Medical Internet of Things: A Survey of the Current Threat and Vulnerability Landscape

Aleise McGowan
University of South Alabama
am1828@jagmail.southaalabama.edu

Scott Sittig
University of South Alabama
sittig@southalabama.edu

Todd Andel
University of South Alabama
tandel@southalabama.edu

Abstract

The Internet of things (IoT) is a system that utilizes the Internet to facilitate communication between sensors and devices. Given the ubiquitous nature of IoT devices, it is seemingly inevitable that IoT would be used as a conduit to transform healthcare. One such medical IoT (mIoT) device that is revolutionizing healthcare is the medical implant device. These mIoT implant devices which control insulin pumps, cardioverter defibrillators and bone growth stimulators have redefined the way patient data is accessed, and healthcare is delivered. These implant devices are a double-edged sword. While they allow for the effective and efficient noninvasive treatment of patients, this external communication makes the medical implants vulnerable to cyberattacks synonymous with IoT devices. As a result, privacy and security vulnerabilities have surfaced as pronounced challenges for mIoT devices. This work summarizes and synthesizes the inherent vulnerabilities associated with mIoT devices and the implications regarding patient safety.

1. Introduction

Internet of things (IoT) is loosely defined as the communication between interconnected sensors and devices designed to utilize the internet for the collection, analyzation, and exchange of data. Keeping with the current trajectory, it is inevitable that IoT will give us the ability to collect and analyze data related to nearly every facet of our lives [1]. IoT is one of the driving factors that is fueling a new era of medical diagnosis and intervention [2, 3]. One such IoT device that is revolutionizing healthcare is the medical implant device. For instance, these devices control insulin pumps that allow for the administration of medication, cardioverter defibrillators that treat patients who show signs of cardiac arrest, and implantable bone growth stimulators [4-6]. Leading factors driving the medical implant market include the aging population, technological advances, increased knowledge of medical implant technology, and an increase in degeneration medical conditions [6]. Responses to a recent trade journal survey show cardiovascular and orthopedic medical implant devices are believed to account for more than half of the medical implant devices projected to make the most impact in fighting disease and improving patient care [6]. While medical Internet of Things (mIoT) devices such as medical implants have the propensity to advance healthcare, they also present unparalleled security challenges [7].

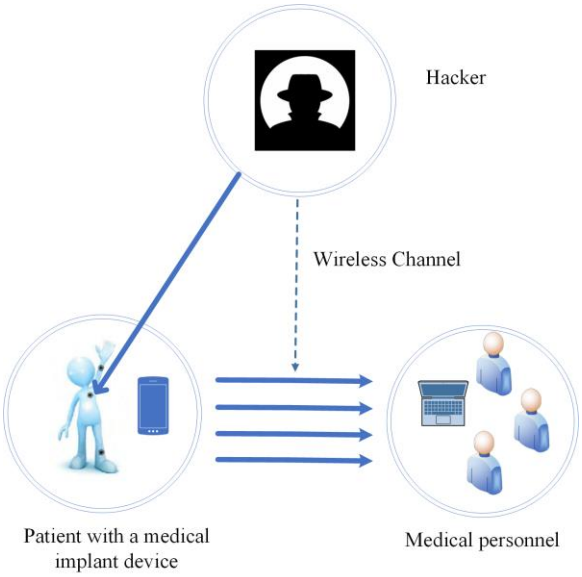

Figure 1. Generic Medical Implant Device Threat Model

Implant devices are a double-edged sword. Medical implants allow for the transmission of medical data to physicians and medical facilities.

URI: https://hdl.handle.net/10125/71082
978-0-9981331-4-0

These devices allow doctors to perform advance medical procedures, such as modifying the implant device without invasive surgical procedures. They also allow for the near real time transmission of the patient's physiological data in treatment centers such as the ICU as well as remotely. Although the benefits these devices yield to patients are numerous, they also expose patients to cyberattacks [8]. It is the communication with systems outside of the patient's body that make medical implants vulnerable to potential attacks [9]. While cyberattacks are common and seemingly expected in network-connected devices, their results, when applied to medical implants, could be life-threatening and lead to a loss of privacy [10]. As shown in Figure 1, a hacker can attack the implantable medical device or the wireless channel between the patient and medical personnel. Hacking medical devices is not uncommon and has been going on for over a decade. Reasons for hacking a medical device include hacktivism, financial motives such as extortion, and political [11, 12]. In 2018, NHS systems, a pacemaker manufacturer, was breached by a ransomware attack designed with the intention to extort money from the company [13]. While there are no published cases of physical harm or loss of privacy to medical implant device patients, the potentially fatal harm that could result from a cyberattack is cause enough for concern.

While a device's security requirements should reflect the risk associated with the device, this is rarely the case. While security is often a reactionary environment in practically every technological environment, security is rarely a design goal in the medical implants industry [9, 14]. Implementing adequate security begins during the foundational development phases when choices like which operating system to use are made [15]. There seemingly exists a gap in the security safeguards being implemented in the medical device industry and other industries with high-security levels already in place [16]. Given the importance of these devices, they are a logical target for cyberattacks. As the importance of these devices continues to rise, so will the level of threats against these devices. However, there seems to be an inverse relationship between threat levels and preventative measures. Hackers are seemingly outpacing manufacturers, leaving providers at a disadvantage concerning security vulnerabilities [17].

There are several challenges to securing medical implant devices. Synonymously with other IoT devices, medical implant devices have very little computing power and memory. These limitations severely hinder the ability of manufacturers to secure these devices [18]. The limitation on battery size also places constraints on security measures that can be implemented. Measures such as encryption are constrained because of the strain they will place on the battery [19]. This poses severe authentication challenges for manufacturers. Furthermore, while system updates are non-invasive, performing some secure system updates can be cumbersome. These updates often require patients to make appointments in order for implants to receive security updates [9].

While medical implant manufacturers struggle to design devices hardened enough to prevent cyberattacks, the Food and Drug Administration (FDA) has failed to produce regulations regarding the safeguards such as security updates that need to be in place [20, 21]. Instead of regulations, the FDA has issued pre and post guidance that focuses more on labeling and documentation to inform patients of cybersecurity issues and encouraging manufacturers to address cybersecurity issues throughout the life of the product rather than on providing technological guidelines to address requirements [22, 23]. Questions also exist as to whether device manufacturers and cloud service providers who collect protected health information on their own and not as associated with entities that are covered by HIPAA are also covered by HIPAA [24].

2. Study Review Process

The objective of this review attempts to survey and summarize the current threat and vulnerability landscape that is faced by health practitioners, medical organizations, and hospitals that use medical IoT devices and manage healthcare-related information on their networks, what academic research has been published, and what attention has been brought to the potential problem. The information from this work is derived from scientific databases and relevant industry documents and publications. The most appropriate documents related to medically implanted IoT devices were selected. Through dependable sources such as IEEE (Institute of Electrical and Economics Engineers), Scopus, Sage Journals, Science Direct, the authors have access to a large number of academic articles as well as industry analysis. These databases were selected from technical and medical literature. The search was limited to peer reviewed journals and conference articles from the last five years. Publications such as books and book chapters were not given consideration. The author used the query "('internet of things' OR 'medical internet of things') AND ('security' OR 'privacy') AND ('healthcare' OR 'mhealth' OR 'm-health' OR 'medicine')". The documents that were analyzed are detailed in Table 1.

Table 1. Articles analyzed in this study

Title	Description of Contribution
[25]	The authors focus on a case example of an implanted medical device cybersecurity threat. The actions taken by stakeholders is outlined and a summary of the position of societies in response to the events is given.
[26]	A framework, based on international common criteria, for fostering security in wireless health devices. The authors aspire to provide a way forward that stimulates security, public trust, and confidence.
[11]	Explores the possible risks of hacking for patients using cardiac implant devices and outline what can be done by multiple stakeholders to improve cybersecurity.
[13]	This study seeks to determine whether or not it is feasible to hack NHS pacemakers. Experiments in this study were performed from the perspective of an average hacker, not of one with intimate knowledge of how to hack a pacemaker.
[27]	The authors seek to develop a new protocol to facilitate wireless communication between implantable medical devices and remote controls that are used to control minor day to day operations.
[12]	Investigates the role of IoT in healthcare by exploring security and vulnerability issues, attacks, and solutions.
[28]	Examines the challenges and requirements of designing authentication protocols to secure the wireless transmission of sensitive data from implantable medical devices.
[29]	Reviews the regulatory frameworks addressing medical devices in the US, Europe, Canada, and Taiwan. The work also examines the status of reaching a global consensus on regulating medical devices.
[30]	The goal of this work is to increase awareness related to the security of medical IoT devices by identifying exploits and evaluating their impacts against a pacemaker automatic remote monitoring system (PARMS).
[31]	Examines and summarizes the literature related to using IoT based principles in implantable medical devices.
[32]	This document assists scholars and practitioners in communicating the extent and scope of the risks of cybersecurity and in advancing education and research in the medical IoT field.
[33]	The authors analyze multiple scenarios in order to understand the actual consequences of IoT based healthcare applications.
[34]	This article discusses the background and issues of possible attack vectors that are likely to be hacked and provides protection strategies that can be implemented.
[35]	Illustrates the measures healthcare organizations can implement until FDA regulations are established to safeguard patient safety.
[36]	Addresses authentication limitations by proposing an energy-aware signature that is appropriate for embedded medical devices with limited resources.
[37]	Relevant information regarding the security of brain implants is addressed, several mechanisms that can be utilized by hackers to gain unauthorized access are identified, and limitations rooted in IoT devices are discussed.
[38]	Reviews the existing threats of cybersecurity risks in implantable medical devices and proposed technical solutions.
[39]	This review article focuses on the challenges, threats, and solutions related to privacy and safety matters related to implantable medical devices.
[40]	This work introduces the problems associated with designing implantable medical devices with cybersecurity as a significant part of the design goal.
[41]	Examines the cybersecurity vulnerabilities associated with implanted medical devices and argues they are a national security risk which needs a joint effort between the government and private sector to protect patient safety.
[42]	Implements a low cost, energy efficient IoT medical system.
[43]	Current implantable medical device vulnerabilities are discussed. Security tests and demonstrations completed by researchers are presented.

3. Study results

As healthcare continues to increasingly utilize digital communication measures such as the internet and wireless communication, it will increasingly become more and more susceptible to cyberattacks.

Risks to healthcare from unintentional threats have long been known, but more recently, risks from intentional threats have been confirmed [21]. Due to the nature of these devices, security issues should also be considered safety issues to patients. Implanted medical devices not only capture and transmit physiological data to medical decision-makers, but they also perform tasks designed to regulate organs. Implanted medical devices that have been compromised can cause harm to a patient or even perform actions that are potentially profound.

3.1. Known cybersecurity vulnerabilities acknowledged by the governing authority

The U.S. Food and Drug Administration (FDA) is the federal agency that is responsible for protecting the public's health. As related to this study, the FDA is tasked with ensuring the safety, efficacy, and security of medical devices used by patients. The FDA has acknowledged that while the digital communication features present in medical devices increase the ability of medical providers to treat their patients, they also increase the risk of cybersecurity threats [22, 23]. As medical devices are being connected to the internet, medical facilities, and other medical devices, manufacturers must remain diligent about protecting their customer's health. Manufacturers and healthcare providers must remain diligent about implementing the recommendations to remediate the vulnerabilities that have been reported by the FDA so that the safety of patients is ensured (Table 2). As of yet, the FDA is not aware of any patient injury or death that is associated with a medical implant device cybersecurity incident [25]. However, it has been noted that devices are not checked for tampering following the death of a patient [13] .

Table 2. Known medical device cybersecurity vulnerabilities

Vulnerability and Description	Date Issued
SweynTooth: Bluetooth Low Energy exploit to crash, deadlock, or bypass security on devices [44]	3/3/2020
URGENT/11: Allow an attacker to remotely take control of a medical device and change its function [45]	10/1/2019
Medtronic MiniMed: Potential cybersecurity risks in Medtronic MiniMed insulin pumps [46]	6/27/2019
Medtronic ICDs or CRT-D: Cybersecurity vulnerability in wireless technology used to communicate between Medtronic's implantable cardiac devices and home monitors [47]	3/21/2019
St. Jude's Medical implantable cardiac devices and Merlin@home Transmitter: these cardiac devices contain devices that are vulnerable to cybersecurity intrusions and exploits [48]	1/9/2017
Hospira infusion pump system: these systems that continuously deliver anesthetic or therapeutic drugs can be programmed remotely through a healthcare providers LAN [49]	5/13/2015

The National Institute of Standards and Technology (NIST) has release documentation designed to assist medical providers with securing their devices on an enterprise level network. SP 1800-8 focuses on wireless infusion pumps and lists the multiple security guidelines designed to help secure these devices [50]. While written specifically for wireless infusion pumps, the guidelines are applicable throughout the entire medical implant device ecosystem. However, absent from the document are the specifications and security standards necessary to meet these security assurances.

3.2. Medical Implantable Devices and Cyberattacks

Figure 2 illustrates the medical implantable devices and cyberattacks landscape. The integration of IoT into healthcare has brought tremendous advances in patient treatment options. The interconnectivity of the devices provides for remote monitoring by healthcare providers and wireless communication. This interconnectivity also introduces a portal by which cyberattacks can occur.

3.2.1. Cardiac devices

One area that has seen a significant amount of research is that of implanted cardiac devices. Multiple cardiac device exploits are being researched:

In battery drain attacks, attackers seek to suddenly deplete the battery of the implanted medical device [11, 25]. Researchers are currently working on implementing an energy-efficient, low power solution

for IoT ECG monitoring devices that don't compromise performance [42]. Wirelessly recharging batteries have been proposed to alleviate the battery constraints, currently limiting security measures [40]. However, this is a novel idea that requires more experiments.

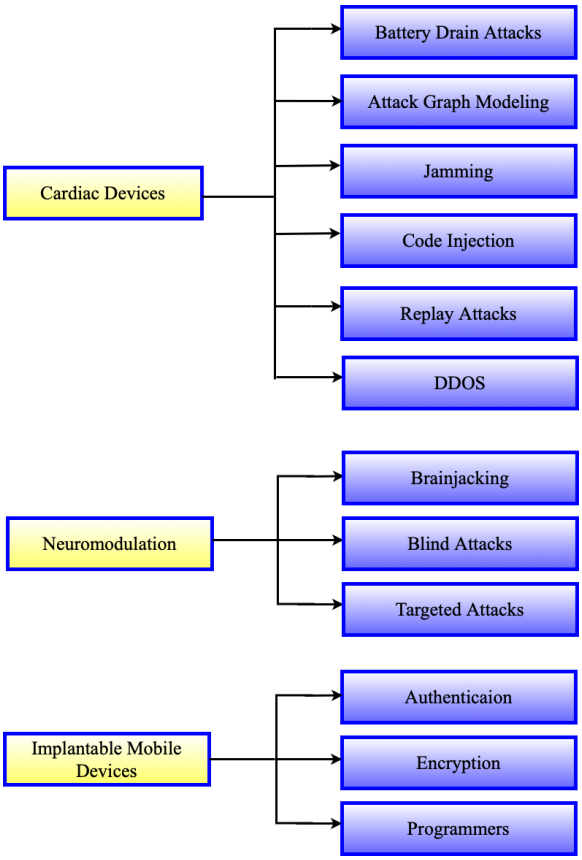

Figure 2. Medical Implantable Devices and Cyberattack Landscape

Attack Graph Modeling is an attack graph visualizing the cybersecurity risks of remote health monitoring systems communicating with implantable devices [30]. The experiment showed that pacemaker automatic remote monitoring systems are prone to cyberattacks and require security measures to protect the patient's data.

Only the communication module was affected by signal jamming. The device did not exhibit any strange behavior, but if jamming was performed during the update session, the update data could be corrupted [13].

Code injection attempts proved to be unsuccessful. This was attributed to the medical device utilizing some form of a checksum [13].

Replay attacks attempting to transfer a data packet from one pacemaker to another subsequently failed [13].

Implantable medical devices like pacemakers not only send data but receive data also. This allows hackers to target these medical devices, leaving patients vulnerable to Distributed denial of service (DDoS) attacks [12].

3.2.2. Neuromodulation

Brainjacking refers to the unsanctioned control of a medically implanted brain implant. There are multiple options for hackers implementing a brainjacking attack [37]:

Blind attacks do not require the attacker to have any knowledge about the patient. Blind attacks include cessation of therapy, battery drainage, administering the overcharge of stimulation, and stealing patient data by eavesdropping.

Targeted attacks require personal knowledge about the patient. Targeted attacks include the modification of stimulation, impeding motor function, inducing pain, altering impulse control, and modifying emotion and alertness.

3.2.3. Implantable mobile devices

Zheng et al. found the following vulnerabilities in pacemakers, IMDs, and insulin pump systems [43]:

Doctors can gain access to an implantable mobile device without being required to authenticate as long as they have the same manufacturer and are the same model as a device for which they have a programmer.

Communication between the programmer and implantable mobile device is not encrypted or is encrypted with a static key. The information related to the static key is stored in the implantable mobile device and can be retrieved at the beginning of the session.

Off the shelf programmers that can be used to access implantable mobile devices.

3.3. Security and attacks

Figure 3 illustrates the security and attacks vulnerability landscape. Currently there are no standards governing security in medical devices. The current lack of security standards not only impacts patients but other stakeholders as well [13]. Government regulations for security, such as HIPAA, the FDA, and NIST, offer guidance instead of actual regulations. Guidance instead of regulation can offer patients using devices that have the approval of these agencies a false sense of security [26]. Security standards should be created through collaborative work between experts from different fields that represent the stakeholders involved [31]. Recommendations from the private sector to realize a national security standard include a national system designed to share information related to medical device cybersecurity [41]. In order to understand the specific security requirements that are needed, a system-wide view of the security issues must be assessed [33]. The FDA has recently begun to initiate an action plan designed to move towards a more security-based approach to the design of medical devices [29, 35]. While these are not regulations, this is a step in the right direction.

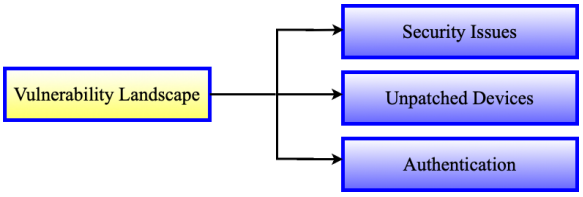

Figure 3. Vulnerability Landscape

3.3.1. Security issues

Multiple issues exist with medical devices. These devices are often omitted from routine scans for IT equipment, causing them to be omitted from software updates and patches. This exacerbates vulnerabilities on the medical facility's network because of the difficulty patching [39].

3.3.2. Unpatched Devices

When reviewing the high-profile St. Jude Medical (currently Abbott) case, Alexander et al. found that although the firmware update was non-invasive and was completed in approximately three minutes, the majority of patients with Abbott pacemakers elected not to receive the update designed to correct the known cybersecurity vulnerability [25]. Factors that may have led to a decreased update rate include possible complications resulting from the update and the life expectancy of the device. The FDA reported that of the devices were updated, 0.62% experienced issues with the update process that required resolving, and 0.14% of the patients experienced stimulations or discomfort during the update process. The age demographic that was more likely to update were younger males with relatively new pacemakers. The age of the pacemaker is a determining factor when deciding to complete firmware because the life expectancy of the device is five to ten years. Patients with older devices had smaller windows in which the vulnerabilities were a threat. Although the "crash attack" and "battery drain attack" were performed on Abbott's pacemaker, these cybersecurity risks extend to other medical devices that connect to the internet to facilitate remote monitoring and programming. A study conducted by Jackson et al. [32] found there to be a breakdown between information about vulnerabilities being relayed to patients. A step towards securing devices and protecting patients is to overcome the culture of non-communication that seems to exist between the multiple stakeholders.

3.3.3. Authentication

While the report detailing Abbott's vulnerability lacked details, it did explicitly mention the use of unauthenticated wireless communication [34]. An analysis conducted by Challa et al. [28] found that for implantable medical devices to function properly, authentication protocols must be designed to be lightweight with minimum processing requirements. When analyzing the wireless communication scheme utilized between an implantable medical device and the remote control used for daily non-critical functions, Belkhoja et al. [27] realized the lack of proper authentication measures. An authentication protocol that relies on plain text messages was proposed in order to avoid high computational costs, such as those common with encryption. Ozmen et al. [36] proposed a low energy digital signature designed for authenticating implanted medical devices. By not using the ephemeral public key in Schnorr-type signatures, and instead using a constant-size public key, they were able to secure an 8-bit AVR microcontroller. The implementation of multi-factor authentication has also been proposed to alleviate implantable medical device security issues [38]. This is considered an easy implementation being that biometric information from the patient can be used.

4. Security Requirements Needed for Medical Implant Devices

The dynamic access permissions needed in the implantable medical device ecosystem require security solutions to be scalable and robust. The integrity and confidentiality of patient data and patient safety lie at the core of the security requirements of medical implantable devices. Patient privacy and safety must be preserved while data transfers to medical personnel remain easy to manage [51]. Data transfers should be encrypted from end to end during the transfer of configurations, commands, and private health data [52].

5. Future Research Directions

Conflicting recommendations currently exist regarding updating medical implant devices. Factors such as the age of the patient are often considered when determining whether to recommend a firmware upgrade. While the FDA has taken a firm stance on firmware upgrades on some implantable devices, such as pacemakers, manufacturers are taking a more lax approach and recommend considering more patient specific details such as the age of the device, the level of dependence on the pacemaker, and patient preference be considered before mandating a firmware upgrade [25]. Governing agencies have directed manufacturers in the right direction, but they have failed to properly define the standards and goals required to ensure the level of assurance that should be maintained for such life sustaining devices.

Also absent from the literature and governing agencies is a method by which to evaluate medical implantable devices. There is no certification in place to assure the safety of these devices. As a way forward, standards and certifications based on rigorous security testing will help establish and quantify the level of assurance required for these life saving devices.

Given the push to allow patients to play a decisive role in the firmware update process, patient education is of the upmost importance. Patients need to be made aware of the security issues and threats associated with medical implant devices so they can make informed decisions and hopefully be more proactive in keeping devices updated and secure. With the lack of regulations in place, patients must be armed with the power to make better decisions concerning the firmware and security risks associated with their device.

6. Conclusion

In this paper we reviewed the current threat and vulnerability landscape being faced by stakeholders that use medical implant devices. Medical implant devices are revolutionizing healthcare. These devices allow for remote monitoring, and some administer therapy as needed. By using the Internet to facilitate communication between mIoT sensors and devices, medical practitioners are exposing their patients to vulnerabilities shared with IoT devices. The external communication used to control and receive data from these devices makes the medical implants vulnerable to cyberattacks.

As a result, privacy and security vulnerabilities have surfaced as pronounced challenges for mIoT device. While the benefits of mIoT devices are bountiful, we have reached a pivotal moment where the continued use of these devices requires the remediation of security vulnerabilities. While guidance is being provided by government agencies such as the FDA, regulations formed by a joint effort between stakeholders is needed. While no patient injuries resulting from cyberattacks have been noted, the time to act is now while this is still the case.

References

1. van Oorschot, P.C. and S.W. Smith, *The Internet of Things: Security Challenges.* IEEE Security & Privacy, 2019. **17**(5): p. 7-9.
2. *Tech Focus: When Doctors Start Prescribing Electronics, What Would the Dosage Be.* Electronics For You, 2015.
3. Yeole, A.S. and D.R. Kalbande, *Use of Internet of Things (IoT) in Healthcare*, in *Proceedings of the ACM Symposium on Women in Research 2016 - WIR '16*. 2016. p. 71-76.
4. Dixon Jr. , H.B., *The wonderful and scary Internet of things!* Judges Journal, 2017. **56**: p. 36-38.
5. Hudson, F. and C. Clark, *Wearables and Medical Interoperability: The Evolving Frontier*, in *Computer*. 2018, IEEE. p. 86-90.
6. *MDT Survey: Implantables Playing Bigger Role in Medicine*. 2019.
7. Kalva, M., *Healthcare IoT will deliver great benefits; the challenge will be mastering IoT security.(HIPAA LIABILITIES)(Internet of Things)(Report).* Health Management Technology, 2016. **37**: p. 19.
8. Nausheen, F. and S.H. Begum, *Healthcare IoT: Benefits, vulnerabilities and solutions*, in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. 2018. p. 517-522.
9. Best, J., *Could implanted medical devices be hacked?* BMJ, 2020. **368**: p. m102.
10. Williams, P.A. and A.J. Woodward, *Cybersecurity vulnerabilities in medical devices: a complex*

environment and multifaceted problem. Med Devices (Auckl), 2015. **8**: p. 305-16.
11. Baranchuk, A., et al., *Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?* J Am Coll Cardiol, 2018. **71**(11): p. 1284-1288.
12. Chacko, A. and T. Hayajneh, *Security and Privacy Issues with IoT in Healthcare.* EAI Endorsed Transactions on Pervasive Health and Technology, 2018. **0**(0).
13. Beavers, J.L., M. Faulks, and J. Marchang, *Hacking NHS Pacemakers: A Feasibility Study*, in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. 2019. p. 206-212.
14. Montalbano, E., *Medical device makers challenged to provide better security to meet increased risks of connectivity.(Medical).* Design News, 2015. **70**(12).
15. Haile, A. *Security & IoT Medical Device Design: Avoiding Disastrous Hacks*. 2017 March 30, 2017; Available from: http://search.proquest.com/docview/1882295442/.
16. Lecklider, T. *Mitigating Medical Device Risk*. 2016 21 Dec. 2016 March 3, 2020]; Available from: www.evaluationengineering.com/test-issues-techniques/cybersecurity/article/13014905/mitigating-medical-device-risk.
17. *FORTIFIED HEALTH SECURITY EARNS TOP RANKING AS A CYBERSECURITY SOLUTIONS PROVIDER FOR MEDICAL DEVICE AND IOT BY BLACK BOOK RESEARCH*, in *PR Newswire*. 2018.
18. vitić, I., M. Vujić, and S.a. Husnjak, *Classification of Security Risks in the Iot Environment.* Annals of DAAAM & Proceedings, 2015. **26**: p. 0731–0740.
19. Mohan, A., *Cyber Security for Personal Medical Devices Internet of Things*, in *2014 IEEE International Conference on Distributed Computing in Sensor Systems*. 2014. p. 372-374.
20. Mikaela, N., et al., *Risk Assessment of Cyber Attacks on Telemetry Enabled Cardiac Implantable Electronic Devices (CIED).* 2019.
21. Sametinger, J., et al., *Security challenges for medical devices.* Communications of the ACM, 2015. **58**(4): p. 74-82.
22. Administration, U.S.F.a.D. *Cybersecurity*. 2020 March 3, 2020 [cited 2020 March 5, 2020]; Available from: www.fda.gov/medical-devices/digital-health/cybersecurity.
23. Landi, H., *Medical devices are the new threat landscape: experts agree: healthcare organizations need to address the security of medical devices and IoT before it becomes a life-and-death issue.* Healthcare Informatics, 2017. **34**(2): p. 22-24.
24. Rasch, M., *PRIVACY AND SECURITY IN THE INTERNET-CONNECTED WORLD OF PRECISION MEDICINE.* Scitech Lawyer, 2018. **15**: p. 18-39.
25. Alexander, B., S. Haseeb, and A. Baranchuk, *Are implanted electronic devices hackable?* Trends Cardiovasc Med, 2019. **29**(8): p. 476-480.
26. Armstrong, D.G., et al., *Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of "Medjacking".* J Diabetes Sci Technol, 2015. **10**(2): p. 435-8.
27. Belkhouja, T., et al., *New Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control*, in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. 2017. p. 1-5.
28. Challa, S., et al., *Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions.* IEEE Consumer Electronics Magazine, 2018. **7**(1): p. 57-65.
29. Chen, Y.J., et al., *A Comparative Study of Medical Device Regulations:: US, Europe, Canada, and Taiwan.* Ther Innov Regul Sci, 2018. **52**(1): p. 62-69.
30. Ibrahim, M., A. Alsheikh, and A. Matar, *Attack Graph Modeling for Implantable Pacemaker*. Biosensors (Basel), 2020. **10**(2).
31. Isler, Y., L.T. Olcuoglu, and M. Yeniad, *Data Security and Privacy Issues of Implantable Medical Devices.* Natural and Engineering Sciences, 2018.
32. W. Jackson, G. and S. S. M. Rahman, *Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications Related to the Medical Internet of Things (MIOT).* International Journal of Network Security & Its Applications, 2019. **11**(4): p. 75-86.
33. Jaigirdar, F.T., C. Rudolph, and C. Bain, *Can I Trust the Data I See?*, in *Proceedings of the Australasian Computer Science Week Multiconference on - ACSW 2019*. 2019. p. 1-10.
34. Khera, M., *Think Like a Hacker.* J Diabetes Sci Technol, 2017. **11**(2): p. 207-212.
35. Martinez, J.B., *Medical Device Security in the IoT Age*, in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. 2018. p. 128-134.
36. Ozmen, M.O., A.A. Yavuz, and R. Behnia, *Energy-Aware Digital Signatures for Embedded Medical Devices*, in *2019 IEEE Conference on Communications and Network Security (CNS)*. 2019. p. 55-63.
37. Pycroft, L., et al., *Brainjacking: Implant Security Issues in Invasive Neuromodulation.* World Neurosurg, 2016. **92**: p. 454-462.
38. Pycroft, L. and T.Z. Aziz, *Security of implantable medical devices with wireless connections: The dangers of cyber-attacks.* Expert Rev Med Devices, 2018. **15**(6): p. 403-406.
39. Rathore, H., et al., *A review of security challenges, attacks and resolutions for wireless medical devices*, in *2017 13th International Wireless*

Communications and Mobile Computing Conference (IWCMC). 2017. p. 1495-1501.
40. Tabasum, A., et al., *Cybersecurity Issues in Implanted Medical Devices*, in *2018 International Conference on Computer and Applications (ICCA)*. 2018. p. 1-9.
41. Woods, M., *Cardiac defibrillators need to have a bulletproof vest: the national security risk posed by the lack of cybersecurity in implantable medical devices.(Regulating Innovation in Healthcare: Protecting the Public or Stifling Progress?)*. Nova Law Review, 2017. **41**(3): p. 419-447.
42. Zagan, I., et al., *Healthcare IoT m-GreenCARDIO Remote Cardiac Monitoring System - Concept, Theory of Operation and Implementation.* Advances in Electrical and Computer Engineering, 2017. **17**(2): p. 23-30.
43. Zheng, G., et al., *From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices*, in *2017 17th International Symposium on Communications and Information Technologies (ISCIT)*. 2017. p. 1-5.
44. Administration, U.S.F.a.D. *SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication*. 2020 03/03/2020 [cited 2020 3/10/2020]; Available from: https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication.
45. Administration, U.S.F.a.D. *URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication*. 2019 10/01/2019 [cited 2020 03/10/2020]; Available from: https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce.
46. Administration, U.S.F.a.D. *Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication*. 2019 09/09/2019 [cited 2020 3/10/2020]; Available from: https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication.
47. Administration, U.S.F.a.D. *Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication*. 2019 01/30/2020 03/10/2020]; Available from: https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home.
48. Administration, U.S.F.a.D. *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication*. 2017 [cited 2020 03/10/2020]; Available from: https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-identified-st-jude-medicals-implantable-cardiac-devices-and-merlinhome.
49. Administration, U.S.F.a.D. *LifeCare PCA3 and PCA5 Infusion Pump Systems by Hospira: FDA Safety Communication - Security Vulnerabilities*. 2015 [cited 2020 3/10/1020]; Available from: https://wayback.archive-it.org/7993/20170112164109/http:/www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm446828.htm.
50. O'Brien, G., et al., *Securing Wireles Infusion Pumps in Healthcare Delivery Organizations.* 2018.
51. Pham, H.L., T.H. Tran, and Y. Nakashima, *A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract.* 2018 IEEE Globecom Workshops (GC Wkshps), 2018: p. 1-6.
52. Strielkina, A., et al., *Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment.* 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018: p. 67-73.