Journal of Physics: Conference Series

PAPER • OPEN ACCESS

A Review on IoMT device Vulnerabilities and Countermeasures

To cite this article: Reshiwaran A/L Jegatheswaran *et al* 2020 *J. Phys.: Conf. Ser.* **1712** 012020

View the article online for updates and enhancements.

A Review on IoMT device Vulnerabilities and Countermeasures

Reshiwaran A/L Jegatheswaran, Isaac Joshua Sakira and Nor Azlina Abd Rahman[*]

Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur

[*]Corresponding author e-mail:TP038338@mail.apu.edu.my

Abstract. According to a report by Allied Market Research they have said that by 2021 the IOMT would most likely reach about $136.8 billion worldwide [12]. This indicates that sooner almost all medical Centre would implement IOMT devices in their Centre and also in their patients' body to get better result. Having a good growth on this it may indicate on the development of medical. It also proves on the movement from traditional medical to technology era medical whereby for checkups patients does not need to turn up as the device of IOMT would present the data. IOMT devices would allow the Medical Centre to cut cost on certain equipment as they could be done by using small IOMT device. This device is designed to generate data and provide indication for the users. IoMT also saves on the patients waiting time since analysis and prescription can be done on the go and there is no need for queuing up at medical facilities. Appointments can also be scheduled remotely depending on availability of the medical personnel.Because of the dependence on the internet for the transfer and storage or medical data, there is a big risk regarding data privacy and security. The aim of this research is to explore the vulnerabilities associated with IoMT devices that focusing on Mobile Cardiac Telemetry and Respiro Smart Inhaler system and suggest suitable protection mechanisms against the possible attacks to the IoMT devices.

Index Terms. IoMT, Mobile Cardiac Telemetry, Respiro Smart Inhaler. Vulnerability, countermeasure

1. Introduction

Although having Internet of Medical Things is much useful for both side party but there are still challenges is being faced by the organization on implementing this Internet of Medical Things. These challenges could be also known as the disadvantages. From the same source, Rick Martin has also stated that "Like most technology, IOMT brings advantage and disadvantage" as we have discussed the advantage and the disadvantage is basically would be the challenges on implementing it [1]. There are basically three main challenges.

Firstly, to implement the IOMT in the Healthcare it would incurred higher cost. This means, implementing the IOMT in a hospital is not as cheap as buying a smart watch. This is because, having this IOMT device in a hospital will require certain number of supporting programs to be implemented too. This shows that these devices are not a standalone as they would need some other device to support their process. Comparing on purchasing a watch and wearing is not expensive but having a system that would replace the traditional medical method requires higher cost and this would be something that needed to be taken in consideration as not all hospital would move in to and if they were smaller hospital they will not be able to incurred a huge amount of cost. For instance, in order to implement an IOMT device the hospital will have to design to have IT networks to transfer the data to cloud and they will need to have block chain to keep the originality of the data. A report by arkenea has also stated that high cost is one of the challenges on implementing the IOMT device [2].

On the other hand, Security Vulnerability is another important aspect that would be taken in consideration. This means, a concern on the security in the IOMT devices. This is something very important. The users will have to see or analyses the vulnerability in order to prevent any hackers to hack the device and retrieving important information. Having information leaked out by hacker would be something that must not happen. We could say nowadays cybercriminal has been increasing drastically and having it in a hospital that have hundreds of millions of patient medical records they will have to always run test on the IOMT devices to see if there is any vulnerability. For instance, MRI machine is used to scan the patient body, and this is an IOMT device because they are connected to internet and the data would be stored in their database. If there were vulnerability, then hackers would have chance to hack those devices to retrieve the data and they would most likely to sell it on the Dark Web.

Lastly, Strain on Existing Networks. This means, it is not easy to bring IOMT devices into the hospital. It is not a simple process whereby they bring the devices connect it to the hospital network and begin using it. It is actually harder. In order to use the IOMT device they will need to use a secured network. These challenges would be interrelated to the security vulnerability. Having a secure network would most likely be a partial solution of security vulnerability. A secured networking would give a hard time for hackers to hack the network to gain access into the device. For instance, taking the MRI machine they will need to be connected to a secured network in order to prevent any middle-man attack.

2. Literature Review on IoMT Devices

A lot of research has been carried out. Many of the findings on the role of the internet in the medical field today. Many devices have been developed with an aim to improve service delivery to the patients. Wearable devices with sensors to monitor various medical conditions have been developed and approved for use. This section will discuss on two IoMT devices which are Mobile Cardiac Telemetry and Respiro Smart Inhaler.

2.1. Mobile Cardiac Telemetry

According to Digirad, Mobile Cardiac Telemetry is basically a cardiac monitoring device [3]. This means, the device is used to monitor the patient's cardiac activity. This device is design in a small portion that classify them as portable device. This device all the user and also the record to look at the patient heartbeat rate as the patient runs, exercise, resting and also sleeping. This would be a much useful as the user and doctor could detect if there is any pattern on the cardiac activity. If there is a pattern that indicate a future heart failure, then the doctor could take an advance treatment or check up to see the cause of it.

Figure 1. Mobile Cardiac Telemetry [3]

According to UnivDatos Market Insight, by the year 2025 this mobile cardiac Telemetry would most likely gain a market worth of US$ 1,264 million [4]. This indicates that by 2025 most of the public would be using it to allow their doctor to track on their cardiac activity. They also added that the growth would be due to the geriatric population and the prevalence of cardiovascular diseases.

2.1.1. How it works

There are three ways on how mobile cardiac telemetry works. The indication or the method they work are by setup, beat-to-beat analysis or reporting heart behavior [3]. Firstly, speaking on the setup they are the beginning step or in other word the beginning stage of having the device. In this setup step the physician will order the device for the patient that really needs it and they will also register the patient with the cardiac monitor provider. In this case, it will be the device organization. This means, upon having a check and they there is a must on wearing the device then the respective person will register the patient into the cardiac monitor provider system and also purchase the device for the patient and this device would be either sent to the home of the patient or they could connect the electrodes. If it were delivered to home, then the patient could just connect the device to the electrodes and that would be an easy step as there is instruction that is being provided. Upon connecting the device, the monitoring office will activate, and a test will conducted in order to detect if the result could be generated from the device to the server via mobile network. This means, having the device implemented on the body the monitoring office will activate it and they will test run the device to see if the device is capable to transmit the data via mobile network to the server that could be monitored by the organization and if they are successful then the patient is good to go. For instance, a patient has faced heart attack and after a checkup he is required to use the Mobile Cardiac Telemetry by the doctor in order to keep on track of the cardiac activity. The nurse will communicate with the Braemar Company to register the patient and also purchase the device. Upon receiving the device, they will connect to the electrodes and later the Braemar would conduct a quick test to look at the success rate on the device transmitting the result to the server [5].

Moving on next they have the beat-to-beat analysis. This means, the device will record every single second or in other word ever single heartbeat. This device basically just records and provide a real time monitoring for the service provider when there is a network that allow them to connect to the server. When there is no connection then the device will store in the storage and wait for a network connection. Upon having connection then the stored data will be transmitted to the server for a quick monitoring to take place. This record will be checked by professional trained staff on looking for any abnormalities. 0

Lastly, there is reporting heart behavior. This means, the device will go along with the heart and learn the heartbeat and understand the heart condition. They will trigger the monitoring department if there were any symptoms of an event that needed medical assistance. Upon sending those indication then a quick medical assistance will be sent to his location. This would be much easier as the device only be used when there is symptoms or heart failure event. Other than they device does not have any activity. This reporting heart behavior has been classified as the most effective methods on cardiac monitoring

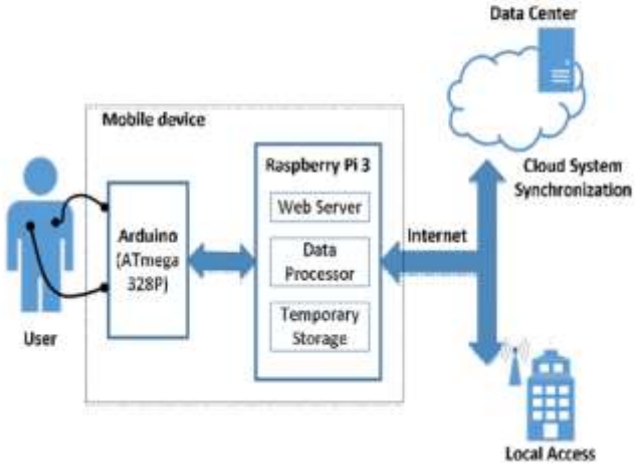

Figure 2. Structure of the connection [6]

2.1.2. Vulnerability of Mobile Cardiac Telemetry

Did you know Vulnerability could be discovered almost on all technology? According from a website Comodo, they have defined Vulnerability as a "term that is used in Cybersecurity which refers to defect on a system that could leave it open to be attacked" [7]. This means, vulnerability could be said as a manufacturing defect on the software which will have a loophole for hackers to make an in and outdoor. In Cybersecurity term it will be known as the Back door.

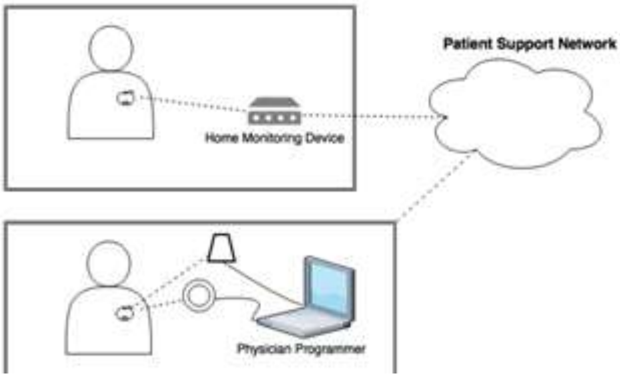

Figure 3. The connection of devices [8]

Figure 3 shows how the Mobile Cardiac Telemetry works. It shows how they connect from the device to the computer.

Mobile Cardiac Telemetry also has vulnerability which allow to be hacked. There are a few vulnerabilities that could be discussed. Firstly, lack of authentication process [8]. This means, there is no any password requirement to access the device. This is a basic security that needed to be adjusted. Speaking in general, every single device will have to be equipped with a password authentication in order to prevent or protect it from being attacked. For instance, a patient that uses the mobile cardiac telemetry and the doctor could just go open the record of the device in their PC and they could get all information. There is no any authentication process and that is a vulnerability. It can be said, they could just hack the doctor's PC and they could access the patient's device and they could retrieve the information regarding the patient. This vulnerability would bring an impact on both the patient and the doctor. Looking at impact on the patient, the hackers could take personal information regarding the patient such as, location, heart rate and more. Having password would give an additional protection on the device and the hackers will have to present password in order to access the device information.

Secondly, Software bugs. This means, an error of fault in the program of the device and this software bugs would produce an incorrect or unexpected result. This could be an advantage for the hackers. This would bring more complicated error for the device too. This can be next vulnerability that need to be paid attention. This vulnerability could be more likely to be used by the hackers. They would hack the device and use the software bug as to attack the device. For instance, the device that is used by the patient would have a bug in the software that sometimes could result on error on the result. The hackers could use the bugs to run code with the bug to make it worse by having malware that would take full control of the device and that would be a problem for the users as it may allow the hacker to collect all personal information. This will allow the hackers to either sell the information or used it to blackmail on the users for money. Anyways both actions would only have a single motive which it will be for money.

Then, access on external computer [9]. This means, those data could be retrieve from an external computer. This a vulnerability as having a device that keep record of the patient should be stored in a computer that needed to keep in a highly secured room. This could prevent hackers from accessing the device physically by using the computer. This could be an issue as if they get to discover the computer, they could make patients life haywire. This is something that could be a simple threat to the users and the doctors. For instance, the hackers could go into the hospital and get into the doctor's room and access it to get into the device and they might image the information to be used in future time. This attack could be done physically as they could get into the doctor computer hack the computer to gain access and they might also place a back door to the software of the computer in order for them to get accessed into the computer from their place with presenting there. By having the back door, they can gather information from time to time and use the information against the users. When they a back door then this could also move into eavesdropping on the doctor's procedure.

Lastly, lack of security patches. This means, over the time almost all internet of things will need to get themselves update on time to time basic on their security patch. Sometime, users would not take it serious on these updates and they might not update it. By not updating it, the hackers could use the loophole to get into the device. For instance, every 3 to 6 months once all service provider would have a security patch. This update will be sent to the device for the owner to update it but sometime the owner does not update it and that would be how the hacker take control of the device. The method of attack is where they would use the malware to inject through the area where the security is not patched. The impact would be lost of information and they would also get the location of the user. Having the live update on location they could conduct more crime such as theft.

2.2. Respiro Smart Inhaler

With every year that passes, Asthma continues to be a major health concern particularly affecting children more being the leading chronic disease among children. If not properly managed, Asthma can become so sever and lead to death. Several treatments are available in the form of inhalers whose aim is to orally administer medicine to those affected. This however requires regular tracking of symptoms and Asthma imaging using CT scans for lung function tests. This all requires frequent visits to medical centers to have all the proper tests done for proper analysis. With the evolution of the Internet into the medical field, many innovations have come up with a goal of improving healthcare. One such innovation is Amiko's Respiro smart inhaler for asthma management.

2.2.1. How it works

Respiro is a clinically approved and validated digital product that combines connected inhaler sensors, digital applications and Artificial Intelligence in respiratory treatment. Respiro's AI embedded sensor monitors keeps track of inhaler data use and generates personalized profiles to monitor progression of the disease. It then transfers the collected data to the users' mobile Application using Bluetooth technology. This mobile application is designed in such a way that it gives the patient coaching and support to improve compliance to the prescription. All the patient data collected by Respiro is stored on the cloud via an internet connection from the users' mobile phone. Through its Respiro Visual, medical personnel can remotely analyze patient information and in turn offer support and advice to their patients.

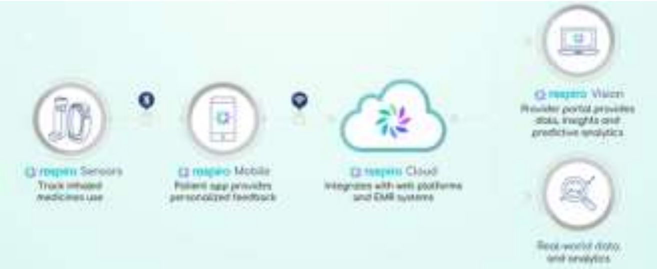
respiro Sensors
Track inhaled medicines use
respiro Mobile
Patient app provides personalized feedback
respiro Cloud
Integrates with web platforms and EMR systems
respiro Vision
Provider portal provides data, insights and predictive analytics
Real-world data and analytics

Figure 4. Respiro Smart Inhaler [13]

2.2.2. Vulnerability of Respiro Smart Inhaler

Vulnerabilities are loopholes in a system or its design that pave way for intruders to gain unauthorized access to data and information. Because of the sensitive nature of information involved in medical care, it will always be a prime target for attack. Reliance on the internet makes IoMT devices prone to attack by well-trained cyber criminals who for one reason or another seek to gain access to patient information.

Many of these devices are built with the end in mind which is end user satisfaction. Little attention is usually given to the security of the data that is being transferred across the network. Some of the vulnerabilities of Respiro if not all can be attributed to carelessness by the users as explained below.

Reliance Bluetooth technology: Well as Bluetooth technology offers a low energy and affordable solution for short range transmission, it has been found to have vulnerabilities over the years. None the less, Respiro employs this technology while transmitting data from the sensors to the mobile phone. Bluetooth technology has tremendously improved its security since it was first invented however new vulnerabilities keep on being exploited. A recent example is the KNOB attack as discussed by Daniel Antonioli, Nils Ole Tippenhauer and Kasper Ramussen [13]. This attack allows third parties to make two or more victims agree on an encryption key of only 8 bits which can easily be brute forced and hence giving away patient data to the attackers who can in turn use this data or manipulate it for their own selfish motives.

Weak password: Many devices are by default built with preset passwords and some users are lazy to change these passwords. This pauses a risk as many of these are easy to guess hence giving access to unauthorized hackers.

Unsecured network access: Respiro relies on the internet to transfer data from the mobile device to the cloud. Depending on the network service provider, some of the networks connected to by the customer are not secure and hence open the system to possible attack.

Unpatched software: In order for software developers to address issues identified in their software, new patches are constantly being developed. It is therefore up to the users to install these security patches or risk leaving their devices open to attack. Users of

Respiro should therefore ensure to always look out for updates of their mobile app to ensure that it is up to date.

Insecure Cloud Storage: Well as the cloud allows remote access to stored data, just like traditional data environments it is not immune to treats. The responsibility of managing this risk however falls on both the Cloud Service provider and the Cloud Consumer. The consumer needs to ensure that the CSP meets their security and privacy objective.

Lost device or Physical access: Respiro relies on a smart phone in order to access the Respiro Application. Access to the mobile phone through theft opens the system to hackers as they can bypass the phone passcode and have access to the mobile application.

3. Solutions to reduce vulnerability in Mobile Cardiac Telemetry and Respiro Smart Inhaler System

Although there is vulnerability, there is also a solution could prevent the vulnerability from being the pathway for hackers. There is no way of clearing the vulnerability, but these recommendations would be classified as a prevention from allowing hackers to discover it. If they success on discovering this recommendation could make things pretty hard. Under this section, I would give recommendation related to the four vulnerability that is related in section above.

Firstly, the recommendation for lack of authentication process would be password. This mean, in this internet era password is always a must for every internet of things. Having password would always keep the account or the data secured. They should upgrade the password in to encrypted form to give hard time for the hackers. These passwords will have to be redesign every six months one for a better security. This could be said as the basic prevention or recommendation that they could make in order to keep data locked. For instance, in order for the doctor to open the patient data the doctor will have to put in the encrypted password so that they could get access. Nowadays, people would say that password was the bad idea, but it has been a traditional activity which was being used in the late 90s. These activity was being placed as most preferable and hence these is why these device will need to have authentication password which will keep it secured.

Secondly, the recommendation for the software bug would be security patches. This means, every three to six months once there would be a security patch that would be recommended to cover any loophole that is developed by the hackers. These patches will cover up any weakness area that would be the vulnerability of the device. This security patches will need to be done so that it could be a prevention of any lack in the device. This is because, these patches would be like covering up a hole that has been dug by the hackers and this is a must so that there won’t be any weakness. Although this patch is not a permanent, but it could be a meanwhile time prevention, and this could keep it save till the next patch. Not updating the patches could give the hackers a pathway for the hackers to conduct their malware attack. For example, every three to six months once the Mobile Cardiac telemetry developer of the device will send the security patches from time to time and the patch would be sent off they detect any loophole the users will just need to click update without any delay to keep their device fully secured.

Next, the recommendation for access on external computer would be having the computer on a secured locked room. This means, having computer that allow doctor to access the devices on patient will have to be kept separated. This means, this computer should not be visible to public and they should be in a room that hold the servers and all. By doing this, it may prevent from the hackers to discover the location of the computer and it can be useful step as it could prevent them from getting the IP address of it to conduct the eavesdropping event. For instance, having the computer at public visibility the hackers could easily hack the computer physically and they could also get the IP Address of the computer and by getting the IP address they could exploit a backdoor to have the eavesdropping.

Lastly, the recommendation for security patches would be a proper awareness on the purpose of security patches. This means, nowadays the users of technology do not know the importance on having the security patch and this would educate the users and will allow them to learn the reason on having updates on security patches. For example, having news update on the social media regarding the importance of security patch and the impact of not updating the security patch could prevent from users getting their device compromised to the hackers.

4. Conclusions

Rick Martin has stated that there are three advantage of having Internet of Medical Things in healthcare [1]. Having these advantages would allow to attract or make Internet of Medical Things much more reliable and therefore it would be picked over traditional treatment.

Firstly, Internet of Medical Things makes accessibility much easier. This means, it allows the doctor to receive data of their patient from time to time without having them physically. This would save up more time for the doctor and also the patient. This is because, having Internet of Medical Things devices in a patient the doctor will get a time-to-time update on the patient health and the doctor does not need to have the patient In front of him to do any checkups to get the result. For instance, smart watches that helps to track the patients heartbeat rate pressure and more save their data and it will update the doctor's devices for them to look at the pattern of the rate and this indicate the patient does not need to be there for checkups as they are always being watched.

Next, they have low per-patient cost. This means, the cost on patient spending on their healthcare would be much lower. This because, most of them could now be under inpatient data and this is because the devices of Internet of Medical Things would update and the doctor and the nurse and the do not need the patient to be there and this would save up some cost for the patient and the doctor or nurse could do other important things. For instance, a patient will have to go monthly for a reading checkup whereby to take heartbeat rate, high blood pressure, and sugar level. This could be solved by having a smart watch or a smart lens that can take this reading and upload it to the cloud whereby the doctor or nurse can look at it without taking the reading physically.

Lastly, fast per-patient implementation. This means, it allows to be fast and easy to be implemented. This is a much needed as implementing a device consume longer time it would not be likely to be used by the users. This is because, the longer it takes the lower the possibility of people to use. Having a short time will make the user to pick it on using it. This will make the user to pick it and use it. This will also allow the doctors to get the result of the patient faster than usual waiting time. For instance, a smart watch is mush easy to be used and this will take fast data for the doctor on knowing their patient's data.

In a nutshell, we could say Internet on Medical Things would eliminate the traditional medical process and this would bring a whole new level of revolution on the medical field. The Mobile Cardiac Telemetry would be used by almost half of the world in future as this would be a safety step on taking care their heart's health. Although they have vulnerability, but the device would be still functioning. The Developer of this device will have to make a few changes and also authority will have to bring awareness on the security patch. By doing this it may allow the device to be secured and the data would be well protected.

According to Kacy Zurkus technology are moving into healthcare and this has made a growth on the cybersecurity risks on the connected devices [10]. This means, as the technology moves into the healthcare there is more cybersecurity risk as they may introduce many new threat actors to the users. Back in 2018 according to Jessica Davis there were a cyber-attack on the Med Associates which has brought an impact on 270,000 patient whereby their records were being extracted by the hackers [11]. In future cybersecurity would be a procurement process.

Nowadays most of the medical device manufacturer are working on the device security instead of working on new devices. By doing this it may keep the device fully secured. Hence, in future cybersecurity will be design in much better and stronger which will keep medical device much safer and stable. Not stopping there, in future medical device would be design with compliance cybersecurity to keep them secured.

References

[1] Martin, R., 2018. Internet of Medical Things (IoMT) – The Future of Healthcare. [Online] Availableat:https://igniteoutsourcing.com/healthcare/internet-of-medical-things-iomt-examples/[Accessed 26 February 2020].

[2] Arkenea, 2019. A Detailed Guide To IoMT Implementation in 2019. [Online] Availableat:https://arkenea.com/blog/iomt/ [Accessed 13 February 2020].

[3] Digirad, 2017. How do Mobile Cardiac Telemetry systems work?. [Online] Available at: https://www.digirad.com/mobile-cardiac-telemetry-systems-work/ [Accessed 27 February 2020].

[4] UnivDatos, 2018. GLOBAL MOBILE CARDIAC TELEMETRY DEVICES MARKET IS EXPECTED TO ATTAIN A MARKET SIZE OF US$ 1,264 MILLION BY 2025, GROWING AT A CAGR OF 12.34% DURING 2019-2025 PERIOD. [Online] Available at: https://univdatos.com/news/global-mobile-cardiac-telemetry-devices-market-is-expected-to-attain-a-market-size-of-usd-1264-million-by-2025
[Accessed 27 February 2020].

[5] Cardiab Nonitoring .com, 2020. Braemar. [Online] Available at: http://cardiacmonitoring.com/mobile-cardiac telemetry/companies/braemar/ [Accessed 27 February 2020].

[6] Jusak, 2016. Internet of Medical Things for Cardiac Monitoring: Paving the Way to 5G Mobile Networks. [Online] Available at: https://www.researchgate.net/figure/Diagram-block-of-the-IMedT-prototype_fig2_312044075 [Accessed 29 February 2020].

[7] Comodo, 2018. Computer Vulnerability: Definition. [Online] Available at: https://enterprise.comodo.com/blog/computer-vulnerability-definition/ [Accessed 28 February 2020].

[8] Collins, K., 2017. Pacemakers have thousands of vulnerabilities hackers can exploit, study finds. [Online] Available at: https://qz.com/997803/pacemakers-have-thousands-of-vulnerabilities-hackers-can-exploit-study-finds/ [Accessed 29 February 2020].

[9] J.Feder, B., 2018. A Heart Device Is Found Vulnerable to Hacker Attacks. [Online] Available at: https://www.nytimes.com/2008/03/12/business/12heart-web.html [Accessed 29 February 2020].

[10] Zurkus, K., 2019. What Does Healthcare Cybersecurity Look Like in a Future of Connected Medical Devices?. [Online] Available at: https://securityintelligence.com/what-does-healthcare-cybersecurity-look-like-in-a-future-of-connected-medical-devices/ [Accessed 29 February 2020].

[11] Davis, J., 2018. 270,000 patient records breached in Med Associates hack. [Online] Availableat:https://www.healthcareitnews.com/news/270000-patient-records-breached-med-associates-hack [Accessed 29 February 2020].

[12] Marr, B., 2018. https://www.marketwatch.com/press-release/internet-of-medical-things-market-2019-growth-at-a-cagr-of-244-expected-in-iomt-industry---09-sep-2019-2019-09-09. [Online] Available at: https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#31713c4d4a3c [Accessed 26 February 2020].

[13] Daniele Antonioli, N. O. T. K. R., 2019. The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Ne gotiation Of Bluetooth BR/EDR. Santa Clara, CA, USA, USENIX.

[14] Amiko. (n.d.). Amiko | Upgrading respiratory care. [online] Available at: https://amiko.io/ [Accessed 2 Mar. 2020].