Risk Mitigation of Cyber Attack on Medical Devices

Daniel Turner
SMU, Data Science
Dallas, TX USA

Ravi Sivaraman
SMU, Data Science
Dallas, TX USA

Apurv Mittal
SMU, Data Science
Dallas, TX USA

***Abstract*—This paper explores the risk of cyberattack on remote medical devices and potential mitigation techniques can be used to prevent loss of human lives. Cyberattacks on medical device and hospitals have been a regular occurrence in the past few years. The healthcare industry is under attack with ever more data breaches. Over one million patient records are stolen per month as measured in 2020. It's estimated to increase as more medical devices are going wireless. Patient managed medical devices like pacemakers and insulin pumps are in danger of cyberattacks and have proven to be vulnerable. Medical devices can be attacked by deactivation or malfunction, interruption, or contamination of data. We recommend immediate steps and future research needed to secure Medical Devices against cyber-attacks.**

I. Introduction

Medicine is of prime importance to society and the field is under constant attack. It has been estimated that, worldwide, cyber crime will cause 6 trillion US dollars a year as of 2021 [1].

Many patients have had medical needs that require devices maintained and operated by the private individual, away from the medical facility. Prominent in this population are the pacemaker and the insulin pump. With developing technologies and infrastructure, there is increasing use of smart systems. This enhances utility for both patient and medical staff.

Since the onset of the COVID-19 epidemic, there has been an elevated use of remote medicine. This is true for both patient-clinician interfaces, as well as patient operated devices. The difficulties of the pandemic have made remote medicine, or telehealth, a requirement to maintain therapeutic interactions without breaking quarantines or physical distancing guidelines. The increase of general telehealth usage is partly a result of relaxed regulation during an emergency. It is expected to continue, albeit at a reduced rate, when the situation has stabilized. This still means an expected distribution of clinical tools and technologies in the hands of the wider population. Any future medical device, or assisting device, is expected to populate the Internet of Things, or IoT. This is a serious potential security hazard.

FDA groups medical devices into three classes based on the risk and the ability to ensure safety and effectiveness of the device. Pacemakers, insulin pumps are considered Class III devices as they are high risk and crucial to maintain health and sustain life [2].

The Federal Bureau of Investigation (FBI) warned in 2015 that IoT devices which includes medical devices as well, IoMT (Internet of Medical Things) are at risk of cyber crimes due to existing vulnerabilities in the devices [3]. This is mostly due to the fact that the vulnerabilities are not routinely patched and the outdated devices are still in use. The health industry has been the most impacted by the cyber-attacks in the recent years. The fact that an attack on a medical institution or device has direct impact on the health of the patient makes it even more severe. MEDJACK 2, an analysis report of malware used to attack IoMT systems, showed how attacks can be successfully implemented in IoMT environments to steal medical data and instantiate ransomware attacks [4]. Every year 6.7 million people receive implantable medical devices in the USA [5], with growing demand and popularity of the IoMT devices the cyber risk is also growing [6] [7]. In the case of mass attack more and more people are at risk.

IoMT devices like insulin pumps are increasingly common as part of artificial pancreas project. It generally comprises of two independent components, the continuous glucose monitoring system and insulin pump. These devices may be able to talk to each other directly, or may connect through smartphones. They are capable of transmitting both data (like blood glucose levels) and the insulin pump commands. Data can be exchanged in clear text allowing easy observation [8]. Devices may have small power requirements which have challenges on having a more advanced chip for encryption. Insulin pumps hacking is bound to stay until this is fixed.

The main ideas of this paper are a Low Power Encryption to reduce the chances of battery drain attacks, Asymmetric redundancy of chips for damage mitigation, secure software updates to prevent malicious updates. The approaches can help prevent cyber attacks, mitigate the damage and eventually recovery of the IoMT devices if attacked.

In addition, this paper raises the necessity of managing the threat of nation state attack. Cyber security should be scalable to a wide variety of threats. It is well to include defense measures that can limit the damage from a large and motivated adversary [9].

The remainder of this paper is organized as follows: In Section II, we present threat estimation of potential cyberattack on remote medical devices. In Section III, we discuss about the IoMT devices and the vulnerabilities. In Section IV, we cover the Cyber Kill Chain principles, In Section V we discuss the preventive techniques for cyber-attacks on IoMT devices. In Section VI we present mitigation techniques in the event of cyberattack. In Section VII, we present Recovery of medical devices post cyberattack. In Section VIII, relevant conclusions and identify future areas of research.

II. Threat Estimates

As technology proliferates, so too will cyber crime. This is true for medical technology as well. Too often, security measures are included as an afterthought or not at all. Security measures should be included into product design from the outset. This can reduce the cost of producing a secure system as well as allow tighter security. The question here should be one of budget allotment. The damages of cyber attack are already in the trillions. A portion of that can be justifiably allotted to reduce damage. How much is to be determined by the developer and/or manufacturer.

Questions the developer should ask:

"If this system is deployed, how many people are affected?"

"If this system is compromised, how many people are harmed?"

"How many excess incidents can medical infrastructure handle?"

In August of 2016, Muddy Waters Research LLC. released a report stating that CIEDs (Cardiovascular Implantable Electronic Devices) manufactured by St. Jude Medical (now Abbott) were at high risk of device hacking [10]. The report in particular pointed out two main possible attacks on these medical devices: a "crash attack" leading to high rate pacing, and a battery drain attack [11]. Additionally, there was a claim that radio frequency telemetry was rendered incapable of communication after bombardment with radio traffic.

The value of security can be measured by evaluating common threats as well as those of maximal damage potential. Hospitals are under attack and there are already developing trends. These are from non-state actors. As technology and methodologies develop, there are increasing cyber-threats to healthcare [12] [13] [14]. There are already news reports attributing deaths to cyber-attack [15]. There are real risks and real damage. An attack can be active, such as in a ransomware attack. An attack can be passive and done only to observe. Either are dangerous. Information gained by passive methods can be precursor to further attack. The threat posed by independent groups should not be minimized. They are still not as great as the threat posed by a hostile power.

Cyber attacks on medical institutions and devices are not victim-less crimes. Several people have lost their lives due to hospitals being under attack. A baby died due to a cyber-attack among other similar incidents [15] [16] [17].

There have been reports in the past that IoMT is not under a great threat of cyber-attack. As the technology proliferates this can change and these reports do not account for state level activities, particularly those conducted as auxiliary actions to armed conflict.

It is to be hoped that a foreign state will not attempt attacks on medical infrastructure. Whether one would do so is a question of risks and benefits. This is effectively in violation of international law [18]. Many military forces attack hospitals anyway. This is done under the guise of engaging enemies exploiting legal loopholes though such claims can be questionable [19]. Worse, a state may not care about international law and pursue any tactic for advantage. A foreign state that can hack into medical infrastructures has access to a great deal of information. An active attack that damages is not only harming patients but also stressing critical infrastructure. This can induce military redeployment in times of war but can also be used to weaken a nation during ostensible peacetime. Cyber weaknesses can provide the avenue of attack for such operations.

Since the onset of COVID-19, the U.S. Census Bureau has been gathering epidemic related data [20] [21]. In later surveys they included telehealth usage. By this data, approximately one in five Americans report to have been using telehealth. This means an unmitigated state level attack can affect one fifth of U.S. citizens at any given time. That equates to many tens of millions of potential victims. The COVID-19 outbreak stressed American health infrastructure to its limits. A malicious actor can cause even more strain on this infrastructure.

III. Vulnerabilities with IoMT

There are reasons for IoMT (Internet of Medical Things) to be at high risk of cyber-attacks. One being a large number of IoMT devices are outdated as they are designed to last several years. A pacemaker can last more than a decade and without any security upgrades. Compare that to any latest computer, we see security patches monthly if not more frequently. The fact that IoMT is capturing and transmitting sensitive patient details on a routine with minimal supervision makes them highly attractive target.

Another big reason for high risk is due the medical suppliers or the manufacturers of the device are not transparent about the security of their devices. It's been reported earlier that several IoMT devices still use default and hard-coded passwords. [5]

Medical devices are increasing reliant upon communicating wirelessly via radio frequencies or WiFi protocol to a remote monitoring site (server) which can be a medical clinic or a company collating data for the hospitals. Hackers can attempt to interrupt this wireless communication and it will not be detected by the system's in-built security mechanisms as it will not be directly on the device but on the communication channel. The attackers may be just passive listeners or can breach the communication and modify the information sent. In a pacing-dependent patient with an implantable cardioverter-defibrillator, over-sensing may inhibit pacing and reprogramming to correct the pacing which is typically used to maintain the heart functioning [22]. In addition, over-sensing may lead to life-threatening shocks [23]. If reprogramming was performed, disabling therapies (Anti tachycardia pacing and shocks) would result in no response from the device upon clinical life-threatening ventricular tachycardia [23].

A pacemaker is a path-breaking device with growing heart diseases, it has come out as a boon for patients which help them lead a longer life. A pacemaker is a device that produce electrical impulses which is delivered by electrodes to make the heart muscle chamber to pump blood by contracting. In doing so it replaces and synchronizes the function of electrical conduction system in the heart. A pacemaker is a small device which is positioned in the torso of the patient to assist abnormal rhythms on the heart. Pacemakers transmit electrical pulses to stimulate the beat of the heart at a regular rate to help patient suffering from arrhythmias [24]. Inability to communicate accurately with the device could have life-threatening impact on the patient. Sudden battery depletion remains a clinical concern in pacing-dependent patients due to the inability to deliver therapies during clinical life-threatening arrhythmia.

It's fairly easy to transmit a malware into a IoMT device such as pacemaker. It can be done in many ways, one being attacking the user at their home setting where they are connected to WiFi with inadequate network security.

Even though the updated to the pacemakers Over the Airwaves (OTA) is not a common practice, medical professionals can get the software updates for the devices from a USB device or can be down-loaded directly from the internet. Programmer a system which is used by the physician's office to connect to the CIEDs to update the firmware using RF telemetry or ICT. However, the RF transmission can be intercepted using a software-defined radio (SDR), and then sensitive data could be viewed or malware implanted into the device during firmware update [25]. Surprisingly, the programs are authentication controlled and anyone with physical access to the device can control it and use for connecting to the patient's CIED. Even so much that programs can be easily bought online on bidding sites like eBay [26].Moreover, pacemaker firmware updates are not cryptographically signed, so pushing custom firmware into a CIED is a theoretical possibility.

Even if the medical professional is not trying to update the firmware of the IoMT device, as a routine process of medical checkups they access the data on the pacemakers by physical connection. If the connecting device is compromised then it can infect the IoMT device as well during this process with malware. Considering a medical professional connecting several hundred patients devices over a month, the risk of infecting the IoMT devices with malware is very high.

As discussed earlier, a hacked pacemaker may lead to life-threatening shocks to the patient [23]. If reprogramming was performed, disabling therapies (Anti tachycardia pacing and shocks) would result in no response from the device upon clinical life-threatening ventricular tachycardia [23]. Inability to communicate accurately with the device to induce arrhythmia due to hacked communication channel or sudden depletion of the battery could have life-threatening impact on the patient.

In addition to the interruption to the mechanism of the pacemaker by overriding its ability to provide controlled life-saving shocks to the patient, another major concerns is the ability of DDoS (Distributed Denial of Service) Attack on the implanted device can lead to sudden battery depletion and will make the device unresponsive and will interfere with the devices ability to to deliver therapies during clinical life-threatening arrhythmia.

The above discussed vulnerabilities are not just limited to the pacemakers but they are applicable to any IoMT devices. For example: an Insulin pump hacked can lead to incorrect doses of insulin in the patient leading to the life-threatening situations.

IV. Hacking Framework

In this section, we review the process followed by hackers to get illegal access to the victims system and how it can be classified into risk management techniques to protect victims and potential victims in an event of an attack.

A. *Cyber Kill Chain*

Lockheed Martin has published a framework of how a cyber-attack or hacking activity initiates and achieve their intended target. This is a concept taken from the military principles which can be applied to the cyber warfare as well. They named the framework as Intrusion Kill Chain [27] [28]. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives. The reason it's called a chain is that any deficiency in any of the links in the process can disrupt the entire operation. This is where lies the opportunity for protect the target from an intended attack.

Cyber Kill Chain		
Step	Description	Protection
Reconnaissance	Research and identification of the target.	Prevent
Weaponization	Build software package required to hack.	Prevent
Delivery	Deliver the malware to the target.	Prevent
Exploitation	Exploiting vulnerabilities on the targeted system.	Mitigate
Installation	Installing malware on a system.	Mitigate
Command and Control	Allowing attacker access to the system.	Mitigate
Action on Objectives	Attacker to implement intended objective.	Recover

TABLE I. Cyber Kill Chain

The protection mechanism can be classified into three parts: Prevent, Mitigate and Recover. All these can apply to different parts of the chain and can help foil the attempt to hack an IoMT device. However, this approach can be used in any step, we are considering this from the perspective of hacking of medical devices.

Throughout this paper we have discussed the approaches that can be taken to disrupt this kill chain and protect the IoMT devices. We will classify the recommended approaches among prevent, mitigate and recover to understand what part of the kill chain will be broken and can be used for the protection of the IoMT devices.

V. Prevention Techniques

It is not possible to know the full threat landscape of IoT devices in the future. There are things that can be inferred. The more common they are, the more they will be targeted. The more they are unsecured, the more they will be targeted. The more valuable their exploitation, the more they will be targeted. Medical devices are inherently valuable just from utility. Device users are more exploitable due to device dependence. Device users are potentially more exploitable as they are often derived from inherently more vulnerable demographics. Standard security precautions apply.

The least expensive and most effective defensive measure is to prevent an attack outright. Automated attack denial, when effective, removes the expense of damage mitigation and correction. Any automatic function will also reduce the human workload. The greatest security vulnerability in the average system is the end user. Tele-health places devices into the hands of the end user. Security implementation should be made as easy as possible for lay users of tech. Clinical personnel need relevant security training as does the end user. The IoT system should be developed with considerations to security accessibility. Inaccessible security will not get used.

Devices need to be developed with security considerations included from the beginning. Retrofitting security measures onto an already developed product can be less effective and more expensive. Medical security has to protect the device user without in any way compromising medical utility. A medical device does not exist in isolation. Security measures must include external device interactions. Security measures must be a part of a security ecosystem. Failures of the ecosystem can compromise device security and vice versa.

A. Against Nation State Threats

Against a state level actor, further countermeasures should be considered. A state level attack can be conducted to observe, influence, and/or damage. No entity can be trusted. This precaution extends to friendly powers as well as hostile ones. A friendly entity may desire inappropriate access to a system. It should be understood that no countermeasure will stop a committed attack at these levels. Countermeasures should emphasize increasing the cost of such an attack as well as slowing progress for effective exterior actions.

First: Decentralize And maintain decentralization. Prevent single points of access or failure in medical infrastructures. A centralized and unified system is easier to attack. Divide and diversify medical systems such that they are not vulnerable to common attacks. There should be no point or terminal by which the entire infrastructure can be directly accessed.

Second: Diversify Multiple disparate systems and devises will fail separately. Even if an opposing nation chooses to engage all devices aggressively, the failures will be staggered and allow more time to mitigate and/or counter. This is for both software and hardware.A threat may exist in the specific chip-set of a device. The manufacturer can install a secret backdoor into a chip. If a device is functional from an equivalent chip from a competing manufacturer, the next device will not share this vulnerability. When viable, use different software or firmware packages in different devices. For security and efficiency reasons, it is best if the core system of an insulin pump does not match that of a pacemaker, even if they have the same user output interface.

Three: Trust No One A security hole from a well meaning ally is still a security hole. This ally can be an allied state, a local government or government agency, or even a medical administration. Disallow deliberate back-doors to security measures. Any deliberate backdoor is exploitable to negative outcomes. Security for the clinician and patient take priority. In medicine, the first principle is 'do no harm'.

Medical IoT security should be considered a matter of national security [29]. In general, this IoT should follow those practices that exist for military and defense networks.

B. Secure Updates

Updating the telehealth devices can be pose a security threat, if left open, anyone can hack the telehealth devices and update the software to remove any restrictions that are developed for this device. Any updates must be secure and must be done only from manufacturer of the devices. To securely update, we can use digital signatures to secure the update package. Every update from the manufacturer can only updated by the device if software updates can be first digitally signed using the private key of the manufacturer, and this can be validated using the public key of the manufacturer stored in the device. Thus any updates to the telehealth device can only be done if the digital signature of the update matches the private key (verified using the public key at telehealth device). This will stop any malicious updates to the telehealth and hijack them.

When checking the digital signatures, telehealth device must also check the the hash and validate the update has changed. This will protect the update changed on the fly, also with the digital signatures, will provide most secure updates.

C. Best Practices

Programmers (system) should have better security controls and users shouldn't be able to maintain weak or default passwords. In addition to that the access to the programmer should be controlled by the role and not one super user to have access to all the features. Updating the IoMT device, Controlling the features, Accessing the data on the device etc. should be controlled based on the role of the user. Having access control will provide better security of devices in long run.

Regular security updates to the IoMT similar to that of other devices like computers and mobile phones will help keeping the devices secured. Manufacturers should be able to patch any security vulnerabilities identified without needing the patient to go to the doctors office.

VI. Damage Mitigation

A medical IoT device is medical first and intelligent second. Any compromised system should be developed to elegantly fail into a minimally harmful state. It is better to lose information and/or digital utilities than to physically harm the patient. Basic physical utility should take priority over IoT conveniences.

A. Asymmetric Redundancy

It is common in many fields to deploy redundant systems. The use of digital redundancy has problems in the medical environment. First, expanding the chip-set can increase the size of a device. Medical devices should be minimally invasive and unobtrusive. Second, more chips require more power which may be at a premium. Third, an attack that will compromise one chip can be expected to compromise any similar chips. Any redundancies should be asymmetric. This defense can be likened to the spare tire on a car. The device can continue operation in a reduced but still useful state. The asymmetric backup chip should provide security against abnormal operations and notify the user in the event one is detected.

An asymmetric redundancy should be just functional enough. This can be incorporated to the algorithms to provide for more secure updates as an emergency fail-safe and assist in maintain low power consumption.

B. Low Power Encryption

Encryption using low power was always not efficient, as long keys are required to make the encryption effective, but that is not very power efficient. There are many GPU operations has to be done, which poses challenge for IoT or medical devices where running on low battery power. These continuous encryption may deplete the battery at much faster rate. To prevent spoofing, medical devices must use PKI, digital signatures, etc. which may be power intensive.

This poses a unique challenge as medical devices are getting more popular and the battery technology is increasing at faster level. Initially these devices ran with no security, and really open for hacking, but the ubiquitous smart phone is making these devices to be hacked more often. In some cases, they may be taken over by a cyberattack and may potentially disrupt a large number of population quickly. [30]

The low power encryption is getting more and more important and we need to find a way to securely communicate with the other devices or controller. We recommend to cut down the communications to just a few trusted devices. If more devices needed to be added then only a reset of the medical devices will make it to connect to another set.

The idea is to first exchange the private key thru RFID mechanism during close contact. Once they have exchanged public keys, device only communicates by encrypting with the public keys of each other. No other devices can (another than another smartphone or smart watch) communicate with the medical device and thus eliminate the need to trust external agents and handle the communications.

The data needs to be sent in batches to avoid continuous power drain, so the data is held locally and sent once every 30 minutes or every hour. If a synchronize is required if user needs to verify, then the device can synchronize by initiating a close contact thru RFID. This will save lot of power as the devices don't transmit data all the time.

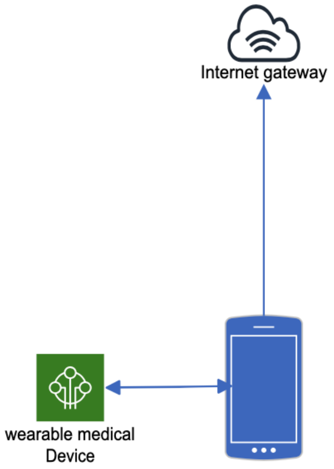

Fig. 1. Internet gateway for medical device only thru an attached smartphone

To eliminate the risk of losing data, the device must be able to store at least one day worth of data before discarding. This gives plenty of time for the smart phone to catch up and get updated. If the smart phone is not close by nor any power left in smartphone, there are plenty of time for smartphone to charge and get synchronized.

This method of communication will eliminate the need for the medical device to connect to insecure Internet network. The medical devices will always communicate to smart phones or smart watch only, and any further communication will need to happen in the app within smartphone. Eliminating the need of devices to be in the network reduces most of the risks, though not all.

Devices must reduce the amount of data that needs to be transmitted, and should use a strict encoding to cut down unnecessary data to reduce the encryption needs. The data must also be compressed before encryption to further reduce the encryption tasks and should transmit data only in batches of predetermined sizes.

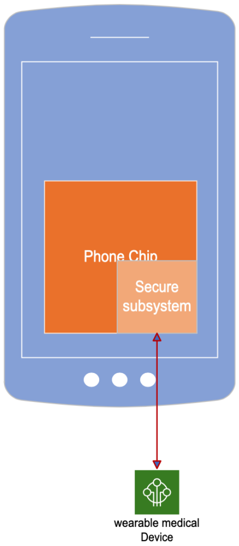

Fig. 2. Device communicating only to secure subsystem of smart phone chip

Devices that receive communications from smartphone must have more access to them, which will require the power requirements.

C. *Other Best Practices*

Network segmentation is an approach to isolate the networks into a smaller sub-networks to improve performance and security. Similar concept can be applicable in IoMT devices by segmenting the devices to their own sub-network which will help contain the security lapses or vulnerabilities if they happen. Keeping the damage in check and not allowing the attackers to get into the system and steal other information. Data captured through the IoMT should be kept separate from the actual device controlling module. Such that if medical professionals needs to access the data don't have to expose the other control mechanism of the device.

Alert mechanism is another important approach which all IoMT devices should have. They should be able to communicate and alert manufacturer, Medical Clinics, Physicians etc. in the even of an hack. [24]

VII. Recovery

The electronics of a medical IoT device will fail eventually even under ideal circumstances. The user should be warned before catastrophic failure. Device replacement needs to be an expected function of infrastructure. This must always be present as an ultimate fallback option to preserve the health of the patient.

A device that is compromised because specific components have failed or have been corrupted should be replaced if this is the easiest and fastest solution. Any software components the patient relies on should be easily transferable. Since the data or data chip may carry a virus or malware, only system configurations should be transferred via configuration synchronization. Superfluous data should not be transferred.

If a device is corrupted but without component damage, it should be easily re-settable. This is likely to be the most common correction to security concerns. The end user should have access to memory clear functions. In a more egregious situation, a user should be able to completely reset the device. Ideally, the patient or an assistant for a patient would have access to a factory default function. Resets should clear memory and all extraneous data.

VIII. Conclusions and Future Research

IoMT devices usage has grown rapidly, along with that the risk of device being hacked and risk the life of the patient. The security of these devices has not been the top priority of the manufacturers. Considering the potential impact of such attacks we recommended Low power encryption which enables the devices to stay connected to smart devices for longer period of times without frequent recharge which degrade battery performance, and strong encryption protects the devices from battery drain attacks (DoS attacks). Asymmetric redundancy can enhance device resilience against attack and failure. At least some token defensive measures should be considered to stymie large scale attacks such as what can be accomplished by national action.

Further research is required to validate the actual implementation of low power eruption and usability of the core functions of the IoMT devices. Best practices for redundant chips and functions should be a matter of continuous study and development. National defense provides an example of state information security but it should be adapted to medical IoT, not directly copied. Research will be required to optimize these translations.

References

[1] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic," *Journal of medical Internet research*, vol. 22, no. 9, p. e23692, 2020.

[2] N. D. Brantly, "Homefront to Battlefield: Why the U.S. Military Should Care About Biomedical Cybersecurity." in *The Cyber Defense Review, vol. 6, no. 2, Army Cyber Institute, 2021*. Army Cyber Institute, 2021, p. 93–110.

[3] Internet crime complaint center (ic3) — internet of things poses opportunities for cyber crime. [Online]. Available: https://www.ic3.gov/Media/PDF/Y2015/PSA150910.pdf

[4] M. smith, medjack 2: Old malware used in new medical device hijacking attacks to breach hospitals. [Online]. Available: tinyurl.com/2zhtxan3

[5] G. Hempel, D. B. Janosek, and D. B. Raziano, "Hacking humans: A case study and analysis of vulnerabilities in the advancing medical device landscape," *Cyber Security: A Peer-Reviewed Journal*, vol. 3, no. 4, pp. 351–362, 2020.

[6] J. J. Martin, "Hacks dangerous to human life," *Columbia Law Review*, vol. 121, no. 1, pp. 119–158, 2021.

[7] O. Dyer, "Abbott laboratories offers fix for 745 000 pacemakers vulnerable to hacking," 2017.

[8] C. Li, A. Raghunathan, and N. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, pp. 150–156, 2011.

[9] J. Adams, "Virtual defense," *Foreign Affairs*, pp. 98–112, 2001.

[10] B. Ransford, D. B. Kramer, D. Foo Kune, J. Auto de Medeiros, C. Yan, W. Xu, T. Crawford, and K. Fu, "Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists," *Pacing and Clinical Electrophysiology*, vol. 40, no. 8, pp. 913–917, 2017.

[11] B. Alexander, S. Haseeb, and A. Baranchuk, "Are implanted electronic devices hackable?" *Trends in cardiovascular medicine*, vol. 29, no. 8, pp. 476–480, 2019.

[12] J. Kolouch, T. Zahradnickỳ, and A. Kučínskỳ, "Cyber security: Lessons learned from cyber-attacks on hospitals in the covid-19 pandemic," *Masaryk University Journal of Law and Technology*, vol. 15, no. 2, pp. 301–341, 2021.

[13] B. N. E.-C. B. a. Argaw, S.T., "The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review," vol. 105. BMC Med Inform Decis Mak, 2019.

[14] A. R. E. S. Sardi, Alberto and A. Guerrieri, "Cyber risk in health facilities: A systematic literature review," vol. 17. Sustainability 12, 2020.

[15] Cyber attack suspected in german woman's death. [Online]. Available: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

[16] A patient has died after ransomware hackers hit a german hospital. [Online]. Available: https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/

[17] Baby died because of ransomware attack on hospital, suit says. [Online]. Available: https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465

[18] D. R. M. T. Givkey A, Kafaei Far M A, "Applicability of international humanitarian law rules in cyber attacks by looking at tallinn manual 2," vol. 17. Iran J Med Law, Special Issue on Human Rights and Citizenship Rights, 2018.

[19] B. McKay, Donna , Heisler, Michele, "Attacks on health care in syria — normalizing violations of medical neutrality?" vol. 17. New England Journal of Medicine, 2015.

[20] National center for health statistics. [Online]. Available: https://www.cdc.gov/nchs/covid19/pulse/telemedicine-use.htm

[21] Household pulse survey public use file (puf). [Online]. Available: https://www.census.gov/programs-surveys/household-pulse-survey/datasets.html#phase3.1

[22] M. Murphy, T. Welch, P. W. Shaw, J. L. Kennedy, and K. C. Bilchick, "Inhibition of pacing in a dependent patient with an implantable cardioverter-defibrillator and a left ventricular assist device," *HeartRhythm case reports*, vol. 2, no. 6, p. 473, 2016.

[23] P. K. Baranchuk A, Refaat MM, "Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?" in *Journal of the American College of Cardiology*. American College of Cardiology, March 2018.

[24] H. A. M. Puat and N. A. Abd Rahman, "Iomt: A review of pacemaker vulnerabilities and security strategy," in *Journal of Physics: Conference Series*, vol. 1712, no. 1. IOP Publishing, 2020, p. 012009.

[25] S. Das, G. P. Siroky, S. Lee, D. Mehta, and R. Suri, "Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices," *Heart rhythm*, vol. 18, no. 3, pp. 473–481, 2021.

[26] B. Rios *et al.*, "Understanding pacemaker systems cybersecurity," *Whitescope IO, Blog for https://WhiteScope. IO*, pp. 1–4, 2017.

[27] E. M. Hutchins, M. J. Cloppert, R. M. Amin *et al.*, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.

[28] M. Webster, *Do No Harm: Protecting Connected Medical Devices, Healthcare, and Data from Hackers and Adversarial Nation States*. Wiley, 2021.

[29] M. E. O'Connell, "Cyber security without cyber war," *Journal of Conflict and Security Law*, vol. 17, no. 2, pp. 187–209, 2012.

[30] A. Zaky, E. Elmitwalli, M. Hemeda, Y. Ismail, and K. Salah, "Ultra low-power encryption/decryption core for lightweight iot applications," *2019 15th International Computer Engineering Conference (ICENCO)*, 2019.