International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7188
***Article Received**: 22 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

Survey on IoT based Cyber Security Issues and Autonomous Solutions for Implantable Medical Devices

Thyagarajan.C[1], Vijay Bhanu.S[2], Suthir.S[3]
[1]Research Scholar, Department of Computer Science and Engineering,
Annamalai University,
Chidambaram, Tamilnadu, South India.
e-mail:thyaguwinner@gmail.com
[2]Research Supervisor, Department of Computer Science and Engineering,
Annamalai University,
Chidambaram, Tamilnadu, South India.
e-mail: svbhanu22@gmail.com
[3]Research Co-Supervisor, Department of Computer Science and Engineering,
Annamalai University,
Chidambaram, Tamilnadu, South India.
e-mail: suthirsriram@gmail.com

Abstract— In today's world the technology has got boomed up to the peak. So as a measure of this technology peak we could see that the enhancement of this has raised very large. This technology booming has also impacted health care sector. In our paper we are going to discuss much on implantable medical devices and its uses which plays a major role in patient's life. This IMD's are going to be the life changing aspect of each and every patient. These devices are highly controlled IoT devices (i.e.) those devices are connected through internet which will help doctors to track the details of the patients remotely. On the other hand since all these devices are connected to internet, these are easily hacked by the hackers. The factors of how those devices are much vulnerable and what are all the threats that will make these devices to malfunction and lead a problem to the patients is discussed. And also this will lead the health sector to fall in their reputation. IMD's are of many types which are in existing in the Medical industry. But we are going to consider some IMD's as example and we have planned to make a detailed study on the problems on those devices. All these devices are vulnerable since it is connected to internet. So our aim is to completely or partially reduce the risks on those devices via communication network. We have also showcased the possible threats and vulnerabilities chances on those devices. The main scenarios of device control issues and possible solutions have been discussed in this article.

Keywords: Implantable Medical Devices (IM)D, IoT, Healthcare, cyber security issues, autonomous solutions

I. INTRODUCTION ON IoT, IoMT and MEDICAL IMPLANTATION DEVICES

The Internet of Things (IoT) is a network of physical objects—"things"—embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. The Internet of Things' goal is to have devices that self-report in real time, increasing efficiency and bringing crucial information to the surface faster than a system that relies on human interaction. The advantages of the Internet of Things (IoT) have altered how small businesses handle device utilization in the workplace. In today's digital world, devices, machines, and objects of various sizes may transmit data automatically through a network, effectively "talking" to one another in real time. The Internet of Medical Things (IoMT) is a network of Internet-connected medical equipment, hardware infrastructure, and software applications that connect healthcare IT. The Internet of Medical Things (IoMT) is a cutting-edge method of connecting medical equipment and their applications to healthcare information technology systems using networking technologies. IoMT devices can track vital signs and heart rate, as well as glucose and other physiological systems, as well as activity and sleeping patterns. Seniors frequently fail to take their prescription medication on time, and IoMT devices can assist remind them and track when they took it.

An implantable medical device is one that is implanted into a person's body during a medical process, such as surgery, and stays there even after the procedure is completed. These types of implantation medical devices are a great boon to patients and as well it has some of the risks took too. There are many implantable medical devices which are currently used in medical sector now days. The following devices are considered to be the global active implantable devices. The devices are Cardiac Defibrillators/Pacemakers, Insulin Pumps, Cochlear implants, Deep brain Neuro stimulators, Gastric stimulators and foot drop implants. Some researchers have already explained about these medical implantation devices that these are hackable and prone to cyber threats. Hacking medical devices is not a new concept, but its popularity has risen dramatically in recent years as the sophistication and amount of electronics in these devices has increased. Medical device hacks, such as pacemakers and insulin pumps, have been known for a long time. The main scenario of IMD’s in medical sector is which is going to give a second life to the patients. Medical field has so many sensitive electronics equipment. The above mentioned IMD’s are too frequently used in Medical industry. One point is to describe the uses and benefits on these devices and in the same way these devices are very sensitive too. Since the technology has widely boomed, these IMD’s can be kept inside human body to help them and also to help doctors or experts to track them remotely. Our Point is to show that since it is also considered as IoT it is easily prone to hacking.

The following are some of the advantages of implantation therapy. Patient compliance is greatly improved by permitting a reduction, or entire elimination, of patient-involved dosage. Although a person may forget to take a tablet, medication distribution from an implant is mostly unaffected by patient input. Medical devices are a critical component of healthcare systems, and the benefits they can give are growing as they're necessary for preventing, diagnosing, treating, and rehabilitating illnesses and diseases in a safe and effective manner. Medical implants are devices or tissues that are implanted either inside or outside the body. Many implants are prostheses or artificial body components that are meant to replace missing bodily parts. Other implants help organs and tissues by delivering medication, monitoring biological functioning, or providing assistance.

Patient comfort and convenience are improved, resulting in higher patient satisfaction and faster recovery periods. IoT healthcare gadgets, wearable technologies, and data access enable clinicians to better monitor patients and give more educated therapy. Smart sensors monitor health conditions, lifestyle choices, and the environment and suggest preventative steps to limit the occurrence of diseases and acute states. The Internet of Things eliminates the need for expensive doctor visits and hospital admissions, as well as makes testing more inexpensive. By facilitating communication between clinicians and patients via web portals, text messaging, and email, technology contributes to patient-centered care. It also improves self-monitoring and patient convenience by increasing access to information such as online medical records.

II. RELATED WORKS:

As of now in many research papers many research authors have explained widely about various issues in medical industry and its Surroundings. In today’s scenario medical industry are boomed up with various technology impacts. This technology growth will help patients to get benefited a lot. This technology growth in the same way it is highly prone to cyber issues also. Many research papers have discussed about cyber security problems in medical fields, medical applications and medical devices particularly in medical implantation devices. We are planning to do a research survey on various papers which have explained about the cyber security issues in these domains. The Following papers are generally explains about the Medical industry and as well about the issues caused with medical industry and the various issues they face with the patient’s data, Internet connected medical devices, cyber security risks with medical wireless devices, Vulnerabilities and attacks that are caused in Medical domain and some solutions to overcome this attacks.

Because medical information plays such an important role in healthcare and human health, this study focuses on the major cyber-attacks that occur in medical domains, which result in significant losses to the health-care business. This paper provides an overview of potential cyber assaults as well as solutions, as well as a brief introduction to the required data flow in the medical area. The vulnerability at each stage is then discovered. In addition, this paper discusses several tactics to cyber attacks and how to deal with them. [1]

This paper basically talks about the development of clinical implantable gadgets which are for the most part utilized for treating persistent illnesses like diabetes, heart arrhythmia, cochlear, gastric infections, and so forth implantable clinical gadgets have given more forward leaps in network transmission by empowering and getting to the innovation. The significant clarification was about the headway of these gadgets as for remote correspondence. This paper talks around a few weak dangers in remote clinical gadgets, for example, data gathering, following the data of patients, DoS assaults and so forth and how these dangers abuse classification, the respectability of these gadgets. For getting implantable clinical gadgets different arrangements have been proposed going from AI procedures. Overall, it talks about the difficulties, dangers, and arrangements which manage the security and wellbeing of clinical gadgets. [2]

This paper deals with the importance of wireless Communications which are mostly used in healthcare applications. By using this technology how the monitoring could be made remotely is widely analyzed. But anyhow the malicious adversaries' nodes will control implantable devices and lead to risks to patients. So this paper mainly speaks about physical layer authentication techniques to improve communication performance on implantable devices. [3]

This study focuses on how the Internet of Things (IoT) works with interconnected devices and their integration. Health-care networks are extremely interconnected in order to monitor patients, yet they are also vulnerable. This study proposes a strategy for improving IoT through the use of formal approaches provided by cyber-physical systems. This also illustrates how patients and health-care providers might benefit from the democratization of medical equipment. [4]

In this section, we compile and present the critical security and utility requirements that must be met in contemporary IMD systems. To evaluate the IMD-security, framework's we look at an embed that can communicate with a peruser/programmer remotely. 1 We accept an attacker whose goal is to either (1) disrupt or hurt IMD activity in order to prevent patient treatment, (2) control patient-related data, or (3) steal patient data. Furthermore, we want the aggressor to have complete control over the remote channel between the user and the IMD.

This means he or she can intentionally listen in on, alter, sup plement, square, or replay messages between these two subs tances. As a result, the IMD-
security framework must meet the following security require ments (SRs): [5]

In this paper, we present CardiWall, a clever discovery, and counteraction framework intended to shield ICDs from digital assaults focused on the software engineer gadget. Our framework has six distinct layers of security, utilizing clinical specialists' information, measurable techniques, and AI calculations. [6]

Assault vectors With the assistance of organization model portrayed in Fig. 1, it tends to be dissected that network availability to wearables, IMDs and on location clinical hardware open assault surface. These gadgets are available to security breaks at various stages. Seven potential assault vectors are distinguished by dissecting the organization model that are recorded underneath. [7]

Software/Firmware/Hardware weaknesses: Attacks are conceivable on this vector because of utilization of shaky practices to foster programming, lacking honesty, and validness checks to refresh firmware and utilization of noxious ICs or inserted equipment Trojans. [7]

BLE/Zigbee/Wi-Fi/RF/Ethernet correspondence convention: This channel could be helpless against designated and complex assaults because of ill-advised arrangement of convention, utilization of outdated restrictive convention and wasteful existing security arrangements. [7]

A PC or cell phone application: Smartphone applications utilized alongside tangible gadgets are inclined to various assaults because of rebelliousness with guidelines and their over-favored nature. [7]

App association with passage through Wi-Fi: The transmission of wellbeing information straightforwardly from sensors, gadgets or by means of an advanced cell application is available to various assaults because of absence of safety components. [7]

Storage of information at door: if there should be an occurrence of lacking security instruments like powerful encryption, verification, and access control, and unseemly approach system, wellbeing information may be in danger. [7]

Gateway association with the cloud: It is one more significant region, which is presented to security breaks in the event that improper security instruments. Secure information transmission to the cloud is testing. [7]

Data put away in the cloud for additional examination: Due to lacking security components like hearty encryption, validation, access control of information put away in the cloud, a few assaults are appropriate. [7]

The objective of this review is to coordinate current innovation into observing, preparing, and making it more available. The proposed work is principally centered around giving an incorporated framework that assembles clinical hardware to complex frameworks, i.e., joint choice emotionally supportive networks (DSS), individual wellbeing information help, and coordinated electronic wellbeing information among different facilities. The creators have proposed a "Cash" multi-convention card going about as a passage, which is a far-off checking stage that can be executed at the patient's side. It gives a connection between the patients' current circumstances and peripherals for preparing and the board to search for inconsistencies. [8]

To better encapsulate the threat model, we've divided the risks into three groups:

Threat 1: Malicious Behavior 1. A nefarious attacker can infiltrate the environment and insert falsified data into the system to carry out malicious behaviours such as changing a patient's medical state. This hazard is represented by the introduction of misleading data into a medical device [11].

Threat2:Malicious Behavior 2 is the second threat.Any medical gadget can be infected with a malicious programme that prevents the device from going into sleep mode. This danger is a device tampering attack [12].

Threat 3:Malicious Behavior 3. An attacker can physically enter the area and tamper with any of the medical devices, rendering them temporarily inoperable. This is a DoS (Distributed Denial of Service) attack [13].

Table 1 Discussions on various State-of-Art Works

Authors	Merits	Demerits
Abdul Razaque et.al [1]	● Necessary Data Flow in the medical domain is identified. ● Various classifications of cyber-attacks are presented. ● Research analysis was done with previous work to focus on solving these cyber-attacks. ● The paper highlights future work to reduce cyber threats and proposes solutions.	● In the future, new threats and problems may occur, making architecture more vulnerable. ● Better ways to modify this weakness have to be identified.
Heena Rathore et.al [2]	● Implantable medical devices have made a significant contribution to network transformation. ● Various solutions have been presented for securing IMD. ● This article primarily addresses and focuses on threats, challenges, and solutions related to medical device privacy and safety.	● To safeguard medical equipment, precise, real-time, and energy-efficient solutions are necessary. ● It is necessary to develop an effective, usable, and privacy-preserving method for concealing a patient's health record.
Z. Esat Ankaral et.al [3]	● Wireless communications play a vital role in healthcare applications particularly in IMD's. ● Physical layer authentication techniques for IMD's are proposed which are not used in cryptology. ● The proposed technique mainly provides the advantages in decreasing the processing complexity of IMD's.	● Only path Loss was considered. ● Other channel effects like dispersion in time, the frequency may be discussed in the future.
Arthur Gatouillat et.al [4]	● IoMT plays a significant role in the medical domain health networks to improve patients' health. ● In this paper, the main focus was on ways for improving the IoMT. ● Many research directions and potential trends are explained to solve the problem.	● More Analysis and frameworks have to be processed in the future for the cyber-physical systems.
Muhammad ali siddiqi et.al [5]	● The IMDfence is a proposed security protocol for the IMD ecosystem. ● This procedure permits emergency access to the services provided without jeopardising patient safety or security.	● We've also demonstrated that IMDfence has no discernible overheads in the implant, allowing for zero-power defence against battery-based DoS attacks.
Matan kintzlinger et.al [6]	● CardiWall is a cutting-edge detection and prevention system that is primarily meant to safeguard ICDs against cyber threats aimed at the programmer's device. ● There are six layers of protection in this system.	● Absence of genuine malicious code. ● At this time, no supervised learning is being done. ● The training set of the system must be expanded.
Tahreem Yaqoob et.al [7]	● Security vulnerabilities present in medical devices are studied by analyzing the security tests and attacks demonstrated by researchers on more devices.	● In future, some open research areas should be identified to grasp the premise in terms of privacy and security-related issues in networked medical devices.
Ikram Ud Din et.al [8]	● A complete picture of the IoMT, as well as associated Machine Learning-based frameworks, was created. ● To perform a proper analysis, you must have a good image of the present IoMT ecosystem.	● Equipment cost and security to patient's information confidentiality are limited and to be considered in the future healthcare units.

Aliya Tabasum et.al [9]	● This paper speaks about the problems in designing IMD's from a cyber security perspective. ● The need of securing IMDs is demonstrated by examining various hypothetical attacks on a variety of IMDs.	● To safeguard data transmitted over the network, stronger and faster encryptions might be designed and implemented.
AKM Iqtidar et.al [10]	● The importance of Smart Healthcare Systems is explained. ● For identifying hostile activity in smart healthcare systems, HealthGuard, an unique machine learning security framework, is provided. ● HealthGuard makes use of four machine learning-based approaches.	● More Secure Frameworks may be improved in the future.

As discussed above, the various research papers illustrate many cyber security issues on current Implantable medical devices which are used in the healthcare sector. There are many pros and cons to these Implantable medical devices. Before using these devices everything has to be known clearly[31]. Many doctors suggest this kind of device for Patient's Life improvement, but since these devices are connected to the global network it has some possibilities of getting threats and vulnerabilities. So from the above-mentioned survey papers, we got more information about Implantable medical devices and their uses and also their drawbacks, and in the same way what are all the threats that can be possible in these IMD's and how this can be controlled, and what are the necessary action can be taken, all these are explained a little bit. With this, we continue with our work.[32]

III. WORKING FLOW AND PROBLEMATIC ASPECTS OF A PACEMAKER:

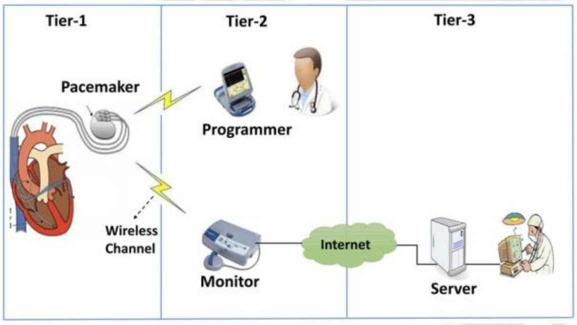

Fig 1: General working flow of a Pacemaker

Here for a sample we are taking one medical implantation device for an example (i.e.) Pacemaker as shown in figure 1. A pacemaker is a small electronic device that is implanted into the human body and powered by a battery. The pacemaker's wires are attached to the heart, which aids in the transmission of impulses from the generator to the heart muscle as well as the detection of the heart's electrical activity. Each impulse is responsible for prompting the heart to beat faster. The health sector, as well as a doctor or specialist, can monitor a pacemaker electronically via a wireless channel. The pacemaker, which is implanted in the human body, will be checked by the doctor on a regular basis to ensure that it is working well and that all of the settings are accurate for the patient. As a result, this could be a reason to hack a pacemaker.[33]

3.1 POSSIBILITIES OF HACKING A PACEMAKER

The world's largest medical device company has stated that many of its implanted cardiac defibrillator or pacemakers use an encrypted wireless protocol which could allow an attacker to change the setting of the life saving devices. Hackers could remotely control defibrillator or pacemaker which was said by the U.S. Homeland security department. Cardiac Defibrillator or pacemakers are the main device used for patients who have basic issue with their functioning of heart. This device could be easily hacked by the user[34]. But as of now no researchers has said that due to hacking of pacemakers patients prone to death. In this paper we are deeply planning to showcase the problems and possibilities where the device can be hacked. There are many cyber security issues with most of the implantable medical devices, in that this pacemaker is one of the devices. [9]

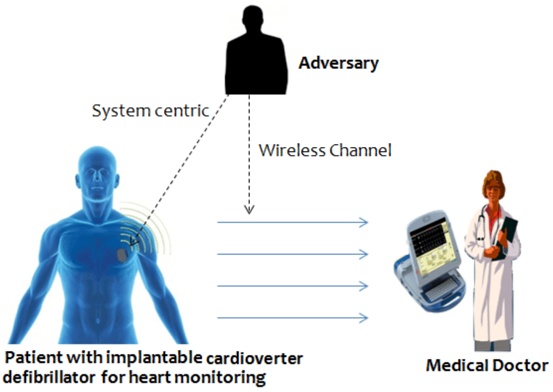
Adversary
System centric
Wireless Channel
Patient with implantable cardioverter defibrillator for heart monitoring
Medical Doctor

Fig 2: Hacking Possibility on a Pacemaker

Figure 2 illustrates shortly about how there is a possibility for unauthorized attack on a patient's implantable device. Doctor has full control on the device, where they basically monitor the device then and there. Between doctor and the patient's Device the communication is in the form of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7188
***Article Received**: 22 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

wireless mode. This is the unauthorized person's advantage in carrying out the attack. As a result, the channel between the doctor and the patient's gadget must be secured. [10] In order to hack a pacemaker the attack has to be conducted in a closer zone to the victim, and only when the device connects to the internet to send and receive data.

3.2 IMPORTANT CATEGORIES OF NETWORKED MEDICAL DEVICES:

The following diagram explains purely about the important categories of networked medical devices. Actually we are concentrating more on Internet of medical things and also about the available networked medical devices.

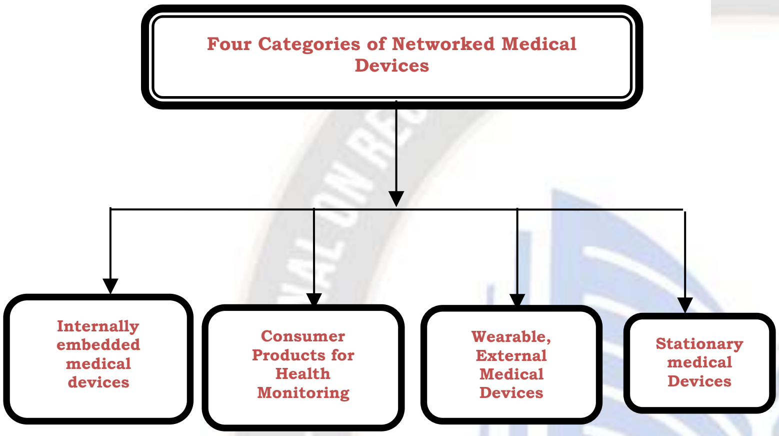
Four Categories of Networked Medical Devices
Internally embedded medical devices
Consumer Products for Health Monitoring
Wearable, External Medical Devices
Stationary medical Devices

Fig 3: Categories of Networked Medical Devices

Figure 3 illustrates the categories of available networked devices which are majorly used in Medical industry. Those devices are internally embedded medical devices, Consumer Products for health monitoring, Wearable External Medical Devices and Stationary Medical Devices.

● Internally embedded medical devices are implantable medical devices that are stored inside the body of a person. Pacemakers and other medical equipment are implanted in patients, but they must be able to interact wirelessly, using proprietary wireless protocols like Bluetooth[35].

● Bluetooth is used by products like FitBit, Nike FuelBand, and Withings to communicate with adjacent personal mobile devices.

● This category contains portable insulin pumps that interact using a proprietary wireless protocol.

● These devices, such as hospital-based chemotherapy dispensing stations or home care cardio-monitoring for bedridden patients, frequently employ more standard wireless networks, such as hospital or patient-owned WIFI networks.[36]

3.3 THREATS ON MEDICAL IMPLANTATION DEVICES:

This section is to describe about the available threats on medical implantation devices which can be too vulnerable. The following are some the threats which could be faced with the implantable medical devices as shown in Figure 4.

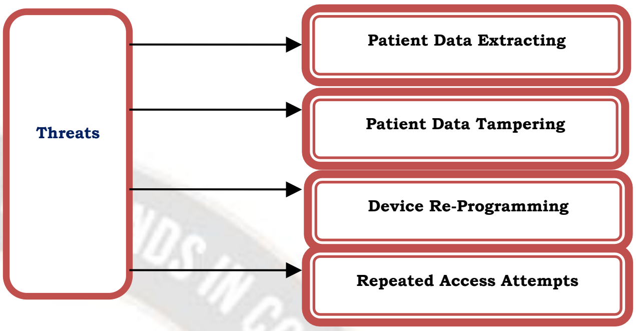

Fig 4: Various Threats on IMD

Patient Data Extracting process is affects the devices by threats which are mainly to extract the sufficient information of a patient. This kind of threat will extract patient's information which will help the attackers to gain more information of the patients and to easily threaten them with the collected information[37]. In Patient Data Tampering effect, the collected information of a patient is tampered by the attacker to see the full details about the patient. This will help the attacker to learn more about the patients. In Device Re-Programming effect**,** threats are mainly to change the device functionality by changing the logical part of the device[38]. By changing the program of a device, the general functionality is suspended and new updated re-programmed functionality of a device will affect the patient. Repeated Access Attempts affects the devices by consistent attempts to access the network of a medical device. If the security is weak the network of a particular device gets compromised. Hence, it is important to secure the network. Figure 5 showcase a Scenario on IMD ecosystem.

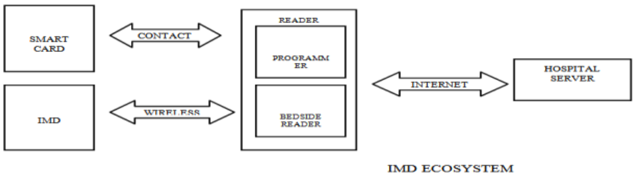

Fig 5: IMD Ecosystem

3.4 HEALTHCARE SECURITY THREATS:

The healthcare industry is increasingly becoming a target for ransomware, crypto mining, data theft, and phishing. Patients and customers are more concerned about the security of their sensitive and protected health information[39]. Connected medical equipment, on the other hand, can be vulnerable to new cyber security concerns, such as denial-of-service and patient data theft, according to a rigorous survey conducted from an IT perspective. Computer viruses and malware have the potential to compromise a patient's and a health-care provider's privacy information [40].

3.5 MAJOR CYBER SECURITY ATTACKS:

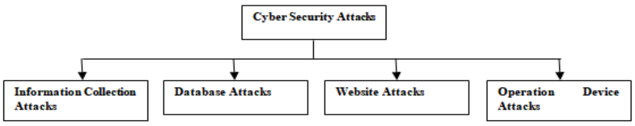

Fig 6: Various cyber attacks

Figure 6 showcases various cyber security attacks in IoT based medical devices . The classifications as shown below

- Information collection Attacks
- Database attacks
- Website Attacks
- Operation Device attacks

IV. ISSUES ON MEDICAL IMPLANTATION DEVICES

Researchers warn that implanted medical gadgets that can be hacked could result in death. The manufacturer of a number of implanted medical devices has decided not to repair nine newly found security flaws, despite the fact that the flaws could cause injury or death if exploited.[41]

According to Bill Alerts, executive director of the University of Michigan's Archimedes Center for Medical Device Security, "many implantable devices, probably practically all of them, have some type of security weakness or potential vulnerability, or haven't been designed with security in mind." " The fact that they have to interface with systems outside the body makes them potentially vulnerable."[22]

Patients are being implanted with an increasing number of electronic devices, many of which will have some type of wireless connectivity. The devices communicate not just with hospital systems, allowing clinicians to remotely update them and gather data on patients' illnesses, but also with consumer electronics, such as cellphones, allowing patients to track their progress.[42]

In principle, these networked gadgets could pose security risks, putting patients at danger. Despite multiple notifications warning of vulnerabilities in medical devices, no real-world attacks have occurred, and no patients have been harmed.[43]

4.1. RISK MANAGEMENT FOR MEDICAL DEVICES

The important scenario which is to be analysed in strengthening the security of IMd's are firmware has to be protected from tampering, securing the data which is stored by the device, proper secure on communications, and device protection from the cyber attacks. These are to be concentrated during the early stages of design.[44]

In medical devices inorder to monitor risks systematically and analyze, control, evaluate there are more procedures, policies and practices are used. Now let us discuss the standard steps required to implement a detailed risk management lifecycle for medical devices.[45]

1. Hazard Management Framework and Planning

Characterizing any danger the board interaction in consistence with the guidelines like FDA or ISO should be set up by a danger the executives system. This system incorporates the cycle which will be utilized to foster the gadget, just as the jobs and obligations of individuals related with the gadget improvement project. Alongside this, appropriate documentation of the danger the executives plan is likewise needed to be set up as a piece of the danger the board structure for clinical gadgets. [25]

2. Hazard Analysis

The danger investigation stage will help the gadget makers direct their danger the executives endeavours towards characterizing the proposed utilization of the item. This will help in zeroing in on the fundamental advances, outlining the pertinent dangers (likely wellsprings of mischief). [26]

During this stage, the predictable dangers should be distinguished as ahead of schedule as workable for surveying the danger. It is intriguing here to take note of that while evaluating hazards, the way toward recognizing potential damages ought comprise of discovering the causes as well as the potential danger identified with them. [46]

3. Hazard Evaluation

Recognizing the seriousness and event (likelihood) of dangers will help in measuring and assessing the danger. Assume, there is a risky circumstance (prone to happen), however with low unsafe impacts and there is another circumstance where the chance of mischief is extremely high, then, at that point legitimate representation of the danger on a grid is a smart thought for choosing which peril should be handled first. [27]

4. Hazard Control

When the danger has been distinguished, the following stage is to control the danger, where the real execution of hazard alleviation happens. The point of hazard control is to moderate or lower the power of hazard to a satisfactory level. [48]

There are a few different ways to moderate or control a danger:

- One way it very well may be done is by changing the plan of the item to a level where the danger is alleviated, however that is not generally conceivable.
- The next choice is to coordinate defensive measures as per a specific danger and abatement the event of mischief.
- The last thing is marking or adding guidelines in the gadget manual in regards to the dangers implied in a specific gadget.

It's likewise critical to take note of that by overhauling the item for hazard control; there are chances that more dangers can be added to the item. [28]

5. Reports and Documents

The last and the main advance is to archive the danger the executives plan and methodologies. It is additionally critical to take note of that, archiving the danger the board plan isn't restricted to the underlying stages. The danger the board archive should contain every one of the activities, reports, evaluations, and outlines made for the danger the executives arranging measure. Since the danger the executives plan is a piece of the entire item advancement lifecycle measure, your archives ought to be state-of-the-art even after the fulfilment of the item improvement measure. [29]

Alongside this current, it's additionally essential to archive the adequacy of the control activities, watching out for the subsequent dangers in the wake of carrying out the danger control activities.

Security Properties The accompanying security properties should be considered to ensure the patients utilizing IMDs.

• Authentication: Before engaging in any activity, it is necessary to understand the character of the conveying parties. Because of IMDs, a lack of sufficient validation can be used to start a rise of benefits assault (EoP) [18].

Authorization: All things considered, the usage and the executives should be obviously referenced and observed. Every activity must be carried out by people who have the necessary advantages. The reconstruction of the IMD, for example, should be overseen by a specialist and an expert.

Availability The assistance that the IMD is giving should be accessible consistently. Because of the basic capacity that IMDs perform, accessibility is a significant prerequisite. The aggressor can obstruct the radio channel utilizing dynamic sticking, delivering the IMD unavailable. The aggressor could likewise flood the gadget with network traffic, hindering admittance to the IMD or depleting its battery.

In the admission log, the Non-Repudiation System should record and certify all client activity. Because of memory constraints, no logging is used in current IMDs. If logging is used, a warning can be set triggered to alert the client if a potentially harmful event occurs [22]. Assailants may try to wipe the admission records in order to hide their tracks.

Integrity The framework should be able to detect and prevent boundary control, as well as protect against changing and figuring out. During transmission, IMD data can be recorded and altered. The IMD may also recognize toxic data, which can be used to carry out certain attacks such as code infusion. The lack of respectable checks allows for the alteration of information stored in the IMD memory. [21]

Only authorised individuals should have access to confidential information. The correspondence is vulnerable to listening in since diverse portions of the IMDs communicate over the organization. If the information isn't encrypted, the patient's sensitive information will be revealed, jeopardizing their security [23].

To avoid unapproved control, control, or impedance, posses sion (or control) is required to get the plan, execution, activit y, and maintenance of frameworks and connected cycles.[24]

Before the arrangement, patching IMDs go through redunda nt security testing. Nonetheless, the devices need be updated to address new security threats.Allowing progressions in a h ighly limited and controlled environment protects the system from malicious updates.[49]

4.2 MEDICAL DEVICE PROTECTION:

It is highly recommended to follow the security measures on the medical devices. In that we are listing some of the possible measures that could be carried out in device protection.[50]

- Software Testing, Verification and validation has to be done properly.
- On acknowledged threats, risk assessment approach should be used.
- System development and operational hazards are managed through risk management.
- Control of user access.
- Vulnerability management and software patching
- Technical audit and accountability for control efficacy.

- Security Incident Response.
- Emergency or system collapse contingency planning. [30]

Because of the sensitivity of health information, the rising interoperability of medical devices, and the reality that human well-being and life are on the line, healthcare creates security issues. [31]

Implantable devices are extremely important because if not correctly secured, they can put patients in life-threatening circumstances.

For millions of patients around the world, medical devices are becoming increasingly crucial. Their growing reliance on software and interoperability with other devices across the internet via wireless transmission has pushed security to the forefront.

4.3 HOW TO MINIMIZE MEDICAL DEVICE CYBER SECURITY RISKS:

- Be Proactive, change default passwords.
- Assess legacy systems.
- Use network Segmentation
- Discard Hardware Carefully.

V. CONCLUSION

As per discussion made it is very important to be familiar about the medical implantation devices and its uses on human body. Medical implantation devices are really playing a major role as it is one of the light changing aspect of each patient. This is highly sensitive issue, which has to be taken care with various aspects. So it is most important to protect those devices from the unauthorised access and providing more secured network technology. As of now in many papers many researchers have discussed many security methodologies on those implantable medical devices. We have just discussed the issues alone. In our future paper we would analyze more extra security concerns on those implantation devices and will take care to reduce the security risks on those devices via communication network.

REFEERENCES:

[1] Abdul Razaque,Fathi Amsaad,Meer Jaro Khan , Salim hariri, Shujing Chen, Siting chen, Xingchen Ji, “Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain”

[2] Heena Rathore, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani, “A Review of Security Challenges, Attacks and Resolutions for Wireless Medical Devices”

[3] Z. Esat Ankaralı, A.Fatih Demir, Marwa Qaraqe2, Qammer H. Abbasi, Erchin Serpedin, Huseyin Arslan1, and Richard D. Gitlin“Physical Layer Security for Wireless Implantable Medical Devices”

[4] Arthur Gatouillat, Youakim Badr, Bertrand Massot, and Ervin Sejdic, “Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine” submitted in IEEE internet of things journal.

[5] Muhammad ali siddiqi , Christian doerr, And Christos strydis “IMDfence: Architecting a Secure Protocol for Implantable Medical Devices” published in IEEE access on Aug 11,2020.

[6] Matan kintzlinger , aviad cohen , nir nissim , moshe rav-acha, Vladimir khalameizer, yuval elovici , yuval shahar , and amos katz, “CardiWall: A Trusted Firewall for the Detection of Malicious Clinical Programming of Cardiac Implantable Electronic Devices” published in IEEE access on Mar 05,2020.

[7] Tahreem Yaqoob, Haider Abbas, Senior Member, IEEE, and Mohammed Atiquzzaman “Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices − A Review” published in IEEE Communications Surveys and Tutorials.

[8] Ikram Ud Din , (Senior Member, Ieee), Ahmad Almogren , (Senior Member, Ieee), Mohsen Guizani , (Fellow, Ieee), AND MANSOUR ZUAIR“A Decade of Internet of Things: Analysis in the Light of Healthcare Applications” published in IEEE Access.

[9] Aliya Tabasum, Zeineb Safi, Wadha AlKhater, Abdullatif Shikfa, “Cybersecurity Issues in Implanted Medical Devices”Submitted in International Conference on Computer and Applications.

[10] AKM Iqtidar Newaz , Amit Kumar Sikder , Mohammad Ashiqur Rahman, and A. Selcuk Uluagac, “HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems” submitted at 6th International Conference on Social Networks Analysis, Management and Security.

[11] J. Radcliffe, “Hacking medical devices for fun and insulin: Breaking the human scada system,” in Black Hat Conference presentation slides, 2011.

[12] P. A. Williams and A. J. Woodward, “Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem,” Medical Devices (Auckland, NZ), vol. 8, p. 305, 2015.

[13] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, “Pacemakers and implantable cardiac defifibrillators: Software radio attacks and zero-power defenses,” in Security and Privacy, 2008. IEEE, pp. 129–142.

[14] Xiaoguang Liu, Ziqing Wang , Chunhua Jin , Fagen Li3 And Gaoping Li ” A Blockchain-based Medical Data Sharing and Protection Scheme:” published in IEEE access.

[15] Z B Zheng, S A Xie, H N Dai, X P Chen, and H M Wang, “An overview of blockchain technology: architecture, consensus, and future trends,” 2017 IEEE

International Congress on Big Data, Honolulu, USA, 2017, pp.557-

[16] 564.

[17] I Bentov, C Lee, A Mizrahi, and M Rosenfeld, "Proof of activity: extending bitcoin's proof of work via proof of stake extended abstract]y," Acm Sigmetrics Performance Evaluation Review, vol.42, no.3, 2014, pp.34-37.

[18] Y Yuan and F Y Wang, "Blockchain: the state of the art and future trends,"Acta Automat. Sinica, vol.42, no.4, 2016, pp.481-494.

[19] M Blaze, G Bleumer, and M Strauss, "Divertible protocols and atomic proxy cryptography," International Conference on the Theory and Applications of Cryptographic Techniques, Espoo, Finland, 1998, pp.127-144.

[20] R Canetti and S Hohemberger, "Chosen-ciphertext secure proxy reencryption,"14th ACM conference on Computer and communications security, Alexandria, USA, 2007, pp.185-194.

[21] L F Guo and B Lu, "Effificient proxy re-encryption with keyword search scheme," Journal of Computer Research and Development, vol.51, no.6, 2014, pp.1221-1228.

[22] L. Pycroft, S. G. Boccard, S. L. Owen, J. F. Stein, J. J. Fitzgerald, A. L. Green, and T. Z. Aziz, "Brainjacking: Implant Security Issues in Invasive Neuromodulation," World Neurosurgery, vol. 92, pp. 454–462, Aug. 2016. Online]. Available:http://linkinghub.elsevier.com/retrieve/pii/S1878875016302728

[23] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," Journal of Biomedical Informatics, vol. 55, no. Supplement C, pp. 272–289, Jun. 2015. Online]. Available:http://www.sciencedirect.com/science/article/pii/S153204641500074X

[24] I. Stine, M. Rice, S. Dunlap, and J. Pecarina, "A cyber risk scoring system for medical devices," International Journal of Critical Infrastructure Protection, 2017.

[25] H. Boyes, "Cybersecurity and cyber-resilient supply chains," Technology Innovation Management Review, vol. 5, no. 4, p. 28, 2015.

[26] S. Nagarakatte et al., WatchdogLite: Hardware-Accelerated Compiler Based Pointer Checking, 12th Annual IEEE/ACM International Symposium on Code Generation and Optimization, Orlando, FL, USA. ACM, p. 175, 2014.

[27] A. Menon, S. Murugan et al., Shakti-T: A RISC-V Processor with Light Weight Security Extensions, 2017 Proceedings of the Hardware and Architectural Support for Security and Privacy. ACM, pp. 12, 2017.

[28] M. Zhang, A. Raghunathan, and N. K. Jha, ''MedMon: Securing medical devices through wireless monitoring and anomaly detection,'' IEEE Trans. Biomed. Circuits Syst., vol. 7, no. 6, pp. 871–881, Dec. 2013.

[29] A. Kaadan and H. H. Refai, ''Securing wireless medical devices,'' in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2012, pp. 942–948.

[30] A. Bordia, S. Verma, and K. Srivastava, "Effect of garlic (allium sativum) on blood lipids, blood sugar, fifibrinogen and fifibrinolytic activity in patients with coronary artery disease," Prostaglandins, leukotrienes and essential fatty acids, vol. 58, no. 4, pp. 257–263, 1998.

[31] D. Klachko, T. Lie, E. Cunningham, G. Chase, and T. Burns, "Blood glucose levels during walking in normal and diabetic subjects," Diabetes, vol. 21, no. 2, pp. 89–100, 1972.

[32] L. Davi, D. Alexandra, E. Manuel, F. Thomas, H. Thorsten, H. Ralf, N. Stefan, and S. Ahmad-Reza Sadeghi, "MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones", NDSS, vol. 26, pp. 27-40, 2012.

[33] L. Cheng, Program Anomaly Detection Against Data-Oriented Attacks, Virginia Polytechnic Institute and State University, 2018.

[34] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," Wireless Netw., vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[35] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review," IEEE Commun. Surveys Tuts., vol. 21, no. 4, pp. 3723–3768, 4th Quart., 2019.

[36] R. M. Seepers, J. H. Weber, Z. Erkin, I. Sourdis, and C. Strydis, ''Secure key-exchange protocol for implants using heartbeats,'' in Proc. ACM Int. Conf. Comput. Frontiers CF, 2016, pp. 119–126.

[37] V. Pournaghshband, M. Sarrafzadeh, and P. Reiher, ''Securing legacy mobile medical devices,'' in Proc. Int. Conf. Wireless Mobile Commun. Healthcare. Berlin, Germany: Springer, 2012, pp. 163–172.

[38] J. Sorber, M. Shin, R. Peterson, C. Cornelius, S. Mare, A. Prasad, Z. Marois, E. Smithayer, and D. Kotz, ''An amulet for trustworthy wearable mHealth,'' in Proc. 12th Workshop Mobile Comput. Syst. Appl. HotMobile, 2012, p. 7.

[39] N. Chandramowliswaran, S. Srinivasan, and C. T. Segar, "A note on linear based set associative cache address system," International Journal on Computer Science and Engineering, vol. 4, no. 8, pp. 1383–1386, 2012.

[40] A. Subasi, M. Radhwan, R. Kurdi, and K. Khateeb, "Iot based mobile healthcare system for human activity recognition," in 2018 15th Learning and Technology Conference (L&T). IEEE, 2018, pp. 29–34.

[41] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, "Ble beacons for internet of things applications: Survey, challenges, and opportunities," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 811–828, 2018.

[42] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-

antenna cellular networks," IEEE Trans. Commun., vol. 62, no. 6, pp. 2006–2021, June 2014.

[43] Joseph Miller, Peter Thomas, Maria Hernandez, Juan González, Carlos Rodríguez. Machine Learning for Decision Support in Uncertain Environments. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/205

[44] Y. Pei, Y. c. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over miso cognitive radio channels," IEEE Trans. on Wireless Commun., vol. 9, no. 4, pp. 1494–1502, April 2010.

[45] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," IEEE J. Sel. Areas Commun, vol. 31, no. 10, pp. 2099–2111, Oct 2013.

[46] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 3807–3827, Aug 2010.

[47] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik,"Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," IEEE Trans. Inf. Forensics Security,vol. 11, no. 6, pp. 1128–1138, June 2016.

[48] T. Cameron, "Safety and effificacy of spinal cord stimulation for the treatment of chronic pain: a 20-year literature review," Journal of Neurosurgery: Spine, vol. 100, no. 3, pp. 254–267, 2004.

[49] S. J. Majerus, P. C. Fletter, M. S. Damaser, and S. L. Garverick, "Low power wireless micromanometer system for acute and chronic bladder pressure monitoring," IEEE Transactions on Biomedical Engineering, vol. 58, no. 3, pp. 763–767, 2011.

[50] C. Srdjan and B. Daniel, "On the security and privacy risks in cochlear implants," Technical report/Swiss Federal Institute of Technology Zurich, Department of Computer Science, vol. 677, 2010.

[51] Arfaoui, Amel, Ali Kribeche, and Sidi-Mohammed Senouci."Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications." Computer Networks 159 (2019): 23-36.

[52] Masdari, Mohammad, and Safiyyeh Ahmadzadeh. "A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems." Journal of Network and Computer Applications 87 (2017): 1-19.