially available Fitbit trackers. Likewise, [42], [44]–[45], [49]–[50], [56], [78] and [86] performed DOS on codeblue, Fitbit TW64 and Mambo HR and are discussed in Table XIX and Table XX. In perspective of implantable and on-site devices, [16], [18], [41], [43], [44]–[45], [50]–[51], [55]–[56], and [60]–[64] discussed these attacks on an implantable insulin pump, cardioverter defibrillator, pacemakers, gastric electric simulator, ICD, MRI machines, X-ray machines and St. Jude cardiac device that is described in Table XVIII. The brief description of such attack is discussed in Table XIII.

10) Side Channel Attack: Such an attack is performed by attackers in order to obtain sensitive health information. Side channel and Electromagnetic (EM) analysis attacks are demonstrated by [17], [83] on commercially available implantable devices by analyzing power consumption and EM radiations multiple times to extract secret information. After having secret information, the attacker has complete control over the device. In the same way, EM signal injection attack is demonstrated by [46], [49] on the Cardiac implantable electric device by introducing strong forged signal in order to overlook legitimate signal. Such strong forged signal ignores legitimate signal due to which patient's health can be at risk. It exploits EMI that effects circuit by inducing forged voltage on conductors. Due to it, defibrillation shocks and pacing can be induced to cardiac device. This attack is also applicable to wearable devices as [80]–[81] exploited vulnerabilities of commercially available smartwatches to demonstrate side channel attack. Motion sensors of smartwatch were used as a side channel in order to gather critical information of the user. Likewise, [82] exploits vulnerabilities of the key-based

TABLE XI
TAMPERING AND MODIFICATION ATTACK ON WEARABLES

Medical device	Attack methodology	Vulnerability
Fitbit tracker [66]	Reverse engineering of the communication protocol	Lack of encryption, authentication and consistency check mechanism
Basis peak [14] [42]	Reverse engineer application code	Code obfuscation is partially considered that allows an attacker to reverse engineer the code
Runtastic Moment Elite [42]	Communication channel and app exploitation	Lack of authentication mechanism and communication protocol privacy is not incorporated
Strivv Fusion [42]	Communication channel and app exploitation	Lack of authentication mechanism and communication protocol privacy is not incorporated
Xiaomi MiBand [42]	Communication channel and app exploitation	Lack of authentication mechanism and communication protocol privacy is not incorporated
Acer liquid leap [67]	Communication channel and app exploitation	Lack of authentication mechanism and communication protocol privacy is not incorporated
Garmin Vivosmart [67]	Reverse engineering of application code	Code obfuscation is not considered that allows an attacker to reverse engineer the code
Fitness tracker [69]	Reverse engineer gateway application and create a fake gateway by exploiting authentication related vulnerabilities	Lack of authentication for a firmware update
Fitbit trackers including flex, Ionic, and Alta [70]	Reverse engineer firmware tracker and official application	Credentials in plaintext are just secured by HTTPS that does not prevent MITM, Weak encryption and verification mechanisms, On activating live mode, after authentication all traffic goes unencrypted, hardcoded private name
TW64 Bong 3 HR band [78]	Traffic analysis using TI SmartRF, and BLETestTool	Lack of encryption mechanism
Thomson TBS705 app [73]	Static and dynamic analysis using opensource tools	Lack of encryption
iChoice S1 app [73]	Static and dynamic analysis using opensource tools using open-source tools	Trust manager issue due to improper certificate validation
A-fit, B-fit and C-fit apps [40]	Reverse engineer gateway and android application. Further, BLE traffic is analyzed through ubertooth	Encryption mechanism is not present. Authentication and integrity check mechanisms are not incorporated
Fitbit Aria (apps) [72]	Static and dynamic analysis using opensource tools	Privileged app and pinning mechanism for SSL is absent
Withings Cardio app [73]	Reverse engineer and traffic analysis	Privileged app and pinning mechanism for SSL is absent
Heart rate sensors [124]	Lack of authentication	With the help of radio frequency electromagnetic waves, the erratic heartbeat can be forged. Moreover, false signals can also be inserted

security system of smartwatch by analyzing the pattern of key entry from sensors to capture hand movement between two consecutive key presses through traffic analysis or malicious app installation as described in Table XIX and Table XX. The summary of this attack is described in Table XIII.

11) Ransomware DOS: This attack is possible on on-site medical equipment due to the use of an obsolete operating system and insecure proprietary protocols [90]–[93] as discussed in Table XX. It is similar to traditional DOS attack in which legitimate users are unable to access medical facilities until hospital administration pays desired ransom. Such an attack has serious consequences as in an emergency; unavailability of medical devices and treatment might kill a human. The summary of this attack is described in Table XIII.

12) Other Attacks: Another important attack discussed by [17] is hardware Trojan on the implantable device. It

TABLE XII
TAMPERING AND MODIFICATION ATTACK ON ON-SITE EQUIPMENT

Medical device	**Attack methodology**	**Vulnerability**
52 medical devices, including X-ray and MRI [90]	Mapped radiology department subnet with nmap and analyzed through OpenVas and Wireshark	Unpatched Windows, Server Message Block (SMB) protocol enabled, Lack of authentication and encryption
Medical Imaging Devices (MID), Computed Tomography (CT) and Medical Resonance Imaging (MRI) [91]	Security analysis	The absence of an authentication mechanism
MRI, X-Ray, Positron Emission Tomography (PET) scanner, CT scanner, Medical ventilator, Anesthetic machine, Heart-lung machine, Dialysis machine [93]	Security analysis, Reconnaissance, Scanning	Default passwords, unpatched obsolete OS
X-ray machine [92] [93]	Malware injection to create a backdoor	Malware injection using shellcode execution technique on x-ray machine that was running Windows NT 4.0
Phillips IntelliSpace Cardiovascular (ISCV) [105], [106], [107]	Improper privilege management, plaintext credentials, and inadequate session expiration	Malware to access ISCV server
Philips Xcelera Cardiology Information Management [106], [108]	Improper privilege management, and plaintext credentials	Malware to access ISCV server
Philips iSite/IntelliSpace PACS [109]	Inadequate addressing of memory locations, insufficient encryption and authentication, and access control	PACS server and memory addressing exploitation
Blood gas analyzer [113]	Lack of encryption and authentication mechanism	Zeus and catidel malware to create a backdoor
Neurostimulator/Implantable Pulse Generator (IPG) [123]	Lack of encryption and default passwords	Traffic analysis
Philips' IntelliVue Patient [125]	Improper authentication mechanism, Lack of limit checks	An unauthenticated attacker can access memory, read it and even can tamper it
Avalon Fetal Monitors [125]	Improper authentication mechanism, Lack of limit checks	An unauthenticated attacker can access memory, read it and even can tamper it
Philips Brilliance CT scanners [126]	Hardcoded credentials and OS vulnerabilities including escalated privileges	Traffic analysis
BD Alaris TIVA Syringe Pump [127]	Improper authentication scheme	With the help of malware or traffic analysis, an attacker can gain unencrypted wireless credentials of the pump

was because of a malicious function embedded in Integrated Circuit (IC) of the device. A buffer overflow was also demonstrated by [35], [43] on a commercially available insulin pump and AED. In addition, the brute force attack was also demonstrated by [63], [75] on an iSatan medical mannequin to extract credentials with help of open source tools. Grey hole, Sybil attack, and masquerading attacks were also demonstrated by [86] on codeblue as described in Tables XVIII, XIX and XX. Furthermore, buffer overflow and remote code execution are also applicable to on-site medical equipment [105]–[109], [124], and [129].

B. Policy Weaknesses

Due to increased acceptance and adoption of networked medical devices, policy and regulatory solutions become extremely important in overcoming security-related challenges. Incorporation of technology in healthcare is making information more transparent and there is a need for formulating stringent policies to prevent unauthorized disclosure. Cybersecurity is an area with an increased risk to the healthcare industry and patients since more medical devices started using wired or wireless network connectivity. Health Insurance Portability and Accountability Act (HIPAA) [94], Federal

TABLE XIII
DOS, RESOURCE DEPLETION AND JAMMING ATTACK

Medical device	Type	Attack methodology	Vulnerability
Cardioverter Defibrillator [43]	Implantable	Reverse engineering of proprietary communication protocol	Lack of authentication, encryption, and integrity mechanism.
Insulin pump [16],[44]	Implantable	Universal Software Radio Peripheral	The pump is bombarded with requests
Automated external defibrillator [45]	Implantable	Reverse engineering (overwrite recent exception handler in order to execute own code)	Input validation checks are missing
Cardiac monitor [49]	Implantable	Communication channel exploitation	Lack of encryption, Hardware/software flaws
Pacemakers [50]	Implantable	Communication channel exploitation	Lack of encryption and access control, Hardware/software flaws
Gastric electrical stimulator [56]	Implantable	Wireless channel exploitation	Lack of encryption and authentication mechanism, Hardware/Software error
St. Jude cardiac device [18],[62]	Implantable	Traffic analysis	Weak encryption mechanism
Fitbit tracker [66]	Wearable	Reverse engineering the communication protocol	Lack of encryption, authentication, and consistency check mechanism
Fitbit trackers including flex, Ionic, and Alta [70]	Wearable	Reverse engineer firmware tracker and official application	Weak encryption and verification mechanisms
TW64 Bong 3 HR band [78]	Wearable	Traffic analysis using TI SmartRF, and BLETestTool	Lack of encryption mechanism
Codeblue [86]	Software tracking physiological data	Traffic analysis	Lack of authentication and encryption mechanism
MRI and Xray machines by ReliOn and CareFusion [92]	On-site equipment	Shodan API to get IP addresses of devices that are pass-through vulnerability scanner	Malware injection to create backdoor
PET scanner, Medical ventilator, Anesthetic machine, Heart-lung machine, Dialysis machine [93]	On-site equipment	Security analysis, Reconnaissance, Scanning	Default passwords and unpatched obsolete OS
Fluoroscopy workstation and radiation oncology system [92],[93]	On-site equipment	Malware injection to create a backdoor	Malware injection using shellcode execution technique
X-ray machine [92],[93]	On-site equipment	Malware injection to create a backdoor	Malware injection
Philips iSite/IntelliSpace PACS [109]	On-site equipment	Inadequate addressing of memory locations insufficient encryption, authentication, and authorization	PACS server and memory addressing exploitation
Qualcomm's Life Capsule Datacaptor Terminal Server (DTS) [116]	On-site equipment	Inadequate authentication and misfortune cookie vulnerability	This vulnerability hands out a crafted HTTP cookie resulting in an arbitrary write to the device's memory
Philips e-Alert unit [117]	On-site equipment	Hardcoded credentials and improper input validation	Traffic analysis and known exploits
GE PACSystems RX3i [121]	On-site equipment	Lack of input validation due to which an attacker can send specially crafted packets exhausting system's resources	Exploitation of missing input validation mechanism

Drug Administration (FDA) [95], European Union (EU) [96], and General Data Protection Regulation (GDPR) [97] are important agencies that regulate privacy, safety and security of health data and medical devices. Researchers have demonstrated that FDA approved medical devices are susceptible to cyber-threats such as unauthorized access, tampering, and ransomware. Networked medical devices do not possess suitable controls and hence interrupt the delivery of health services leading to patient harm. To deal with such security issues and to ensure the public that the networked medical devices are

TABLE XIV
RANSOMWARE, EM SIGNAL INJECTION, AND SIDE-CHANNEL ATTACKS

Medical device	Type	Attack methodology	Vulnerability
Implantable wearable medical device [17]	Implantable	Analyzing power consumption and EM radiations multiple times to extract secret information and reverse engineering	Analyzing power consumption and EM radiations multiple times to extract secret information, Malicious function embedded in the device's IC.
Boston Scientific Cognis, Medtronic Adapta and InSync Sentry [46]	Implantable	Introduce strong forged signal in order to overlook legitimate signal	Lack of low pass filters
Ambulatory BP monitoring device [156]	Device tracking physiological information	Lack of information, signal reduction, and noise addition techniques	Algorithm AmbBP and VHA antenna
MID, CT, and MRI [91]	On-site equipment	Security analysis	The absence of authentication mechanism since modification and tampering is possible
PET scanner, Medical ventilator, Anesthetic machine, Heart-lung machine, Dialysis machine [93]	On-site equipment	Security analysis, Reconnaissance, Scanning	Majority of the devices uses default passwords that can be found online by using maintenance and operating manuals. Moreover, devices used unpatched obsolete operating systems including Windows XP and service pack 2
Fluoroscopy workstation and radiation oncology system [92], [93]	On-site equipment	Malware injection to create a backdoor	Malware injection using shellcode execution technique on Fluoroscopy workstation and radiation oncology system that was running Windows XP operating system
X-ray machine [92], [93]	On-site equipment	Malware injection to create a backdoor	Malware injection using shellcode execution technique on x-ray machine that was running Windows NT 4.0
Bayer Medrad medical device [128]	On-site equipment	Windows OS vulnerabilities	National Security Agency (NSA) hacking tools

effective, safe and secure, FDA reviews the pre-market submissions that are submitted by manufacturers to market devices. According to FDA, cybersecurity is the process of averting unauthorized access, unauthorized use, unauthorized modification, or misuse of information, which is accessed, stored or transmitted from a device to an external receiver [98]. FDA categorizes medical devices in three major classes based on risks associated with them as shown in Fig. 2. Class I devices are simple and are liberated from regulatory controls. The devices in class II have more security issues comparatively and are more concerned about effectiveness and safety. Class III devices pose the highest security risks and require the most stringent controls. Regulatory classification is based on the risk device poses to human and the level of controls required for ensuring its safety and effectiveness.

Important regulations that FDA requires to manage the effectiveness and safety of medical devices are discussed below.

- *Medical device listing and establishment registration:* The distributors and manufacturers of medical devices should register their organization with the FDA in order to market or sell their devices. The registrations can be done through FDA Unified Registration and Listing System (FURLS). The verification of registration information every year is mandatory. Moreover, organizations must provide details of the device that they are manufacturing.
- *Labeling:* It is essential for devices to label devices in the form of information and description that go with device usage.
- *Medical Device Reporting (MDR):* In case medical device malfunctions or causes a serious injury or death, it is essential for manufacturers/importers/healthcare facility to report FDA. The basic objective of such a regulation is to detect and correct issues by monitoring and identifying the substantial negative effects of a particular device.

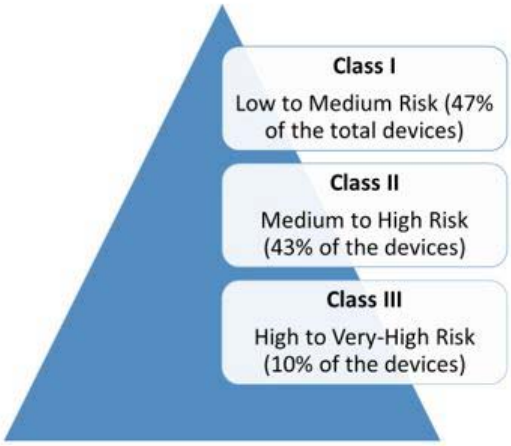

Fig. 2. Medical Devices Classification.

- *Quality System (QS) regulations:* QS specifies requirements related to controls, facilities, and methods used for entire medical device lifecycle, such as designing, purchasing, manufacturing, labeling and packaging, servicing, and installation of the devices. The FDA commands to ensure that the devices fulfill pertinent specifications and requirements reliably.
- *Investigational Device Exemption (IDE) for clinical studies:* Such provision permits manufacturers to gather device-specific effectiveness and safety data prior to commercialization that can be utilized to support 510-k application or PMA.

C. FDA's Regulation of Medical Devices

FDA legalizes medical devices through a total product lifecycle method that consists of two important phases including premarket and post-market. To receive FDA approval, manufacturer necessarily submits proper documentation proving that the device is effective and safe to use. After clearance, FDA conducts oversight activities including sharing of security vulnerabilities when identified, monitoring and examination of connected medical device's effectiveness and safety. Generally, to approve medical device through FDA, the manufacturer must submit one of the two important premarket submissions and is shown in Fig. 3. These include Pre-market notification/510-k approval or PMA. Devices that pose a medium risk to an individual usually goes through the 510-k approval process. A manufacturer who submits a 510-k application should provide appropriate assurance of device's effectiveness and safety by proving that the particular device is substantially equivalent to an existing legally marketed device, which is not subject to PMA. Unlike PMA, the 510-k application does not require non-clinical and clinical data showing effectiveness and safety of the device. On the other side, high-risk devices require PMA, which is a comprehensive review of the device along with clinical and non-clinical trials and testing.

Majority of the class I devices are exempted from any of the regulations. However, the rest of them should comply with

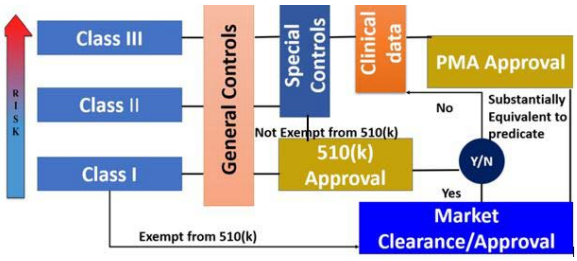

Fig. 3. Regulatory Process of FDA.

general controls in which pre-market notification is the significant provision. Class II devices are subject to general and special controls for which 510-k or PMA is required. If new device manufacturer can find substantially equivalent predicate, then he can request FDA to approve device through 510-k. Otherwise, PMA is essential. Class III devices must undergo strict systematic review and get clear through PMA. Fig. 3 shows the overall procedure of the device's approval with respect to the device's classes. FDA has classified MDDS including e-health solutions as class I devices, which are exempt from 510-k or PMA.

1) FDA Submissions Review Process: FDA staff reviews all submissions in two phases, including initial and substantive review. In the initial review stage, the FDA team determines whether the manufacturer has submitted complete, correct and appropriate documentation. In the next phase, staff assesses performance and software data along with labeling and cybersecurity information to determine the device's effectiveness and safety. Devices that fulfill all these requirements get clearing or approving status.

D. European Union

Medical Device Directive (MDD) [97] is the body which regulates the marketing and safety of medical devices in Europe since the 1990s. In contrast to FDA, EU classifies medical devices into four classes depending upon its risk level and intended purpose. These include class I (Is and Im), IIa, IIb and III. The higher the class, the greater the level of assessment. The devices cannot be advertised in the EU countries without adherence to rigorous regulations. The most important regulation is the Conformite Europe (CE) marking [99]. All devices should have CE mark prior to marketing in Europe. This mark ensures that the device fulfills the safety criteria and can be sold freely without some additional controls. This process is managed by EU accredited private organizations named notifying bodies (NBs). NBs are observed, appraised and nominated by the member states by means of the national competent authorities. Important functions of this body include device certification, class designation, quality system verification and assessment, and design dossier reviews. For approval, a manufacturer must select an NB to endow certification of a new device for CE marking. NB, in turn, will require technical details and other literature based on the class of device to review device's safety. Class I (with sterility requirements or measuring functions) to III should put forward Declaration of Conformity to appropriate EU directives and the specifics

TABLE XV
COMPARISON BETWEEN U.S. AND EU REGULATIONS

Specifications	U.S. Regulations	EU Regulations
Medical device regulation	Federal food, drug, and cosmetic act	MDD
Pre-market and post-market supervision of devices	FDA is primarily accountable for such supervision and granting clearance or approval	The autonomous private enterprise NBs are responsible for supervision and certification
Risk classification	Three important classes including class 1 devices (low-risk), class 2 devices (moderate risk and class 3 devices (highest risk)	Four important classes including class I (Is and Im), IIa, IIb and III
Approval system	Class I devices: general controls Class II devices: 510(k) clearance Class III devices: PMA	CE mark on medical devices is essential for ensuring safety and effectiveness

of the conformity assessment plan being followed. In addition, the highest risk devices also require design examination. Rest of the class I devices are exempt from such regulations; however, they should follow vital propositions of efficacy and safety in their design along with labeling and construction obligations. After device approval, post-market surveillance is the authority of member states through a competent authority. The brief summary of the differences between both regulatory bodies is presented in Table XV.

E. Cybersecurity Initiative of FDA and EU

FDA has taken an initiative to manage cybersecurity issues present in the networked medical devices through premarket and post-market cybersecurity guidance. The manufacturers should discuss cybersecurity issues associated with the device during PMA or 510-k submissions. FDA's QSR requires manufacturers to develop and maintain procedures for risk analysis and software validation. FDA also requires devices to incorporate cybersecurity risks through analysis. During the course of the last few years, FDA has delivered some important guidance documents, especially to manage cybersecurity issues. Despite all these efforts, cybersecurity has not been fully integrated, but FDA is proactively taking steps to consider security issues of medical devices properly. Some of the important guidance documents are discussed below.

- *Premarket Cybersecurity Guidance 2014:* In October 2014, FDA issued a guidance document to help manufacturers in preparing submissions regarding cybersecurity issues during the design and development of networked medical devices. The guidance document suggests that manufacturers should consider potential cybersecurity threats, their severity, impact, and approaches to address them.

EU is working on improving the safety of medical devices as they published the new Medical Device Regulations (MDR) [100], [101] which will be applied after three years in case of medical devices and five years for vitro diagnostic devices. These regulations will improve the medical devices' safety by firming up the rules while placing new devices on the market and by tightening scrutiny once they are available on the market. Such guidance requires manufacturers to incorporate security mechanisms in the devices which have electronic programmable systems including software. Therefore, new regulations will be properly implemented by 2020 in the case of Regulation (EU) 2017/745 and 2022 for vitro diagnostic devices. It will strengthen clinical investigations for the availability of reliable clinical data. After enforcement of regulations, the notified bodies can perform unannounced on-site audits of the manufacturers in order to ensure safety, security, quality, and performance of these medical devices.

The regulations are much needed as the devices are now even more innovative and sophisticated. The current regulations date back to 1990s and have not kept pace with technical and scientific developments in the domain of healthcare. Currently, devices do not undergo through pre-market assessments. Instead, medium to high-risk devices goes through a conformity assessment in which notified body considers technical documentation of the device. The notified body decides the required controls of the device to maintain its safety which varies from country to country.

F. HIPAA

It establishes standards in order to protect personal health information and medical records. HIPAA rules are applicable to covered entities, including healthcare providers, health plans and healthcare clearinghouses in case they transmit information in electronic form. The HIPAA privacy rule protects Personal Identifiable health information (PHI) by requiring suitable privacy-related controls. However, HIPAA does not cover medical devices and pharmaceutical companies. Nevertheless, such organizations generally do participate in activities and programs that involve disclosure or use of PHI by a business associate or covered entity. Even HIPAA does not apply directly, but these companies are fortified to follow best practices in order to protect the privacy and security of PHI which is in their control. Therefore, manufacturers must use de-identified information instead of PHI. The non-compliance with HIPAA leads to serious consequences. In the first five months of 2017, nine legal cases were filed by Health and Human Services Office for Civil Rights (OCR) for HIPAA defilements which lead to a fine of million dollars [102].

G. GDPR

GDPR is the EU privacy-related regulation which is applicable to the processing of personal data by a processor or

controller in EU. Personal data is the information linking to an identifiable person. This regulation is applicable to all sectors that process personal information of EU citizens. In the healthcare sector, biometric data, genetic data, and data concerning health is sensitive information. The regulation forbids the processing of such data until consent is given. All healthcare organizations, including private and public hospitals, health insurance companies, and medical device manufacturers must comply with GDPR [103].

H. Limitations of Existing Regulations

1) Critical Analysis of 510-k and PMA Submissions: Although FDA has taken an initiative to handle cybersecurity vulnerabilities present in medical devices, but it is still not properly integrated [104]. The premarket cybersecurity guidance provides an approach to consider cybersecurity risks present in devices but only 25% class III devices go through pre-market review. Among them, just 51% of the manufacturers actually refer to these guidance documents. While rest of the manufacturers receive FDA's 510 (k) treatment that means these devices irrationally clear the test of substantially equivalence. These devices get FDA clearance by showing them equivalent to a legally marketed device that might not adopt cybersecurity from scratch. For instance, devices that substitute hardware with some software are authorized without an analysis procedure regardless of the instances like Therac-25, which exhibit that these replacements often introduce perilous bugs [131], [132]. By analyzing 510 (k) summary documents of Hospira Sapphire Sets infusion pump and Epiphany Healthcare Programmable diagnostic computer [133], it can be noted that the predicate device Hospira plum sets and PCA infusion systems are vulnerable to cyberattacks [134]. Furthermore, neither report discusses security issues or controls to address them. Similarly, Class III CardioMEMS Heart Failure Monitoring System [135] PMA summary report does not demonstrate security tests, static code analysis, dynamic analysis, and cybersecurity risks. This comprehensive report discussed test cases, component information, device's functionality, adverse events and compliance with international standards such as ISO 10555-1, EN 62304, IEC 60601 etc. but cybersecurity tests and vulnerabilities have not been considered separately.

2) Limitations of Standard Tools and Documents Used for Review: FDA team uses two important tools to review 510-k or PMA submissions of networked medical devices. First tool Refuse-To-Accept checklist [136] is used to screen applications for completeness during the initial review of FDA. Whereas, for substantial review, another template named SMART is used by reviewers in order to organize and guide outcomes of their review. Both documents lack a dedicated section for cybersecurity. Since these documents are publicly available and serve manufacturers with the minimum criteria that FDA uses to accept an application for initial and substantive review [104]. In the case that any of the mandatory information is lacking, FDA might refuse the application until the manufacturer provides it. Therefore, the manufacturer can use it as a guideline to prepare their submissions properly. The Refuse-To-Accept checklist requires documentation on labeling, testing, software, engineering, and sterilization. However, documentation regarding cybersecurity is not required based on this checklist. Likewise, the SMART template used by reviewers for 510-k submissions also does not incorporate a separate section for cybersecurity in which all concerns regarding device's vulnerabilities and controls can be considered [104]. Although, software section is present in the template, but it cannot cover malicious cybersecurity vulnerabilities and non-software aspects of the device. For instance, physically protecting the device or restricting functionalities to authorized and authenticated users. As cybersecurity section is missing in both of the tools, therefore, submissions from manufacturers might miss it due to which severe safety issues can arise.

3) Critical Analysis of Pre-Market Cybersecurity Guidance: FDA has proposed cybersecurity guidance document back in 2014. It suggests manufacturers to incorporate security in the design phase of medical devices. To analyze cybersecurity risks present in medical devices, FDA recommended NIST's critical infrastructure framework. This framework is effective, but it is not tailored for medical device and cannot be exactly fit in such an industry. Medical devices are different from traditional IT system and hence risks are also of a different nature. Traditional risk assessment approach cannot be used for medical devices as non-malicious (software bugs) and malicious (security vulnerabilities) errors can cause hazards. It is critical to identify software bugs that can cause hazards. Likewise, it is essential to find security vulnerabilities, which have the potential to cause hazardous events. A unified approach to determine security and safety risks is much needed as it provides a fair idea of all malicious and non-malicious errors that may cause hazards influencing patient safety.

4) Minimum Security Control Criteria: As the comprehensive description of safety-related controls has been defined by FDA with respect to a device class, therefore, it became easy for both regulators and manufacturers to comply with them. However, such guidance for security-related controls is missing. Due to which, it is difficult for manufacturers to incorporate security in their devices.

5) Cybersecurity in Labeling and Branding: QSR, labeling and branding controls required for almost all medical devices lack cybersecurity issues. As QSR provides a guide for maintaining quality in the medical device's design, risk assessment, production, and procurement, but it lacks cybersecurity concerns. The pre-market cybersecurity guidance document is still not properly enforced. Most of the medical devices are neither networked nor software-based due to which these considerations are missing. However, in the case of connected medical devices, QSR must cover security considerations in all these phases as well.

6) Medical Device Reporting: Another important regulation is to report adverse events associated with medical devices. The existing guidance provides an approach to manufacturers regarding reporting of adverse events that cause death or serious impairment. However, underreporting of medical devices issues by hospitals is a major concern as hospital staff

uses a variety of devices throughout the day [137]. According to current regulations, hospitals should report device problems within 10 days of adverse events to FDA and manufacturers. In 2016, FDA inspected 17 hospitals to check whether they report adverse events [138]. The results demonstrated that six hospitals didn't report both injuries and deaths within 10 days while 5 hospitals didn't report serious impairments in time. One important reason for such misreporting is lack of awareness, training or plan to comply with reporting requirements. For hospitals, well-drafted documented measures have not been developed, implemented and maintained by regulatory bodies. Due to these limitations, device reporting by hospitals is problematic.

7) Classification of Devices in the Context of Security Issues: FDA and EU classification can be misleading, as it does not reflect cyber-attack risks impersonated by the specific medical device. The classified based on the level of risk device poses to human and regulatory controls it requires safety and effectiveness. This classification is similar for all devices including networked, software-based, and hardware-based devices. All of these are not vulnerable to security breaches, therefore, this classification could not regulate devices with the appropriate security controls to avoid patient safety concerns. As by considering security issues, some class II devices can be critical enough to go through stringent regulatory reviews but are overlooked [131]. Based on security risk, its likelihood and impact, stringent security controls must be incorporated into medical devices. FDA, nowadays, has been working in this domain and proposed a draft guidance [139], which describes two tiers where tier 1 lists devices with an increased cybersecurity risk and tier 2 devices exhibit low-security risk as they do not contain software or networking capabilities. So, the traditional device classification cannot be followed in this case [140].

Similarly, Class I mobile related application or mobile app can acquire sensitive information from sensors, but FDA tends to exercise enforcement discretion, which means the regulatory body does not intend to regulate a device as they pose a low risk to patient safety [141]. Therefore, it can be exploited as an entry point to attack health systems. On the other hand, HIPAA also does not regulate medical devices, as manufacturers developing these devices do not comply with laws because they do not transmit sensitive data and are not required to use such mechanisms in the initial phase. Almost 84% of health applications are open to HIPAA violations and hacks due to non-compliance [142]. A study directed by BMC Medicine discovered that approximately 89 percent of mobile applications transfer information to online services while 66 percent of them transmit health information without encryption and 20 percent has no privacy policy [143]. Therefore, challenges related to the security of PHI and patient privacy increased rapidly.

8) Privacy Considerations: The regulatory bodies are now focusing on managing security vulnerabilities present in medical devices as some of these weaknesses impact patient safety. However, some of these vulnerabilities impacting patient safety can also impact their privacy as shown in Fig. 4. All of these vulnerabilities are interrelated and have a major impact

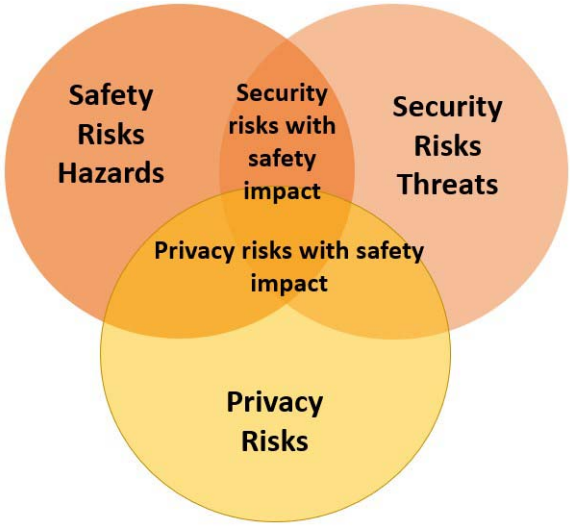

Fig. 4. The relationship between safety and privacy aspects of security vulnerabilities.

on both patient's safety and privacy. But regulatory bodies including FDA does not regulate the privacy-related risks of a medical device [144].

9) Lack of Medical Device Software Components Identification by Manufacturers: Another important issue in managing cybersecurity issues of medical devices is the identification of software and hardware components that hackers can exploit. Generally, medical devices seem black box as details of their software and technical specifications are not known. Therefore, FDA has decided to incorporate software details of medical devices by considering Software Bill of Materials (SBoM) [145]. SBoM covers softwares' version and release date of these softwares to help to manage the security weaknesses of medical devices. It will be cross-referenced with the Common Vulnerability Scoring System (CVSS) and National Vulnerability Database (NVD) for known vulnerabilities. However, some challenges associated with the SBoM includes the absence of configuration settings. Since the operating systems like Windows and Linux offer different services and in case medical devices which do not require these capabilities can simply disable them. Therefore, without knowing configuration settings, it would be difficult to analyze the security weaknesses and their exploitation [145]. Another important issue is the presence of SBoM within the SBoM. Majority of the third-party software present in medical devices also incorporate other open-source third-party functions and software. Hence, such details will be missing due to which some vulnerabilities present in these devices would be ignored altogether.

10) Wrong Classification of the Devices: During the last few years, there has been an increased recall of the devices [146]. One of the major reasons for these recalls is the wrong class designated to the device. Most of the devices were not considered high-risk device at the time of regulatory approval due to which they do not go through a stringent review process [147]. Therefore, such a wrong classification of the device might put human life in danger [147].

11) Lack of Harmonized Cybersecurity Standard Evaluation Framework: The national oversight bodies in Europe and EU have provided a limited guidance regarding cybersecurity mechanisms and practices, particularly for medical devices. Currently, NBs evaluates safety and effectiveness of medical devices and overseen by national authorities. However, new MDRs require manufacturers to develop devices in accordance with security mechanisms but does not provide comprehensive guidance regarding these mechanisms. It is a major limitation as the standards which combine conventional criteria for the functional safety of device with suitable IT security requirements are still missing. As a result, the certification bodies and manufacturers which evaluate devices for safety are left to develop their own medical IT security evaluation and certification frameworks. Therefore, cybersecurity standards, especially for medical devices, are fragmenting across Europe or even within EU member states.

12) Transparency Challenges: Transparency in the case of EU regulations is a challenge as different member states have established their own registration tools which are not always compatible with one another. This also places a pointless burden on the manufacturers who intend to market their devices in more than one country [148].

I. Fines and Penalties Due to Non-Compliance

Due to regulatory non-compliance, complaints have been filed by regulatory bodies. FDA has issued 44 warning letters to different medical devices industries due to pre-market issues, quality issues, poor reporting of adverse events and lack of approval [149]. Some of the non-compliance issues resulting in fines and penalties are discussed below.

- *RJX Implants, Inc. (TMJI):* FDA filed a complaint requiring Civil Money Penalty (CMP) for deteriorating to file MDRs. The company failed to report almost 21 MDRs associated with an implant device, which caused serious injury. FDA primarily sought 210,000 dollars which were then reduced to 170,000 dollars for each respondent [150]. The corporate appealed the decision to the United States Court of Appeals, but the final decision is not yet announced.
- *Advanced Bionics, Inc.:* Another complaint FDA has filed was against Advanced Bionics, Inc. for shipping cochlear implants to the United States without filing a complement to its PMA. Due to this, FDA was unable to review device for effectiveness and safety [150]. However, in 2008, FDA reached a settlement with FDA and corporate admitted paying 1.1 million dollars while its president conceded to pay 75,000 dollars.
- *Lahey Hospital and Medical Center:* HIPAA charged fine of 850,000 dollars to this hospital for losing PHI of 600 patients due to weak logical and physical security controls deployed in medical devices. Lahey hospital used these vulnerable devices in a Boston area medical facility. PHI was also stored in unencrypted form without authentication and access control mechanisms [152].
- *Alaska mental health services:* Due to use of unpatched software in a medical facility, HIPAA fined health organization 150,000 dollars. The software present in medical equipment exfiltrates PHI to unauthorized agencies [152].
- *Acclarent, Inc.:* This medical device company was fined 250,000 dollars for violating FDA regulations. The company marketed misbranded medical devices without approval. Furthermore, executives were imprisoned for three years [153].
- *Guidant LLC:* The subsidiary of Boston Corp. was fined 296 million dollars for serious safety issue in the life-critical cardiac device, i.e., implantable defibrillator [154]. The major issue of this device is short-circuiting which makes the device unavailable. Furthermore, the instructions to deal with short-circuiting issues were also false and misleading.
- *St. John's Regional Medical Center:* The medical center incurred a fine of 75,000 dollars for errors in a heart-lung medical device which led to the death of a patient during surgery [155].
- *UC San Diego Health-Hillcrest:* This health organization was charged a fine of 44,000 dollars due to issues associated with the death of a cardiac patient who was not properly connected to the telemetry monitor.
- *Riverside Community Hospital, Methodist Hospital of Sacramento, Mercy General Hospital, and Madera (Calif.) Community Hospital:* These hospitals were fined of 31,500, 47,452, 75,000 and 47,025 dollars for medication errors [156], [157].
- *Kaiser Permanente's Woodland Hills hospital:* This hospital has incurred a fine of 50,000 dollars due to a patient's death from erroneous dosage using a pain management system. The regulators are of the view that the hospital must have had controls which avert device from giving out a great amount of medicine within a limited time frame [158].
- *Palomar Medical Center in Escondido and Rideout Memorial Hospital in Marysville:* These hospitals were fined due to the problem in the bedside alarm system which did not activate in an emergency [159].

IV. Countermeasures for Securing Medical Devices

Medical devices are generally in direct connection with the human body and deals with sensitive information. These devices collect critical health information from users and transmit it through a wireless or wired communication channel. However, most of the low power sensor-based devices are really ill-prepared in the context of security challenges associated with network connectivity and therefore exposes surface for both active and passive attacks. It is due to the fact that the manufacturers tried to integrate software and hardware optimization, custom functionalities and low power consumption at the lowest cost. Therefore, security-related hazards are entirely overlooked as devices are complex. Similarly, the legacy on-site medical equipment lacks security features as they were developed long ago and at that

TABLE XVI
SUMMARY OF SOLUTIONS

Technique	Methodology	Overcomes attack	Advantage	Disadvantage
Attestation based mechanisms C-FLAT, LO-FAT, HAFIX and HCFI [160]-[167]	These approaches manage the flow of execution of the program through computing hashes and labeling vertexes	Remote code execution and buffer overflow	These techniques verify that the medical device application is following the accurate execution stream	Such approaches do not consider attacks related to data modification. Moreover, such an approach is not compatible with medical devices software developers must use a specific compiler and adjust coding styles accordingly.
Isolation based schemes Intel SGX, Sanctum, TrustZone, TyTAN, and Trustlite [168]-[170]	It isolates the resources of particular application in numerous distinct spaces including trusted and untrusted zones	Remote code execution, MITM, and Buffer overflow	These schemes secure specific nodes from others. Moreover, such mechanisms segregate tasks and assure confidentiality of code effectively. Similarly, it verifies the integrity of the code present in the trusted zone properly. It secures sensitive functions present in a device from insensitive one.	Isolation-based schemes do not protect against run-time attacks originating from the trusted zone. These schemes do not protect sensitive patient information as it is entirely dependent upon the integrity of data at runtime. The technique is complex to implement. These measures also consume great power and memory.
DFI based mechanisms, PointGuard, Low-fat pointer, Shakti-T, DFI and DSR [171]-[175]	These approaches focus on maintaining the integrity of pointers to validate the execution flow of a program	Remote code execution, Buffer overflow, and Information disclosure	Such approaches secure the integrity of each data that the application uses at runtime. It prevents an attacker to modify the data flow which affects the device's critical operations.	These mechanisms only secure pointers without considering the protection of direct data. Furthermore, they are not binary compatible which stringently limits the development of a complex medical application. Moreover, these schemes are just concepts without comprehensive frameworks that can be incorporated into the medical device industry.
Inherently secure computing platform [56]	It proposed a secure application development toolchain which segregates security assets and application module.	Buffer overflow, Remote code execution, and Information disclosure	The scheme is effective as developers do not need to define software and hardware blocks in the secure environment. Instead, they should only enlist secure assets within the application based on security specifications of the device.	Validation of such a framework through simulation and real devices is missing.
Bio-cryptographic key generation approach [177]-[180]	These schemes rely on IPI extracted from ECG, BP, EEG, and PPG that is random and unique and is optimal for cryptographic keys	Eavesdropping, MITM, Information disclosure, and Tampering	The efficient approach that does not require a key predistribution mechanism to generate key	This system is vulnerable as [64] discussed the possibility of attacks with help of EEG generative model based on factual ECG and EEG data
Fuzzy vault physiological schemes [182]-[185]	It uses PSKA to allow secure communication using IPI and fuzzy vault	Eavesdropping, MITM, and Information disclosure	This scheme improves security by minimizing the rate of data exchange during the key management process and thus increases network lifetime and energy efficiency	Security of such scheme is entirely dependent upon the vault size that is weak because of the small size of attributes

time manufacturers never thought that such equipment can be hacked. Developers were not aware of the safety and security perceptions concentrating on functional requirements. The software protocols and hardware chipset embedded in legacy equipment is often out of date having several security vulnerabilities. As a result, these devices are vulnerable

TABLE XVII
SUMMARY OF SOLUTIONS

Technique	Methodology	Overcomes attack	Advantage	Disadvantage
Lightweight key management and encryption scheme [60], [187] and [190]	Vibration-based lightweight key exchange protocol [53] is used for key generation and sharing. A lightweight scheme based on AES-128 data frame along with modern HMAC and nonce is used for verification and encryption. Elliptic curve point functions and fuzzy extractor techniques authenticate users. Polynomial based key distribution protocol is used for key generation.	Eavesdropping, MITM, Information disclosure, Spoofing, Unauthorized access, Replay, Tampering	Lightweight with minimal computational cost. Polynomial based key distribution protocol preserves collision resistant and unconditional security property	A weak mechanism as an adversary is capable of extracting keys from vibration signals. Signals are acoustic and electromagnetic waves that can be captured
BLE security [13], [74], [76], [81], [202] and [203]	LE secure connection pairing, passkey, numeric comparison and just works modes are used to provide security	Eavesdropping, replay attack, sniffing, MITM, and identity tracking	BLE standard ensures privacy and authentication to a great extent	An individual can still be tracked through traffic analysis and distinct gait features
Proximity-based scheme [191]	Diffie-Hellman modified (DHM) based plaintext authentication mechanism. The scheme also incorporates packet expiration and time constraint mechanism to authenticate users	Replay, Resource depletion, and DOS	The scheme does not complicate the daily interactions of medical staff	DHM mechanism does not use encryption techniques and therefore puts the privacy of users in danger
Machine learning [199], [200] and [201]	Decision tree algorithm is used to track the normal behavior of IMD to detect attacks. Psychological and behavioral parameters along with machine learning classifiers are used to authenticate users	Resource depletion, DOS, Unauthorized access, and Information disclosure	The scheme is efficient and detects attacks accurately. Similarly, it authenticates users with great precision	Running such algorithms on medical devices would consume more energy and will eventually influence the medical process
Hybrid mechanisms [194], [195], [196], [197] and [198], Fitlock [21]	Heterogeneous cryptosystems i.e. symmetric and asymmetric are used. Authentication is done through biometrics, nonce and a shared secret symmetric key, Fitlock uses the secret symmetric key to encrypt messages shared between tracker and server	Spoofing, tampering, interception, and replay attacks	The scheme is secure as it uses three-factor authentication	It causes great computation overhead for sensory devices
Embedded symmetric key [192], [193] and [194]	Firmware authentication and verification using MAC and shipped symmetric key with the device	Firmware modification	It authenticates firmware before updates	If the key is compromised, security of the whole system will jeopardize
External mechanism [195], [206] and [207]	IMDShield, IMDGuard, and Cloaker	Eavesdropping, tampering and sniffing	Fast response time	It drains the battery quickly

to reverse engineering techniques and common exploits and can be easily set up to violate the availability and integrity of such systems. For devices to be connected, it is significantly important to secure these devices from both software and hardware layers. Several properties including static and dynamic integrity, safety and privacy, high availability, authenticity, and confidentiality are essential in order to develop highly secure devices, as they deal with real-time sensitive information and losing such information leads to increased privacy issues. Furthermore, sniffing and tampering such critical information without authorization affect patient safety as well. Therefore, securing such information is significant for both patient's privacy and safety. Researchers from all over the world have been striving hard to secure these devices but due

to the resource-constrained nature of implantable and wearable sensor devices, conventional security algorithms cannot be adopted. Solutions based on asymmetric cryptography require additional computational cost and hence are not suitable for resource-constrained devices. Moreover, security solutions founded on the trusted server are exposed to the single point of failure. In addition, the static nature of symmetric keys also makes key pre-distribution solutions vulnerable. During the last few years, researchers proposed different lightweight secure algorithms to prevent CIA related attacks in these medical devices, but have some limitations. Some of the solutions have been incorporated in wearables and implants but are not secure enough as cyberattacks are possible. However, in the case of on-site medical equipment, these solutions are mere researches as MRI and X-ray machines are still vulnerable to cyberattacks. Some of the state-of-the-art countermeasures are discussed and analyzed in Table XVI and Table XVII.

1) Attestation-Based Architecture: To prevent run-time attacks impacting device's integrity and control flow, which exploits poor programming practices including memory management and buffer overflows, different countermeasures are proposed in the literature. This subsection reviews these solutions by analyzing their strengths and weaknesses. The first approach is based on the path signatures. Lo-Fat [160] and C-Flat [161] architectures determine a hash based on the execution path that the device takes. Such a concept works with a prover and verifier. The prover is a low-end device managing software while the verifier is a remote computer that handles the flow of execution of the device's software. The application takes the path by sending a challenge to the prover. Each time the flow of execution changes, a cumulative hash is computed. The verifier then uses this hash value to validate the precision of the execution flow program takes. However, such mechanisms do not secure sensitive patient information and control flow hijacking is also possible as discussed in [163].

The second approach identifies each vertex with a label in the execution flow graph. In HCFI [164] and HAFIX [167] approaches, the label of each destination node is verified during the execution flow transfer. In case of control flow hijacking, the engine can easily detect it as vertex label will be different. However, HAFIX considers backward edges only due to which an adversary can simply alter a forward edge in order to circumvent such security measure. Moreover, such approaches are vulnerable to data attacks.

2) Isolation-Based Mechanisms: Isolation-based control flow integrity mechanisms are used to isolate the resources of particular application in numerous distinct spaces. Using such an approach, the functions and resources existing in the trusted area are segregated and inaccessible from the untrusted area. Special syscalls or entry points are used for managing communication between trusted and untrusted environment. To classify the security level of the resources, Trustzone [168] makes use of a special bit at the hardware level. To navigate between trusted and untrusted zone, software level syscalls are used. In the case of Intel SGX [167] and Sanctum [168], CPU provides instructions code and Application Programming Interfaces (APIs) are used to allot secure memory area which is known as enclaves. Enclaves are separated from other processes and are reachable through distinct entry points. Likewise, TyTan [169] and Trustlite [170] provide segregation between functions with hardware primitives. These approaches are dependent on the hardware as they both utilize a protected Memory Protection Unit (MPU). It uses a microprocessor register in order to make sure that each isolated function can access the allotted memory unit only. However, these isolation techniques do not prevent attacks originated from inside the secure area. Moreover, security of patient data is entirely dependent upon the runtime data integrity. The technique is complex since it requires fine-grained analysis in order to identify the code belonging to the trusted zone from a security perspective.

3) Data Flow Integrity: Low-fat [171], WatchdogLite [172], and Shakti-T [173] pointers focus on maintaining track of pointers integrity. These pointers pointing to some data have both base and a limit in memory. Each pointer in the source code is marked at compilation time. Then base and bound of these pointers are stored in an unreachable area in the hardware. When the pointer is accessed, the system checks for the validity of pointer. In case the pointer is modified in an unauthorized manner, then it will be detected as a base and bound values do not match with the figures stored in shadow memory. However, such approaches utilize custom hardware to ensure software pointer integrity.

Furthermore, specialized skills are required at the assembly level in order to use custom hardware. PointGuard [174] focuses on improving pointers integrity by encrypting all of them in memory. When CPU acquires data through a pointer, it gets its value. Then it retrieves the data referenced by the pointer. By altering the pointer value, an adversary can decide the accessed value. The pointer value is decrypted before it is being retrieved by the processor. In case an adversary modifies the pointer value, the decryption process fails to cause an invalid memory reference error. However, such an approach cannot guard against conditions in which an adversary directly modifies the pointer value. Data space randomization [175] extends this concept by encrypting each variable with different key pairs. Whenever data is accessed, or operations are performed, its value is encrypted. Another Data Flow Integrity (DFI) [176] approach prevent data only attacks. Using such an approach, write instructions are recognized at the software level. DFI maintains a record of the last instruction which retrieved a variable during runtime and hence can distinguish data corruption. Development of these approaches is also difficult as developers must use a specific compiler and adjust coding styles accordingly.

Abera *et al.* [161] proposed a secure application development tool chain which can ease the tasks of the developer by segregating security assets and application module. An interface is provided to developers for associating security functions with the application. The security assets will generate a secure code that will be associated with the functional code to permit secure run-time features. The major objective of such an approach is to ease the job of non-security developers as they are not aware of the security capabilities of medical devices.

TABLE XVIII
IMPLANTABLE DEVICES VULNERABILITIES AND DEMONSTRATED/APPLICABLE CYBERATTACKS

Medical device	Attacks	Communication medium	Attack methodology	Vulnerability
Cardioverter Defibrillator [43]	DOS, Spoofing, Replay attack [43], Eavesdropping, Interception, Information disclosure, Tampering, Resource depletion [16],	Long range RF channel	Reverse engineering of proprietary communication protocol	Lack of authentication, encryption, and integrity mechanism. An implementation flaw keeps the device in standby mode due to which there is no need to be in close proximity in order to attack device.
Insulin pump [16][44]	Eavesdropping, Man in the middle, Information disclosure, Unauthorized access [44], Spoofing, DOS, Resource depletion, Jamming, Buffer overflow attack [16]	Wireless sensor devices and MICS transceiver	Universal Software Radio Peripheral	Lack of encryption mechanism due to which messages were transmitted in plain text. Moreover, the prevention mechanism against DOS is also missing.
Automated external defibrillator[45]	Counterfeit firmware modification, Buffer overflow, Unauthorized access, Spoofing, Information disclosure, Eavesdropping, MITM, DOS, Jamming, Resource depletion [16][45]	Wireless communication interface	Reverse engineering (overwrite recent exception handler in order to execute own code)	Input validation checks are missing. The inadequate use of CRC as a digital signature does not ensure integrity. Weak authentication mechanisms as passwords are obfuscated with simple XOR mechanism that can easily be compromised. Passwords in plaintext are stored on the local drive and can be easily extracted.
Implantable wearable medical device [17]	Side channel attacks, Power analysis attacks, EM analysis attacks, Hardware Trojan [17]	Wireless communication interface	Analyzing power consumption and EM radiations multiple times to extract secret information and reverse engineering	Analyzing power consumption and EM radiations multiple times to extract secret information, Malicious function embedded in device's IC.
Boston Scientific Cognis, Medtronic Adapta and InSync Sentry [46]	EMI signal injection attack [46]	Wireless communication interface	Introduce strong forged signal in order to overlook legitimate signal	Lack of low pass filters, Inadequate protection against backdoor coupling, intentional low-power and high-power EMI leaks, unintentional low-power and high-power EMI leaks
Brain-Computer Interfaces (BCI)[47][48]	Eavesdropping, Interception, Information disclosure [47][48]	Wireless channel	Brain spyware	Intercept signals by using malicious software i.e. spyware to extract sensitive information
Cardiac monitor [49]	Eavesdropping, Information disclosure, Tampering, Jamming, Side channel [49]	Wireless channel	Communication channel exploitation	Lack of encryption, packets travel in plaintext and can be sniffed, Hardware/software flaws, insufficient verification of data authenticity
Pacemakers [50]	Eavesdropping, Information disclosure, Tampering, Jamming, Side channel, Resource depletion [50]	Wireless channel	Communication channel exploitation	Lack of encryption and access control, Hardware/software flaws, packets travel in plaintext and can be sniffed, Insufficient verification of data authenticity
Insulin pump system [51]	Spoofing, Eavesdropping, Information disclosure, MITM [51]	Wireless communication	Exploit wireless communication channel	Lack of encryption and authenticity validation mechanisms
Oximeter [52]	MITM, Relay attack [52]	Bluetooth	Communication channel exploitation	Lack of security PIN required for pairing

(to be continued)

4) Bio-Cryptographic Key Generation Schemes: Key agreement and generation is an important technique to secure medical devices. These schemes are based on physiological features such as Inter Pulse Interval (IPI) that is random and unique and is optimal for cryptographic keys[177]. Different researchers used such metric to generate keys that are discussed below.

The research [178] proposed bio-cryptographic key management protocol to secure communication of implantable and wearable medical devices. To generate secure cryptographic

TABLE XVIII
CONTINUED

Accelerometer [53]	Acoustic Eavesdropping, Sniffing, Information disclosure, Spoofing [53]	Wireless channel	Communication channel exploitation (Captures sound produced by vibration motor to extract key with help of signal processing techniques)	Lack of encryption and authentication mechanisms in the communication protocol
Hermes medical shoe platform [54]	Calibration attack and Interception/Modification [54]	Wireless channel	Communication channel exploitation (Alter values of pressure sensor)	Weak encryption and authentication techniques
Syringe Infusion Pump [55]	Unauthorized access, Information disclosure, Tampering, MITM [55]	Wireless channel	FTP server exploitation	Lack of authentication mechanism in the FTP server while allowing FTP connections, Lack of validation of host certificates
Gastric electrical stimulator [56]	Eavesdropping, Information disclosure, Tampering, Jamming, Resource depletion [56]	Wireless communication	Wireless channel exploitation	Lack of encryption, authentication and validation mechanisms, Hardware/Software error
Insulin delivery alarm system [156]	Physiological information eavesdropping	Wi-Fi	Lack of information, signal reduction, and noise addition techniques	Initialization-based method, confirmation-based technique, and duration-based method is used to determine medical condition, injected insulin and device's battery status
Infusion pumps [58]	Unauthorized access, Information disclosure [58]	Wireless communication channel	Embedded system vulnerabilities exploitation	Lack of encryption, authentication and access control mechanisms, Default hardcoded administration passwords
ICD [59]	Replay attack, MITM, Information disclosure, Resource depletion, Firmware modification [59]	Wireless channel	Reverse Engineering the communication protocol	Lack of encryption, validation, and authentication
Cardiac Science G3 Plus Automatic External Defibrillator (AED) [60]	Firmware alteration, Unauthorized access, Tampering [60]	Wireless channel	Transferring malicious commands to device	Lack of secure key exchange, authentication and input validation mechanisms due to which remote code can be executed
Pacemakers [61]	Unauthorized access, Information disclosure, Tampering [61]	Wireless communication	Operating system (XP) vulnerabilities exploitation	Windows XP vulnerabilities
St. Jude cardiac device [18][62]	Unauthorized access, Resource depletion [18][62]	Wireless communication	Traffic analysis	Weak encryption and authenticity validation mechanisms
OneTouch Ping Pump [14]	Unauthorized access [14]	Wireless communication	Traffic analysis	Lack of encryption and authorization mechanisms
iSatan medical mannequin [63]	DDOS, Brute force attacks [63]	Wireless communication	Open source tools including backtrack and reaver	OS related vulnerabilities
Prosthetic limb [64]	Interception, Information disclosure, Tampering [64]	Wireless communication	Traffic analysis	Weak encryption and authentication mechanism

keys, research utilized psychological parameters including blood pressure, photoplethysmogram (PPG) and electrocardiogram (ECG) tracked by sensors. To generate a secret key from these physiological signals, two important approaches including time-domain physiological parameter generation to derive IPI and frequency-domain physiological parameter generation to derive cross power spectral density (CPSD) are proposed. Both of them are important candidates to be cryptographic keys due to their randomness and temporal variance characteristics.

Similarly, heartbeats based Random Binary Sequences (RBSs) [179] is another approach to secure communication of sensory medical devices. The research used finite monotonic increasing sequence generation mechanism and

TABLE XIX
WEARABLE DEVICES VULNERABILITIES AND DEMONSTRATED/APPLICABLE CYBERATTACKS

Medical device	Attacks	Communication medium	Attack methodology	Vulnerability
Withings Activite fitness tracker [65]	Firmware Attack, MITM [65]	BLE	Reverse engineer firmware Health Mate version 2	Design flaws and weak authentication mechanism to verify updates
Fitbit tracker [66]	Information disclosure, Unauthorized access, Modification, Resource depletion [66]	BLE	Reverse engineering the communication protocol	Lack of encryption, authentication, validation and consistency check mechanism
Apple watch [42]	Tampering [42]	BLE	Exploitation of communication protocol vulnerabilities	Unencrypted connections due to unaltered MAC in BLE
Basis peak [14][42]	Modification [14][42]	BLE	Reverse engineer application code	Code obfuscation is partially considered that allows an attacker to reverse engineer the code, Inadequate authenticity validation mechanisms
Microsoft band 2 [42]	Tampering [42]	BLE	Reverse engineer application code	Code obfuscation is partially considered that allows an attacker to reverse engineer the code, Inadequate authenticity validation mechanisms
Mobile action Q-band [42]	Tampering, Unauthorized access, Spoofing, MITM [42]	BLE	Exploitation of communication protocol and app	Lack of authentication and encryption mechanism
Pebble time [42]	Spoofing [42]	BLE	Communication channel exploitation	BLE privacy policy is not properly considered and incorporated
Runtastic Moment Elite [42]	Information disclosure, Tampering [42]	BLE	Communication channel and app exploitation	Lack of authentication and validation mechanisms and communication protocol privacy is not incorporated
Strivv Fusion [42]	Spoofing, Tampering, Information disclosure [42]	BLE	Communication channel and app exploitation	Lack of authentication mechanism and communication protocol privacy is not incorporated
Xiaomi MiBand [42]	Tampering, Information disclosure [42]	BLE	Communication channel and app exploitation	Lack of authentication and validation mechanisms and communication protocol privacy is not incorporated
Acer liquid leap [67]	Tampering, Information disclosure [67]	BLE	Communication channel and app exploitation	Lack of authentication and validation mechanisms and communication protocol privacy is not incorporated
Garmin Vivosmart [67]	Modification [67]	BLE	Reverse engineering application code	Code obfuscation is not considered that allows an attacker to reverse engineer the code, Lack of authenticity validation
Huawei Talkband [67] [19]	Firmware modification, Information disclosure [67] [19]	BLE	Reverse engineer the application code	Lack of encryption, authentication and integrity check mechanisms
LG Lifeband Touch FB84 [67]	Modification [67]	BLE	Reverse engineer the application code	Code obfuscation is not considered that allows an attacker to reverse engineer the code, Lack of authenticity validation mechanism
Withings Plus Ox [67]	Modification [67]	BLE	Reverse engineer the application code	Code obfuscation is not considered that allows an attacker to reverse engineer the code, Lack of authenticity validation mechanism
Nike+ Fuelband SE [67][19]	Unauthorized access, Information disclosure [42]	BLE	Reverse engineer the application code	Lack of robust authentication and encryption mechanisms

(to be continued)

Hamming Distance metric to excerpt entropic bits from IPI derived from ECG. From each signal, sixteen random bits could be excerpted and through a concatenation of eight consecutive IPIs, 128-bit RBSs are generated to authenticate users. Such bio-cryptographic technique is an efficient approach to generate cryptographic keys since it does not require key pre-distribution mechanism or proper network setup to generate the key. In addition, this approach provides an opportunity to re-keying automatically. Bio-cryptographic technique ensures key sharing among nodes having contact with the

TABLE XIX
CONTINUED

Pebble steel watch [13]	MITM, Sniffing [13]	BLE	Traffic analysis	Lack of robust authentication and encryption mechanisms
Fitness tracker [69]	Firmware modulation attack, Tampering [69]	BLE	Reverse engineer gateway application and create a fake gateway by exploiting authentication related vulnerabilities	Lack of authentication for a firmware update
Fitbit trackers including flex, Ionic, and Alta [70]	MITM, Replay attack, DOS, Sniffing, Firmware modification, App modification, Spying [70]	BLE	Reverse engineer firmware tracker and official application	Credentials in plaintext are just secured by HTTPS that does not prevent MITM, Weak encryption and verification mechanisms, On activating live mode, after authentication all traffic goes unencrypted, hardcoded private name
Fitbit charge and surge [71][72]	Eavesdropping, Identity tracking [71][72]	BLE	Traffic analysis using ubertooth, adafruit, and HCI snoop log	Fixed MAC address and weak authentication mechanism
Xiaomi Huami [72]	Eavesdropping, Identity tracking [72]	BLE	Traffic analysis using ubertooth, adafruit, and HCI snoop log	Fixed MAC address and weak authentication mechanism
Samsung gear 2 3 live [72]-[74]	Unauthorized access, Information disclosure, Sniffing [72]-[74]	BLE	Injecting counterfeit message to forget the previous key and generate a new key	Weak encryption and authentication mechanisms
Samsung smartwatch [75]	Brute force attack, Unauthorized access [75]	BLE and Wi-Fi	Traffic analysis	Weak authentication mechanism
Google glass [76]	Unauthorized access, Eavesdropping, MITM, Sniffing [76]	BLE and Wi-Fi	Traffic analysis	Weak authentication and encryption mechanisms
Nike+ Fuelband [77]	Firmware modification [77]	BLE	Reverse engineer the band	The absence of read and write protection on the device. Checksum value can easily be modified
TW64 Bong 3 HR band [78]	DOS, Sniffing, Tampering [78]	BLE	Traffic analysis using TI SmartRF, and BLETest-Tool	Lack of encryption and authenticity validation mechanisms
Dexcomrx glucose monitor, Gear Fit, OTbeat, Forerunner, UpMove [79]	Eavesdropping [79]	BLE	Traffic analysis	Lack of MAC address randomization
Smartwatch and Fitness tracker [80]-[82]	Side channel attack [80]-[82]	BLE	Exploits pattern of entering key using slope-based moving direction scheme to capture movement by traffic analysis or malware	Weak key-based security system

body. This type of scheme assures security without necessitating any human interference by eradicating the prospect of overlooking secret keys. Random numbers produced from physiological signals are used to secure exchanged data.

5) Fuzzy Vault Physiological Scheme: Another scheme is based on fuzzy vault and IPI that uses Physiological Signal-based Key Agreement (PSKA) to allow secure communication [180], [181] and [182]. This system uses shared symmetric key to allow communication and require one entity to project security attributes calculated from physiological signals on a polynomial and transfer the attribute points along with chaff points to the former side that would recreate the polynomial centered on some common attributes. This scheme improves security by minimizing the rate of data exchange during the key management process and thus increases network lifetime and energy efficiency [182]. However, the security of such scheme is entirely dependent upon the vault size that is weak because of the small size of attributes [183] and [184] demonstrated that an adversary is capable of estimating appropriate points in the vault.

6) Lightweight Encryption and Key Management Protocol: An important scheme presented by [53] and [185] is a vibration-based lightweight key exchange protocol and ultra-low battery resilient mechanism between external and

TABLE XX
VULNERABILITIES AND DEMONSTRATED CYBERATTACKS OF APPS TRACKING PHYSIOLOGICAL INFORMATION

Medical device	Attacks	Communication medium	Attack methodology	Vulnerability
Codoon band [65]	Firmware modification [65]	BLE	Reverse engineer application	The robust authentication mechanism is not present
Fitbit mobile app [83][84]	Information disclosure [83][84]	BLE	Commercial use of patient sensitive data due to policy weaknesses	The vendor can use and exploit personal health data as the user does not retain the right of controlling their own data. After account deletion, the anonymized data will be used for analysis
Basis watch [85]	Unauthorized access, Information disclosure [85]	BLE	Policy weakness regarding data usage, collection, transfer, and storage	The vendor can use and exploit personal health data as the user does not retain the right of controlling their own data. Further collected data is not stored in encrypted form
A-fit, B-fit, and C-fit apps [40]	Information disclosure, DNS Spoofing, Sniffing, Firmware modification, Tampering android application, Unauthorized access [40]	BLE	Reverse engineer gateway and android application. Further, BLE traffic is analyzed through ubertooth	Encryption mechanism is not present. Authentication and integrity check mechanisms are not incorporated
Fitness trackers (with the app) [69]	Scanning, Sniffing, Information disclosure, Unauthorized access [69]	BLE and Wi-Fi	Reverse engineer application code	Single MAC address is used to advertise device for connection establishment, Lack of encryption (passwords in plaintext), Absence of privacy policies and security mechanisms
Codeblue [86]	DDOS, Modification attack, Grey hole attack, Sybil attack, Spoofing attack, Masquerading attack [86]	IEEE 802.15.4	Traffic analysis	Lack of authentication and encryption mechanism
UbiMon [87][41]	Unauthorized access [87][41]	Bluetooth and Wi-Fi	Traffic analysis	Lack of authentication and encryption mechanism
Fitbit Aria (apps) [72]	Replay attack, Tampering [72]	Wi-Fi	Static and dynamic analysis using open-source tools	Privileged app and pinning mechanism for SSL is absent
Withings WS-30 app [73]	Replay attack [73]	BLE and Wi-Fi	Static and dynamic analysis using open-source tools	Privileged app and pinning mechanism for SSL is absent
Activ8rLives /Body Analyser [73]	Replay attack [73]	BLE and Wi-Fi	Static and dynamic analysis using open-source tools	No password policy, Over-privileged and trust manager issue due to improper certificate validation
Thomson TBS705 app [73]	Replay attack, Tampering [73]	BLE	Static and dynamic analysis using open-source tools	Lack of encryption

(to be continued)

wearable device. The two-feature on-off keying mechanism allows reasonable bit-rate for exchanging keys. Initially, such a vibration signal is perceived by measuring the vibration of an accelerometer. To remove low-frequency noise from the action of patients or inner organs, high pass filter is used. RF module is activated in case high-frequency signal is perceived after filtering process. Once the RF module is initiated, the symmetric key is shared between external and wearable device. In order to exchange key, the external device produces key and modifies it into a vibration signal. On the other side, the wearable receives signals and using the two-feature On-off Keying (OOK) demodulation mechanism transforms that signal into bit string and encrypts further communication. The lightweight encryption algorithm proposed by [182] is AES with optimum size. Such an approach has limitation, i.e., an adversary would be capable of extracting keys from vibration signals since they are acoustic and electromagnetic waves that can be captured [60].

7) Proximity-Based Scheme: The scheme proposed by [186] is based on plain text authentication scheme to prevent replay, resource depletion, DOS, and MITM attacks. The scheme uses Diffie-Hellman modified (DHM) approach

TABLE XX
CONTINUED

iChoice S1 app [73]	Tampering [73]	BLE	Static and dynamic analysis using open-source tools using open-source tools	Trust manager issue due to improper certificate validation
Withings Cardio app [73]	Replay attack, Tampering [73]	BLE and Wi-Fi	Reverse engineer and traffic analysis	Privileged app and pinning mechanism for SSL is absent
1301 Android smartwatch apps, 512 Apple smartwatch apps, 129 Samsung smartwatch apps [88]	Information disclosure [88]	BLE, Wi-Fi, and 3G	Static and dynamic analysis using MITM proxy	Due to weak security mechanisms, 57 android apps leak unique information while 17 among them exfiltrates credentials. 71 of the total Android apps reveal location while 57 apple apps leak location
Withings Plus Ox [67]	Modification [67]	BLE	Reverse engineer application code	Code obfuscation is not considered that allows an attacker to reverse engineer the code
Android applications including Healthiply, mMR, Nfc Medic, Patient Chart, Zibdy, Yalova Devlet, Health Files, Smart Medical, Diagnose, Pedometer and Web MD [69]	Information disclosure [69]	BLE or Wi-Fi	Penetration testing of apps using burb suite, Genymotion emulator, Vezir v2 Linux Distro, and Wireshark	Lack of encryption for local data storage. Apps have dangerous permissions and can access critical information. Most of the apps do not establish secure transmission channel. The proper authentication mechanism is also missing in most of the apps
Heart rate sensors [124]	Tampering of physiological information	BLE/Zigbee	Lack of authentication	With the help of radio frequency electromagnetic waves, an erratic heartbeat can be forged. Moreover, false signals can also be inserted
Analog sensors [124]	Physiological information disclosure	BLE/Zigbee	Communication channel weaknesses	Exploitation of communication channel
Heart rate monitoring sensors	Unauthorized access to physiological information	BLE	Lack of encryption and authentication schemes	Since signals are not encrypted and authentication is not enough therefore wireless radio i.e. oscilloscope and some open-source tools can send false signals
Ambulatory BP monitoring device [161][162]	Acoustic and EM signal-based attack to capture physiological information disclosure	Wi-Fi	Lack of information, signal reduction, and noise addition techniques	Algorithm AmbBP and VHA antenna

along with packet expiration and time constraint mechanism to authenticate users. Average time will be calculated for legitimate users and in case packets travel for a long time, it will be rejected. Since the mechanism does not use encryption techniques and therefore puts the privacy of users in danger.

8) Authentication Mechanisms: Similarly, the work presented by [187] focuses on robust authentication and encryption mechanism to prevent information disclosure and unauthorized access. For authentication, a lightweight scheme based on AES-128 data frame along with modern hash message authentication code (HMAC) and nonce is used to verify the identity of client medical device and gateway server. Once both are authenticated, the messages will be encrypted for transmission. The nonce will be the initialization vector (IV) for encryption using AES-128. The scheme is efficient in terms of preventing unauthorized access; however, computational cost emerges as an important challenge.

The research [188] proposed an authentication scheme through which controller node and user mutually authenticate one another and create a session key for further communication by using ECC cryptogram. Three factors are used to authenticate users including a mobile device, password, and biometrics. Elliptic curve point functions and fuzzy extractor techniques are used for authentication. However, for key generation, polynomial-based key distribution protocol is adopted as it preserves collision resistant and unconditional security property. The scheme is efficient in terms of preventing replay, MITM, tampering and information disclosure related attacks.

On the other hand, resources are required to perform such computations.

Self-authentication mechanism [189] divides software of medical devices into two executables, i.e., main program and verifier program. The verifier program is in encrypted form and comprises a section of the parameters or critical instructions without which medical device is unable to perform its intended functions while the main program contains instructions to decrypt aforementioned program and other related functionalities. The decryption key present in the main program is in obfuscated form. Such a mechanism is prone to cyber-attacks. A sophisticated attacker can obtain the key since it is present in the main program source or RAM.

9) Hybrid Mechanisms: The hybrid security protocol is presented by [190], [191] and [192] to facilitate different security levels for implantable and wearable devices in WBAN. The protocol presented in [189] utilizes two heterogeneous cryptosystems that are asymmetric and symmetric to ensure authentication and confidentiality. To authenticate wearable sensors, biometric features of the patient, including ECG are used. However, implanted devices are manually authenticated by the base station through random nonces. However, further communication between devices and cloud servers is encrypted by symmetric key with help of elliptic curve cryptography (ECC). This scheme helps in preventing spoofing, tampering, interception and replay attacks. However, the scheme requires excessive storage and computational resources that are major issues in these resource-constrained devices.

To secure wearable with authorized official apps, [193] proposed OS level access control mechanism that produces and applies security-related policies automatically. Once device starts the pairing process and attempts Bluetooth connection, the model checks bonding policy and its compliance. In case the app is in connecting policy, the connection will be established otherwise declined. This model makes use of an un-pairing controller to accomplish such pairing relations. During un-pairing, the controller will check the bonding pairing policy and if the policy is lacking then the app will be described as unauthorized and bonding will stop.

To overcome the resource depletion attack on Fitbit devices, the comprehensive survey presented by Seneviratne *et al.* [21] discussed FitLock. It incorporates bind and upload procedure that associates tracker to social network account, whereas the upload method is responsible for improving security. The bindtrackeruser protocol is used to authenticate the user by taking inputs (ID, shared a secret symmetric key) and returns 6 digits random code that user must enter in order to connect with a social network account. Furthermore, the secret key is utilized to encrypt all communication between tracker and Web server. Each session possesses monotonically increasing session key that prevents an attacker to access or replay data during uploading.

10) Machine Learning Approaches: Machine-learning algorithms are widely used by researchers to detect attacks on IMD and wearable. The work presented by [194] incorporates a decision tree algorithm to detect malicious attacks on IMD. In this approach, the normal behavior of IMD is tracked and in case of any deviation, the algorithm detects the presence of an attack. Another research makes use of psychological and behavioral parameters including calorie burn, average step counts, minute heart rate and metabolic activity with help of machine learning classifiers including Support Vector Machine (SVM), Trees and Ensemble to authenticate users [195]. Although the mechanism provides accurate results but running such algorithms on medical devices would consume more energy and will eventually influence the medical process. To overcome DDOS attacks on WBAN, a survey [196] investigated different techniques.

11) BLE Security Mechanisms: BLE makes use of any of four secure pairing approaches. These approaches entail minimal contact of the user in order to provide encryption channel. Such approaches include LE secure connection pairing, passkey, numeric comparison and just works [13]. When some peripheral device turns on, it starts transmitting advertising packets. The user uses operating system level or application specific user interface in order to transmit a scan request that pledges pairing or polls advertising channel for accessible devices. The simplest pairing approach is just working and does not entail user involvement. It does not possess a user interface or screen and is suitable for wearables [33]. However, such a pairing mechanism is least secure and is prone to MITM attack, identity tracking, sniffing and eavesdropping [19] and [197].

Second important security approach is a numeric comparison. This approach needs user interface at both peripheral and central ends to show a numeric key. While pairing external device for the very first time, both peripheral and central devices will exhibit four to six digit numeric code. Then, a user on a central device is requested to accept or deny the connection by matching those two numbers to confirm that they are similar. It is relatively secure, however, is still prone to eavesdropping, sniffing and identity tracking [79].

The third security mechanism is passkey entry. To use this approach, it is essential for both central and peripheral devices to have some interface or keypad to enter key. For pairing, it is important to enter the passkey. It is more secure than previous two approaches; however, identity tracking due to static MAC address is still successful [72]. Fourth and final security approach is LE secure connection pairing that uses Elliptic Curve Hellman-Deffie (ECDH) to generate keys. Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK) are shared between slave and master for ensuring privacy and authentication. It is the most secure mechanism [198]. It overcomes MITM and eavesdropping related attacks. Moreover, Resolvable Private Address (RPA) scheme is used to randomize the MAC address to prevent identity tracking to some extent. However, individual can still be tracked through traffic analysis and distinct gait features [199].

12) External Mechanisms: To deal with security issues, external devices, including IMD shield, IMDGuard and Cloaker are studied in the literature. IMD shield contains a

TABLE XXI
ON-SITE MEDICAL EQUIPMENT VULNERABILITIES AND DEMONSTRATED/APPLICABLE CYBERATTACKS

Medical device	Attacks	Communication medium	Vulnerability	Attack Methodology
52 medical devices manufactured by Siemens Healthcare, GE Healthcare, Canon, Philips Healthcare, Toshiba Medical Systems, Samsung and RainbowFish Software were tested against known security exploits [90]	Unauthorized access, MITM, Information disclosure, Sniffing, Scanning, Spoofing, Tampering, Eavesdropping, Ransomware attack, Remote code execution [90]	Wi-Fi	Approximately, 2038 vulnerabilities were reported as result of scans. Majority of the medical devices uses • Unpatched Windows (XP, Service Pack 2 and Service Pack 3. • In addition, 70% of the overall hosts enabled SMB protocol. Majority of the devices lacks authentication mechanism or use default passwords. • Among 144 networked items, 142 does not have antivirus protection. • 84 percent devices have no read/write protection for USB devices. • Data was in unencrypted form during rest and transit	Mapped radiology department subnet with nmap and analyzed through OpenVas and Wireshark
MID, CT and MRI [91]	Ransomware DOS, Information disclosure, Tampering, Modification [91]	Wi-Fi	The absence of authentication mechanism since modification and tampering is possible	Security analysis
MRI and X-ray machines by ReliOn and CareFusion [**?**]	Remote code execution, DOS, MITM [**?**]	Wi-Fi	Outdated operating systems including Windows XP and service pack 2. They enabled SMB port and have weak authentication mechanisms	Shodan API to get IP addresses of connected medical devices that are pass-through Nessus vulnerability scanner to analyze devices for known vulnerabilities
MID, CT, and MRI [91]	Ransomware DOS, Information disclosure, Tampering, Modification [91]	Wi-Fi	The absence of authentication mechanism since modification and tampering is possible	Security analysis
MRI, X-Ray, Positron Emission Tomography (PET) scanner, CT scanner, Medical ventilator, Anesthetic machine, Heart-lung machine, Dialysis machine [93]	Spoofing, Ransomware, Tampering, DOS, Unauthorized access [93]	WLAN/Wi-Fi	Majority of the devices uses default passwords that can be found online by using maintenance and operating manuals. Moreover, devices used unpatched obsolete operating systems including Windows XP and service pack 2	Security analysis, Reconnaissance, and Scanning

(to be continued)

full-duplex radio device that consists of a receiver and jamming antenna. The receiving antenna obtains a signal and deciphers it using receive chain. On the other hand, jamming antenna transfers an arbitrary flag to prevent eavesdropping by blocking interception of IMDs transmission. IMDGuard uses ECG signals for key exchange. It ignores the broadcasting of periodic messages for detecting the presence of a device that assists in preventing spoofing related attacks. A challenge-response technique is used to enter an emergency mode in which device sends two challenges at different time intervals. It authenticates programmer by verifying the signature of the device by issuing temporary session keys. However, it is prone to MITM attack [200]. Cloaker is another important gadget to provide security to IMD [201]. In case cloaker is activated, implantable devices simply ignore all communication requests. In the second case, IMD will be

TABLE XXI
CONTINUED

Fluoroscopy workstation and radiation oncology system [92][93]	Tampering, Modification, DOS, Ransomware [92][93]	WLAN/Wi-Fi	Malware injection using shellcode execution technique on Fluoroscopy workstation and radiation oncology system that was running Windows XP operating system	Malware injection to create a backdoor
X-ray machine [92][93]	Tampering, Modification, DOS, Ransomware [92][93]	WLAN/Wi-Fi	Malware injection using shellcode execution technique on X-ray machine that was running Windows NT 4.0	Malware injection to create a backdoor
Phillips IntelliSpace Cardiovascular (ISCV) [105][106][107]	Information disclosure, Privilege escalation, remote code execution, unauthorized access, and tampering	Ethernet	Improper privilege management, unquoted search path, plaintext credentials, and inadequate session expiration	An attacker with local user privileges and access to the ISCV server can access folders comprising executables (windows services) where authenticated users can execute arbitrary code with local system permissions.
Philips Xcelera Cardiology Information Management [106][108]	Information disclosure, Privilege escalation, remote code execution, unauthorized access, and tampering	Ethernet	Improper privilege management, unquoted search path, and plaintext credentials	An attacker with local user privileges and access to the ISCV server can access folders comprising executables (windows services) where authenticated users can execute arbitrary code with local system permissions.
Philips iSite/IntelliSpace PACS [109]	Information disclosure, unauthorized access, remote code execution, DOS, and tampering	Ethernet	Inadequate addressing of memory locations which allows attackers to execute malicious code alter flow control, crash the device or access sensitive information. Moreover, source code weaknesses including insufficient encryption, and authentication, poor authorization and access control and hard-coded weak credentials are also present	PACS server and memory addressing exploitation
Philips Alice 6 Polysomnography System (PSG) [110]	Information disclosure	Ethernet/Wi-Fi	An improper authentication mechanism in the device along with lack of encryption and integrity check scheme due to which passwords are in plaintext and network packets also travel in plain-text	Traffic analysis and analysis of network packets
General Electronics (GE) optima medical imaging system [111]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets

(to be continued)

in open access mode and accepts all requests. The reliability of this scheme is entirely dependent upon knowledge of IMD regarding the presence of cloaker. However, such device is prone to jamming attack. In order to counter this attack, different techniques including in-body signaling are already proposed in the literature [190].

V. FUTURE DIRECTIONS

A. Technical Countermeasures

1) Security Mechanisms for On-Site Legacy Medical Devices: Based on the comprehensive review of the security vulnerabilities present in the medical devices, it can be observed that the following improvements in the

TABLE XXI
CONTINUED

GE digital radiographic imaging systems [111]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Traffic analysis
Revolution medical imaging systems [111]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Traffic analysis
Centricity PACS imaging systems [112]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets
Thunis stationary fluoroscopic and radiographic X-ray system [112]	Unauthorized access and information disclosure	Ethernet	Traffic analysis	
Entegra nuclear medicine workstation [112]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets
CADstream medical imaging software [112]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets
Image vault medical imaging software [112]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets
Millennium medical imaging system [112]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets
The precision medical imaging system [112]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets
Xeleris medical imaging workstations [113]	Unauthorized access and information disclosure	Ethernet	Hardcoded or default credentials	Gaining credentials by analyzing network packets
Withings wireless blood pressure monitor [114]	Information disclosure	Wi-Fi	Insufficient encryption mechanisms as user's information are captured in plaintext	Traffic analysis through Wireshark
Mayo clinic 20,000 networked medical equipment including CT, MRI, formulary systems, infant abduction system and infusion pumps [115]	DOS, information disclosure, MITM, unauthorized access and tampering	Ethernet and Wi-Fi	No passwords or weak hardcoded passwords, disabled security software, Old transfer and communication protocols, default configurations on device's hardware and software, old proprietary systems, unpatched software, unencrypted communication and legacy operating system's vulnerabilities	Traffic analysis, reverse engineering, vulnerability scanning, and fuzz testing

(to be continued)

legacy medical equipment are essential in order to secure them.

- *Programming issues:* Securing legacy medical devices is an important challenge as these devices were developed a while ago without security considerations. At that time, developers were not aware of the safety and security perceptions and were focused on functional requirements. The software protocols and hardware chipset of the legacy medical equipment are often out of date having several security vulnerabilities. As a result, these devices are vulnerable to several reverse engineering techniques and common exploits and adversary can easily set up to violate the availability and integrity of such systems. Common vulnerability present in these medical devices is poor programming practices including poor memory management and buffer overflows whose exploitation assists hackers to launch several cyberattacks. So, an open research area is to design security mechanisms through

TABLE XXI
CONTINUED

Qualcomm's Life Capsule Datacaptor Terminal Server (DTS) [116]	Unauthorized access and DOS	Ethernet	Inadequate authentication scheme and misfortune cookie vulnerability	This vulnerability hands out a crafted HTTP cookie to the device which results in an arbitrary write to the device's memory. Such an action can be performed without authentication and the write can be used to login without credentials, crash the device and get administrator-level privileges
Philips e-Alert unit [117]	Information disclosure, DOS, Unauthorized access, and MITM	Ethernet	Hardcoded credentials, transmission of sensitive information in plaintext, improper input validation, cross-site scripting and forgery	Traffic analysis and known exploits
Blood gas analyzer [113]	Information disclosure, tampering, and unauthorized access	Ethernet	Lack of encryption and authentication mechanism	Zeus and catidel malware to create backdoor by using Nova Biomedical CCX (CriticalCare Express) in order to recreate cyberattack in the virtual environment
PACS [114]	Information disclosure	Ethernet	Lack of encryption and input sanitization	Malicious code injection
X-ray systems [114]	Information disclosure	Ethernet	Lack of encryption and input sanitization	Malicious code injection
GE Infinia/Infinia with Hawkeye 4 medical imaging systems [120]	Unauthorized access	Ethernet	Default or hardcoded credentials	Traffic analysis to obtain credentials
MRI and X-ray machines by ReliOn and CareFusion [92]	Remote code execution, DOS, MITM [97]	Wi-Fi	Shodan API to get IP addresses of connected medical devices that are passthrough Nessus vulnerability scanner to analyze devices for known vulnerabilities	Outdated operating systems including Windows XP and service pack 2. They enabled SMB port and have weak authentication mechanisms
Neurostimulator/IPG [123]	Tampering, information disclosure and unauthorized access to physiological information	BLE	Lack of encryption during communication between network and programming software and default passwords	Traffic analysis
Natus Xltek NeuroWorks 8 EEG systems [114]	Remote code execution, DOS, and buffer overflow to extract physiological information	Ethernet	Lack of input validation scheme	Due to the lack of input validation mechanism, an attacker can send crafted packets which run malicious code and exhaust resources of the device
Philips' IntelliVue Patient [125]	Unauthorized access, information disclosure, and tampering	Ethernet	Improper authentication mechanism, Lack of limit checks	Due to lack of authentication and limit checks, an unauthenticated attacker can access memory, read it and even can tamper it
Avalon Fetal Monitors [125]	Unauthorized access, information disclosure, and tampering	Ethernet	Improper authentication mechanism, Lack of limit checks	Due to lack of authentication and limit checks, an unauthenticated attacker can access memory, read it and even can tamper it

(to be continued)

which buffer overflows can be detected and mitigated especially for medical devices.

- *Execution flow of medical equipment:* Similarly, it is significant to handle execution flow of medical devices. To serve this purpose, different approaches have been proposed by researchers but have some limitations. Isolation based techniques along with DFI can be an effective approach to mitigate run-time attacks. DFI can

TABLE XXI
CONTINUED

Philips Brilliance CT scanners [126]	Unauthorized access	Ethernet	Hardcoded credentials and OS vulnerabilities including escalated privileges	Traffic analysis
BD Alaris TIVA Syringe Pump [127]	Unauthorized access and tampering	Wi-Fi	Improper authentication scheme	With the help of malware or traffic analysis, an attacker can gain unencrypted wireless credentials of the pump
Bayer Medrad medical device [128]	Ransomware	Ethernet	Windows OS vulnerabilities	National Security Agency (NSA) hacking tools
Philips IntelliSpace Portal (ISP) [124]	MITM, Unauthorized access, remote code execution, and DOS	Ethernet	Inappropriate input validation, Windows SMB information disclosure, insecure windows permission, Remote desktop access, Legacy SSL encryption and certificates, and code debugging methodologies are enabled	The improper management of windows permissions allows an attacker to execute arbitrary code and gain sensitive information remotely through Remote Desktop Protocol (RDP) exploitation. Similarly, an attacker can execute arbitrary code at runtime as code debugging module is enabled in the device. Weak cryptography mechanisms also lead to the disclosure of sensitive information. The adversary can execute arbitrary code as there is no mechanism for validating inputs given by the user in windows server.

effectively mitigate data-based attacks while isolation-related mechanisms secure sensitive functions present in a device from insensitive one effectively. Therefore, frameworks based on such an approach will help in protecting legacy medical devices.

- *Validation of secure computing platform:* Inherently secure computing platform proposed by Cyrin *et al.* is effective as it reduces development overhead and developers do not need to define software and hardware blocks in the secure environment. Instead, they should only enlist secure assets within the application based on the security specifications of the device. Moreover, using such platform security will be incorporated at hardware and therefore will balance power consumption and memory overhead. Therefore, validation of such framework through simulations and real-life devices is another open research area and will provide an approach to secure medical devices.
- *Self-authentication mechanisms:* Self-authentication method discussed by Jagannathan and Sorini focuses on dividing medical devices software into two executable, i.e., main program and verifier program. The verifier program is in encrypted form and contains instructions without which device is unable to perform its intended functions while the main program contains instructions to decrypt encrypted program and other related functionalities. The decryption key present in the main program is in obfuscated form. Such a mechanism is prone to cyber-attacks. A sophisticated attacker can obtain the key since it is present in the main program source or RAM. Since legacy medical devices are expensive and cannot be replaced therefore self-authentication mechanisms that can be incorporated in the legacy equipment is an open research area. Securing decryption keys in this approach for self-authentication remains an open research area.
- *Encryption techniques:* Encryption mechanisms play a pivotal role in securing sensitive information stored in legacy medical devices. Majority of these devices stores and transmit medical images which aid physicians in treating chronic diseases. Unavailability and tampering of such data can lead to serious injury or even a patient's death. Therefore, secure transmission and storage of sensitive patient information is a challenge.
- *Access control mechanisms:* Another open research area is the incorporation of access control mechanisms in legacy medical devices. Adequate implementation of role-based and attribute-based access control measures can assist manufacturers and healthcare professionals to secure medical devices. A lot of research is required in these domains to ensure the safety and privacy of patients using the networked medical equipment.

2) Security Mechanisms for Implantable and Wearable Medical Devices: Following are some of the open-research areas, which can contribute towards the improvement of wearable and implantable medical devices security.

- *The accuracy of IMDs, sensor-based wearables and non-wearable physiological devices:* All of these devices have

a major role in improving the quality of health-related facilities. These devices have embedded sensors that can be used for determining heart rate, pulse rate, EEG, and pressure values. Unauthorized alteration of these values can put human life in danger; therefore, ensuring their authenticity and accuracy is vital. Mechanisms to ensure accuracy and integrity without additional computational power remains an open research area.

- *Trust management:* Since sensor-based medical devices track critical physiological information whose application in critical healthcare operations can improve the quality of services, therefore maintaining a certain level of trust can help physicians in using that information. Trust quantification in the domain of medical devices is significant as it assists in identifying the legitimate and malicious node. Therefore, more research is required in trust management particularly for medical devices.
- *Standardized key-management technique:* Thirdly, there is also a requirement of standardized key management techniques, which assists in transmitting data between different kinds of devices in a secure way.
- *Lightweight cryptographic protocols and authentication mechanisms:* Secure lightweight cryptographic protocols and authentication mechanisms are required in order to secure implants and wearables. A lot of research has been carried out in this domain but has some limitations. In the case of vibration-based cryptography mechanisms, an adversary can extract keys from vibration signals as these are acoustic and electromagnetic waves that can be captured. Moreover, for bio-cryptographic schemes, Li *et al.* [64] provided an approach to get an unauthorized access to the device through ECG and EEG.
- *Technology constraints:* Majority of the wearables and IMDs are designed in a way that they communicate with BCU, mobile app, or an access point. These devices are equipped with BLE, Near-field communication (NFC), and Wi-Fi. On the other hand, IMDs make use of RF and in some cases BLE. These devices use different frequencies for communication whereas other medical equipment connects at different frequencies. Therefore, communication between implants, wearable, and non-wearable sensor-based physiological devices is another open research area.
- *Firmware modification prevention schemes:* It is one of the most frequent attacks on wearables and IMDs. As updates are essential for improving the performance of the device but due to lack of proper firmware integrity check mechanisms, adversaries exploit such an issue and replace legitimate device's firmware with a malicious one.

3) Communication Technologies: As medical devices have now become network-connected, therefore, security of these devices has emerged as an important challenge. Following are some research areas, which can consider such an issue.

- *BLE security mechanisms:* Most of the wearables and IMD rely on BLE for communication; therefore, there is a need of BLE communication standard as the majority of the wearables uses BLE as a communication code and are prone to several cyber-attacks. These wearables establish a connection through pairing with controller devices or mobile app using BLE. Such a mechanism ensures that further communication will be secure. However, information shared during the pairing process can be collected through sniffing tools. Likewise, fixed MAC address during advertisement is another important challenge. Due to these factors, an MITM attacker can modify the information exchange during the pairing process. Therefore, addressing these issues is an important challenge.
- *Radio channel interference:* Wearables and some of the non-wearable sensor-based medical devices experience radio channel interference, which distorts communication. Therefore, appropriate scheduling method is essential to reduce data collision or interference at the point of data collection for ensuring accurate transmission of sensitive data in the real-time.

B. Regulatory Countermeasures

1) FDA's Regulations: Following is the list of FDA's regulation's limitations that can be improved in order to ensure approval considering both safety and security aspects of medical devices.

- *Cybersecurity in Refuse-To-Accept checklist and SMART template:* Cybersecurity is not fully integrated into the Refuse-To-Accept checklist and SMART template. These are used to screen applications for completeness during the initial review of FDA. Whereas, for substantial review, another template named SMART is used by reviewers in order to organize and guide outcomes of their review. Both documents lack a dedicated section for cybersecurity. Since these documents are publicly available and serve manufacturers with the minimum criteria that FDA uses to accept an application for initial and substantive review [104]. In case any of the mandatory information is lacking, FDA might refuse the application until the manufacturer provides it. Therefore, the manufacturer can use it as a guideline to prepare their submissions properly. As cybersecurity section is missing in both of the tools, therefore, submissions by manufacturers might miss it due to which severe safety issues can arise. So, research regarding mandatory cybersecurity requirements that manufacturers should follow during design and development of medical devices is significant.
- *Unified safety and security risk assessment:* To manage cybersecurity risks of medical devices, FDA has proposed pre-market and post-market guidance documents in which FDA has recommended NIST's critical infrastructure framework. This framework is effective, but it is not tailored for medical device and cannot be exactly fit in such an industry. Medical devices are different from traditional IT system and hence risks are also of a different nature. Traditional risk assessment approach cannot be used for medical devices as non-malicious (software bugs) and malicious (security vulnerabilities) errors can

cause hazards. It is critical to identify software bugs that can cause hazards. Likewise, it is equally important to find security vulnerabilities, which have the potential to cause hazardous events. Then, to calculate the actual risk value, it is significant to determine integrated risk. Therefore, a unified approach to determine security and safety risks is much needed as it provides a fair idea of all malicious and non-malicious errors that may cause hazards influencing patient safety.

- *Minimum security controls criteria:* FDA has provided a comprehensive description of safety-related controls with respect to a device class, which makes it easy for both regulators and manufacturers to comply with the regulations. However, such guidance for security-related controls is missing. It is, therefore, difficult for manufacturers to incorporate security in their devices. Thus, minimum security controls and their details with respect to a class of a medical device is an open research area.
- *Cybersecurity in General Controls FDA:* QSR, labeling and branding controls required for almost all medical devices lack cybersecurity issues. Although premarket cybersecurity guidance document discusses security issues but is still not properly enforced. Most of the medical devices are neither networked nor software-based due to which these considerations are missing. However, in the case of connected medical devices, QSR must cover security considerations in all these phases as well and remains an open research domain.
- *Medical device reporting framework:* Another important regulation is to report adverse events associated with medical devices. The existing guidance provides an approach to report adverse events causing serious impairment or death for manufacturers. However, underreporting of medical devices issues by hospitals is a major concern as hospital staff uses a variety of devices throughout the day. An important reason for such misreporting is lack of awareness, training or plan to comply with reporting requirements. For hospitals, well-drafted documented measures had not been developed, implemented and maintained by regulatory bodies. A framework is much needed to guide physicians and hospital administration to report adverse events to both manufacturers and FDA in a timely manner.
- *Medical devices classification with respect to safety and security risks:* Traditional risk assessment approach of medical devices is based on the level of risk device poses to human and regulatory controls it requires for safety and effectiveness. This classification is the same for all type of devices, including networked, software-based and hardware-based devices. Since all of them are not vulnerable to security breaches; therefore, this classification could not regulate devices with the appropriate security controls to avoid patient safety concerns. As by considering security issues, some class II devices can be critical enough to go through stringent regulatory reviews but are overlooked [131]. Based on security risk, its likelihood and impact, stringent security controls must be incorporated into medical devices. FDA, nowadays, has been working in this domain and proposed a draft guidance which describes two tiers where tier 1 lists devices with an increased cybersecurity risk and tier 2 devices exhibit low-security risk as they do not contain software or networking capabilities. However, still, some research is required to identify medium and high-risk devices within tier 1.
- *Mobile apps security issues and privacy challenges:* Mobile apps are the major target of attackers due to regulatory limitations. Class I mobile-related application or mobile app can acquire sensitive information from sensors, but FDA tends to exercise enforcement discretion, which means the regulatory body does not intend to regulate a device as they pose a low risk to patient safety. Therefore, it can be exploited as an entry point to attack health systems. In addition, privacy issues are another major concern for medical devices. Although, regulatory bodies are now trying to consider security vulnerabilities present in medical devices that have a major impact on patient safety. However, some of these vulnerabilities impacting patient safety also have a major impact on their privacy. But regulatory bodies, including FDA do not consider them. In addition, HIPAA also does not regulate medical devices, as manufacturers developing these devices do not comply with laws because they do not transmit sensitive data and are not required to use such mechanisms at the initial phase. Almost 84% of health applications are open to HIPAA violations and hacks due to non-compliance [142]. A study directed by BMC Medicine discovered that approximately 89 percent of mobile applications transfer information to online services while 66 percent of them transmit health information without encryption and 20 percent has no privacy policy [143]. Therefore, there is a need for a framework to handle both safety and privacy impact of security vulnerabilities through integrated risk assessment and appropriate security and privacy controls.
- *Tool to identify software technologies, third-party modules and critical configurations of medical devices:* An important issue in managing cybersecurity issues of medical devices is the identification of software components that hackers can exploit. Generally, these devices seem black box as details of their software and technical specifications are not known. Therefore, research is required to develop a tool that can identify software specifications, critical configurations, and third-party software details. Further, it can be cross-referenced with CVSS and NVD for known vulnerabilities. It will assist in understanding the software modules of devices, their security vulnerabilities, and applicable cyberattacks.

2) E.U. Regulations: This section discusses some open-research areas in the domain of E.U. regulations that can address cyber-security issues of medical devices.

- *Harmonized cybersecurity standard evaluation framework:* The national oversight bodies in Europe and EU have provided a limited guidance regarding cybersecurity mechanisms and practices particularly for medical

devices. Currently, NBs evaluates safety and effectiveness of medical devices and overseen by national authorities. However, new MDRs require manufacturers to develop devices in accordance with security mechanisms but does not provide comprehensive guidance regarding these mechanisms. It is a major limitation as the standards which combine conventional criteria for the functional safety of device with suitable IT security requirements are still missing. As a result, the certification bodies and manufacturers which evaluate devices for safety are left to develop their own medical IT security evaluation and certification frameworks. Therefore, cybersecurity standards, especially for medical devices, are fragmenting across Europe or even within EU member states. In such scenario, harmonized medical IT security evaluation and certification framework along with guidance documents is another open research area.

- *Transparency challenges:* Transparency in the case of EU regulations is a challenge as different member states have established their own registration tools which are not always compatible with one another. This also places a pointless burden on the manufacturers who intend to market their devices in more than one country. Therefore, the development of standardized registration tools is another important research domain.

VI. Conclusion

Modern technical innovations with the introduction of networked medical devices have transformed the canvas of healthcare operations. Therefore, interest in the security of networked medical devices has been increasing rapidly. During the last few years, a great number of networked medical devices have hit the market. Consequently, security concerns present in these medical devices have gained the attention of researchers from all over the world and research articles regarding medical devices vulnerabilities and cyber-attacks has been increasing exponentially. This survey studies more than a hundred devices to understand their security issues with an emphasis on demonstrated cyber-attacks. These devices are prone to critical cyber-attacks, including tampering, sniffing, unauthorized access, MITM, DOS, ransomware and many more. The survey not only reviews security challenges of medical devices but also studies available countermeasures to address these concerns. Furthermore, this research also the research highlights and analyzes policy and regulatory weaknesses that serve these issues in the first place. Finally, we have identified some open research areas that must grasp the premise in terms of privacy and security related issues in networked medical devices.

Appendix
Cyberattacks on Medical Device

See Tables XVIII–XXI.

References

[1] M. Chen *et al.*, "5G-smart diabetes: Toward personalized diabetes diagnosis with healthcare big data clouds," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 16–23, Apr. 2018.

[2] G. Syringe. (2013). *Overview: FDA Regulation of Medical Devices*. Accessed: Mar. 2, 2018. [Online]. Available: http://www.qrasupport.com/FDA-MED-DEVICE.html

[3] G. Tanev, P. Tzolov, and R. Apiafi, "A value blueprint approach to cybersecurity in networked medical devices," *Technol. Innov. Manag. Rev.*, vol. 5, no. 8, pp. 17–25, 2015.

[4] (2017). *How U.S. Life Expectancy Ranks in the World*. Accessed: Mar. 2, 2018. [Online]. Available: https://www.huffingtonpost.com/2013/11/21/us-life-expectancy-oecd_n_4317367.html

[5] B. Yu *et al.*, "An elastic second skin," *Nat. Mater.*, vol. 15, pp. 911–918, May 2016.

[6] R. Llamas, J. Ubrani, and M. Shirer. (2016). *IDC Forecasts Worldwide Shipments of Wearables to Surpass 200 Million in 2019, Driven by Strong Smartwatch Growth and the Emergence of Smarter Watches*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.businesswire.com/news/home/20160317005136/en/IDC-Forecasts-Worldwide-Shipments-Wearables-Surpass-200

[7] V. Woods and R. Meulen. (2016). *Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016*. Accessed: Feb. 16, 2018. [Online]. Available: https://www.gartner.com/newsroom/id/3198018

[8] B. Japsen. (2016). *Medical Technology Sales to Hit $500B Within Five Years*. Accessed: Feb. 1, 2019. [Online]. Available: https://www.forbes.com/sites/brucejapsen/2016/10/17/medical-technology-sales-to-hit-500b-within-five-years/#54ebe57e11be

[9] A. Chaudhri. (2015). *North America to Lead Global Wearable Technology Market, Healthcare Sector Dominates Demand: Transparency Market Research*. Accessed: Feb. 17, 2018. [Online]. Available: https://www.cnbc.com/2015/10/20/globe-newswire-north-america-to-lead-global-wearable-technology-market-healthcare-sector-dominates-demand-transparency-market-research.html

[10] S. Smith. (2017). *Wearable Technology Market—Global Opportunity Analysis and Industry Forecast, 2014–2022*. Accessed: Feb. 19, 2018. [Online]. Available: https://www.prnewswire.com/news-releases/wearable-technology-market—global-opportunity-analysis-and-industry-forecast-2014-2022-300460342.html

[11] V. Laxmi, *Medical Devices: Technologies and Global Markets*, BCC Res., Wellesley, MA, USA, pp. 4–50, 2018. Accessed: Aug. 10, 2019. [Online]. Available: https://www.bccresearch.com/market-research/healthcare/medical-devices-technologies-and-global-markets.html

[12] S. Sudip. (2016). *Global Wearable Medical Devices Market—Transparency Market Research*. Accessed: Feb. 20, 2018. [Online]. Available: https://www.transparencymarketresearch.com/pressrelease/global-wearable-medical-devices.htm

[13] L. Kerolos and M. Hale, "Assessing pairing and data exchange mechanism security in the wearable Internet of Things," in *Proc. IEEE Int. Conf. Mobile Services (MS)*, Jun. 2016, pp. 25–32.

[14] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of medical things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.

[15] K. Fu, *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*. Washington, DC, USA: Nat. Acad. Press, 2013.

[16] X. Hei and X. Du, *Emerging Security Issues in Wireless Implantable Medical Devices*. Heidelberg, Germany: Springer, 2013.

[17] Y. Kim, W. Lee, A. Raghunathan, and V. Raghunathan, "Reliability and security of implantable and wearable medical devices," in *Implantable Biomedical Microsystems*, 1st ed., S. Bhunia, S. Majerus, and M. Sawan, Eds., Elsevier, 2015, pp. 167–199.

[18] B. Ransford *et al.*, "Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists," *Pacing Clin. Electrophysiol.*, vol. 40, no. 8, pp. 913–917, 2017.

[19] L. Kelvin and Y. Jin, "Security studies on wearable fitness trackers," in *Proc. 38th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, 2016, p. 1.

[20] M. Rushanan, A. Rubin, D. Kune, and C. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Security Privacy*, 2014, pp. 524–539.

[21] S. Seneviratne *et al.*, "A survey of wearable devices and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2573–2620, 4th Quart., 2017.

[22] G. Fortino, G. Di Fatta, M. Pathan, and A. Vasilakos, "Cloud-assisted body area networks: State-of-the-art and future challenges," *Wireless Netw.*, vol. 20, no. 7, pp. 1925–1938, 2014.

[23] R. Negra, I. Jemili, and A. Belghith, "Wireless body area networks: Applications and technologies," *Procedia Comput. Sci.*, vol. 83, pp. 1274–1281, May 2016.

[24] M. Chen *et al.*, "Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 54–61, Jan. 2017.

[25] *Medical Device Networking for Smarter Healthcare: Part 3*. Accessed: Feb. 10, 2019. [Online]. Available: https://www.lantronix.com/wpcontent/uploads/pdf/Part3LantronixMedicalDeviceNetworkingNextGenWirelessDeployments_WP.pdf

[26] T. Yaqoob *et al.*, "Feasibility analysis for deploying national healthcare information system (NHIS) for Pakistan," in *Proc. IEEE 19th Int. Conf. E-Health Netw. Appl. Services (Healthcom)*, 2017, pp. 1–6.

[27] M. Chen, W. Li, Y. Hao, Y. Qian, and I. Humar, "Edge cognitive computing based smart healthcare system," *Future Gener. Comput. Syst.*, vol. 86, pp. 403–411, Sep. 2018.

[28] A. Sasan, *Mobile Health: A Technology Road Map*. Berlin, Germany: Springer, 2015, p. 1172.

[29] A. Boulemtafes and N. Badache, "Design of wearable health monitoring systems: An overview of techniques and technologies," in *mHealth Ecosystems and Social Networks in Healthcare*, vol. 20, 1st ed., A. Lazakidou, S. Zimeras, D. Iliopoulou, and D. Koutsouris, Eds. Cham, Switzerland: Springer, 2016, pp. 79–94.

[30] S. Pathak, M. Kumar, A. Mohan, and B. Kumar, "Energy optimization of ZigBee based WBAN for patient monitoring," *Procedia Comput. Sci.*, vol. 70, pp. 414–420, Nov. 2015.

[31] X. Cao *et al.*, "Ghost-in-ZigBee: Energy depletion attack on ZigBee-based wireless networks," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 816–829, Oct. 2016.

[32] P. Cope, J. Campbell, and T. Hayajneh, "An investigation of Bluetooth security vulnerabilities," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–7.

[33] J. Xu *et al.*, "Pairing and authentication security technologies in low-power Bluetooth," in *Proc. IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber Phys. Soc. Comput.*, Aug. 2013, pp. 1081–1085.

[34] T. Panse and V. Kapoor, "A review on security mechanism of Bluetooth communication," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 2, pp. 3419–3422, 2012.

[35] A. Boulemtafes and N. Badache, "Design of wearable health monitoring systems: An overview of techniques and technologies," in *mHealth Ecosystems and Social Networks in Healthcare*. Cham, Switzerland: Springer, 2016, pp. 79–94.

[36] J. Granjal, E. Monteiro, and J. S. Silva, "Security in the integration of low-power wireless sensor networks with the Internet: A survey," *Ad Hoc Netw.*, vol. 24, pp. 264–287, Jan. 2015.

[37] W. Sun, M. Choi, and S. Choi, "IEEE 802.11 ah: A long range 802.11 WLAN at sub 1 GHz," *J. ICT Stand.*, vol. 1, pp. 83–108, May 2013.

[38] M. Ahmed, M. Jilani, K. Khan, and M. Ahmed, "A security framework for wireless body area network based smart healthcare system," in *Proc. Int. Conf. Young Res. Informat. Math. Eng. (ICYRIME)*, Kaunas, Lithuania, 2017, pp. 80–85.

[39] M. Khera, "Think like a hacker," *J. Diabetes Sci. Technol.*, vol. 11, no. 2, pp. 207–212, 2016.

[40] D. Kim, S. Park, K. Choi, and Y. Kim, "BurnFit: Analyzing and exploiting wearable devices," in *Proc. Inf. Security Appl.*, vol. 9503, 2016, pp. 227–239.

[41] N. Fatema and R. Brad, "Security requirements, counterattacks and projects in healthcare applications using WSNs—A review," *Int. J. Comput. Netw. Commun.*, vol. 2, no. 2, pp. 1–9, 2014. Accessed: May 10, 2019.

[42] C. Eric, M. Schiefer, and M. Morgenstern, *Internet of Things: Security Evaluation of Nine Fitness Trackers*, Independent IT-Security Inst., AV TEST, Magdeburg, Germany, 2015.

[43] E. Marin *et al.*, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proc. 32nd Annu. Conf. Comput. Security Appl. (ACSAC)*, 2016, pp. 226–236.

[44] N. Ellouze, M. Allouche, H. B. Ahmed, S. Rekhis, and N. Boudriga, "Security of implantable medical devices: Limits, requirements, and proposals," *Security Commun. Netw.*, vol. 7, no. 12, pp. 2475–2491, Nov. 2013.

[45] D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," in *Proc. 13th Annu. Conf. Privacy Security Trust (PST)*, Jul. 2015, pp. 145–152.

[46] D. F. Kune *et al.*, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *Proc. IEEE Symp. Security Privacy*, May 2013, pp. 145–159.

[47] T. Bonaci, J. Herron, C. Matlack, and H. J. Chizeck, "Securing the exocortex: A twenty-first century cybernetics challenge," in *Proc. IEEE Conf. Norbert Wiener 21st Century (21CW)*, Jun. 2014, pp. 1–8.

[48] T. Bonaci, R. Calo, and H. J. Chizeck, "App stores for the brain: Privacy & security in brain–computer interfaces," in *Proc. IEEE Int. Symp. Ethics Sci. Technol. Eng.*, May 2014, pp. 1–7.

[49] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.

[50] Z. E. Ankarali *et al.*, "A comparative review on the security research for wireless implantable medical devices," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare (Mobihealth)*, Athens, Greece, 2014, pp. 3–5.

[51] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky, "Patient infusion pattern based access control schemes for wireless insulin pump system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 11, pp. 3108–3121, Nov. 2015.

[52] M. Zhang, A. Raghunathan, and N. K. Jha, "Towards trustworthy medical devices and body area networks," in *Proc. 50th Annu. Design Autom. Conf. (DAC)*, 2013, pp. 1–6.

[53] Y. Kim, W. S. Lee, V. Raghunathan, N. K. Jha, and A. Raghunathan, "Vibration-based secure side channel for medical devices," in *Proc. 52nd Annu. Design Autom. Conf. DAC*, 2015, pp. 1–6.

[54] R. Yan, T. Xu, and M. Potkonjak, "Semantic attacks on wireless medical devices," in *Proc. IEEE SENSORS*, Nov. 2014, pp. 482–485.

[55] D. Gray. (2017). *Wireless Syringe Infusion Pumps Vulnerable to Cyber-Attacks*. [Online]. Available: https://www.medicalplasticsnews.com/news/wireless-syringe-infusion-pumps-vulnerable-to-cyber-attacks/

[56] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1495–1501.

[57] A. M. Nia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Physiological information leakage: A new frontier in health information security," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 3, pp. 321–334, Jul./Sep. 2016.

[58] A. Archimendes. (2015). *Research Center for Medical Device Security*. [Online]. Available: http://secure-medicine.org/

[59] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015.

[60] A. Mosenia and N. K. Jha, "OpSecure: A secure unidirectional optical channel for implantable medical devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 4, no. 3, pp. 410–419, Jul./Sep. 2017.

[61] IBM. (2014). *Will the Demise of XP Shut Down Your Business or Heart?* [Online]. Available: http://privacyguidance.com/blog/will-the-demise-of-xp-shut-down-your-business-or-heart/

[62] *Information Security Guide Broadband Kit*, St. Jude Med., St. Paul, MN, USA, 2017.

[63] W. Glisson, T. Andel, T. McDonald, M. Jacobs, M. Campbell, and J. Mayr, "Compromising a medical," *arXiv preprint arXiv:1509.00065*, 2015.

[64] Q. Li, D. Ding, and M. Conti, "Brain–computer interface applications: Security and privacy challenges," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Sep. 2015, pp. 663–666.

[65] J. Rieck, "Attacks on fitness trackers revisited: A case-study of unfit firmware security," *arXiv preprint arXiv:1604.03313*, 2016.

[66] M. Rahman, C. Bogdan, and B. Madhusudan, "Fit and vulnerable: Attacks and defenses for a health monitoring device," *arXiv preprint arXiv:1304.5672*, 2013.

[67] E. Clausing, S. Michael, and M. Maik, *Internet of Things: Security Evaluation of Nine Fitness Trackers*, Independent IT-Security Inst., AV TEST, Magdeburg, Germany, 2016.

[68] S. Magaritelli. (2015). *Nike+ FuelBand SE BLE Protocol Reversed*. [Online]. Available: https://www.evilsocket.net/2015/01/29/nike-fuelband-se-ble-protocol-reversed/

[69] J. Shim *et al.*, "A case study on vulnerability analysis and firmware modification attack for a wearable fitness tracker," *IT Converg. Pract.*, vol. 5, no. 4, pp. 25–33, 2017.

[70] J. Classen, D. Wegemer, P. Patras, T. Spink, and M. Hollick, "Anatomy of a vulnerable fitness tracking system: Dissecting the fitbit cloud, app, and firmware," *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 2, no. 1, pp. 1–24, Mar. 2018.

[71] R. Goyal, N. Dragoni, and A. Spognardi, "Mind the tracker you wear," in *Proc. 31st Annu. ACM Symp. Appl. Comput. (SAC)*, 2016, pp. 131–136.

[72] B. Cusack, A. Bryce, W. Gerard, and M. Shaunak, "Assessment of security vulnerabilities in wearable devices," in *Proc. Aust. Inf. Security Manag. Conf.*, 2017, pp. 42–48.

[73] Indian Institute of Technology Kanpur Commonwealth of Learning Vancouver. (2018). *Sensors on Android Phones*. [Online]. Available: http://m4d.colfinder.org/sites/default/files/Slides/M4D_Week2_sensors.pdf

[74] R. Goodrich. (2013). *Accelerometer vs. Gyroscope: What's the Difference?* Accessed: Mar. 2, 2018. [Online]. Available: https://www.livescience.com/40103-accelerometer-vs-gyroscope.html

[75] K. W. Ching and M. M. Singh, "Wearable technology devices security and privacy vulnerability analysis," *Int. J. Netw. Security Appl.*, vol. 8, no. 3, pp. 19–30, May 2016.

[76] S. Safavi and S. Zarina, "Improving Google glass security and privacy by changing the physical and software structure," *Life Sci. J.*, vol. 11, no. 5, pp. 109–117, 2014.

[77] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in Internet of Things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr. 2015.

[78] Q. Zhang and Z. Liang, "Security analysis of Bluetooth low energy based smart wristbands," in *Proc. 2nd Int. Conf. Front. Sensors Technol. (ICFST)*, Apr. 2017, pp. 421–425.

[79] K. Fawaz, K. Kyu-Han, and K. G. Kang, "Protecting privacy of BLE device users," in *Proc. USENIX Security Symp.*, 2016, pp. 1205–1221.

[80] A. Maiti, M. Jadliwala, J. He, and I. Bilogrevic, "(Smart)watch your taps: Side-channel keystroke inference attacks using smartwatches," in *Proc. ACM Int. Symp. Wearable Comput.*, 2015, pp. 27–30.

[81] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang, "When good becomes evil: Keystroke inference with smartwatch," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, 2015, pp. 1273–1285.

[82] C. Wang, X. Guo, Y. Wang, Y. Chen, and B. Liu, "Friend or foe: Your wearable devices reveal your personal pin," in *Proc. 11th ACM Asia Conf. Comput. Commun. Security (ASIA CCS)*, 2016, pp. 189–200.

[83] G. Paul and J. Irvine, "Privacy implications of wearable health devices," in *Proc. 7th Int. Conf. Security Inf. Netw. (SIN)*, 2014, p. 117.

[84] Fitbit. *Website Terms and Conditions*. Accessed: Sep. 2017. [Online]. Available: http://www.fitbit.com

[85] BASIS. *Basis Privacy*. Accessed: Mar. 2018. [Online]. Available: http://www.mybasis.com/legal/privacy/

[86] M. Fouad, E. Nashwa, A. Rabie, and A. Hassanien, "Wireless sensor networks: A medical perspective," in *Wireless Sensor Networks: Theory Applications*. Boca Raton, FL, USA: CRC Press, 2013.

[87] V. Agrawal, "Security and privacy issues in wireless sensor networks for healthcare," in *Internet of Things. User-Centric IoT*. Cham, Switzerland: Springer, 2015, pp. 223–228.

[88] J. Chauhan, S. Seneviratne, M. A. Kaafar, A. Mahanti, and A. Seneviratne, "Characterization of early smartwatch apps," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2016, pp. 1–6.

[89] A. Demir and T. Emin, "Security analysis of medical devices within wireless body area networks and mobile health applications," *Int. J. Inf. Technol.*, vol. 11, no. 1, pp. 1–8, 2018.

[90] V. Moses and I. Korah, "Lack of security of networked medical equipment in radiology," *Amer. J. Roentgenol.*, vol. 204, no. 2, pp. 343–353, Feb. 2015.

[91] T. Mahler *et al.*, "Know your enemy: Characteristics of cyber-attacks on medical imaging devices," in *Proc. RSNA Conf.*, Chicago, IL, USA, 2017, pp. 1–6.

[92] E. McMahon *et al.*, "Assessing medical device vulnerabilities on the Internet of Things," in *Proc. IEEE Int. Conf. Intell. Security Informat. (ISI)*, Jul. 2017, pp. 176–178.

[93] L. Ayala, *Cybersecurity for Hospitals and Healthcare Facilities*. Berkeley, CA, USA: Apress, 2016.

[94] (1996). *HIPAA—Health Insurance Portability and Accountability Act*. Accessed: Nov. 17, 2018. [Online]. Available: https://www.hippa.com/

[95] (2016). *Wireless Medical Devices*. Accessed: Nov. 17, 2018. [Online]. Available: https://www.fda.gov/MedicalDevices/DigitalHealth/WirelessMedicalDevices/default.htm

[96] D. Cicco *et al.* (2018). *Toward an Enhanced EU Cybersecurity Framework: Political Agreement Reached on EU Cybersecurity Act—Security—European Union*. Accessed: Nov. 17, 2018. [Online]. Available: http://www.mondaq.com/uk/x/709760/Security/Toward+An+Enhanced+EU+Cybersecurity+Framework+Political+Agreement+Reached+On+EU+Cybersecurity+Act

[97] (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA Relevance)*. Accessed: Dec. 13, 2018. [Online]. Available: https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

[98] FDA. (Oct. 2, 2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. Accessed: May 21, 2018. [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/sUCM356190.pdf

[99] S. Gupta, "Medical device regulations: A current perspective," *J. Young Pharm.*, vol. 8, no. 1, pp. 6–11, 2016.

[100] (2017). *Regulation (Eu) 2017/745 of the European Parliament and of the Council, Official Journal of the European Union*. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745&from=EN

[101] (2017). *Regulation (EU) 2017/746 of the European Parliament and of the Council, Official Journal of the European Union*. [Online]. Available: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX32017R0746&from=EN

[102] D. Biddle and L. Reath, *Regulatory Considerations for Cybersecurity and Data Privacy in Digital Health and Medical Applications and Products*, St. Paul, MN, USA: CSC, 2018.

[103] (2018). *Patients and Privacy: GDPR Compliance for Healthcare Organizations—Security News—Trend Micro GB*. Accessed: Oct. 31, 2018. [Online]. Available: https://www.trendmicro.com/vinfo/gb/security/news/online-privacy/patients-and-privacy-gdpr-compliance-for-healthcare-organizations

[104] *FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices*, U.S. Dept. Health Human Services, Washington, DC, USA, 2018. [Online]. Available: https://www.oig.hhs.gov/oei/reports/oei-09-16-00220.pdf

[105] (2018). *Philips IntelliSpace Cardiovascular Vulnerabilities—ICS-CERT*. Accessed: Nov. 1, 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-226-01

[106] (2018). *Philips IntelliSpace Cardiovascular System Vulnerability—ICS-CERT*. Accessed: Nov. 1, 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-025-01

[107] M. Rohman. (2018). *Philips Issues Security Advisory for Cardiac Imaging, Information Management Software," Health Imaging*. Accessed: Nov. 1, 2018. [Online]. Available: https://www.healthimaging.com/topics/imaging-informatics/philips-issues-security-advisory-pacs-softwares

[108] (2017). *Philips IntelliSpace Cardiovascular System and Xcelera System Vulnerability—ICS-CERT*. Accessed: Nov. 1, 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-17-318-01

[109] (2018). *Philips iSite/IntelliSpace PACS Vulnerabilities (Update A)—ICS-CERT*. Accessed: Nov. 1, 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-088-01

[110] (2018). *Philips Alice 6 Vulnerabilities—ICS-CERT*. Accessed: Nov. 1, 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-086-01

[111] F. Donovan. (2018). *ICS-CERT Flags Philips, GE Medical Device Vulnerabilities*. Accessed: Nov. 1, 2018. [Online]. Available: https://healthitsecurity.com/news/ics-cert-flags-philips-ge-medical-device-vulnerabilities

[112] (2017). *GE Centricity PACS CVE-2017-14008*. [Online]. Available: https://www.cvedetails.com/cve/CVE-2017-14008/v

[113] (2018). *GE Xeleris Medical Imaging Systems*. [Online]. Available: https://www.cvedetails.com/cve/CVE-2017-14006/

[114] D. Wood, N. Apthorpe, and N. Feamster, "Cleartext data transmissions in consumer IoT medical devices," in *Proc. IoT-S&P*, Dallas, TX, USA, 2017, pp. 7–12.

[115] F. Hudson. (2017). *Biomedical Device Security: New Challenges and Opportunities*. Accessed: Nov. 1, 2018. [Online]. Available: https://nchica.org/wp-content/uploads/2015/06/Bruemmer-Hudson.pdf

[116] D. Gray. (2018). *Cyber Vulnerabilities Found in Two Major Medical Devices*. Accessed: Nov. 1, 2018. [Online]. Available: http://digitalhealthage.com/cyber-vulnerabilities-found-in-two-major-medical-devices/

[117] (2018). *Advisory (ICSA-18-242-01) Philips E-Alert Unit*. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-18-242-01

[118] D. Storm. (2015). *MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks*. Accessed: Nov. 1, 2018. [Online]. Available: https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

[119] C. Beek. (2018). *McAfee Researchers Find Poor Security Exposes Medical Data to Cybercriminals*. [Online]. Available: https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/

[120] (2018). *GE Infinia/Infinia With Hawkeye 4 Medical Imaging Systems*. [Online]. Available: https://www.cvedetails.com/cve/CVE-2017-14002/

[121] (2018). *GE PACSystems RX3i*. [Online]. Available: https://www.cvedetails.com/cve/CVE-2018-8867/

[122] (2018). *LiberHealthIO*. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-19165/Librehealth.html

[123] *The Memory Market: Preparing for a Future Where Cyberthreats Target Your Past*, Kaspersky Lab, Moscow, Russia, 2018. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/10/29094959/The-Memory-Market-2018_ENG_final.pdf

[124] C. Duplantis. (2018). *Vulnerability Spotlight: Natus NeuroWorks Multiple Vulnerabilities*. [Online]. Available: https://blog.talosintelligence.com/2018/04/vulnerability-spotlight-natus.html

[125] (2018). *Advisory (ICSMA-18-156-01) Philips' IntelliVue Patient and Avalon Fetal Monitors*. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-156-01

[126] HealthITsecurity. (2018). *Philips CT Scanner Cybersecurity Vulnerabilities Pose PHI Risk*. [Online]. Available: https://healthitsecurity.com/news/philips-ct-scanner-cybersecurity-vulnerabilities-pose-phi-risk

[127] (2018). *Advisory (ICSMA-18-235-01) BD Alaris Plus*. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-235-01

[128] McAfee Secure. (2017). *Most Dangerous Hacked Medical Devices*. [Online]. Available: https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices

[129] University of Michigan. (2017). *Security Risks Found in Sensors for Heart Devices, Consumer Electronics*. [Online]. Available: www.sciencedaily.com/releases/2013/05/130516123920.htm

[130] (2018). *Philips Intellispace Portal ISP Vulnerabilities—ICS-CERT*. Accessed: Nov. 1, 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

[131] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices Evid. Res.*, vol. 8, pp. 305–316, Jul. 2015.

[132] F. Bastani and T. Tang, *Improving Security of Wireless Communication in Medical Devices*, Massachusetts Inst. Technol., Cambridge, MA, USA, 2015.

[133] (2016). *Hospira Sapphire Sets Infusion Pump*. Accessed: Oct. 13, 2018. [Online]. Available: https://www.accessdata.fda.gov/cdrh_docs/pdf16/K160492.pdf

[134] (2018). *Epiphany Healthcare Programmable Diagnostic Computer*. Accessed: Oct. 13, 2018. [Online]. Available: https://www.accessdata.fda.gov/cdrh_docs/pdf18/K181720.pdf

[135] K. Zetter. (2015). *Hacker Can Send Fatal Dose to Hospital Drug Pumps*. [Online]. Available: https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/

[136] *CardioMEMS Heart Failure Monitoring System*. Accessed: Nov. 13, 2018. [Online]. Available: https://www.accessdata.fda.gov/cdrh_docs/pdf10/P100045B

[137] (2018). *Refuse to Accept Policy for 510(k)s, Guidance for Industry and Food and Drug Administration Staff*. [Online]. Available: https://www.fda.gov/ucm/groups/fdagov-public/fdagov-meddevgen/documents/document/ucm315014.pdf

[138] S. Barlas, "FDA flags inconsistent hospital reporting of medical device problems: Hazy reporting rules beget confusion," *Pharm. Ther.*, vol. 42, no. 2, pp. 97–115, 2017.

[139] J. Shuren. (Oct. 24, 2016). *FDA Is Working With Hospitals to Modernize Data Collection About Medical Devices*. Accessed: Dec. 29, 2016. [Online]. Available: http://blogs.fda.gov/fdavoice/index.php/2016/10/fda-is-working-with-hospitals-to-modernize-data-collection-aboutmedical-devices

[140] (Oct. 2018). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices-Draft Guidance for Industry and Food and Drug Administration Staff*. [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

[141] L. Tyler, "FDA issues draft to update prior final guidance on premarket cybersecurity for medical devices," 2018.

[142] B. Sidki, *8 Out of 10 Mobile Health Apps Open to HIPAA Violations, Hacking, and Data Theft*, Healthcare IT News, Portland, ME, USA, 2018. [Online]. Available: http://www.healthcareitnews.com/news/8-out-10-mobile-health-apps-open-hipaa-violations-hacking-data-theft

[143] K. Huckvale *et al.*, "Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment," *BMC Med.*, vol. 13, p. 214, Sep. 2015. [Online]. Available: http://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-015-0444-y

[144] B. Macfarlane. *FDA Regulation of Mobile Medical Apps*. Accessed: Dec. 10, 2018. [Online]. Available: https://www.namsa.com/wpcontent/uploads/2015/10/WP.006FDARegulationofMobileMedicalApps_a06.pdf

[145] M. McGee. (2016). *Critiquing FDA Medical Device Cybersecurity Guidance*. [Online]. Available: https://www.careersinfosecurity.com/critiquing-fda-medical-device-cybersecurity-guidance-a-9200

[146] K. Hoyme, *Developing a—Software Bill of Materials for the Future of Cybersecurity*, AAMI, Arlington, VA, USA, 2018. [Online]. Available: https://aamiblog.org/2018/10/02/ken-hoyme-developing-a-software-bill-of-materials-for-the-future-of-cybersecurity/

[147] C. Heneghan, M. Thompson, M. Billingsley, and D. Cohen, "Medical-device recalls in the U.K. and the device-regulation process: Retrospective review of safety notices and alerts," *BMJ Open*, vol. 1, no. 1, 2011, Art. no. e000155.

[148] D. M. Zuckerman, P. Brown, and S. E. Nissen, "Medical device recalls and the FDA approval process," *Arch. Int. Med.*, vol. 171, no. 11, pp. 1006–1011, 2011.

[149] S. S. Dhruva and R. F. Redberg, "Medical device regulation: Time to improve performance," *PLoS Med.*, vol. 9, no. 4, 2012, Art. no. e1001277.

[150] New Regulations. (2017). *Danish Medicines Agency*. Accessed: Oct. 31, 2018. [Online]. Available: https://laegemiddelstyrelsen.dk/en/devices/legislation-and-guidance/new-regulations/

[151] B. Zegeralli, *Drop in Warning Letters for Medical Devices Raises Interesting Questions About the Industry*, Insight Center, London, U.K., 2018. [Online]. Available: https://www.mintz.com/insights-center/viewpoints/2018-04-drop-warning-letters-medical-devices-raises-interesting

[152] V. Pollard and M. Davar. (2017). *FDA's Evolving Civil Money Penalty Authority: Simple Violations Can Lead to Major Costs*. [Online]. Available: https://www.mastercontrol.com/gxp-lifelinecivil_money_penalty_authority_0609

[153] P. Roberts. (2017). *Latest HIPAA Settlement Underscores Medical Device Risk*. [Online]. Available: https://digitalguardian.com/blog/latesthipaasettlementunderscoresmedicaldevicerisk

[154] (2015). *FDA Inspections, Compliance, Enforcement, and Criminal Investigations*. [Online]. Available: https://wayback.archive-it.org/7993/20170406212527/https://www.fda.gov/ICECI/CriminalInvestigations/ucm443650.htm

[155] (2010). *Medical Device Manufacturer Guidant Charged in Failure to Report Defibrillator Safety Problems to FDA*. [Online]. Available: https://wayback.archive-it.org/7993/20170723082015/https://www.fda.gov/ICECI/CriminalInvestigations/ucm272226.htm

[156] (2015). *St. John's Regional Medical Center*. [Online]. Available: https://www.cdph.ca.gov/Programs/CHCQ/LCP/CDPH%20Document%20Library/Hospital%20Administrative%20Penalties/Ventura/St.John's-Regional-MC-POC-2567-Redacted.pdf

[157] M. Knowles, *California Fines 13 Hospitals $1M-Plus for Patient Safety Issues*, ASC Commun., Chicago, IL, USA, 2018. [Online]. Available: https://www.beckershospitalreview.com/quality/california-fines-13-hospitals-1m-plus-for-patient-safety-issues.html

[158] B. Zimmermann, *California Fines 9 Hospitals $500k+ for Patient Safety Issues*, ASC Commun., Chicago, IL, USA, 2018. [Online]. Available: https://www.beckershospitalreview.com/quality/california-fines-9-hospitals-500k-for-patient-safety-issues.html

[159] A. Brino, *Grisly Medical Errors, Some Deadly, Lead to 700K in Fines for 10 California Hospitals*, Healthcare Finance, HIMSS Media, Portland, ME, USA, 2015. [Online]. Available: https://www.healthcarefinancenews.com/news/grisly-medical-errors-some-deadly-lead-700k-fines-10-california-hospitals

[160] G. Dessouky *et al.*, "LO-FAT: Low-overhead control flow attestation in hardware," in *Proc. 54th Annu. Design Autom. Conf. (DAC)*, Austin, TX, USA, 2017, pp. 1–24.

[161] T. Abera *et al.*, "C-FLAT: Control-flow attestation for embedded systems software," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, Vienna, Austria, 2016, pp. 743–754.

[162] A. Mosenia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Wearable medical sensor-based system design: A survey," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 3, no. 2, pp. 124–138, Apr./Jun. 2017.

[163] C. Bresch, S. Chollet, and D. Hely, "Towards an inherently secure run-time environment for medical devices," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2018, pp. 140–147.

[164] N. Christoulakis, G. Christou, E. Athanasopoulos, and S. Ioannidis, "HCFI: Hardware-enforced controlflow integrity," in *Proc. 6th ACM Conf. Data Appl. Security Privacy*, New Orleans, LA, USA, 2016, pp. 38–49.

[165] L. Davi *et al.*, "HAFIX: Hardware-assisted flow integrity extension," in *Proc. 52nd Annu. Design Autom. Conf.*, San Francisco, CA, USA, 2015, pp. 1–74.

[166] "Security technology building a secure system using TrustZone technology," ARM, Cambridge, U.K., Rep. PRD29-GENC-009492C, 2009.

[167] F. McKeen *et al.*, "Innovative instructions and software model for isolated execution," in *Proc. 2nd Workshop Hardw. Archit. Support Security Privacy*, Tel Aviv-Yafo, Israel, 2013, p. 10.

[168] V. Costan, I. A. Lebedev, and S. Devadas, "Sanctum: Minimal hardware extensions for strong software isolation," in *Proc. 25th USENIX Security Symp. USENIX Security*, Austin, TX, USA, 2016, pp. 857–874.

[169] F. Brasser *et al.*, 'TyTAN: Tiny trust anchor for tiny devices," in *Proc. 52nd Annu. Design Autom. Conf.*, San Francisco, CA, USA, 2015, pp. 1–34.
[170] P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan, "TrustLite: A security architecture for tiny embedded devices," in *Proc. 9th Eurosys Conf.*, Amsterdam, The Netherlands, 2014, pp. 1–10.
[171] G. J. Duck and R. H. C. Yap, "Heap bounds protection with low fat pointers," in *Proc. 25th Int. Conf. Compiler Construct.*, Barcelona, Spain, 2016, pp. 132–142.
[172] S. Nagarakatte, M. M. K. Martin, and S. Zdancewic, "WatchdogLite: Hardware-accelerated compiler-based pointer checking," in *Proc. 12th Annu. IEEE/ACM Int. Symp. Code Gener. Optim.*, Orlando, FL, USA, 2014, p. 175.
[173] A. Menon, S. Murugan, C. Rebeiro, N. Gala, and K. Veezhinathan, "Shakti-T: A RISC-V processor with light weight security extensions," in *Proc. ACM Hardw. Archit. Support Security Privacy*, 2017, pp. 1–2.
[174] L. Davi *et al.*, "MoCFI: A framework to mitigate control-flow attacks on smartphones," in *Proc. NDSS*, vol. 26, 2012, pp. 27–40.
[175] L. Cheng, *Program Anomaly Detection Against Data-Oriented Attacks*, Virginia Polytech. Inst. State Univ., Blacksburg, VA, USA, 2018.
[176] T. Ramezanifarkhani and R. Mohammadreza, "Principles of data flow integrity: Specification and enforcement," *J. Inf. Sci. Eng.*, vol. 31, no. 2, pp. 529–546, 2015.
[177] H. Zhao, R. Xu, M. Shu, and J. Hu, "Physiological-signal-based key negotiation protocols for body sensor networks: A survey," in *Proc. IEEE 12th Int. Symp. Auton. Decentralized Syst.*, Mar. 2015, pp. 63–70.
[178] D. K. Altop, A. Levi, and V. Tuzcu, "Deriving cryptographic keys from physiological signals," *Pervasive Mobile Comput.*, vol. 39, pp. 65–79, Aug. 2017.
[179] S. Pirbhulal *et al.*, "Heart-beats based biometric random binary sequences generation to secure wireless body sensor networks," *IEEE Trans. Biomed. Eng.*, vol. 65, no. 12, pp. 2751–2759, Dec. 2018.
[180] C. Hu *et al.*, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2274–2282.
[181] F. Miao, S.-D. Bao, and Y. Li, "Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security," *IET Inf. Security*, vol. 7, no. 2, pp. 87–96, Jun. 2013.
[182] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *J. Med. Syst.*, vol. 39, no. 10, p. 115, Aug. 2015.
[183] E. K. Zaghouani, A. Jemai, A. Benzina, and R. Attia, "ELPA: A new key agreement scheme based on linear prediction of ECG features for WBAN," in *Proc. 23rd Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2015, pp. 81–85.
[184] B. Tams, P. Mihailescu, and A. Munk, "Security considerations in minutiae-based fuzzy vaults," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 985–998, May 2015.
[185] J. Kim, B. J. Lee, and S. K. Yoo, "Design of real-time encryption module for secure data protection of wearable healthcare devices," in *Proc. 35th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2013, pp. 2283–2286.
[186] T. Belkhouja, X. Du, A. Mohamed, A. K. Al-Ali, and M. Guizani, "New plain-text authentication secure scheme for implantable medical devices with remote control," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–5.
[187] W. J. Long and W. Lin, "An authentication protocol for wearable medical devices," in *Proc. 13th Int. Conf. Expo Emerg. Technol. Smarter World (CEWIT)*, Nov. 2017, pp. 1–5.
[188] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.
[189] S. Jagannathan and A. Sorini, "Self-authentication in medical device software: An approach to include cybersecurity in legacy medical devices," in *Proc. IEEE Symp. Product Compliance Eng. (ISPCE)*, May 2016, pp. 1–5.
[190] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Security Commun. Netw.*, vol. 9, no. 17, pp. 4777–4803, Oct. 2016.
[191] D. He, C. Chen, S. Chan, J. Bu, and P. Zhang, "Secure and lightweight network admission and transmission protocol for body sensor networks," *IEEE J. Biomed. Health Inform.*, vol. 17, no. 3, pp. 664–674, May 2013.
[192] S. Irum, A. Ali, F. A. Khan, and H. Abbas, "A hybrid security mechanism for intra-WBAN and inter-WBAN communications," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Jan. 2013, Art. no. 842608.
[193] M. Naveed, X. Zhou, S. Demetriou, X. Wang, and C. A. Gunter, "Inside job: Understanding and mitigating the threat of external device isbonding on Android," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2014, pp. 1–14.
[194] S. Gao and G. Thamilarasu, "Machine-learning classifiers for security in connected medical devices," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–5.
[195] S. Vhaduri and C. Poellabauer, "Wearable device user authentication using physiological and behavioral metrics," in *Proc. IEEE 28th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–6.
[196] R. Latif, H. Abbas, and S. Assar, "Distributed denial of service (DDoS) attack in cloud- assisted wireless body area networks: A systematic literature review," *J. Med. Syst.*, vol. 38, no. 11, p. 128, Sep. 2014.
[197] M. Barcena, W. Candid, and L. Hon, *How Safe Is Your Quantified Self*, Symantech, Mountain View, CA, USA, 2014.
[198] *Archived Specifications—-Bluetooth Technology Website*. Accessed: Jan. 3, 2018. [Online]. Available: https://www.bluetooth.com/specifications/archived-specifications/
[199] A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, "Uncovering privacy leakage in BLE network traffic of wearable fitness trackers," in *Proc. 17th Int. Workshop Mobile Comput. Syst. Appl. (HotMobile)*, 2016, pp. 99–104.
[200] M. Rostami, W. Burleson, A. Juels, and F. Koushanfar, "Balancing security and utility in medical devices?" in *Proc. IEEE Design Autom. Conf. (DAC)*, 2013, pp. 1–6.
[201] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access control schemes for implantable medical devices: A survey," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017.

Tahreem Yaqoob received the B.S. degree in computer science with emphasis in security of cloud network from Fatima Jinnah Women University, Pakistan, and the M.S. degree in information security from the National University of Sciences and Technology, Islamabad, Pakistan, in 2018. Her research interests include security issues in healthcare environment and medical devices.

Haider Abbas (SM'16) received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from KTH, Sweden, in 2006 and 2010, respectively. He is currently heading the National Cyber Security Auditing and Evaluation Lab with MCS-NUST. He is a Cyber Security Professional who took professional trainings and certifications from the Massachusetts Institute of Technology, USA; Stockholm University, Sweden, IBM, and EC-Council. He is an Associate Editor or on the editorial board of a number of international journals, including the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, the *Journal of Network and Computer Applications*, *Electronic Commerce Research*, IEEE ACCESS, *Neural Computing and Applications* and *Cluster Computing*. He also won many awards and received several research grants for ICT-related projects from various research funding authorities and working on scientific projects in U.S., Europe, Saudi Arabia, and Pakistan. He is the principal advisor for several graduate and doctoral students with the National University of Sciences and Technology, Pakistan, Al-Farabi Kazakh National University, Kazakhstan, the Florida Institute of Technology, USA, and Manchester Metropolitan University, U.K.

Mohammed Atiquzzaman (SM'95) received the M.S. and Ph.D. degrees in electrical engineering and electronics from the University of Manchester, U.K. He currently holds the Edith Kinney Gaylord Presidential professorship with the School of Computer Science, University of Oklahoma. His research interests include communications switching, transport protocols, wireless and mobile networks, ad hoc networks, satellite networks, quality of service, and optical communications. He is the Editor-in-Chief of the *Journal of Networks and Computer Applications* and has served on the editorial boards of several journals and on the review panels of several funding agencies.