12-2018

Security and Privacy of Wearable Internet of Medical Things: Stakeholders Perspective

Swapnika Reddy Putta
sputta@stcloudstate.edu

Security and Privacy of Wearable Internet of Medical Things: Stakeholders Perspective

by

Swapnika Reddy Putta

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

December, 2018

Starred Paper Committee:
Abdullah Abu Hussein, Chairperson
Lynn Collen
Balasubramanian Kasi

Abstract

Internet of medical things (IoMT) is a fast-emerging technology in healthcare with a lot of scope for security vulnerabilities. Like any other internet connected device, IoMT is not immune to breaches. These breaches can not only affect the functionality of the device but also impact the security and privacy (S&P) of the data. The impact of these breaches can be devastating as well as life-threatening. The proposed methodology used a stakeholder-centric approach to Improve security of wearable IoMT devices. The proposed methodology relies on a set of S&P attributes for wearable IoMTs that are identified to quantify security in these devices. Second, presented a method to quantify security in these devices. Finally, presented a case study to show how the proposed framework can be used to rank Wearable IoMTs in terms of S&P. This work aimed to (1) guide hesitant users when choosing a secure IoMT device, (2) encourage healthier competition among manufacturers of IoMT devices, and therefore, (3) improve the security of wearable IoMT devices.

Keywords: IoT (Internet of things), IoMT (Internet of Medical Things), Wearable devices, sensors, Security, Privacy, Healthcare, Stakeholder.

Table of Contents

Page

List of Table 5

List of Figures 6

Chapter

I. Introduction 7

Introduction 7

Problem Statement 7

Nature and Significance of the Problem 8

Objective of the Study 8

Definition of Terms 8

Summary 9

II. Background and Review of Literature 10

Introduction 10

Background Related to the Problem 10

Literature Related to the Problem 13

Literature Related to the Methodology 25

Summary 31

III. Methodology 32

Introduction 32

Design of the Study 32

Data Collection 32

Chapter Page

Summary 35

IV. Data Presentation and Analysis 36

Introduction.. 36

Data Presentation 36

Data Analysis 52

Summary 54

V. Results, Conclusion, and Recommendations 55

Introduction 55

Results 55

Conclusion 61

Future Work 62

References 63

Appendix 69

List of Table

Table Page

1. Stakeholder-Centric Approach 53

List of Figures

Figure Page

1. IOT devices 11

2. IOT architecture 12

3. Internet of medical things architecture 16

4. Organizations in healthcare compromised 17

5. Typical architecture of wireless sensor networks in healthcare applications 20

6. Wearable internet of medical things 20

7. IOT and the security and privacy issue 22

8. Device map of the fuelband 23

9. Social Sensor Network (SSN) illustration 24

10. Fitbit system components 24

11. Fitbit service logs 25

12. The life cycle of data and processing 26

13. e-health security domain touch points 27

14. The connected world of translational research in medicine 28

15. Medical services with MobiCare 30

16. Architecture of a wearable health monitoring system 31

17. Attributes and considerations 34

18. Comparison of two wearable IOMT devices 59

19. Comparison of a doctor and a patient for Dexcom g5 60

20. Comparison of a doctor and a patient for MiniMed 530G 61

Chapter I: Introduction

Introduction

The emergence of medical devices has transformed the face of healthcare. Instead of a regular visit to a hospital, monitoring our own health is at our fingertips now. Though this radical change is very much appreciated we need to take a step back to review the security of such devices.

Security and privacy of these devices is at risk. The consequences are very dire when it comes to security of medical devices as many patient's lives depend on proper functioning of these devices. So, security in healthcare is of utmost importance.

Wearable Internet of medical things are smart electronic devices that can be worn on the body to improve patient's quality of health. These devices can track nearly everything–physical activity, temperature, glucose, sleep, heart rate and much more. These devices are available from head to toe in many forms such as smart wristbands, watches, eyeglasses, belts, necklaces, patches.

Wearable systems incorporate sensors, memory, solar cells and batteries. They help in data collection, display, and wireless transmission of the data collected. These devices can monitor the health signs of the patients/users and send them directly to the physicians to cut down a personal visit.

Problem Statement

The use of wearable Internet of Medical Things is increasing year by year (Markets, 2017). The global wearable medical device market is expected to reach an estimated $9.4 billion by 2022. While all the technological advancements made in wearable Internet of Medical

Things, the S&P of these devices is often overlooked by both the users and manufacturers. while shopping for the wearable Internet of Medical Things, customers often focus on the design, price and performance of these devices. This is because customers are unable to choose or rank these devices in terms of security and privacy. Also, different stakeholders have different objectives and tolerance to risk.

Nature and Significance of the Problem

This project helps hesitant users to choose a better secure wearable IoMT (Internet of medical things) device. This project also encourages healthier competition among manufacturers of wearable IoMT devices. And this project helps to improve the security of wearable IoMT devices.

Objective of the Study

The objective of the study is to guide hesitant users when choosing a secure wearable IoMT device in terms of Security and Privacy. This study helps the user to choose a better secure device.

Definition of Terms

IOT–Internet of Things

IOMT–Internet of Medical Things

S&P–Security and Privacy

HIPAA–Health Insurance and Accountability Act

DDOS–Distributed Denial of Service

Summary

Introduction about IOMT and wearable devices, problem statement, nature and significance of the problem and definition of terms were discussed in this chapter.

Chapter II: Background and Review of Literature

Introduction

This chapter covers background to the problem, introduction, and challenges of IOT, IOMT and wearable IOMT devices.

Background Related to the Problem

The internet is a massive global network that can be used to communicate with each other. It can be used to send emails, instant messages and share data. The data is sent from client devices like laptop, PC or smartphones and it go to the servers and the servers analyze or transmit the data further. The internet is made of up three major actors the people, client device and a server. But the new thing that is being added to the internet is Internet of Things (IOT). An Internet of thing is any smart device that has a sensor and/actuators attached to it. The sensor collects the data and sends it to the cloud for further analysis. The data analyzed can be used to make decisions. A “smart device” is any electronic device that can take its own decisions. A “sensor” is a small chip that senses the data and an “actuator” is another small chip that responds to the sensed data. Example of such devices include smart phones, smart tv, smart air conditioner, smart car, etc.

Internet of things is a system of systems. All the electronic devices are connected to each other forming a system and further these systems will be connected to each other forming a bigger network system (How IoT works–An overview of the technology architecture, 2015). There are four building blocks of IOT.

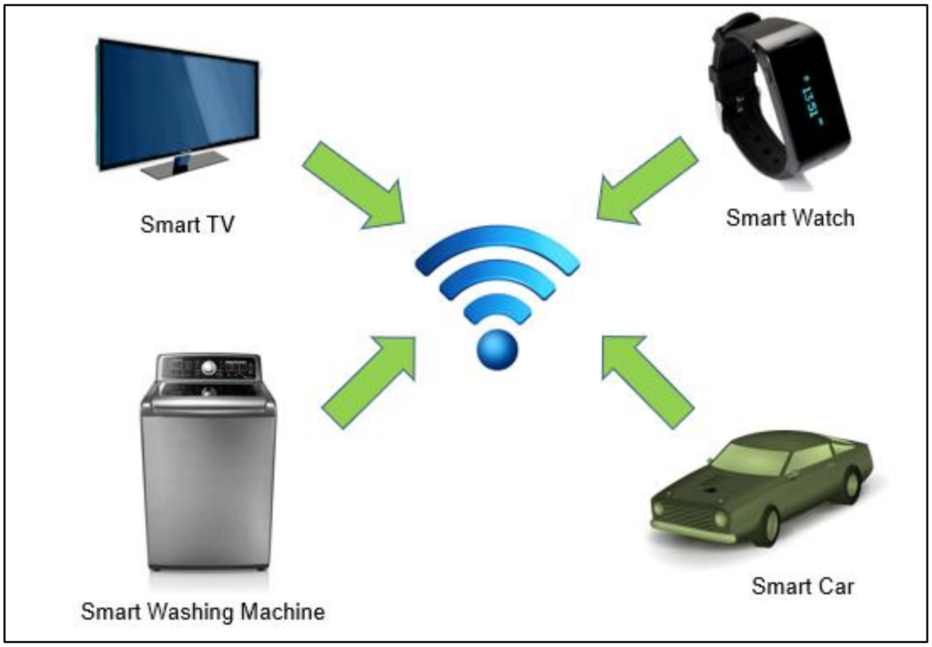


Figure 1: IOT devices.

End devices/nodes: This is an essential part of the IOT. This is the “T” or “Things” in the IOT. These are active sensing devices and actuator collects data and perform ground level processing. Examples can be temperature sensors at home, cameras at highways, etc.

Gateways/local processing nodes: These connect the end nodes to the network or cloud. Some gateways only transfer the data to internet that is collected from the sensors, but some gateways also process the data to some extent and then forward the relevant data to cloud for making predictions. It also provides the intelligence to the end nodes by sending back the data received from the applications or cloud.

Connectivity: As IOT is a networked system, connectivity is an essential part. Service providers are providing many solutions around IOT to connect the End nodes to the gateways and gateways to the cloud. As this is a duplex system, which means the communication flows to and from between the application and hardware. Data or the signal also flows in reverse. Connectivity can be a wireless or a wired mechanism. Example Bluetooth, Wi-Fi, ZigBee, etc.

Cloud-based application and storage: The cloud or cloud-based application is used to compute the collected data, analyze it and then make predictions. The predictions made can be sent back to the sensors and node and can also be sent to the business application for continuous improvement. These applications also store the collected data and can be easily accessible from anywhere at any time.

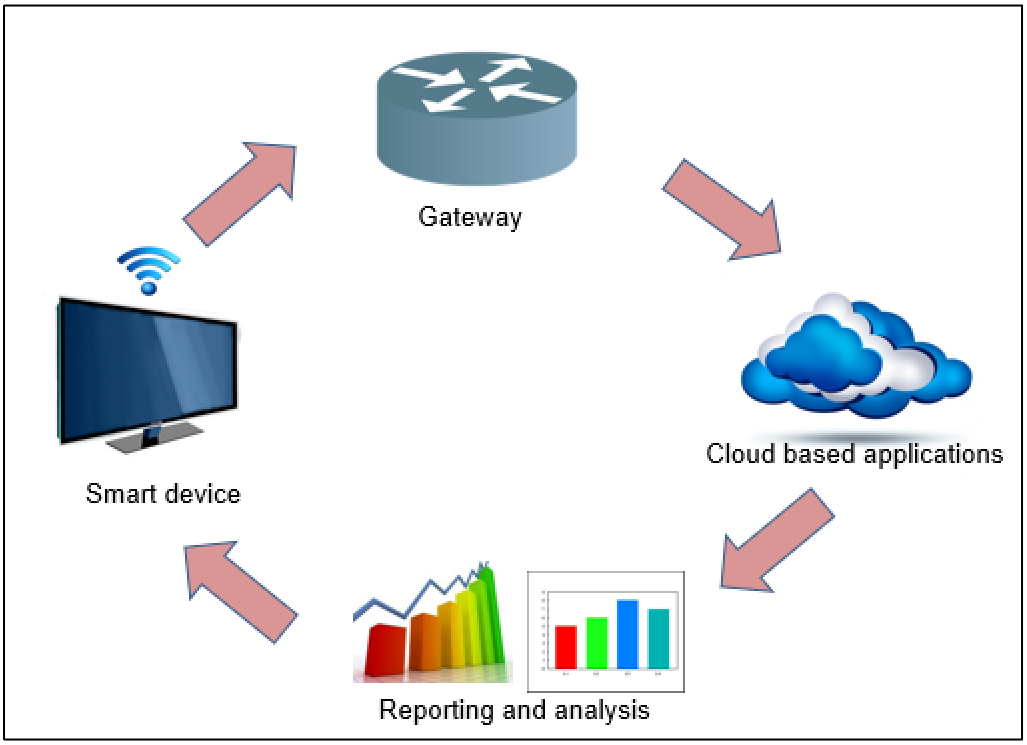


Figure 2: IOT architecture.

Challenges of IOT: There are several challenges for internet of things. The main technical challenge in IOT devices is collecting and sending data. The challenges can also be hardware and software issues. According to ISOC (Internet Security Operations Center), the top five challenges of IOT include Security, Privacy, Standards, Regulations, Development (Challenges in the internet of things | TI.com, n.d.). Other challenges include Sensing a complex environment, connectivity, power, complexity.

Literature Related to the Problem

Security and privacy issues of IOT devices: In "Security and Privacy Issues in IOT" explains clearly about the security and privacy of IOT devices. According to this paper, Authentication, Identification and device heterogeneity are the major security and privacy issues in IOT. Also, the major challenges about IOT devices include integration, scalability, ethics communication mechanism, business models and surveillance (Rehman, Rehman, Khan, Moiz, & Hasan, 2016). This paper explains about the security and privacy issues of IOT devices (Ankitha & Balajee, 2016). The authors of this paper analyzed about the privacy issues of their proposed model by referring to the five-Dimensional model. The five-Dimensional model for privacy include Identity privacy, Query privacy, Location privacy, Footprint privacy and Owner privacy (Puraskar, 2016). This paper clearly explains about the overview and background of IOT devices. Explaining about the IOT protocol stack, this paper explained about the applications of IOT in different fields like medical applications, smart homes, Intelligent community security system. After explaining about IOT and its applications, the authors also explained about the security and privacy of IOTs. Security concerns of IOT are Front-end sensors and equipment, network, Back-end of IT systems. Privacy concerns of IOTs are privacy in device, privacy during communications and privacy at processing.

This paper explains about IOT, security threats of IOT and some open challenges in the domain of IOT (Abomhara & Køien, 2014). This paper also discusses about the security requirements for the current IOT technologies. This paper explains about the challenges of IOT devices (Jing, Vasilakos, Wan, Lu, & Qiu, 2014). The authors also explained about the three layers of IOT which include perception layer, transportation layer and application layer and also focused on the security problems of each layer. This paper also analyzed the cross-layer heterogeneous integration issues, security issues, and discussed the solutions to them. A paper on "Survey on Security and Privacy Issues in Internet-of-Things" contains four segments. In the first segment, the authors explained about the limitations of IOT devices and their solutions. In the second segment, they focused on the classification of IOT attacks. In the third segment they presented the mechanisms and architecture for authentication and access control. In the last segments, the authors analyzed the security issues in different layers of IOT (Yang, Wu, Yin, Li, Zhao, 2017).

The paper "Review on security and privacy concerns in Internet of Things" focused on common IOT vulnerabilities like Distributed Denial of service (DDOS) and attacks concerning integrity of data like data modification attacks. This paper explains about the security and privacy problems in different areas like web interface vulnerabilities, device connections, spamming, data storage issues, IOT network related problems like Sybil attacks, cloud connectivity considerations and industrial IOT attacks (Kumar, Madhuri, & ChanneGowda, 2017). "Security for the Internet of Things: A survey of Existing Protocols and Open Research Issues" analyzes the existing protocols and mechanisms to secure communications in the IOT. The authors also explained about the existing approaches to ensure fundamental security requirements to protect communications on IOT (Granjal, Monteiro, & Silva, 2015). "This paper gives an introduction to Industrial IoT systems, the related security and privacy challenges, and an outlook on possible solutions towards a holistic security framework for Industrial IoT systems" (Sadeghi, Wachsmann, & Waidner, 2015). This paper also lists the attributes that increases the attack surfaces in internet of things mentioning the attacks that are targeting internet of things. Despite explaining about the security and privacy issues in internet of things, this paper does not focus on medical IOT devices (Abdur, Habib, Ali, Ullah, 2017). This paper focuses mainly on Security issues in the Internet of things. This paper clearly explains the threats in IOT devices. The authors categorized the attacks as low level, medium level, high level, and extremely high-level attacks. They also mentioned the nature and behavior of the attacks and mentioned some countermeasures to those attacks. The authors also suggested that considering the threats in IOT devices, it is important to have security mechanisms in these devices.

Internet of Medical Things (IOMT): Internet of medical things means connecting different things to different people within a healthcare organization or across the healthcare ecosystem to acquire aggregate and analyze data in order to glean IOT actionable insights. The more common use cases in healthcare involve connecting people, consumers, clinicians and caregivers. Healthcare organizations have piloted many connected health projects mainly aiming at consumer engagement. The ability to connect consumers and patients and affect their behavior will encourage them to make healthier decisions, which in turn will lead to better outcomes and lower healthcare costs. Monitoring to consumers vital signs and activity and thus holding them accountable for healthcare decisions will help further drive compliance. Across the globe, there is an evolving focus on improving the health of the population to control healthcare costs. A stronger focus on consumer engagements and innovative approaches to integrate IOT based health care into new care delivery models is encouraging the adoption of connected health technology.

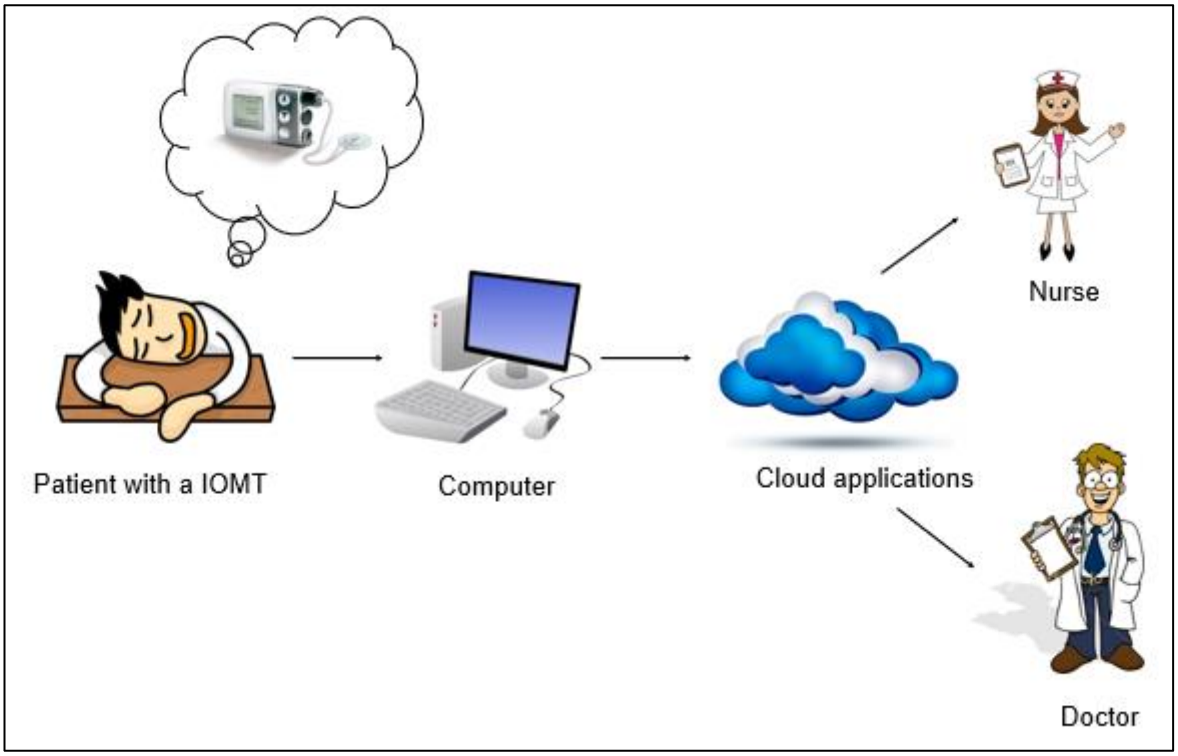


Figure 3: Internet of medical things architecture.

Security and privacy issues of Internet of Medical Things (IOMT): The three challenges for medical device manufacturers in 2017 are security, compliance and cost of product development (Khandelwal, 2017). Medical devices like pacemakers, insulin pumps, and the signal between the pacemaker-defibrillator and the programmer are vulnerable. These vulnerabilities can be life threatening. People rely on pacemakers to keep their heart running but researchers discovered over 8600 vulnerabilities in pacemakers (Peck, 2011). In August 2011 on “Black Hat Technical Security conference” stage, Las Vegas a person named Jerome Radcliffe successfully hacked into an insulin pump that was attached to his abdomen and completely disabled it. Radcliffe was a diabetic and this pump was part of an insulin delivery system that was intended to keep in alive by monitoring and stabilizing his blood glucose levels. This on-stage demonstration has reopened the debate on the safety of wearable medical devices and whether the manufactures of such medical devices are taking necessary steps to avoid such attacks (Filkins, 2014). Healthcare cyber threat report by SANS shows that healthcare is the prime target for cyber-attacks. Figure 4 shows 72% of the organizations compromised in healthcare are medical devices providers.

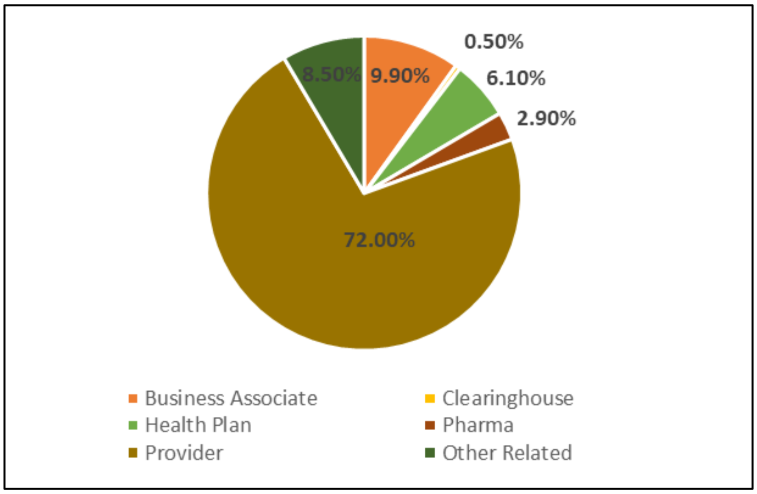


Figure 4: Organizations in healthcare compromised.

In May 2017, a ransomware called WannaCry shutdown 65 hospitals in the United Kingdom. This cyber-attack not only affected computers in the hospitals but also affected the storage refrigerators and MRI machines (Fears of hackers targeting US hospitals, medical devices for cyber attacks - *ABC News*, 2017).

In "The Internet of Things for Health Care: A Comprehensive Survey" (Islam, Kwak, Kabir, Hossain, & Kwak, 2015) surveyed diverse aspects of IoT-based healthcare technologies. The paper Classified medical devices and smartphone health apps by their functionality and discussed generic IoT healthcare challenges (Islam et al., 2015). In the Survey of Security and Privacy Issues of Internet of Things (2015) spoke about a general survey of all the security issues involved in IoT (Borgohain et al., 2015). The paper gives a basic understanding of security issues in IoT and is not specific to Healthcare. They mentioned only high-level attacks. They also mentioned some of the security and privacy issues in internet connected wearable health monitoring devices as clear text login information and clear text HTTP data processing. This means that most of the health monitoring wearable devices have login in clear text and the passwords of these devices are recorded in logfiles as plaintext. The data transmitted between different domains is sent as plain text and no security measures are used like encryption while transmitting the data. The Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey (2012) discuss the overview of IoT architecture and propose classification and security requirements of IoT devices. This paper discussed IoT layers, components and communication technologies. This paper concentrated only on IoT devices for disabled users. Security requirements in this paper were proposed with no evaluation methods (AL-Mawee, 2015.).

Dehling, Gao, Schneider, and Sunyaev (2015) mentioned information security and privacy of mobile health apps on IOS and android. “Various kinds of mHealth apps collect and offer critical, sensitive, private medical information, calling for a special focus on information security and privacy of mHealth apps”. The results of this paper show that 95.63% of applications are vulnerable to some damage through information security and privacy aspects. Most of the data in apps are stored in cloud or the application storage database. The security and privacy of the patient data is highly at risk stored in the medical health applications (Ameen, Liu,

& Kwak, 2012). The paper “Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications” is focused on the wireless sensor networks (WSN) in healthcare applications. The authors explained about the sensors in wireless network and how they collect data from the patients. This paper also mentioned about the security and privacy issues of these applications. The authors mentioned that public should be made aware of these issues and government agencies, research institutes and manufacturers need to overcome these obstacles to have a smooth implementation. Figure 5 shows the typical architecture of wireless sensor networks in healthcare applications. It shows how the wireless network communicate through the internet. Date collected by the sensors is sent wirelessly to the gateway. The gateway then sends the data to the cloud network or directly to the server. The data then is stored in the database and can be accessed be anyone at any time through the internet.

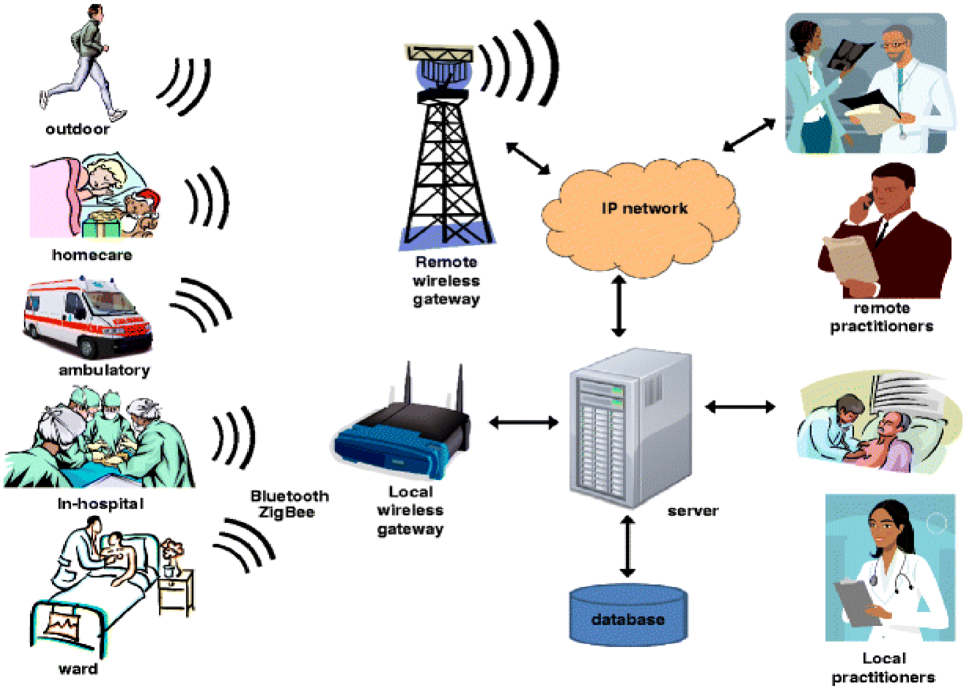


Figure 5: Typical architecture of wireless sensor networks in healthcare applications (Ameen et al., 2012).

Wearable internet of medical things:

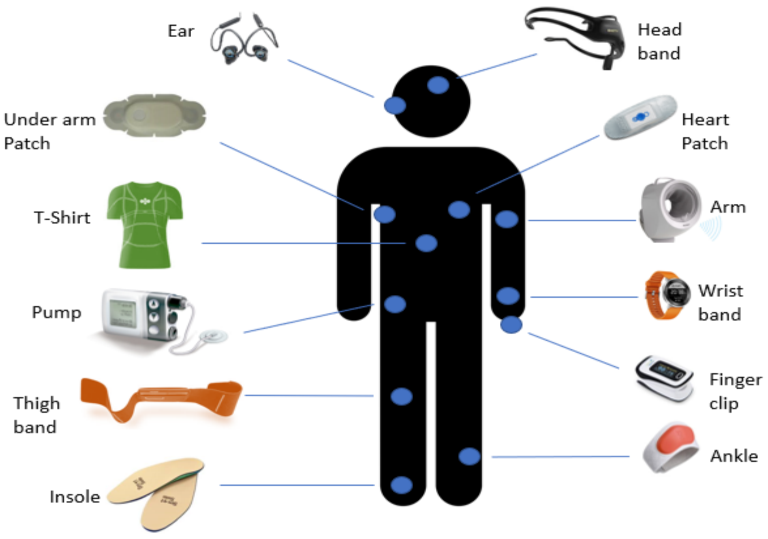


Figure 6: Wearable internet of medical things.

Blood pressure monitoring systems, e.g., Withings

- Sleep monitoring systems, e.g., Pebble time
- Brain activity monitoring systems, e.g., Muse
- Temperature monitoring systems, e.g., Temptraq
- Pulse monitoring systems E.g. Wahoo device
- Daily physical activities monitor, e.g., Fitbit
- Heart electrical monitor, e.g., EKG an electrocardiogram
- Cardiac fitness monitor, e.g., Tinke
- Stress level monitor, e.g., Pip device
- Insulin pump, e.g., Animas Vibe

Challenges of wearable IOMT:

- If a device is lost or misplaced, anyone can access the information stored locally

- Wireless transmission of data
- Data transfer between the parties can be intercepted by hackers
- They tend to be small and more discreet, which makes it easier to steal sensitive data
- They are connected to smartphones and can be infected with virus

Security and privacy issues of wearable internet of medical things: On average, amount of Patient-generated Health Data (PGHD) collected using wearables is ~310 MB per person annually. For 100,000 patients, the total sum will be ~31 TB per year. Taking into account heavy use of wearables in healthcare, the amount of patient data will only grow (Altoros Offices, n.d.; Zhou & Piramuthu, 2014.) This paper discusses about the security and privacy vulnerabilities in fitness tracking wearable devices. “The necessity of security and privacy in internet connected devices signifies that more sensitive information that occurs in IoT communications should be categorized, managed, and protected with high priority.” The figure below clearly shows that the privacy information from the user data is being transmitted by the internet. Most of the wearable devices are with the technology of automation. The process of automating the data increases the deal of convenience but also keeps the data at risk.

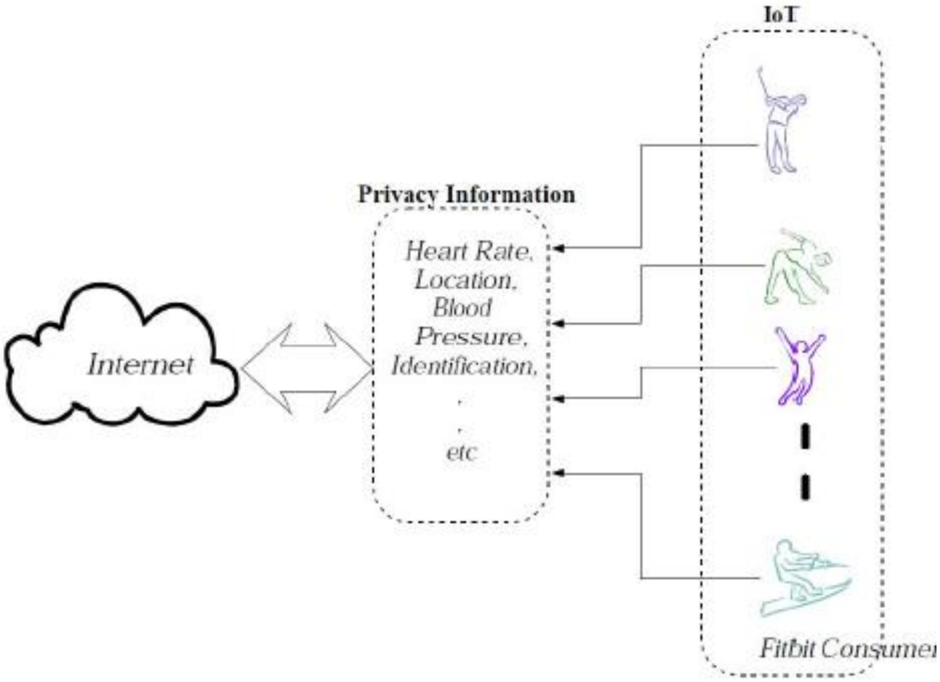


Figure 7: IOT and the security and privacy issue (Zhou & Piramuthu, 2014).

(Hiremath, Yang, and Mankodiya (2014) in their paper focused on conceptualizing wearable internet of medical things in terms of their design, function and applications. They also identified & discussed building blocks of wearable internet of medical devices that are key to its future success in healthcare domain applications. They presented a new system science for wearable internet of medical devices suggesting future directions which include operational and physical aspects. The paper “Privacy and Security in Internet of Things and Wearable Devices” concentrates on design flow of IOT and wearable devices and their security and privacy implications. The authors selected Google Nest Thermostat and Nike+ Fuelband as examples and discussed the consequences of user’s security and privacy of these devices and also explained how enhancements through security mechanisms can be added to these devices effectively (Arias, Wurm, Hoang, & Jin, 2015).

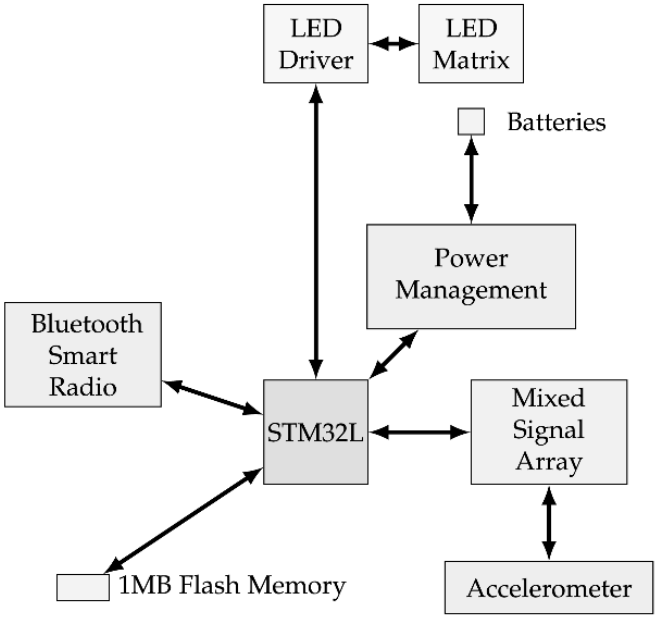
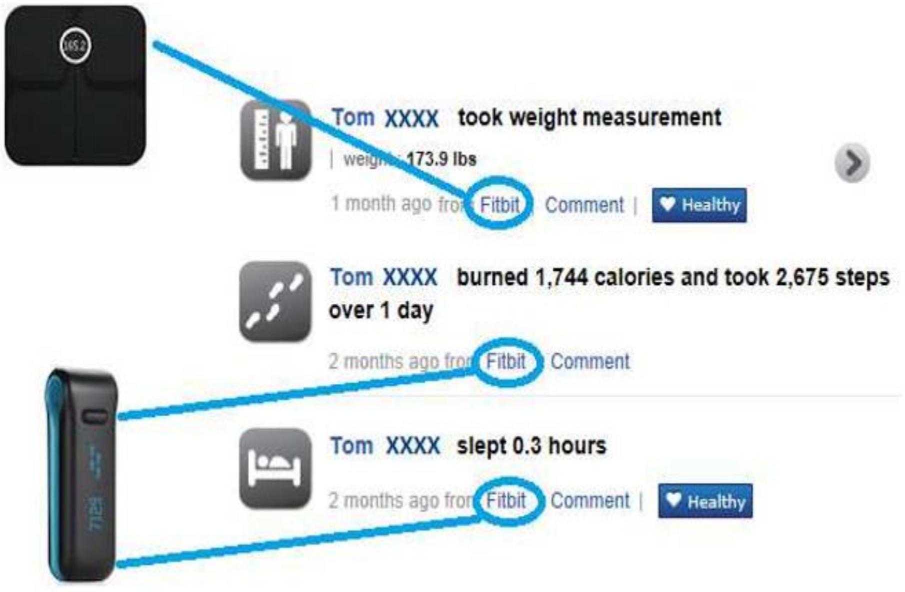


Figure 8: Device map of the fuelband (Arias et al., 2015).

In Rahman, Carbunar, and Banik's (2016) paper authors identified several vulnerabilities in fitbit by reverse engineering the communication protocol, storage details, operation codes and also mentioned about the security and privacy concerns in sharing health data in the social networks. “We have built FitBite, a suite of tools that exploit these vulnerabilities to launch a wide range of attacks against Fitbit. Besides eavesdropping, injection and denial of service, several attacks can lead to rewards and financial gains. We have built FitLock, a lightweight defense system that protects Fitbit while imposing only a small overhead.”



Tom XXXX took weight measurement

| weight: 173.9 lbs

1 month ago from Fitbit Comment | ♥ Healthy

Tom XXXX burned 1,744 calories and took 2,675 steps over 1 day

2 months ago from Fitbit Comment

Tom XXXX slept 0.3 hours

2 months ago from Fitbit Comment | ♥ Healthy

Figure 9: Social Sensor Network (SSN) illustration (Rahman et al., 2016).

The illustration of Social sensor networks is in fig. Health sensor devices like fitbit and the corresponding data of the user are reported, displayed and shared in social networks. The user’s last name is anonymized. The social networks cannot be used only to share personal details like location, status, etc. but can also be used to share health related data.

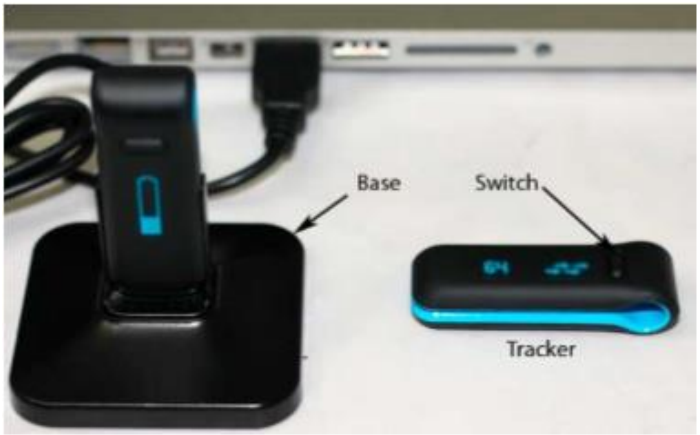
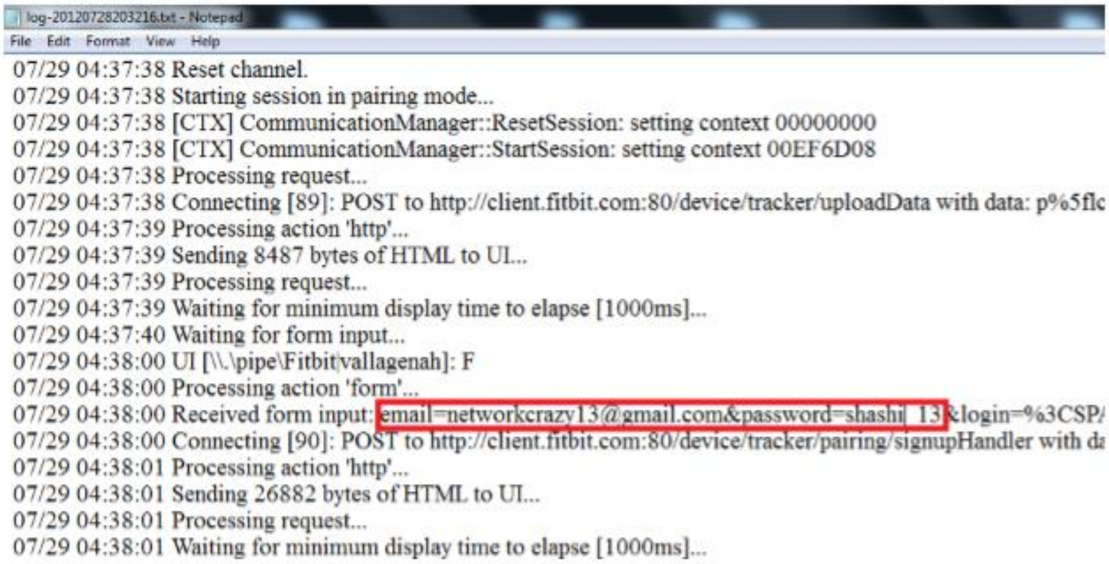


Figure 10: Fitbit system components (Rahman et al., 2016).

Figure 10 shows the components of fitbit tracker. A fitbit tracker is used to monitor daily physical activity like the distance travelled, footsteps covered, stairs climbed, calories burnt etc. It consists of trackers, the base, and a user laptop. Base is used to mount the tracker. Tracker has a switch that is used to display the fitness data of the user. The user laptop is used to retrieve the data from the tracker and store the data.



```
07/29 04:37:38 Reset channel.
07/29 04:37:38 Starting session in pairing mode...
07/29 04:37:38 [CTX] CommunicationManager::ResetSession: setting context 00000000
07/29 04:37:38 [CTX] CommunicationManager::StartSession: setting context 00EF6D08
07/29 04:37:38 Processing request...
07/29 04:37:38 Connecting [89]: POST to http://client.fitbit.com:80/device/tracker/uploadData with data: p%5flc
07/29 04:37:39 Processing action 'http'...
07/29 04:37:39 Sending 8487 bytes of HTML to UI...
07/29 04:37:39 Processing request...
07/29 04:37:39 Waiting for minimum display time to elapse [1000ms]...
07/29 04:37:40 Waiting for form input...
07/29 04:38:00 UI [\\.\pipe\Fitbit|vallagenah]: F
07/29 04:38:00 Processing action 'form'...
07/29 04:38:00 Received form input: email=networkcrazy13@gmail.com&password=shashi| 13&login=%3CSP/
07/29 04:38:00 Connecting [90]: POST to http://client.fitbit.com:80/device/tracker/pairing/signupHandler with da
07/29 04:38:01 Processing action 'http'...
07/29 04:38:01 Sending 26882 bytes of HTML to UI...
07/29 04:38:01 Processing request...
07/29 04:38:01 Waiting for minimum display time to elapse [1000ms]...
```

Figure 11: Fitbit service logs (Rahman et al., 2016).

Figure 11 shows the service logs of fitbit. The highlighted text shows that the login credentials are sent in plain text which contains Account id and password. This is the request sent from the base to the web server.

Literature Related to the Methodology

Lake, Milito, Morrow, and Vargheese's (2014) paper explains that security and privacy is the major problem that is to be overcome by the internet of things in healthcare. This paper proposed a secure architecture framework for IOT in healthcare.

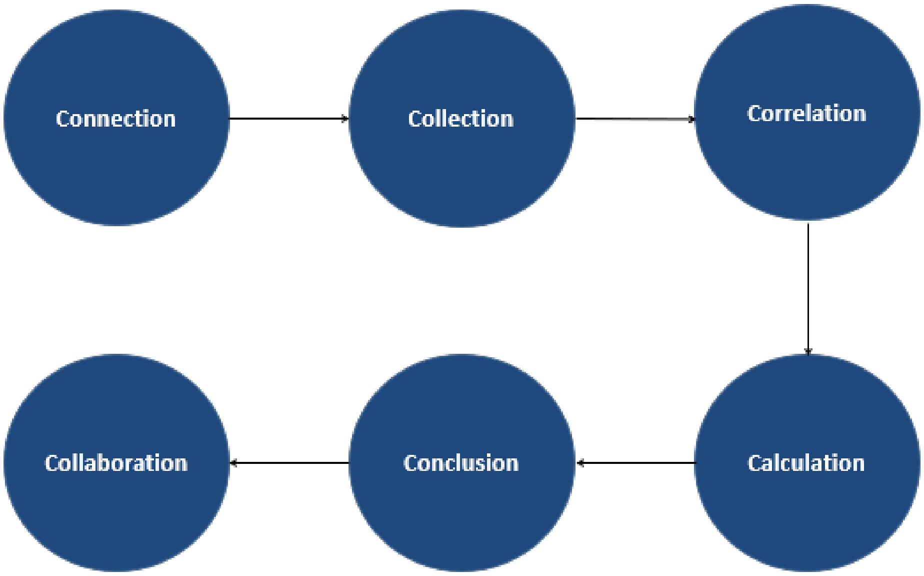


Figure 12: The life cycle of data and processing (Lake et al., 2014).

The authors explained the life cycle of device data. Fig shows the life cycle of data and processing which can be summarized using 6 C's. Connection is related to how the device is connected. Collection is related to how data is collected by the sensor from the body. Correlation is related to mapping the data to a context to create meaningful data that can be used to make decisions. Calculation is related to making a decision based on the data that has been filtered through an algorithm. Conclusion is related to taking appropriate actions. The action can be anything like ignoring or to escalate. Collaboration is related to collaborating the patient and the care teams. Data can be used in different domains for different purposes. The security at each domain is at risk. This paper also discussed about a security architecture for e-health. They used different sections in the architecture and evaluated the security challenges of each domain.

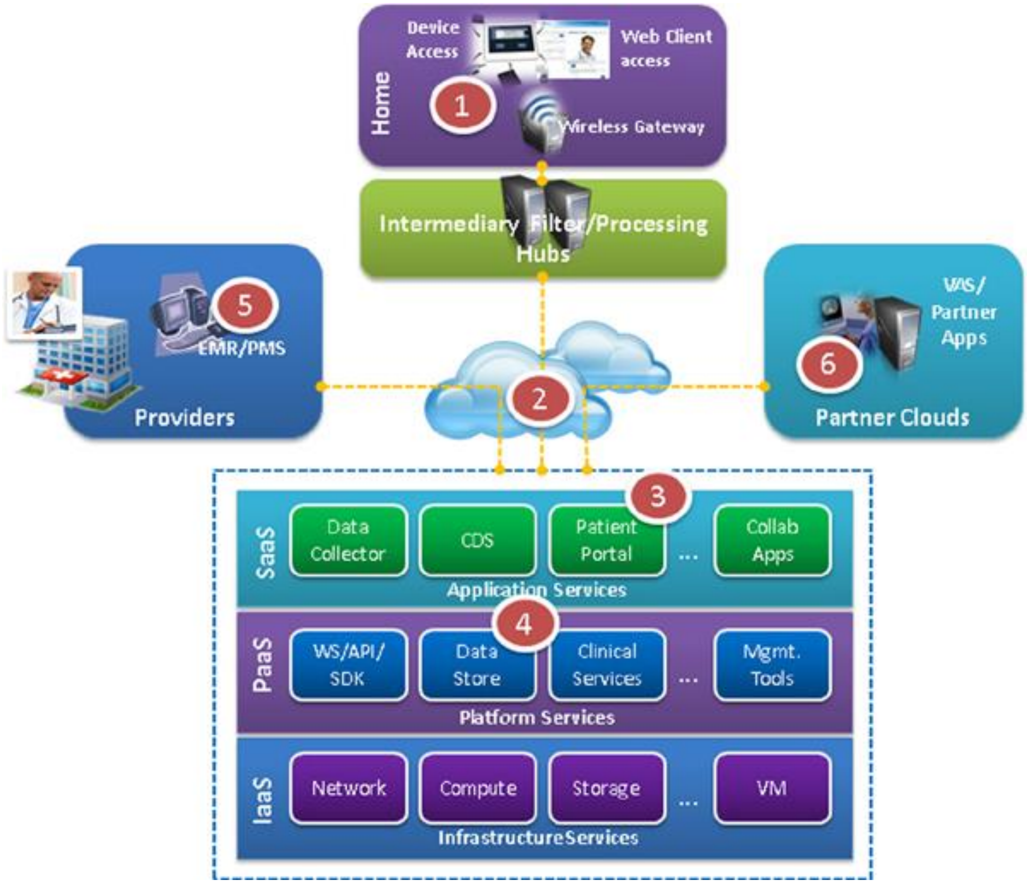


Figure 13: e-health security domain touch points (Lake et al., 2014).

Figure 13 shows the risk points that are to be considered. The main domains include end points and access, cloud services, partners and providers. This paper also briefly explained about the security issues in device design and its use. This paper explained about the security issues in terms of IOT in Healthcare. This paper is not specific to wearable devices.

Filkins et al. (2016) paper explains about the situation of security and privacy of healthcare data. The authors explained about the security and privacy concerns in the digital health era, and also discussed the tools and techniques that are available to help reduce the risk. The authors explained about the data at various levels across various platforms as shown in Figure 14.

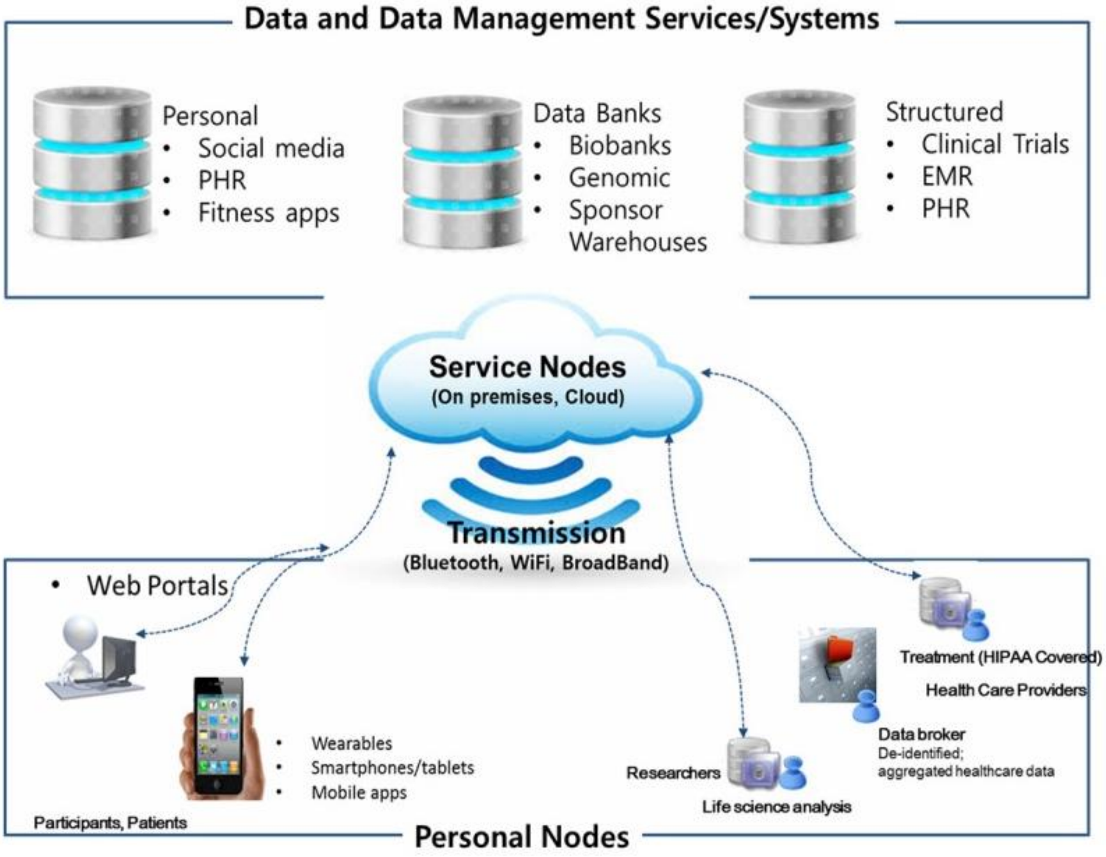


Figure 14: The connected world of translational research in medicine (Filkins et al., 2016).

There are three layers for patient data. The first layer is personal node where the patient, researchers, healthcare providers, doctors, nurses are the users. The second layer is the communication channel where the data is being transmitted to different platforms through different protocols. These protocols can be Bluetooth, Wi-Fi, Broadband, etc. The third layer is the service node which includes the interfaces where the patient’s data is stored. Although the authors discussed about the security and privacy concerns in digital healthcare, the issues that they discussed are very general to all IOT devices like Man in the middle attack, Phishing attacks, communication through SSL etc. and not specific to wearable internet of medical things.

Seneviratne et al.'s (2017) paper is “A survey on Wearable Devices and Challenges”. The authors of this paper surveyed more than 100 commercial products and classified them based on their functionalities and wearing modes. This survey showed that there are communication security issues for wearable devices and discussed various approaches to address them. This survey also included wearable computing topics such as offloading and in-device machine learning. This paper only concentrated on communication issues. Apart from the communication security issues there are many security problems on wearable medical internet of medical things which need a serious attention. Chakravorty's (2006) paper is about a programmable service architecture for mobile medical care. This project helps to reduce medical costs and improve quality of patient care. The author (Chakravorty, 2006, p. 1) “introduces MobiCare–a novel service architecture that enables a wide range of health-related services for efficient and mobile patient care. These services include: (1) health-related services in medical devices and sensors to remotely install, self-activate, reconfigure or even self-repair with new health services and applications, (2) secure and reliable dynamic software upgrade or update services applied to the native code of the clinical device, and, (3) remote registration and (re)configuration of body sensors as well as remote health-data services such as patient health report downloads and diagnosis data uploads with provider servers”. Figure 15 shows the MobiCare architecture. The author considered all the clinical sensors in the patient’s body as Body sensor network. The data collected by the sensors from the patient’s body is sent to the MobiCare client. From this MobiCare client, data is sent to the MobiCare server through a cellular link. Though the author tried to improve the patient’s quality of life with this project, this is only focused on the mobile care. This project cannot be used by the stakeholders to improve the security of the device itself.

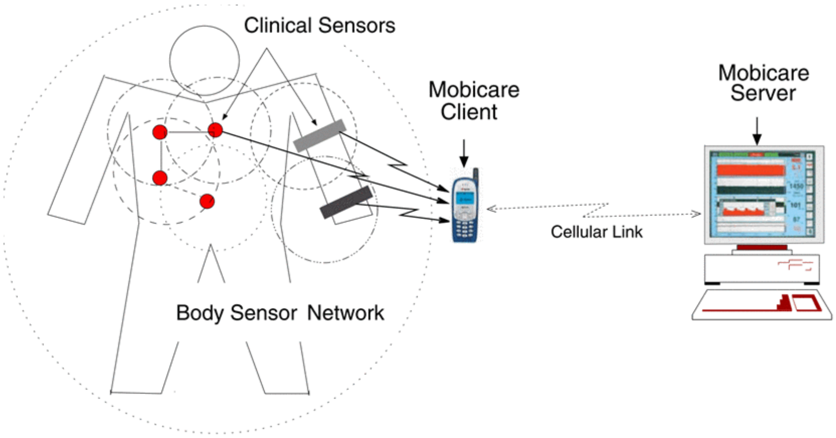


Figure 15: Medical services with MobiCare (Chakravorty, 2006).

Pantelopoulos and Bourbakis' (2010) paper helps to understand about the architecture of biosensor wearable systems. This paper also compared various system implementations to identify the shortcomings of current wearable biosensor solutions. Figure 16 shows the architecture of a wearable health monitoring system. The data from the patients is collected by the biosensors in the device and the data from all the sensors is sent to the Central Node through wireless or wired communication. In the Central Node, a Central Processing Unit is used to do all the processing of the data collected and then the data can be sent to other applications through a wireless transmission.

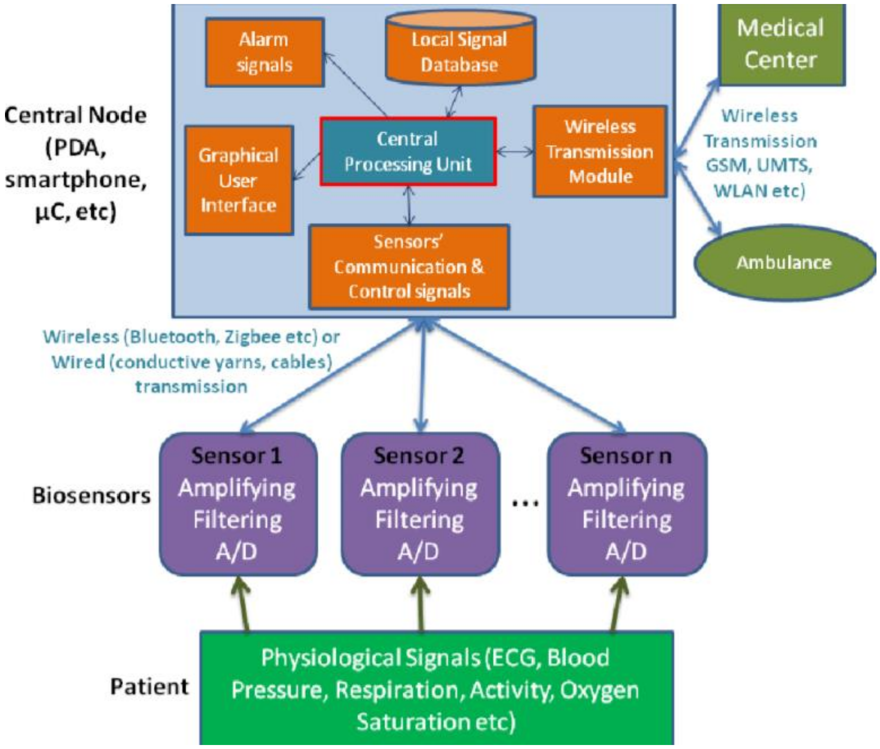

Alarm signals
Local Signal Database
Medical Center
Central Node (PDA, smartphone, µC, etc)
Graphical User Interface
Central Processing Unit
Wireless Transmission Module
Wireless Transmission GSM, UMTS, WLAN etc)
Sensors' Communication & Control signals
Ambulance
Wireless (Bluetooth, Zigbee etc) or Wired (conductive yarns, cables) transmission
Biosensors
Sensor 1 Amplifying Filtering A/D
Sensor 2 Amplifying Filtering A/D
...
Sensor n Amplifying Filtering A/D
Patient
Physiological Signals (ECG, Blood Pressure, Respiration, Activity, Oxygen Saturation etc)

Figure 16: Architecture of a wearable health monitoring system
(Pantelopoulos & Bourbakis, 2010).

Although this paper explained about the architecture of wearable health monitoring systems, the authors did not propose any methodology to secure these devices.

To the best of my knowledge, there is no research published that is related to security and privacy of wearable internet of medical things from stakeholder's perspective. All the papers in this section helped me to get an overview of the architecture of these devices, how these devices communicate and the security and privacy issues of these devices.

Summary

Chapter II covered the background, challenges, and literature review related to IOT, IOMT and Wearable IOMT. The next chapter covers about the methodology to solve the problem.

Chapter III: Methodology

Introduction

This section covers the approach and plan used to evaluate the study.

Design of the Study

The main goal of the study is to guide hesitant users when choosing a secure wearable internet connected medical device (IOMT), encourage healthier competition among manufacturers of IOMT devices and therefore improve the security of wearable IOMT devices. MCDM (Multiple Criteria Decision Making) approach was used in this study. MCDM is a qualitative approach, which considers multiple conflicting criteria for decision-making. The focus of this paper involves evaluating existing medical devices security, provide an understanding of underlying reasons, educate and propose solutions from a stakeholder's perspective.

Data Collection

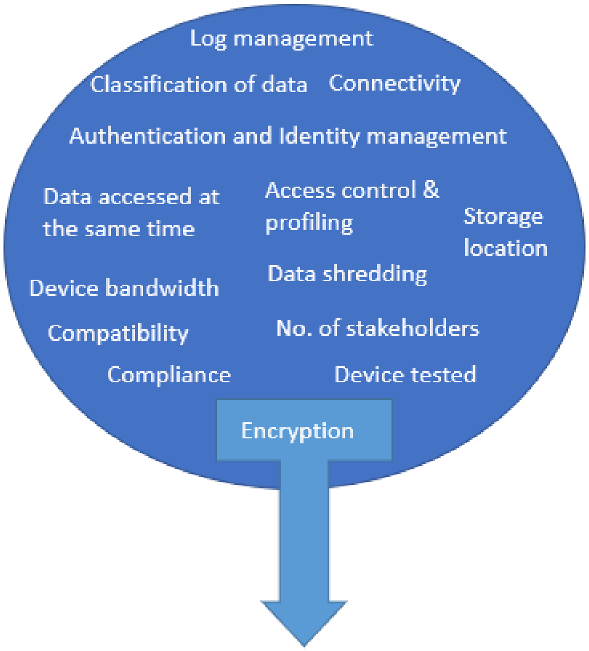
To evaluate the problem, certain key attributes that are critical for security and privacy of Internet connected wearable medical devices were identified. Each attribute was clearly defined as “what is it?”, “why is it important?”, and “how is it important?”. Under “how is it important?”, each attribute was defined with a set of considerations. These considerations are a set of Questionnaire (with a YES or NO answer). The attributes and their considerations are explained in the next chapter.

This work presents a methodology to assist the stakeholders of wearable IOMT device. Every stakeholder's interaction with the device is different. All the attributes are not necessary for all the stakeholders. The stakeholder centric approach helps stakeholders with different requirements, goals and tolerance to risks. The different stakeholders for these devices include patient, doctor, hospital, nurse, manufacturer, security researcher, regulatory authorities, insurance.

This has a 2-step mechanism.

STEP 1: The wearable medical devices were evaluated by answering the attribute questionnaire. Device specifications & privacy policies were considered to answer these questions.

STEP 2: The score of each attribute is computed using its considerations. The scores for all the attributes were normalized to a score of 10 (to account for variable considerations).



Does the device allow the user to select the data for encryption?
Does the device encrypt the passwords?
Does the device encrypt the data that is at rest?
Does the device encrypt the data in transit?
Does the device encrypt the data that is in use?
Does the device follow any of the standard encryption techniques?
If yes, Does the device comply with regulations in the country where it is used?
Does the device allow the user to choose an encryption technique?

Figure 17: Attributes and considerations.

Figure 17 clearly shows the attributes that are required for the security and privacy of the wearable internet of medical things and also considerations for the attribute “Encryption”.

Summary

The methodology with a 2-step mechanism and data collection approach used for this study were defined and identified. The next chapter covers the definitions of all the attributes and also considerations for every attribute.

Chapter IV: Data Presentation and Analysis

Introduction

This chapter covers the definitions of attributes and considerations of the study with a stakeholder-centric approach.

Data Presentation

The set of Security and privacy attributes for wearable internet of medical things that were identified to quantify the security in these devices were explained below. Each attribute is defined with a set of considerations. All these considerations were later used in the case study to evaluate the security and privacy of the two wearable internet connected medical devices.

1. **Authentication and Identity management.**

   a. What is this measure?

   This measures the device ability to verify stakeholder (patient/doctor/devices/ applications) identity. Identity is associated to a user with unique username or unique ID. Authentication is proving the identity of the user such as with a password or a key.

   b. Why this is important?

   Because it defines how well is the authentication method in protecting device and data from unauthorized access. The authentication process means going through some extra steps to prove the identity of the user.

c. How this is important?

1. Does the device allow MFA?–MFA (Multi Factor Authentication) is the combination of two or more types of authentication. It is always difficult to bypass multi-layer security than a single layer security.
2. Is the minimum size of the password 8? –Recommendations for minimum length of the password is 8. However, the recommendations vary depending on the accounts.
3. Does the password require each of uppercase/lowercase/ number/ special characters?–A strong password is a combination of all the different types of characters.
4. Does the device have password expiration?–Users should change their passwords regularly at least for every 45-90 days. Users should be sent a notification to change their password before 10–12 days their set period.
5. Does the device have password recovery option?–It is always important to have a password recovery option and it is also important to identify the user before resetting the password.
6. Does the device have password history option?–A password history stores the previous passwords and prevents the users to reuse the same password after password expiration.
7. Does the Device have biometric authentication?–Biometric methods use a physical characteristic. They can be fingerprint scanner, retina scanner, iris scanner, voice recognition or facial recognition.

8. Does the device allow to have same username and password? – Using the password as the username can be easily guessed by any hacker. The device should display an error message if the user is using the password as his own username.

2. Access Control and Profiling

a. What?

This measures the device ability by which users are granted access and privileges to the resources. These resources can be data or the device. This access is defined by the rights and permissions assigned based on the authorization to the data and the device. It also measures the ability to define and customize profiles for the stakeholders based on the patient's requirements.

b. Why?

Because it helps the owner to limit the access to the device and the privileges that each user has. Only the owner of the device (i.e., patient) should have the highest privilege.

c. How?

9. Does the device have Role-based access control?–Role-based access control uses roles to grant/deny permissions. The stakeholders can be categorized into roles and the stakeholder has all the rights and permissions of that role.

10. Does the device have Rule-based access control?–Rule-based access control uses rules. These rules are typically static. The rules stay the same until the owner changes them again.

11. Does the device have Discretionary access control?–In Discretionary access control, owner establishes access to the other stakeholders.
12. Does the device have Mandatory access control? – Mandatory access control uses labels to determine access. These labels can be referred as data sensitivity labels or security labels.
13. Does the device have Attribute-based access control? – Attribute-based access control evaluates attributes and grants access based on the value of these attributes.
14. Does the device have any other access control system? – The device can have any of the above access control systems or any other access control system to manage the privileges in the device.

3. Storage location

a. What?

This measures the device ability to store the data in various secure locations. Data storage locations include cloud storage, mobile storage, and device storage.

b. Why?

Because it helps the user to know the locations where the data is stored and hence the user can limit the storage locations as it increases the redundancy. Storing the data in multiple locations helps to back up the data but also increases the attack surface if the data can be managed from any storage location.

c. How?

15. Does the device allow to store the data in the device itself?–Data stored in the device is easily accessible and can be tracked easily since the device is a wearable device and is always worn on the body.
16. Does the device allow to store, manage, control the device from the device itself?–Since the device is a wearable device and is worn on the body, it is more secure if the device and the data can be controlled from the device itself.
17. The user cannot store, access, manage and control the device from smartphone?–Smartphones are the easily accessible devices. If the wearable medical device can be controlled and managed by the smartphone, anyone accessing the user smartphone can easily control the device on the patient's body.
18. The user cannot store, access, manage and control the device from cloud/Third party apps?–Most of the cloud applications are in the control of a third party. If these applications are hacked and if the device can be managed from these applications, the hacker can easily control the device on the patient's body.
19. Does the device allow the user to select the locations where the data can be stored? – Storing the data in cloud/third parties is always at risk. The user should be able to decide the storage location depending on his requirements and security.

4. Encryption

a. What?

This measures the ability of the device to make the data unreadable at various levels like data at rest, data in transit, and data in use. The data can only be read by the user who has the encryption key which again converts the data to the clear text.

b. Why?

Because it helps the user to know how securely the data is stored. If the data is stored in plain text, it can be read by anyone when the device is lost or during communicating the data or using the data.

c. How?

20. Does the device allow the user to select the data for encryption?–Although encrypting data is secure, it consumes time and space. The processing time of the device increases every time a data is encrypted and decrypted for a result. Hence the customer should be given an option to select the sensitive data for encryption to reduce the time and space.
21. Does the device encrypt the passwords?–Passwords are usually stored in plaintext in these devices. If the passwords are stored in plaintext, anyone who has the access to the device can easily read the password.
22. Does the device encrypt the data that is at rest?–Data at rest is when the data is not being used but is stored physically in the device. If the data is not encrypted when it is at rest, the data can be easily read by anyone if the device is lost or misplaced.
23. Does the device encrypt the data in transit?–Data in transit is when the data is being transmitted from one location to the other. If the data is being

communicated in clear text between the two devices/locations, this data can be read by anyone who tries to eavesdrop the communication.

24. Does the device encrypt the data that is in use?–Data in use is when the data is being used or when the data is active. The data should be encrypted even when the data is being used in device because it helps to protect the sensitive and active data.
25. Does the device follow any of the standard encryption techniques?–There are standards for encryption techniques which proves that the encryption technology used is approved.
26. If yes, Does the device comply with regulations in the country where it is used? –The regulations depend on the countries. Every country has their own regulations to be followed. It is also necessary for the user to check if the device comply with the regulations in the country where the device is being used.
27. Does the device allow the user to choose an encryption technique?–There are different encryption technologies available depending on the time and reliability.

5. Compliance

a. What?

This measures that the device ability to follow the rules and guidelines set by the regulatory authorities.

b. Why?

Because it defines that the device is compliant from such regulatory authorities and this increases the trust worthiness of the device.

c. How?

28. Is the device FDA compliant?–"FDA (Food and Drug Administration) is a federal agency of the United States Department of Health and Human Services which is responsible for protecting and promoting public health" (Food and Drug Administration, 2018).
29. Is the device HIPAA compliant?–"HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information" (What is HIPAA [Health Insurance Portability and Accountability Act], n.d.).
30. Is the device ISO/IEC 80001 compliant? –"ISO (International Organization for Standardization)/IEC 80001 is Application of risk management for IT-networks incorporating medical devices. The key properties are risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security" (IEC 80001-1:2010–Application of risk management for IT-networks incorporating medical device, n.d.).
31. Is the device ISO 14971 compliant?–"ISO 14971:2007 specifies a process for a manufacturer to identify the hazards associated with medical devices, including in vitro diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the

controls” (ISO 14971:2007–Medical devices–Application of risk management to medical devices, n.d.).

32. Is the device compliant to any other medical device regulatory?–There are different regulations and authorities for medical data and security.
33. Is the device compliant to any regulatory authority where the device is manufactured?–Different authorities have different guidelines based on the location and rules. The device should be compliant to the regulatory where it has been manufactured.
34. Is the device compliant to any regulatory authority where the device is used?–Different authorities have different guidelines based on the location and rules. The device should be compliant to the regulatory where it is being used.

6. Connectivity

a. What?

This measures the device ability to connect to other devices through different medium.

b. Why?

Because it defines how the device can be connected with the other devices. Each connectivity has their own challenges. The device should be able to connect to the correct device on the other side.

c. How?

35. Does the device allow to select the type of connectivity? – Each user might feel comfortable and secure with different connectivity methods hence the device should allow the user to select how he/she would like to connect with internet or other devices.
36. Does the device allow to connect with other devices through internet? – Internet helps to connect and view data in different devices globally. It helps the user to view and share the data at any time through the private network. Connecting to internet in public places always helps the hackers to easily hack the devices.
37. Does the device have ability of mutual authentication when connecting with other devices? – Mutual authentication is a two-way authentication, that helps both the devices to authenticate before they connect to each other.
38. Does the device can be anonymous when connected to other devices? – Being anonymous can make the user feel safe even if the data has been stolen while communicating with other devices.

7. Data Shredding

a. What?

This helps to determine the device ability to ensure that all patient identifiable data is securely and correctly removed/deleted from the equipment prior to disposal or reuse.

b. Why?

Because it defines that the device does not store any previous data or malware installed by previous user and safe to dispose or reuse. Data shredding permanently wipes the data so that it cannot be recovered.

c. How?

39. Is the device under MDISS?–MDISS is Medical Device Innovation, Safety & Security consortium. It checks if the medical device is ready to use, no previous data is present in the device and also helps the device fix any vulnerabilities.
40. Does the device contain any data shredding mechanisms?–Data shredding mechanisms help the medical devices to clear all the data previous stored in the device by other users.
41. Is the device capable of installing any data shredding tools?–There are different open source data shredding tools available which helps to wipe all the previously stored data and malware.

8. Classification of data

a. What?

This helps to determine the type of data that is stored in the device and helps to categorize the data depending on the sensitivity.

b. Why?

Because it helps the user to have the ability to select the data that is to be stored in the device. The more sensitive data in the device the more likely to get attacked.

c. How?

42. Does the device allow to catalog or categorize or classify data to very sensitive, moderate sensitive, not sensitive data?–Categorizing the data helps the user to know which data can be encrypted and which data should be given privileges.

43. Does the device allow the owner to select the validity for the data stored in the device?–User can delete the less important data after a period of time which helps the device to increase the storage space and helps to increase the processing time.

9. Data accessed at the same time

a. What?

This measures the device ability to access the data by different people/programs at the same time.

b. Why?

Because data accessed at the same time by different people/programs increases the attack surface. It is difficult to find who, or which system is attacking.

c. How?

44. The device can restrict the stakeholders connecting to the device at the same time?–Each device has difference stakeholders. If all the stakeholders can connect to the device at the same time, the functionality of the device decreases, and it also becomes hard to track the stakeholder or any program used by the stakeholder.

45. Does the device have an option to limit number of stakeholders accessing the device at the same time?–If the user can limit the connections to the device, it helps to track the stakeholder or the program if the device is compromised.

10. Number of stakeholders

a. What?

This measures the device ability in sharing the data with a certain number of people who are likely to know the data.

b. Why?

Because it defines the number of people who are accessing the data and who can access the data. As the number of stakeholders increases the attack surface also increases.

c. How?

46. Does the device allow the owner to select the stakeholders? – The owner of the device should have the privilege to select the stakeholders.

11. Device bandwidth

a. What?

Bandwidth is measured in bits per second. This measures the device ability to transfer the number of bits in one second over a channel.

b. Why?

Because if the traffic exceeds a bandwidth, that means an unauthorized traffic is entering the device and can also be a chance for denial of service.

c. How?

47. Does the device allow the owner to limit the bandwidth? – Bandwidth should be limited based on the data that is being transmitted.
48. Does the device allow to limit the bandwidth for different stakeholders? – There are different bandwidth recommendations for different stakeholders. (Recommended bandwidth for health care providers, 2014) According to federal communication commission for healthcare, the recommended bandwidths are:

    - Single Physician Practice–4 megabits per second (Mbps)
    - Small Physician Practice (2-4 physicians)–10 Mbps
    - Nursing home–10 Mbps
    - Rural Health Clinic (approximately 5 physicians)–10 Mbps
    - Clinic/Large Physician Practice (5-25 physicians)–25 Mbps
    - Hospital–100 Mbps
    - Academic/Large Medical Center–1,000 Mbps
49. Does the device allow to limit the bandwidth based on the number of users?– There might be situations where the number of stakeholders accessing the device at the same time increases, at that time the device should allow the user to increase the bandwidth depending on the number of stakeholders.
50. Does the device allow to limit bandwidth based on the user locations?–There might be unwanted traffic in public networks, So depending on the location, the user should be allowed to limit the bandwidth.

12. Tested?

a. What?

This measure if the device is tested and can be trusted by addressing all the vulnerabilities in the device.

b. Why?

Because it helps to determine the current level of security of the device and the vulnerabilities that were in the device and if they are patched?

c. How?

51. Is the device tested in terms of security and privacy? –According to a survey by Synopsys, 36% of the medical device makers and 45% of the Healthcare Delivery Organizations do not test their medical devices in terms of security and privacy (Medical-device-security-ponemon-synopsys.pdf, 2017).
52. Is the device addressed with any security vulnerabilities?–("medical-device-security-ponemon-synopsys.pdf," 2017). According to a survey by Synopsys, approx. 35% of medical device makers and app 26.7% of Healthcare Device Organizations say that their medical devices contain significant vulnerabilities. 18.3% of Device makers and 13% of Healthcare Device Organizations say their tested medical device contain malware.
53. Are all the vulnerabilities patched?–The medical device manufacturers should release a patch immediately if any vulnerability is known.

13. Log management

a. What?

This measure the device ability to monitor and analyze the traffic like records the users who accessed the data.

b. Why?

Because it helps the owner of the device to know the users who logged in, to check the data and can find if any unauthorized user is able to see the data.

c. How?

54. Does the device have a log management system?–Log management system helps the user to know the users who accessed the device and the data.
55. Is the log management system in the device trustworthy?–There are some basic log management systems available which are not reliable.
56. Is the device capable to install a log management system?–There are different log management systems available which can be easily installed based on the requirement, e.g., Logsign, Splunk, Log packer.

14. Compatibility

a. What?

This measures the device ability of compatibility to share the data with other devices.

b. Why?

Because if the device says it is compatible with other devices, it automatically shares the data with those devices.

c. How?

57. The device is compatible to iOS but notifies the user before sharing the data?–ios is a mobile operating system created and developed by Apple Inc. exclusively for its hardware (iOS, 2018).
58. The device is compatible to Mac OS but notifies the user before sharing the data?–Macintosh OS is an operating system developed and marketed by Apple Inc. It is the primary operating system for Apple’s Mac family of computers (macOS, 2018).
59. Is the device compatible to android OS but notifies the user before sharing the data?–Android is a mobile operating system developed by Google, based on a modified version of the Linux kernel and other open source software (Android [operating system], 2018).
60. Is the device compatible to windows OS but notifies the user before sharing the data?–Microsoft Windows is a group of several graphical operating system families, all of which are developed, marketed, and sold by Microsoft (Microsoft Windows, 2018).

Data Analysis

To normalize the score of attributes, the following formula was used:

$$Attribute\ score = \sum_{i=1}^{N} Consideration_i\ X\ \frac{10}{N}$$

N = number of considerations

Stakeholder–Centric approach. All the attributes and their considerations were clearly defined in the previous section. This section explains the stakeholder centric approach of the proposed model. The stakeholders for the wearable internet of medical things include patients, doctor, hospital, nurse, manufacturer, security researcher, regulatory authorities, insurance. All the stakeholders do not require all the attributes that were defined. Each stakeholder is classified with the attributes that were required for that stakeholder.

Table 1

Stakeholder-Centric Approach

Stakeholders	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Patient	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Hospital			X			X			X					X
Doctor			X	X	X	X	X		X			X		X
Nurse				X		X			X					X
Manufacturer	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Regulatory authorities		X		X							X	X		X
Insurance			X	X	X					X		X		
Security Researchers		X	X	X	X	X	X	X			X			X

Key:

1 – Authentication and Identity management
2 – Access control and profiling
3 – Storage location
4 – Encryption
5 – Compliance
6 – Connectivity
7 – Data Shredding
8 – Classification of data
9 – Data accessed at the same time
10 – Number of stakeholders
11 – Device bandwidth
12 – Device tested
13 – Log management
14 – Compatibility

Summary

This chapter covered the detailed description of the attributes and their considerations. This chapter also explained about the stakeholder-centric approach. The results of the methodology are explained in the next chapter.

Chapter V: Results, Conclusion, and Recommendations

Introduction

This chapter clearly evaluates and analyzes the security and privacy of two different internet connected wearable medical devices from stakeholder's perspective.

Results

Step 1: In step 1, consider 2 wearable medical devices (Zak.Huber, 2016) Dexcom g5 and (MiniMed 530G Insulin Pump | Diabetes Pump System With SmartGuard Technology, 2018). MiniMed 530G. These 2 devices are evaluated by answering all the attribute questions.
The result of the considerations for Dexcom g5 and MiniMed 530G are attached in appendix.

Step 2: After answering all the questions, the second step is to compute the score for each attribute using its considerations. The scores for all the attributes are normalized to score of 10.

$$Attribute\ score = \sum_{i=1}^{N} Consideration_i\ X\ \frac{10}{N}$$

N = number of considerations

1) The score for authentication and identity management:

   Device 1 –

   Authentication and Identity Management = $3X\ \frac{10}{11}$ = 30/11 = 2.72

   Device 2 –

   Authentication and Identity Management = $6X\ \frac{10}{11}$ = 60/11 = 5.45

2) The score for Access control and profiling

   Device 1 –

Access control and profiling = $1X\ \frac{10}{4}$ = 10/4 = 2.5

Device 2 –

Access control and profiling = $1X\ \frac{10}{4}$ = 10/4 = 2.5

3) The score for Storage location

Device 1 –

Storage location = $2X\ \frac{10}{5}$ = 20/5 = 4

Device 2 –

Storage location = $2X\ \frac{10}{5}$ = 20/5 = 4

4) The score for Encryption

Device 1 –

Encryption = $0X\ \frac{10}{8}$ = 0/8 = 0

Device 2 –

Encryption = $0X\ \frac{10}{8}$ = 0/8 = 0

5) The score for Compliance

Device 1 –

Compliance = $3X\ \frac{10}{7}$ = 30/7 = 4.28

Device 2 –

Compliance = $2X\ \frac{10}{7}$ = 20/7 = 2.85

6) The score for Connectivity

Device 1 –

Connectivity = $1X\ \frac{10}{4}$ = 10/4 = 2.5

Device 2 –

Connectivity = $1X\ \frac{10}{4}$ = 10/4 = 2.5

7) The score for Data Shredding

Device 1 –

Connectivity = $0X\ \frac{10}{3}$ = 0/3 = 0

Device 2 –

Connectivity = $0X\ \frac{10}{3}$ = 0/3 = 0

8) The score for Data Categorization

Device 1 –

Data Categorization = $0X\ \frac{10}{2}$ = 0/2 = 0

Device 2 –

Data Categorization = $1X\ \frac{10}{2}$ = 10/2 = 5

9) The score for Data accessed at the same time

Device 1 –

Data accessed at the same time = $2X\ \frac{10}{2}$ = 20/2 = 10

Device 2 –

Data accessed at the same time = $2X\ \frac{10}{2}$ = 20/2 = 10

10) The score for Number of stakeholders

Device 1 –

Number of stakeholders = $1X\ \frac{10}{1}$ = 10/1 = 10

Device 2 –

Number of stakeholders = $1X\ \frac{10}{1}$ = 10/1 = 10

11) The score for Device bandwidth

Device 1 –

Device bandwidth = $0X\ \frac{10}{4}$ = 0/4 = 0

Device 1 –

Device bandwidth = $0X\ \frac{10}{4}$ = 0/4 = 0

12) The score for Device tested

Device 1 –

Device Tested = $1X\ \frac{10}{2}$ = 10/2 = 5

Device 2 –

Device Tested = $0X\ \frac{10}{2}$ = 0/2 = 0

13) The score for Log management

Device 1 –

Log Management = $0X\ \frac{10}{3}$ = 0/3 = 0

Device 2 –

Log Management = $0X\ \frac{10}{3}$ = 0/3 = 0

14) The score for Compatibility

Device 1 –

Compatibility = $0X\ \frac{10}{4}$ = 0/4 = 0

Device 2 –

Compatibility = $0X\ \frac{10}{4}$ = 0/4 = 0

All the above attribute scores were plotted in a graph for better visualization. Figure 17 clearly shows the graph of all the attribute scores for Dexcom G5 and MiniMed 530G.

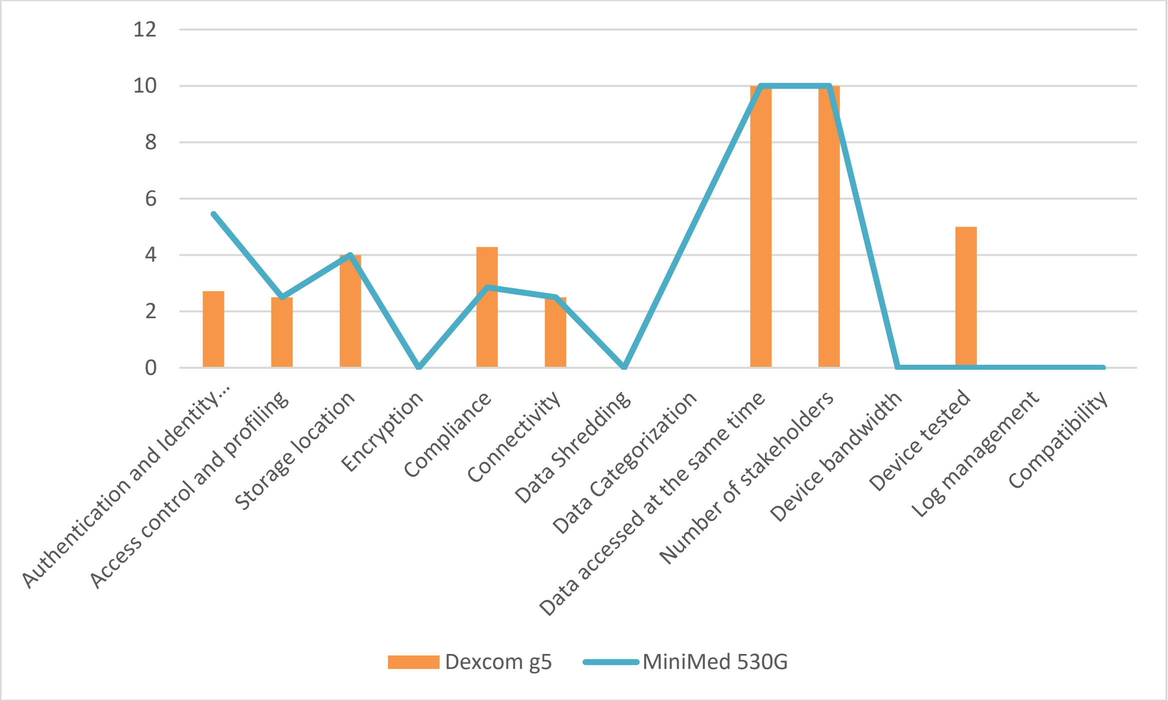


Figure 18: Comparison of two wearable IOMT devices.

Stakeholder-Centric approach. As explained about the stakeholder centric approach in the previous chapter, every stakeholder has a different requirement, goal and tolerance to risks. Hence the values of the device changes with the stakeholder. Below are the figures, which clearly shows that the graph changes with the stakeholder. Figure 18 shows the values of 2 stakeholders, i.e., patient and a doctor for a device called Dexcom g5. Figure 19 shows the values of 2 stakeholders i.e., patient and a doctor for a device called MiniMed 530G

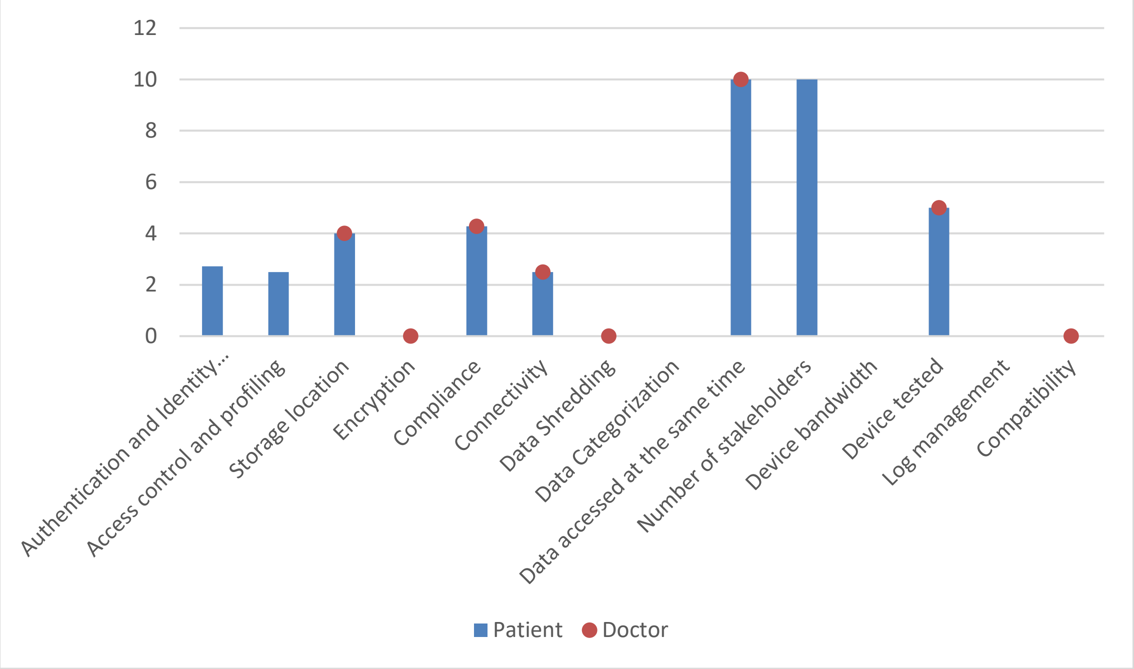


Figure 19: Comparison of a doctor and a patient for Dexcom g5.

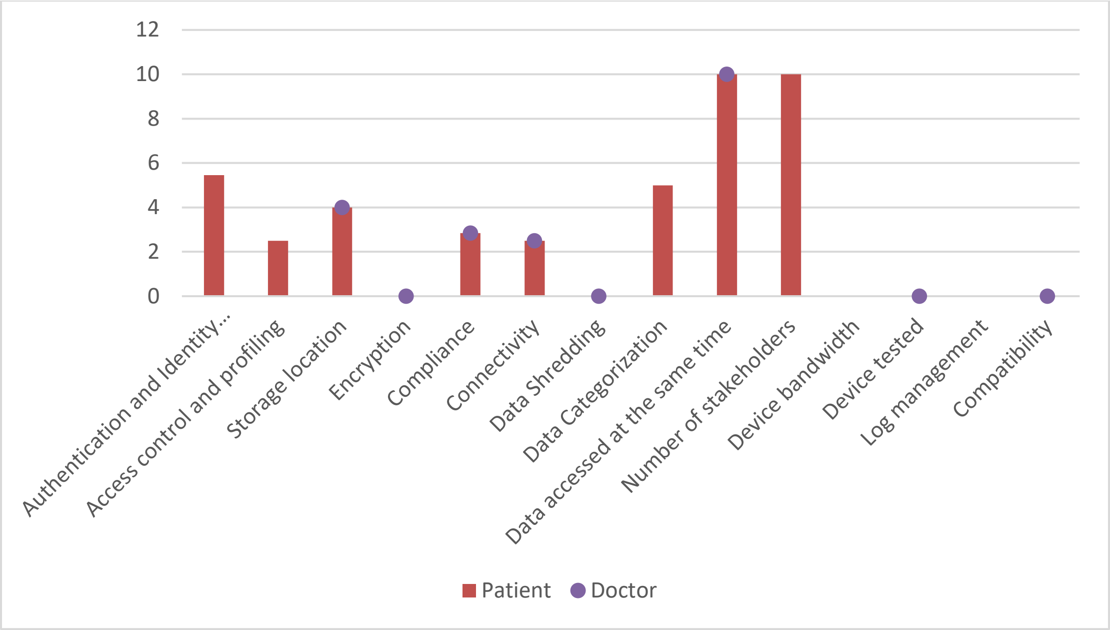


Figure 20: Comparison of a doctor and a patient for MiniMed 530G.

Conclusion

According to a survey by HIMSS (“HIMSS Survey Finds Two-Thirds of Healthcare Organizations Experienced a Significant Security Incident in Recent Past,” 2015), two-thirds of healthcare organizations experienced a significant security incident in recent past. Many researchers and manufactures of IoMT devices are concentrating on the S&P of these medical devices. Also, many regulatory authorities have recognized the importance of this problem and started serious steps towards ensuring (1) the protection of patient health information and (2) compliance of medical devices.

Stakeholders of IoMT, (i.e., Healthcare practitioners and patients) focus more on the functionality and performance of the device but often overlook the S&P issues associated with these devices. In most cases, the reason to overlook these security issues is due to lack of proper awareness.

This work presented a methodology to assist IoMT stakeholders (e.g., doctor, nurses, etc.) to rank wearable IoMT devices in terms of their protection and deterrence. The proposed methodology uses a stakeholder-centric approach to improve security of wearable IoMT devices. The novelty of this work lies in that it defines security according to every stakeholder's interaction with the wearable IoMT device. This approach assists stakeholders with different requirements, goals, and tolerance to risks manage issues that arise from stakeholders' conflicts of interests broadly and thoroughly.

Future Work

This research could be expanded further to help both manufacturers and customers of these devices. A tool can be developed with this methodology to easily evaluate the values of any wearable IOMT device. This tool can also be developed to store the values of previously evaluated devices and help the customers to retrieve these values. For each attribute, weightage can be added as pertinent to the stakeholder.

References

Abdur, M., Habib, S., Ali, M., & Ullah, S. (2017). Security issues in the internet of things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications, 8*(6). https://doi.org/10.14569/IJACSA.2017.080650

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the internet of things: Current status and open issues. In *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)* (pp. 1-8). https://doi.org/10.1109/PRISMS.2014.6970594

AL-Mawee, W. (2015). *Privacy and security issues in IoT healthcare applications for the disabled users a survey,* p. 57. (Unpublished thesis), Western Michigan University.

Altoros Offices. (n.d.). Retrieved April 13, 2018, from https://www.google.com/maps/d/viewer?mid=1pBwJc_lTuAZKIuEmmnCK57PYH18.

Ameen, M. A., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems, 36*(1), 93-101. https://doi.org/10.1007/s10916-010-9449-4

Android (operating system). (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Android_(operating_system)&oldid=864526292.

Ankitha, S., & Balajee, M. (2016). Security and privacy issues in IoT, 8. *SCIREA Journal of Agriculture, 1*(2), 135-142.

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-scale Computing Systems, 1*(2), 99-109. https://doi.org/10.1109/TMSCS.2015.2498605

Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. *International Journal of Advanced Networking Applications*, *6*, 2372-2378.

Chakravorty, R. (2006). A programmable service architecture for mobile medical care. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, pp. 500-536. https://doi.org/10.1109/PERCOMW.2006.11

Challenges in the internet of things | TI.com. (n.d.). Retrieved April 13, 2018, from http://www.ti.com/ww/en/internet_of_things/iot-challenges.html.

Dehling, T., Gao, F., Schneider, S., & Sunyaev, A. (2015). Exploring the far side of mobile health: Information security and privacy of mobile health apps on iOS and android. *JMIR MHealth and UHealth*, *3*(1). https://doi.org/10.2196/mhealth.3672

Fears of hackers targeting US hospitals, medical devices for cyber attacks–*BC News*. (2017). Retrieved April 13, 2018, from http://abcnews.go.com/Health/fears-hackers-targeting-us-hospitals-medical-devices-cyber/story?id=48348384.

Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., … Steinhubl, S. R. (2016). Privacy and security in the era of digital health: What should translational researchers know and do about it? *American Journal of Translational Research*, *8*(3), 1560-1580.

Filkins, S. (2014). *Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon* (p. 44). SANS Institute.

Food and Drug Administration. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Food_and_Drug_Administration&oldid=863162821.

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys Tutorials*, *17*(3), 1294-1312. https://doi.org/10.1109/COMST.2015.2388550

HIMSS survey finds two-thirds of healthcare organizations experienced a significant security incident in recent past. (2015). Retrieved from https://www.himss.org/news/himss-survey-finds-two-thirds-healthcare-organizations-experienced-significant-security-incident

Hiremath, S., Yang, G., & Mankodiya, K. (2014). Wearable internet of things: concept, architectural components and promises for person-centered healthcare. In *2014 4th International Conference on Wireless Mobile Communication and Healthcare–Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)* (pp. 304-307). https://doi.org/10.1109/MOBIHEALTH.2014.7015971

How IoT works–An overview of the technology architecture. (2015, May 13). Retrieved April 13, 2018, from https://www.embitel.com/blog/embedded-blog/how-iot-works-an-overview-of-the-technology-architecture-2.

IEC 80001-1:2010–Application of risk management for IT-networks incorporating medical devices–Part 1: Roles, responsibilities and activities. (n.d.). Retrieved October 18, 2018, from https://www.iso.org/standard/44863.html.

iOS. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=IOS&oldid=864214633.

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access*, *3*, 678-708. https://doi.org/10.1109/ACCESS.2015.2437951

ISO 14971:2007–Medical devices–Application of risk management to medical devices. (n.d.). Retrieved October 18, 2018, from https://www.iso.org/standard/38193.html.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501. https://doi.org/10.1007/s11276-014-0761-7

Khandelwal, S. (2017). *Over 8,600 vulnerabilities found in pacemakers*. Retrieved April 13, 2018, from https://thehackernews.com/2017/06/pacemaker-vulnerability.html.

Kumar, N., Madhuri, J., & ChanneGowda, M. (2017). Review on security and privacy concerns in internet of things. In *2017 International Conference on IoT and Application (ICIOT)* (pp. 1-5). https://doi.org/10.1109/ICIOTA.2017.8073640

Lake, D., Milito, R. M. R., Morrow, M., & Vargheese, R. (2014). Internet of things: Architectural framework for ehealth security. *Journal of ICT Standardization*, *1*(3), 301-328. https://doi.org/10.13052/jicts2245-800X.133

macOS. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=MacOS&oldid=862750369.

Markets, R. (2017). *Global wearable medical device market opportunities to 2022*. Retrieved April 13, 2018, from https://www.prnewswire.com/news-releases/global-wearable-medical-device-market-opportunities-to-2022-300542952.html.

Medical-device-security-Ponemon-Synopsys.pdf. (2017). Retrieved from https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf.

Microsoft Windows. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Microsoft_Windows&oldid=864179849.

MiniMed 530G Insulin Pump | Diabetes Pump System with SmartGuard Technology. (2018). Retrieved October 18, 2018, from https://www.medtronicdiabetes.com/products/minimed-530g-diabetes-system-with-enlite.

Pantelopoulos, A., & Bourbakis, N. G. (2010). A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40*(1), 1-12. https://doi.org/10.1109/TSMCC.2009.2032660

Peck, M. E. (2011, August 12). *Medical devices are vulnerable to hacks, but risk is low overall.* Retrieved April 13, 2018, from https://spectrum.ieee.org/biomedical/devices/medical-devices-are-vulnerable-to-hacks-but-risk-is-low-overall.

Rahman, M., Carbunar, B., & Banik, M. (2016). Fit and vulnerable: Attacks and defenses for a health monitoring device. *IEEE Transactions on Mobile Computing*, *15*(2), 447-459. https://doi.org/10.1109/TMC.2015.2418774

Recommended bandwidth for health care providers. (2014). Retrieved October 18, 2018, from https://www.greatsys.com/recommended-bandwidth-for-health-care-providers/.

Rehman, A., Rehman, S., Khan, I. U., Moiz, M., & Hasan, S. (2016). Security and privacy issues in IoT. *International Journal of Communication Networks and Information Security (IJCNIS)*, *8*(3). Retrieved from http://www.ijcnis.org/index.php/ijcnis/article/view/2074.

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1–6). https://doi.org/10.1145/2744769.2747942

Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., … Seneviratne, A. (2017). A survey of wearable devices and challenges. *IEEE Communications Surveys Tutorials*, *19*(4), 2573-2620. https://doi.org/10.1109/COMST.2017.2731979

What is HIPAA (Health Insurance Portability and Accountability Act) ? - Definition from WhatIs.com. (n.d.). Retrieved October 18, 2018, from https://searchhealthit. techtarget.com/definition/HIPAA.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844

Zak.Huber. (2016, March 3). Dexcom G5 Mobile CGM System | Glucose on your phone [Text]. Retrieved October 18, 2018, from https://www.dexcom.com/g5-mobile-cgm.

Zhou, W., & Piramuthu, S. (2014). Security/privacy of wearable fitness tracking IoT devices. In *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-5). https://doi.org/10.1109/CISTI.2014.6877073

Appendix

Result of considerations for Dexcom g5 and MiniMed 530G

S.No	Considerations	Dexcom g5	MiniMed 530G
1.	Does this device allow MFA?	0	0
2.	Is the minimum size of the password 8?	0	1
3.	Password must have an alphabet?	0	1
4.	Password must have an uppercase alphabet?	0	1
5.	Password must have a number?	1	1
6.	Password must have a character?	0	1
7.	Does the device have password expiration?	0	0
8.	Does the device have password recovery option?	1	1
9.	Does the device have password history option?	0	0
10.	The device does not allow to have same username and password?	1	0
11.	Does the Device have biometric authentication?	0	0
12.	Does the device have Role based Access control?	0	0
13.	Does the device have Rule based access control?	0	0
14.	Does the device have Discretionary access control?	1	1
15.	Does the device have Mandatory access control?	0	0
16.	Does the device allow to store in the device itself?	1	1
17.	Does the device allow you to manage, control the device from the device itself?	1	1

18.	The user cannot store, access, manage and control the device from smartphone?	0	0
19.	The user cannot store, access, manage and control the device from cloud/Third party apps?	0	0
20.	Does the device allow the user to select the locations where the data can be stored?	0	0
21.	Does the device allow the user to select the data for encryption?	0	0
22.	Does the device encrypt the passwords?	0	0
23.	Does the device encrypt the data that is at rest?	0	0
24.	Does the device encrypt the data in transit?	0	0
25.	Does the device encrypt the data that is in use?	0	0
26.	Does the device follow any of the standard encryption techniques?	0	0
27.	If yes, Does the device comply with regulations in the country where it is used?	0	0
28.	Does the device allow the user to choose an encryption technique?	0	0
29.	Is the device FDA compliant?	1	1
30.	Is the device HIPAA compliant?	1	1
31.	Is the device ISO/IEC 80001 compliant?	0	0
32.	Is the device ISO 14971 compliant?	0	0
33.	Is the device compliant to any other regulatory authority?	1 (HITECh Act)	0
34.	Is the device compliant to any other regulatory authority where the device is manufactured?	0	0

35.	Is the device compliant to any other regulatory authority where the device is used?	0	0
36.	Does the device allow to select the type of connectivity?	1	1
37.	Does the device allow to connect with other devices through internet?	0	0
38.	Does the device have ability of mutual authentication when connecting with other devices?	0	0
39.	Does the device have ability to be anonymous when connected to other devices?	0	0
40.	Is the device under MDISS (Medical device innovation, safety & security consortium?	0	0
41.	Does the device contain any data shredding mechanisms?	0	0
42.	Is the device capable of installing any data shredding tools?	0	0
43.	Does the device allow to catalog or categorize or classify data to very sensitive, moderate sensitive, not sensitive data?	0	1
44.	Does the device allow the owner to select the validity for the data stored in the device?	0	0
45.	The device can restrict the stakeholders connecting to the device at the same time?	1	1
46.	Does the device have an option to limit number of stakeholders accessing the device at the same time?	1	1
47.	Does the device allow the owner to select the stakeholders?	1	1

48.	Does the device allow the owner to limit the bandwidth?	0	0
49.	Does the device allow to limit the bandwidth for different stakeholders?	0	0
50.	Does the device allow to limit the bandwidth based on the number of users?	0	0
51.	Does the device allow to limit bandwidth based on the user locations?	0	0
52.	Is the device tested in terms of security and privacy?	1	0
53.	Is the device addressed with any security vulnerabilities?	0	0
54.	Does the device have a log management system?	0	0
55.	Is the log management system in the device trustworthy?	0	0
56.	Is the device capable to install a log management system?	0	0
57.	The device is compatible to iOS but notifies the user before sharing the data?	0	0
58.	The device is compatible to Mac OS but notifies the user before sharing the data?	0	0
59.	Is the device compatible to android OS but notifies the user before sharing the data?	0	0
60.	Is the device compatible to windows OS but notifies the user before sharing the data?	0	0
Total:		14	16