Performance Evaluation of Security Enabled Surgically Implantable Smart Pacemakers in Cardiac Risk Patients

Kinshuk[1], Niyati Shrivastava[2], Aishwarya Verma[3] , Sushruta Mishra[4]
[1,2,3,4] Kalinga Institute of Industrial Technology, Deemed to be University, India

Abstract

The healthcare sector is benefiting from medical equipment' connectivity in several ways, such as enhanced patient outcomes, automatic alarms, and remote observing. After analyzing the current IoT-driven healthcare applications, creative tech-based solutions are still required to meet the difficulties in the medical setting. In this study, we examine connected pacemaker security challenges in an organized way. While methods exist for formal affirmation of pacemaker software, these are not suitable to prevent security weakness. To this end we develop a operating-time approach. We examine security threats and challenges related to automated Pacemakers and patients' privacy are mostly driven by monetary motives with analysis of several automated device safety solutions currently in place needs improvement by wearing wearable devices. Our approach proposes a wearable device that non-contact senses the familiar radiation signals in order to determine if a pacemaker has been compromised in features along with safety measures. We develop a set of timed policies to be monitored at run-time. We provide a methodology for the design of the wearable device and results illustrate the technical practicality of the developed concept.

Keywords

Remote observing, Pacemaker, Security threats, Patients' privacy, monetary motives, Wearable devices.

1. Introduction

Automated devices have become an important part of our lives, in this era of automation. These devices enhance the level of comfort and quality of living. Automation in the healthcare sector has many supporters and opponents, but one thing is certain: it is here to stay. By enabling the development of a broad range of uses, including as telehealth, fast medication, and remote physiologic monitoring of medical resources, the IoMT plays a important role in the growth of School Health Services(SHS). Patients remain faithful to their treatment plans and their behavior. IoMT refers to the networked and sensor-equipped medical devices used in the healthcare industry. Because they frequently use out-of-date software and operate on old-fashioned operating systems, the majority of IoT devices are open to attack. Pacemakers, X-ray machines, and CT scanners are examples of devices which use outdated software that is not regularly put back together. Automobiles with integrated sensors or humans with a heart monitor are examples of products in the Internet of things(IoT) that may collect and transport data with little to no human interaction after they are given IP addresses. Smart clothing, smart watches, light bulbs, door locks, refrigerators, vehicles, RFID, wearable, and pacemakers are examples of Internet of Things devices.

Proceedings of SNSFAIT 2024: International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies, Delhi, India, August 08-09th, 2024

[*] Corresponding author: Sushruta Mishra(sushruta.mishrafcs@kiit.ac.in)

[†] These authors contributed equally.

[1,2,3,4]Kalinga Institute of Industrial Technology, Bhubaneswar, India

22051087@kiit.ac.in, 22051051@kiit.ac.in, sushruta.mishrafcs@kiit.ac.in

An electrical device that regulates erratic heart rhythms is called a cardiac pacemaker. A set of leads is used to connect the pacemaker to the sufferer's heart when pacemaker is placed beneath the skin of their chest, directly below the collarbone. The erratic heartbeat caused by arrhythmia is treated using pacemakers. A pacemaker is a device that uses electrical impulses in order to keep the heartbeat regular. Patients with irregular heartbeats are advised to get a pacemaker. Since the first pacemaker was introduced in 1958, yet significant security issues remain . Pacemaker fall under the category of Implantable Cardioverter Defibrillator (ICD is a small electrically powered device placed in the chest). ICD detects and stops non-uniform heartbeats, also known as arrhythmia's. Since pacemakers are known to be extremely important medical equipment, an interruption in the device might compromise the patient's life. In the event that a pacemaker's programming malfunctions, the device will automatically convert to one of its "fail-safe" modes, which will continue to produce a steady pulse until the patient sees a pacemaker technician who can reprogram the device.

The result of insufficient security in IoMT healthcare systems can be, for example, compromised patients' privacy caused by intruding, and delayed recognition of life threatening incidents due to the disturbance of regular operations of IoMT devices induced by Denial of Service (DoS) assaults. The trade-off between providing medical professionals with emergency device access and guaranteeing that the device blocks any unofficial access is a major issue with pacemaker security. The complete survey discusses this exchange for cyber-physical systems (CPS), such as pacemakers, which are cyber-components that regulate the heart's regular beat (physical systems). The primary motivation for attacks on patient privacy is money: the desire to profit from the sale of medical records on the black market. Pacemakers have potentially fatal security flaws, turning a life-saving equipment into a weapon. Wireless connectivity between the pacemaker and existing monitoring systems is necessary.

Main contributions of the paper are as follows:

1. Examine security ultimatum and challenges related to computerized healthcare devices(Pacemakers).
2. Analyse the several automated device safety solutions currently in place and suggest improvements.
3. Examine patients' privacy are mostly driven by monetary motives.

2. Related Works

In [1] with objective to give an opportunity to explore privacy and security in the field of Internet to end-users methods to how the entire system can help by providing a way developing and designing secured and isolated modern systems in the field of IoT dealing with two factors: exposure and outcome along with different hacking methods from sleep to standby of the pacemaker communicating with the surrounding.

In [2] Security problems and hurdles in Automated Healthcare Devices. This writing explores automation devices mostly used in the healthcare industry discussing the security concerns as well as future usage difficulties with possible ways like having distance from the magnetic materials with validation during run time which can be used to check any irregular activity at run-time to protect automated healthcare devices in several ways. Patients details should be saved in encoded format, to make this more difficult for an attacker to decrypt this encoded text. The precautionary solutions concludes the responsibility of both the patients as well as doctors.

In [3] IoMT: A Pacemaker sensitivity analysis and Strategies in security analyses the functioning and possible vulnerabilities of several IoMT devices, including wireless vital monitors, smart pens, implanted cardiac devices (pacemakers), and other devices. concluding Security Analysis of IoMT by attacking Graph Modeling for Implantable Pacemaker.

In [4] This piece uses architecture analysis and design language (AADL) to model a pacemaker autonomous remote monitoring system (PARMS),concluding with increase in testing and verification methods to ensure the effectiveness of safety and security measures and highlights the need to increase awareness about the security of IoT medical devices and to consider cyber-attacks and vulnerabilities when designing these devices.

In [5] The safety aspects of ICD which is an implanted cardioverter defibrillator are examined in the article 'Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses'.This study leads our community to analyze and exploit previous radio communications protocols which were not known by using general-purpose software radios with investigations of an ICD that will work for bitter attacks which endangers the safety of patient data and medical measures, and may have critical experience to the honesty of information , including patient data and therapy settings for when and how shocks are addressed. Because of such disputes between security and safety, this research's traditional method to access control may not always be correct.

In [6] Privacy and safety for the Internet of Medical Things Enabled Healthcare Systems: A Survey where study imparts an overview of the state-of-the-art methodologies by reviewing the security problems, needs, risks, and other research objectives in Internet of Medical Things sector concluding to the quick development of IoMT devices in healthcare solutions has made preventative as well as individualized patient care possible. However, these devices' network connectivity presents security risks and vulnerabilities that could endanger users' lives. Novel approaches that integrate physical, digital, and human aspects into the design space are needed to guarantee the security and safety of such gadgets. In order to defend their systems from malicious attacks, administrators must have records of the anti-virus libraries and patches updated . Thus new methods and techniques for attacking networks are continually being developed.

In [7] Secure techniques of Pacemakers by using verification at runtime offers a wearable device design process, and findings show that the created concept is practical. This study presents a formal approach to address this by integrating an ECG processing framework that will detect and forward the timing events of interest to the device with such verification that is based on monitoring of attributes that are time tracked. Although this works and opens the door for formal techniques driven approaches to pacemaker security, it is not without flaws.

In [8] Trust along with privacy in the IoMT Enabled Healthcare System that are smart with a systematic evaluation of Current and upcomming trends examines the most promising approaches for protecting IoMT, particularly with regard to authentication as well as the and safetyand authors, the usage of block-chain for safe data sharing, is the goal of this article. In comparison to traditional methods, the survey research shows that the block-chain approach, lightweight authentication, and ECC algorithm provide the best security. It is necessary to find some different solution that can satisfy all security needs and hold the entire design of the cyber space in order to guarantee the protection of such smart gadgets.

In [9] Challenges analysis on Electronic Healthcare recording systems .The ecosystem of Internet of Things (IoT)-based electronic devices and its pertinent elements are presented in this article. The main objective of this piece is to examine the relationship between wearable and implanted technology and the healthcare system and the IOT Technology used in an electronic health care system should be patient-centered, flexible, reliable, safe, and power-efficient.

In [10] Experimental Security Analysis of Pacemakers that are connected explains the security challenges in a methodical manner. This paper presents the outcomes of our research regarding the ecosystem of pacemakers of the medical device manufacturer BIOTRONIK along with Home Examining Units. They examined various iterations of the devices and found flaws in each one of them.

3. Proposed Model

Since pacemakers emit radiation ranging between 10 to 15 micrometers from the body,techie are able to communicate and decide with them by manipulating their settings, which could have major consequences. Scientists have developed a watch that allows radiation to remain inside the body. Some opposite party person may sometimes fail to detect the radiation coming from the pacemaker, so this watch will be very helpful. In the event that there are any irregularities in a heartbeat, watches can also be used to monitor heartbeat. We can also lessen an attacker's effects by using this watch. Watches can also be used to measure depression levels. We can use watches to track our level of fitness and to see how far we have walked.

It's also possible to do a run-time verification to look for any unusual activity during runtime. An alarm is set off to notify the patient in the event that any such activity occurs. Programmers and doctors should create strong passwords for pacemakers that are difficult for attackers to decipher. Examples of such passwords include combining capital, lowercase, numeric, and special characters with one another to create an extremely difficult-to-guess password. When it comes to security, the manufacturer is extremely important. Pacemakers should only be purchased by a genuine company. However the smartwatch should be stopped right away if patients have symptoms of dizziness, chest pain or palpitations. One safety measure to consider when using a pacemaker is to have magnetic materials at a larger distance and not near. Any material that generates an electromagnetic field will negatively impact a pacemaker; therefore, one must exercise extreme caution when near magnetic materials. Mobiles have an effect on pacemakers as well. Patients should use their phones as little as possible and should never keep them in their shirt pockets. Also where the Pacemaker is insatalled there on the opposite side of the ear a portable can be used. Figure 1 highlights the proposed model solution.

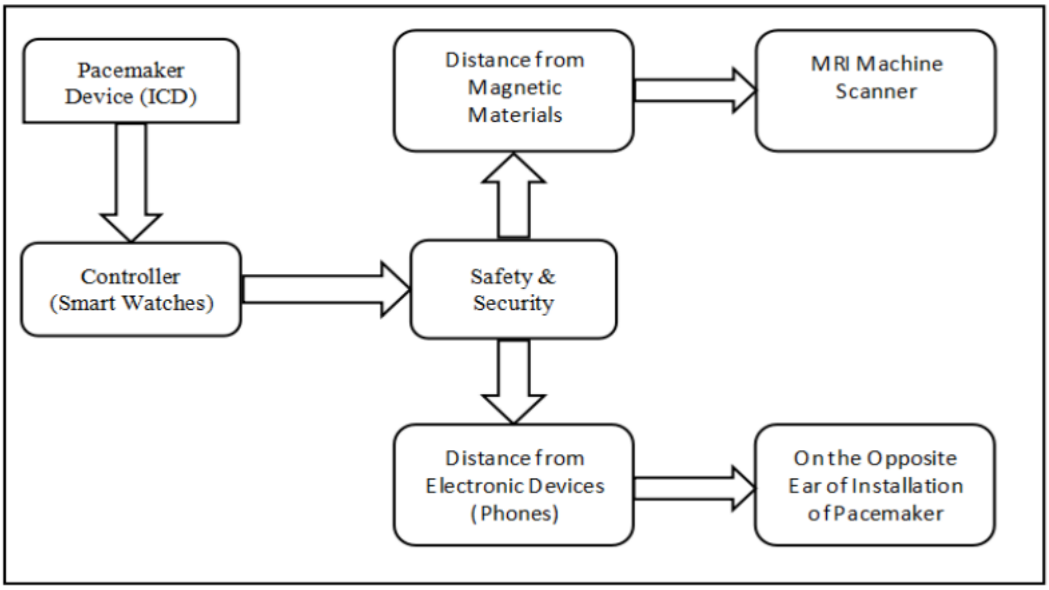
Pacemaker Device (ICD)
Controller (Smart Watches)
Safety & Security
Distance from Magnetic Materials
MRI Machine Scanner
Distance from Electronic Devices (Phones)
On the Opposite Ear of Installation of Pacemaker

Figure 1. Shows the diagrammatic view of the proposed Solution

4. Result Analysis

As per the survey conducted with the various heart related devices we have arrived to a result that many pacemakers are much more suitable than other heart related devices when evaluated against some vital performance indicators.

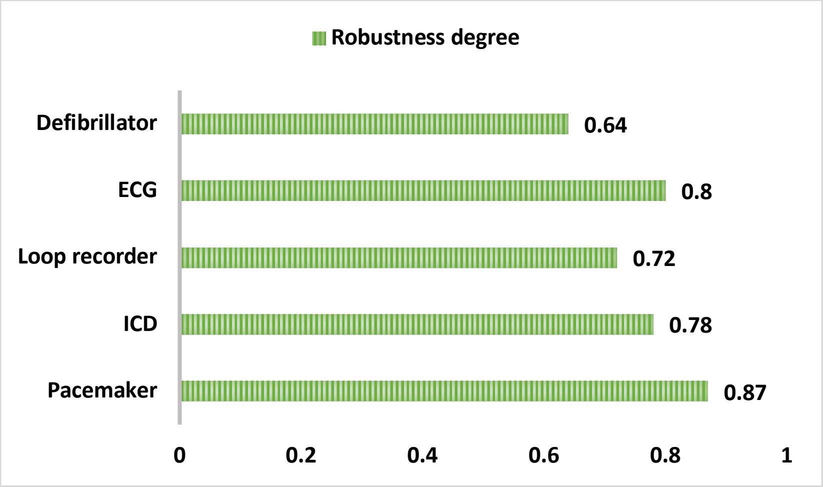

Figure 2. Robustness degree analysis of pacemaker with other devices

Figure 2 demonstrates the degree of robustness of different related heart devices. Robustness is determined by analyzing the compatibility level in various types of patients and it is observed that pacemaker recorded the maximum robustness degree of 0.87 while defibrillator noted the least value of 0.64.

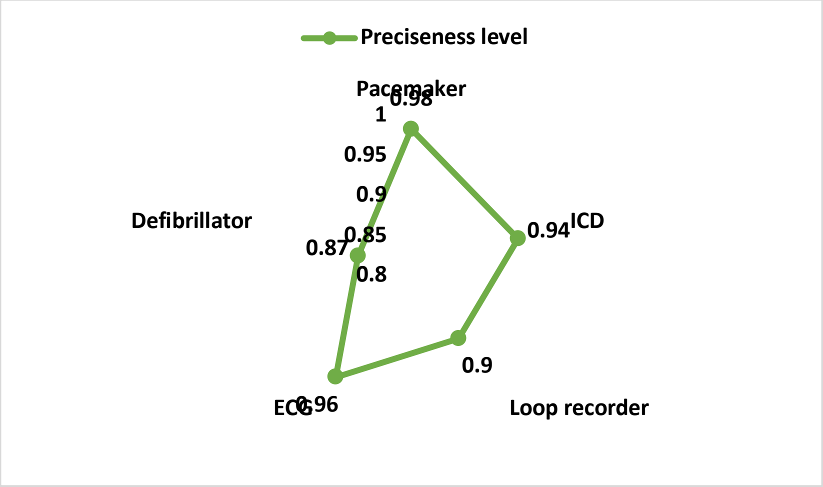

Figure 3. Preciseness level analysis of pacemaker with other devices

The preciseness level of an automated healthcare device indicates the frequency of accurate outcome among all outcomes generated. Figure 3 determines the preciseness level of various heart related devices and it is noted that pacemaker recorded the highest level of 0.98 which is higher than its comparing devices.

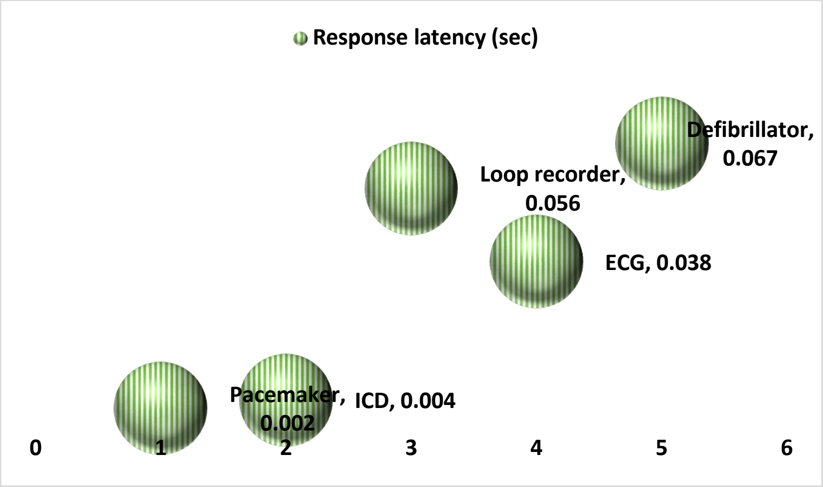

Figure 4. Response delay period analysis of pacemaker with other devices

Response latency period is a critical element for heart related functionalities. Pacemaker recorded the best response time with a value of 0.002 seconds as compared to other devices like ECG and loop recorders. Figure 4 demonstrates the overall results.

5. Conclusion

To sum it up, the introduction of medical equipment connectivity into the healthcare industry has transformed patient care, offering advantages like improved results and remote monitoring. But there are serious security issues, as this study has shown, especially with regard to connected pacemakers. Even with current techniques for formal verification of pacemaker software, vulnerabilities cannot be completely eliminated. A novel runtime approach is suggested in order to close this gap, along with the creation of wearable technology that can identify potential compromises to pacemaker functionality.

The development of a radiation-blocking watch offers a viable way to lessen hacker interference and protect patient privacy. Furthermore, the multi-functionality of these devices—which can track fitness, measure depression, and monitor heartbeats—adds even more value to patient care. To further protect against potential threats, strict security measures—such as the use of strong passwords and careful consideration of device manufacturers—are necessary. Additionally, patients need to be informed about safe procedures, like avoiding magnetic materials and keeping cell phone use to a minimum when near pacemakers. To put it briefly, even though medical technology is advancing and has never been better, protecting connected devices security and safety is still critical. In order to address changing challenges and boost patient well-being in the digital age, healthcare professionals, engineers, and policymakers must continue their research, create, and collaborate.

References

[1] Fazeldehkordi, Elahe et al. “Security and Privacy in IoT Systems: A Case Study of Healthcare Products.” 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT) (2019): 1-8.

[2] Jangid, A., Dubey, P.K., & Chandavarkar, B.R. (2020). Security issues and challenges in Healthcare Automated Devices. 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 19-23.

[3] Puat, H.A., & Rahman, N.A. (2020). IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. Journal of Physics: Conference Series, 1712.

[4] Puat, H.A., & Rahman, N.A. (2020). IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. Journal of Physics: Conference Series, 1712.

[5] 2008 IEEE Symposium on Security and Privacy Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.

[6] Sun, Y., Lo, F.P., & Lo, B.P. (2019). Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. IEEE Access, 7, 183339-183355.

[7] Pinisetty, S., Roop, P.S., Sawant, V., & Schneider, G. (2018). Security of Pacemakers using Runtime Verification. 2018 16th ACM/IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE), 1-11.

[8] Vaiyapuri, T., Binbusayyis, A., & Varadarajan, V. (2021). Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: A Systematic Review of Current and Future Trends. International Journal of Advanced Computer Science and Applications, 12.

[9] T.Poongodi, D., Balusamy, D.B., Sanjeevikumar, D.P., & Holm-Nielsen, D.J. Internet of Things (IoT) and E-Healthcare System – A Short Review on Challenges.

[10] Bour, G., Moe, M.E., & Borgaonkar, R. (2022). Experimental Security Analysis of Connected Pacemakers. International Conference on Biomedical Electronics and Devices.