Creation of a Socio-Technical Framework for Securing Personal Monitoring Devices (PMD)

Eng. H.P.Asanka Pathirana (PATH0037)

Supervisor: Professor Trish Williams

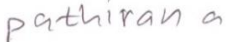
COMP9710: Master Research (18 Units)

October 2017

Submitted to the College of Science and Engineering in partial fulfilment of the requirements for the degree of Master of Science (Computer Science) at Flinders University – Adelaide Australia.

DECLARATION OF ORIGINALITY

I certify that this work does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.



Signature

Date: 2017-10-06

ACKNOWLEDGEMENT

The Master Thesis is a challenge for everyone. I also get into Master Thesis beforehand considering the advices of my lecturers and senior students. Further, I would like to convey my special thanks for Dr. Denise de Vries teaching Enterprise Information Security in 2016 – S1 and directing me to Professor Trish Williams for the research. I thank them all at first instance.

Secondly, Professor Trish Williams is the key person for me as supervisor towards successful completion of the Master Thesis. I appreciate her invaluable advice and timely feedback to successfully finish my Master Thesis, and she is teaching us Advanced Enterprise Security at present in 2017 – S2. Finally, Mr. Scott Anderson, a PhD student of Professor Trish Williams, helped on my research at different points for quick questions and proofread the entire thesis for me. I thank them indeed on bottom of my heart.

A research paper has been submitted with Professor Trish Williams on this topic at **the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)**, and it has already been accepted, so this research has contributed for the future researchers. I am really appreciative contribution of the supervisor for making this happen.

TABLE OF CONTENTS

TABLES

FIGURES

ACRONYMS

BLE – Bluetooth Low Energy

BAN – Body Area Network

GPS – Global Positioning System

HIoT – Healthcare Internet of Things

IoT – Internet of Things

LE – Low Energy

MAC – Media Access Controller

NFC – Near Field Communication

PAMT – Physical Activity Monitoring Technologies

PMD – Personal Monitoring Device

PMDs – Personal Monitoring Devices

QoS – Quality of Service

RFID – Radio Frequency Identification

SOA – Service Oriented Architecture

ABSTRACT

New healthcare technologies facilitate additional care pathways and opportunities for the patient beyond that of traditional care. This includes patient care using the Internet of Things (IoT), such as monitoring fitness and blood pressure on a regular basis, and the storage of data for later detailed analysis. Chronic disorders such as respiratory illness, physiological disorders, cardiovascular diseases, stroke, and diabetes have benefited from using Personal Monitoring Devices (PMDs). In addition to the previously above mentioned sectors, both aged care and child care sectors are vitally dependent on the regular monitoring. The objective is either maintaining health or having timely treatment using data collected using PMDs. Further, many individuals are interested in using PMDs for learning about their daily activities such as calories burned, diet, exercise regime and the impact of these on heart rate and other vital signs. However, there are increasing concerns for privacy and security of personal health information generated by PMDs, yet the users themselves also contribute to leakage of such as when they breach best practices in the use of PMDs.

Statement of Problem: The Healthcare Internet of Things (HIoT) consists of smart medical devices with various applications and using differing communication technologies. It is essential to educate consumers on how to interact safely and securely within the HIoT environment without introducing additional vulnerabilities that may lead to unnecessary risks to their information. At present, there is insufficient attention paid to this socio-technical perspective specific to HIoT. Further there is no guidance for consumers on the human factors of HIoT. The research question considers the possibility of developing a socio-technical impact framework to assist users with the secure use of Personal Monitoring Devices.

Methodology: A review of the literature using a case study approach to investigate the current use of HIoT PMDs, the security measures of HIoT, and the specific security problems attributed to consumers, was undertaken to identify vulnerabilities. Subsequently, supplementary experimentation with PMDs in HIoT is undertaken to assess the level of device security. The case study and experimentation were used to introduce prospective countermeasures. Then, a framework was developed to map the countermeasures that could be applied to improve the security and privacy of information based on the human factors of HIoT. Finally, guidelines were constructed for PMD users based on the new framework.

Impact: The research identifies the level of involvement of consumers in their personal security posture when using HIoT PMDs. This research may assist in educating people in secure information usage, and explore mechanisms to improve a secure user experience with such devices. Such research is important given the sensitive nature of health addressing lapses in health information security.

1 INTRODUCTION

The Internet of Things (IoT) was introduced as a panacea for effectively connecting smart objects equipped with sensors and actuators, over the Internet (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012). The IoT is a useful tool that presents technological enhancement contributing the global economy, moving to the forefront of society providing improved human experiences. The Gartner Research Institute predicts that the Internet will represent more than 50 billion devices by year 2020, while the IoT global market drive to an extent of $14.4 trillion by 2022 as per CISCO.

The Healthcare Internet of Things (HIoT) is one main branch of the IoT environment that has to consider the sensitivity of the data in the HIoT environment over IoT, because the unauthorised access of data can lead to integrity violations and subsequently incorrect treatment. In extreme cases, this may cause a death of a human being. There is no way to calculate a price on human life or for the quality of life, because it is priceless. Every person worries about their health, so the healthcare requirements of people is very broad. This means that technology such as HIoT is increasingly being embraced by consumers due to the personnel requirement to be healthy and aided by the technological enhancement for convenient use of PMDs.

The quality of life of everyone, from new born baby to senior citizens, can be maintained from a HIoT technological approach. HIoT has drawn a lot of consideration from the researchers as is indicated by the increase in research and development despite the complexities of the HIoT environment and the heterogonous communications (Sungmee & Jayaraman, 2013). As costs for healthcare is increasing due to the treatments, and the world ageing population is increasing who needs additional care, it is important to monitor the health status of a patient despite the fact a person is away from the hospital in their home surroundings(Hao & Foster, 2008). In recent years, a variety of system prototypes and commercial products have been produced to address this demand, aiming to provide real time information about personnel health conditions, for the patient themselves, medical centres and clinicians. This introduces a practical approach to facilitate real time care for patients.

The cost of healthcare treatment remains significant, considering the requirements of individually targeted treatment (Kodali, Swamy, & Lakshmi, 2015), so preventing the need for treatment is beneficial to both health and financial wellbeing for the individual and the healthcare system. Currently self-monitoring of health has been introduced by the prevalent usage of PMDs, to avoid extra costs and long period of hospital stays as per a research finding (Darshan & Anandakumar, 2015). Further, PMDs are not isolated, and connected to each other for inter communication by introducing a new era of HIoT. As a result, multiple monitoring devices attach to the human body introduces the Body Area Network (BAN) (Castillejo, Martinez, Rodriguez-Molina, & Cuerva, 2013), since multiple devices are communicating with each other. Moreover, HIoT provides access to the healthcare monitoring anytime and anywhere, motivating people to use HIoT.

HIoT can be introduced as umbrella term for many technologies in healthcare. In the HIoT environment, the technological improvements introduce advance use of devices to improve and enhance levels of care. Unfortunately, the pervasive use also becomes a security problem for users as indicated by recent episodes involving unauthorised access due to the complexity of the interconnections. Moreover, the involvement of the consumer in the equation makes the situation more risky by introducing vulnerabilities due to the poor understand of available technological implementations (Darshan & Anandakumar, 2015). The benefits of HIoT are not important enough if personal healthcare data makes its way into the wrong hands. Considering both factors, the security in HIoT is crucial, and significant compared to the security of IoT considering the sensitivity of healthcare information of HIoT. That factor is crucial with increasing number of devices connected with HIoT infrastructure, because each device can be introduced as entry point to the network. This research focuses on preventing such situations by introducing a framework to preserve the

information security for the user by introducing recommendations, to create an environment that provides a high level of secure use of PMDs.

1.1 Background of the Study

People are interested in monitoring their specific healthcare status on a regular basis, because it helps people to maintain their health condition at some level by addressing multiple healthcare needs. Governments, who have a responsibility for healthcare, are also encouraging personal health monitoring since it reduces the costs for treatment significantly (Hao & Foster, 2008). However, the increasing use of PMDs introduces information security risks in line for the complex environment and the human-social factors.

In general, information security is assured in three main ways, using: confidentiality, integrity and availability (Whitman & Mattord, 2011). These three aspects are not addressed adequately in the present technological HIoT environment due to the complexity of intercommunication among interconnected devices (Whitman & Mattord, 2011). Moreover, the requirements of people such as use of multiple devices, synchronising them real time and how people use these technologies are significantly impacted. Considering the technological enhancement, the three dimensional model has been introduced to consider every aspect of information security as shown in Figure 1 (Whitman & Mattord, 2011). Healthcare information security also considers all those aspects represented in McCumber model.

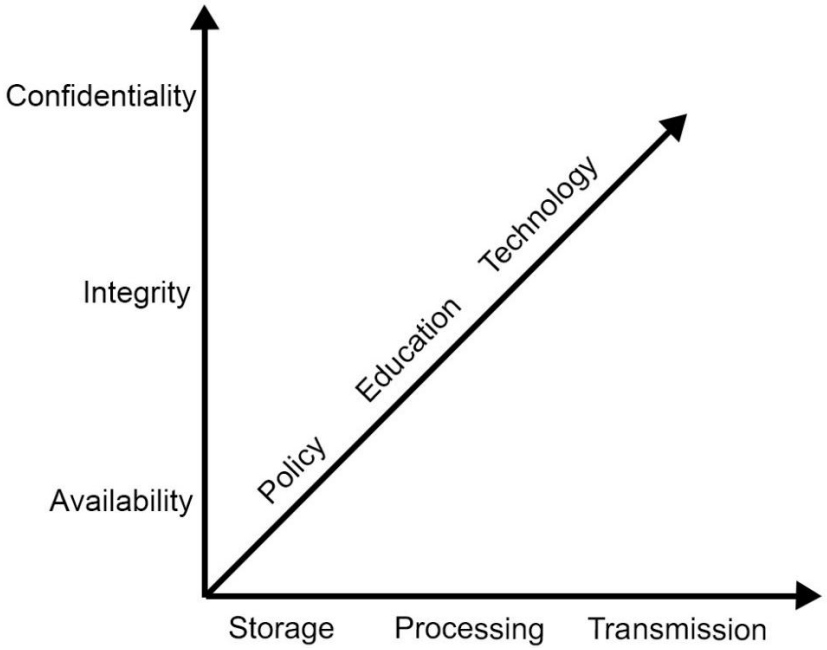


Figure 1: McCumber Model for Information Security (Whitman & Mattord, 2011)

The McCumber model uses one dimension for describing the three different states of information which are stored, being processed and in transmission (Whitman & Mattord, 2011). The electronic healthcare information is also identifiable in those three forms in the HIoT environment. The stored data is resting on servers or temporary residing on the device/edge computing devices, and system/database administrators are responsible on those data. The data at the 'processing stage' is where interaction with people occurs.

Finally, transmission of data is either private network or public network. The transmission over the public network is possible to intercept by the third party. The connectivity has been established over either wired or wireless or both manner as per the nature of requirement (Hao & Foster, 2008). The wired network is much more secure than wireless, but healthcare requirements heavily rely on wireless technologies due to the mobility requirements; for example, Bluetooth or ZigBee due to the mobility of devices and people. It is essential to maintain connectivity in much secured manner to avoid third party involvement on transmission of data by intercepting the communication channel, considering those different aspects, it is essential to address all three forms adequately over both technical and non-technical aspects.

The third dimension of McCumber Model is Policy, Education and Technology to preserve information security (Whitman & Mattord, 2011). There are evidences supporting adequate technical implementations available in the current world, however these are not always followed by consumers due to their poor understanding of the importance (Whitman & Mattord, 2011). One major reason is the lack of awareness of people utilising these devices. As such, priority may be given to better education and training for people in the secure usage of existing technological infrastructure.

Moreover, policy implementation for consumers of PMDs, in both technical and non-technical aspects is required, when they interact with available technological infrastructure, since consumer introduces vulnerabilities unintentionally. A policy describes acceptable and unacceptable employee behaviour in specific environment. Further, technical implementations are also guided with policy to ensure required aspects are addressed. Same nature exists in the healthcare industry requirements for security of information.

The introduction of framework is the approach in this research for addressing information security needs. A technical approach aims to preserve information security by using lightweight encryption, which can be either using symmetric key cryptography or asymmetric key cryptography by reducing the impact on sensitive health data due to consumer's misbehaviours.

The information security considerations must be continually evaluated in any scenario, and one such approach is the Plan-Do-Check-Act approach (Siponen & Willison, 2009). This continual evaluation will include auditing and constant identification of new threats and their appropriate countermeasures.

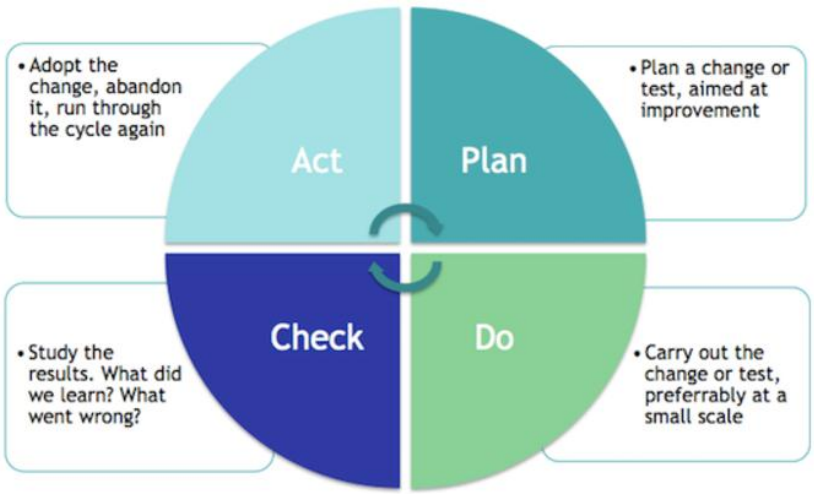


Figure 2: The Plan-Do-Check-Act Approach (Otterloo, 2017)

The Plan-Do-Check-Act approach is also applicable for healthcare environment for introducing a secure envirement to assure the information security (Darshan & Anandakumar, 2015). Risk management is the ultimate objective of this approach. The operational environment consists of information technology and human resources. It is a continual process with regular auditing to develop available mechansiams to assure the quality of the service. The reporting on security concern address accordingly, and the policy is well planned approach to assure secuity supporing existing technical implimentation to assure information security. The framework provides required intiatives for implementing policy.

The Information Risk Management interests on continuous use of technology in the healthcare environment introduce required countermeasures for affordable price. Further, the necessary legal requirements are also addressed in this stage. The Information Security Management considers the human resources in the operational environment of use of information technology. The quality and Performance Management is dedicated to auditing the environment for assuring the required quality.

The scope of information security consideration in above discussions is very broad, however this research focuses on considering socio-technical impacts on security of HIoT with the use of Personal Monitoring Devices(PMDs) only, because the use of PMDs is increasingly becoming popular among society, and the secure use of PMDs must be assured considering the sensitivity of the individual healthcare information (Hao & Foster, 2008).

1.2 Significance of the Study

The HIoT environment is complex due to the increasing use of devices and technological advances, however, it is essential to preserve information security over complex use to strengthen the trust of the user (Darshan & Anandakumar, 2015). The consumers should be interested in assuring that their healthcare information remains private due to the sensitivity of data, so consumers will not introduce vulnerabilities intentionally, however their own contribution is significant to the security of their data (Price et al., 2017; Zhou & Piramuthu, 2014). Even though HIoT is still evolving due to the variety of applications, technology and social view (Islam, Kwak, Kabir, Hossain, & Kwak, 2015), this research aimed to address the security aspects of HIoT specific to personal monitoring devices. The goal is to motivate consumers to use PMDs in HIoT environment by assuring information security. It establish trust for consumer to us PMDs.

The overall understanding of the use of PMDs in the HIoT environment is illustrated in Figure 3. People are the main unit, considering all other aspects are for the people to fulfil their healthcare requirements, leading to a better quality of life (Darshan & Anandakumar, 2015). People interact with devices to use the healthcare information generated for the PMDs, and the application software provides interface for stored data captured by corresponding sensors in the devices. The server side of either application or devices is a central place to keep data coming from different devices. The devices store data temporarily within the device temporary, and the data is synced with storage services for decisions making accordingly. All the involvements are shown in Figure 3 around the people.

Therefore, the potential impact of the research will be on all stakeholders in this environment:

1. the individual and their ability to play a part in the protection of their own information;
2. the device manufacturers who may better understand the needs of the users' security, and incorporate additional protections in the device design;

3. the application developers (who may or may not be the same as the device manufacturers), would be able to incorporate better user data security protections in the transfer and storage of data, and in advising the user of potential issues;
4. the medical practitioner, caregivers uses health data for assigning treatment and
5. the operating system/data storage device, usually smart phones, manufacturers to recognise the increased complexity and information security issues associated with using PMDs, and provide additional provisions in the handsets and operating platforms to accommodate PMD security.

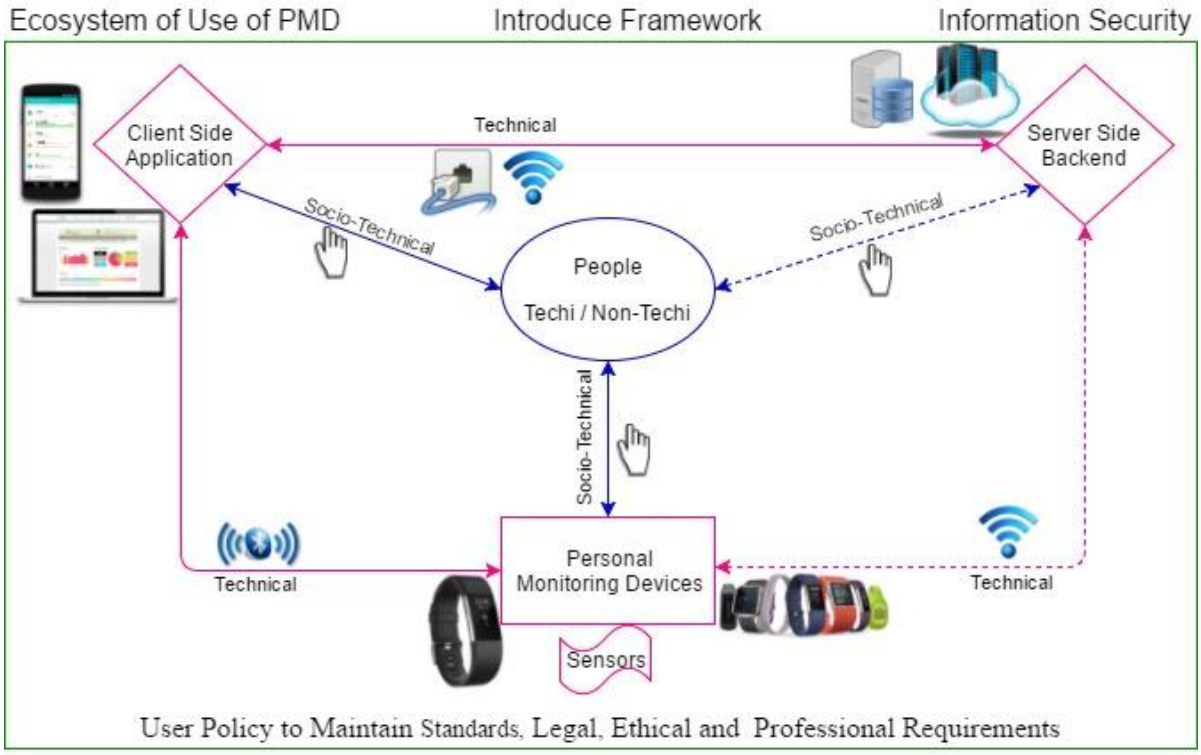


Figure 3: Conceptual View of the HIoT Environment of Use of PMD

1.3 Purpose of the Study

The use of PMD's has become more popular over recent years spurred forwards by the IoT technologies (Darshan & Anandakumar, 2015). However, this technological influence introduces more avenues for third party interception and security issues. Intercommunication with multiple sub systems over multiple connection technologies is the point for introducing security standards in such environment (Darshan & Anandakumar, 2015). It is not discussed in present research adequately, so this is achieved through the development of a socio-technical security framework.

The use of a PMD introduces vulnerabilities to the HIoT environment, and it has negatively impacted on available secured HIoT environment due to the poor understand of people. The PMD user keeps device unattended due to the poor interest of using, however it allows third party to capture device information leaking sensitive information violating the privacy. Further, PMD user enables Bluetooth in their mobile device to synchronise data captured, however it is not recommended to do in public areas considering possibility of third-party Bluetooth receiver around (Hao & Foster, 2008). Finally, use of untrusted Wi-Fi to synchronise captured data from the mobile device to storage space is not recommended, as a result trusted Wi-Fi connection and short range connection have identified as appropriate approaches (Darshan & Anandakumar, 2015).

Using Figure 3, this research has identified 5 areas for information security analysis:

1. the PMD;
2. the link between PMD and client-side application (possibly BLE);
3. the client-side application;
4. the link between client application and server-side backend; and
5. the server side back end.

The link between client-side application and server-side application has no unique consideration attached with the PMD, however there are common consideration on securely maintaining the link; malware, denial of service, hacking for example. Further, server-side backend specific considerations are not addressed here assuming there are enough research continuing in that area, since it is not unique for this research area.

1.4 Aim of the Project

There are existing technological solutions to assure secure use of information in three forms; storage, processing and transmission, but as shown in figure 3, socio-technical practices (the way people use them) creates insecurities due to the people involvement. Therefore, user is a threat to the secure use of information in healthcare (Huang & Li, 2010). Security measurements can be introduced technologically, but people are not allowed to maintain them. Moreover, there is not enough literature specific on security of HIoT in the use of PMD. Considering those aspects, preserving security in the use of PMD in the socio-technical aspects is the aim of the project.

1.5 Objectives of the Study

The objective is to facilitate a secure environment for the use of HIoT by introducing a framework to address socio-technical impact on security in the use of Personal Monitoring Devices. In this case, the framework is an explicit representation of theoretical findings and experimental outcomes allowing users of PMDs to evaluate critically. The theoretical findings of the research study are introduced the background for the experiment in this research for introducing a framework. Framework allows information security experts to intellectually transform the generalized context of the framework to several aspects of the different context benefiting the users of PMDs (Darshan & Anandakumar, 2015). Further, the framework introduces the limits, since it describes the key influencing factors of interest highlighting the need to examine how those key variables might differ and under what circumstances.

1.6 Research Question

Information security vulnerabilities are inherent risk of interconnectivity. As new vulnerabilities are continually discovered, minimisation of these vulnerabilities is the objective of this research. As a result, threats have no opportunity to exploit once vulnerabilities do not exist.

The research question is “Can a socio-technical impact framework be developed to assist users with the secure use of Personal Monitoring Devices?” The socio-technical impact framework is introduced followed by the guidelines for PMD users. Further, framework is introduced to evaluate the present environment for a greater understanding of potential improvements.

2 LITERATURE REVIEW

The findings of the Institute of Medicine of U.S. disclose that the healthcare on-time delivery of treatments is not consistent (Sungmee & Jayaraman, 2013). Over 98000 people die due to medical errors at hospitals in any given year, and this is more than the death of motor vehicle accidents, AIDS and breast cancer which are three significant causes in public health (Sungmee & Jayaraman, 2013). The early, systematic interventions are significantly important for many diseases avoiding risks towards the end of diagnosis.

The cost for healthcare is significantly high, and it is possible to reduce the cost while maintaining the high quality of services using the technology to support real-time monitoring (Kodali et al., 2015). Access to healthcare needs to be arranged for many people over the earth, because it is not possible to service all needs of the population at any one time (Huang & Li, 2010). Even, the specialised professionals are not easily accessible often due to time and distance(Whitmore et al., 2015). The use of technology using IoT will shift the cost for treatments to cost for prevention with the appropriate infrastructure. The Healthcare Internet of Things(HIoT) can reduce the stay in hospital providing effective decentralised healthcare facilities (Hao & Foster, 2008).

This literature review mainly focuses on two aspects; the environment of the HIoT, and the associated information security considerations. The approach of literature review is organised as follows.

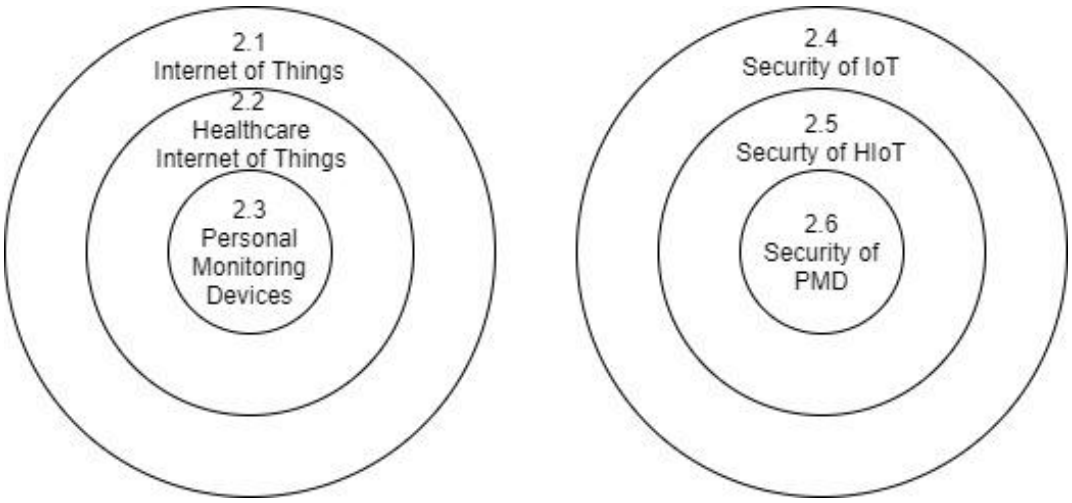


Figure 4: Approach for the Literature Review

2.1 The Internet of Things (IoT)

The Internet has been evolving constantly over last couple of decades. IoT is used as an umbrella term for covering various aspects related to the extension of the Internet to large scale embedded sensor devices interacting with the physical realm (Andrea, Chrysostomou, & Hadjichristofi, 2015). The trends are indeed observable in everyday life particularly in smart street lights, noise monitoring, traffic congestion detection, large scale waste management, smart homes and smart cities. The device mobility and overflow of data due to the sensing and communication introduces a very complex environment for IoT(Josyula & Gupta, 2016).

In the early days, a network of linked HTML codes residing on the Internet infrastructure was introduced as Word Wide Web in early days (Miorandi et al., 2012). Those static HTML documents were improved significantly by the introduction of Web 2.0 platform which enable two-way communication between two devices interactively, and the currently dominant Web 2.0 is focused to

enhance semantic web, and it is referred to Web 3.0 (Dong, Yian, Wangbao, Jianhua, & Yunlan, 2010; Valera, Zamora, & Skarmeta, 2010). The objective of Web 3.0 is introducing an environment which can be understood by machines, so the devices and search engines are able to be more intelligent (Xu, Wendt, & Potkonjak, 2014). The machine can involve the processing part without the involvement of human (Josyula & Gupta, 2016). Alongside the Internet technologies are developed in the Near Field Communication, sensor networks areas, and those influenced the evolution of Internet into Web 3.0 level (Josyula & Gupta, 2016). As a result, machine-to-machine communication is introduced over the Internet. It was a motivation factor for more machines to be online and intercommunicate, and ultimately it is introduction for Internet of Things (IoT) paradigm (Huang & Li, 2010).

There is no universally used and accepted definition of IoT, although the IEEE has attempted to establish a baseline definition (Josyula & Gupta, 2016), however the concept is to equip with identifying, sensing, networking and processing capabilities for devices allowing them to communicate each other devices over services on top of the Internet to accomplish some worthwhile objectives (Whitmore, Agarwal, & Da Xu, 2015).

Moreover the core concept of IoT is not totally new like use of sensor network, client-server communication over network infrastructure, but the use of technology is evolved such that the number and kind of devices, plus interconnection of networks of devices across the internet (Bandyopadhyay & Sen, 2011). As a result, most of the devices in the present world are capable to be part of the Internet with required networking supports for processing and storing data. Those devices go beyond the common devices like server, desktops, laptop, smart phones and tablet. The IoT based devices are attached to everyday devices like home appliances, healthcare, smoke detector, and audio/video receiver and traffic detectors.

Further, all those devices are based on sensors to detect naturally changing values , and there should be mechanism to connect with the Internet. For example, the product can be traced in the certain part of the supply chain for product specific information by using the Radio Frequency Identification (RFID) tag, however once product is away from the retail outlet, there is no use of RFID to track the device, and consumer is also unable to gain access to the lifecycle information of purchased product (Bandyopadhyay & Sen, 2011), so the IoT enables solution for that problem by allowing to trace the product throughout the life cycle by introducing unique identification for the product and having relevant data accessible over the web.

2.1.1 Technology

The everyday things are represented behind IoT such as vehicles, medical devices, general consumer goods, refrigerators, air conditioners for example, and those are equipped with sensing and tracking capabilities (Miorandi et al., 2012). These things must contain networking capability and more sophisticated processing capabilities enabling them to be smart objects for understanding the environment and interacting with the people. The IoT rely on hardware, software and architecture like any other information system, however those are not completely disjointed (Xu et al., 2014).

Hardware: the specific hardware introduces the unique infrastructure for IoT, and those already exist very commonly for example sensor networks, RFID and Near Field Communication (NFC).

The RFID uses both RFID tag and RFID reader. When the reader is close enough to the tag, the radio-frequency electromagnetic fields is used by reader to read the tag which is an Electronic Product Code (EPC) (Josyula & Gupta, 2016). Moreover, a universally unique number is used for the EPC for an instance of object. However, this is not a technology specific for IoT, but its tracking capability is very

useful for IoT implementation, and the extension of use of RFID is facilitating the relevant data to be available online remotely (Huang & Li, 2010).

NFC is a newer technology over RFID, and it is allowing devices to engage in radio communication with each other when the devices are close enough; short range communication (Josyula & Gupta, 2016). The NFC tag has unique way to identify; Unique Identifier (UID) (Castillejo et al. 2013). The smart phone utilises this approach to communicate with one another, when they are close enough. Moreover, the unpowered NFC tag, attached with objects, is also connected passively. The smart poster is one common use; it contains readable smart tag, and smart phone can read the data in the smart tag (Huang & Li, 2010).

Sensor networks: the characteristics like humidity, temperature, quantity and movement can be measured by using sensors. The Wireless Sensor Network (WSN) introduces when multiple sensors are intercommunicating for the same objective (Hao & Foster, 2008). The WSN can contain both isolated sensors and gateways for reporting multiple sensors to a server. The IoT is applicable for WSN, where sense of sensors is input for a system to react accordingly. For example, the sensor data is used for an actuator to perform an action accordingly. It might be emitting light, radio waves, sounds or even smells, and those are use of IoT in practice. The use of actuator in sensor network introduces sensor-actuator network, and it enables sensor to instantaneously be aware of the situation to interact with people needs. The use of sensors is common in a healthcare environment an example of which is a Body Area Network(BAN). Fitness trackers are also operated in the same way that a BAN works.

Software: the software facilitates the interoperability in between the elements in the IoT hardware infrastructure (Darshan & Anandakumar, 2015). Further, the data generated in IoT environment is utilised effectively by using software. More importantly, middleware is sitting in between application and data and hardware to facilitate numerous heterogeneous environment (Aberer & Hauswirth, 2006). It supports the different infrastructure element to introduce same set of services to access them, so there is no need to consider device wise in the IoT platform. The semantic middleware is based on XML and ontologies to interoperate among dissimilar types of devices communication through diverse communication arrangements (Huang & Li, 2010). It is similar to semantic web, and semantic middleware introduces general framework enabling data sharing capabilities across the devices located in different places.

The current search engines and web browsers are introduced to retrieve and index established web content, however the IoT environment consists with devices having mobility in nature and changing dynamically (Castillejo et al. 2013). Further, those devices produce enormous volume of repeatedly altering information. As a result, browsing is complex for IoT environment due to the addition requirement of recognizing smart infrastructure element, determining services and interacting those devices (Macias, Alvarez-Lozano, Estrada, & Lopez, 2011), and searching is also complex in that environment due to frequently altering information (Ostermaier, Römer, Mattern, Fahrmair, & Kellerer, 2010).

Architecture: the IoT architecture can be used effectively to represent overall structure. The IoT infrastructure is influenced by the layout of its sub systems; architecture of physical infrastructure, software, process and general (Aberer & Hauswirth, 2006).

The architecture of physical infrastructure is represented by hardware and network. The peer-to-peer architecture is very common with no intermediate devices, and it is very important part of IoT environment (Andreini, Crisciani, Cicconetti, & Mambrini, 2010). Moreover, an automatic-oriented

architecture is introduced for controlling the communications between these distributed entities through network devices (Pujolle, 2006). Finally, the different architectures are used for introducing the IoT as per different view points and standards in practice (Koshizuka & Sakamura, 2010).

The shared services are offered by the devices are access through software, so software architecture is necessary to understand using some services. The Service Oriented Architecture (SOA) is one common use of software architecture (James, Cooper, Jeffery, & Saake, 2009). Moreover, due to the service and flexibility consideration in IoT environment, the Representational State Transfer (REST) model is increasingly popular (Guinard, Trifa, Mattern, & Wilde, 2011).

The business process is influenced by IoT environment, so the process architectures are required to successfully arrange different workflows to utilise IoT effectively (Kawsar, Kortuem, & Altakrouri, 2010). The healthcare environment also has a unique nature with the introduction of IoT, so it is necessary to introduce relevant business processes. All systems are not unique as they share the common IoT denominator (Kawsar et al., 2010). There are various designs introduced at the conceptual level for considering the different requirements.

2.1.2 Application

The applications domain areas are introduced as per the use of IoT. As per the available literature, there are few domains of application; supply chain, social application, smart infrastructure and healthcare (Miorandi et al., 2012).

The supply chain is mainly based on sensor network and RFID. Assembly line manufactures uses sensors, and RFID is used for tracking the product through supply chain (Zhengxia & Laisheng, 2010). These technologies have been used for long time, but the use of IoT enhanced the effectiveness of those by ignoring the geographical boundaries for information to exist (Castillejo et al. 2013). It will link all the stakeholders, so the supply chain and logistics can work cooperatively with no delay. Further it reduces counterfeiting and improves product traceability (Darshan & Anandakumar, 2015).

The social applications are connecting peoples and objects to fulfil personal needs and social interaction, and Twitter, Facebook are possible example for that (B. Guo, Yu, Zhou, & Zhang, 2012). These applications are intelligent enough to gather events, locations, relevant advertisement, and prompt them accordingly considering present location, age group (Hao & Foster, 2008). The IoT enabled mobile phones can communicate directly with other devices, once predefined profiles are compatible.

The smart infrastructure introduces the property of efficiency, reliability and flexibility, moreover this introduces some cost saving due to the reduced man power and the enhanced safety (Liu, Li, Chen, Zhen, & Zeng, 2011). The sensors and actuators are used to introduce IoT in domestic and office environment for tracing utilities, monitoring and controlling environment and surveillance needs (Castillejo et al. 2013). Further, the energy consumption is important to consider, and smart grids facilitates a mechanism to collect related data and to make them available publicly by using IoT. The energy consumption can be analysed by using that data to come up with recommendation for energy saving. Considering a broad view, smart cities can be introduced by introducing traffic controls, indicating parking spaces and nature of air by connecting a large number of different and heterogeneous end systems (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014). The healthcare is another main application area, and this research focus on the healthcare separately.

Moreover, cloud computing platform is driving force of IoT for creating a smart world (Botta, Donato, Persico, & Pescapé, 2014; Josyula & Gupta, 2016). There are different types of services, but there are only two architectures; private cloud architecture and public cloud architecture (Hiremath, Yang, &

Mankodiya, 2014). The use of private cloud architecture is effective in a security sense, since there is no third party access, however it is expensive to establish and maintain. As a result, the public cloud architecture is popular, and the user is paid as per service requirement. Figure 5 illustrates the use of cloud in different approaches (Singh, Pasquier, Bacon, Ko, & Eyers, 2016). Visualisation represents the importance of use of cloud in different environments.

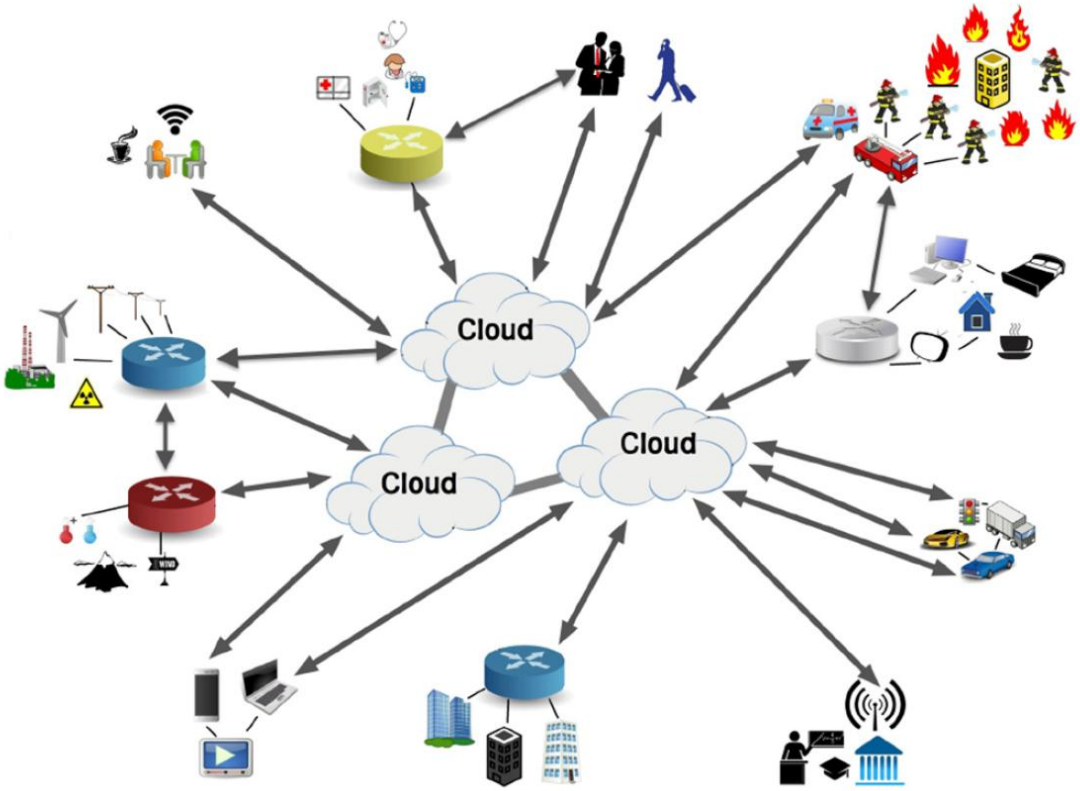


Figure 5: Use of Cloud in IoT environment (Singh et al., 2016)

The HIoT environment is unique over many other use of IoT, because sensitive health data use for making decision on treatment, so it is discussed separately in next section.

2.2 The Healthcare Internet of Things (HIoT)

The use of IoT in the healthcare environment is one another application of IoT, and it is known as HIoT. This approach redesigns modern healthcare infrastructure to another level with technological, social and economic evolvements from traditional healthcare approaches (Islam et al., 2015; Williams & McCauley, 2016). Further, chronic diseases, remote health monitoring, elderly care and fitness programs are most commonly evolved field with the use of IoT in healthcare.

Moreover, the healthcare providers are interested in HIoT for arranging medication and treatment for the patient living outside the hospital with remote monitoring approaches. Further, the efficient scheduling of limited resources is another advantage of HIoT. More importantly, HIoT is useful for reducing cost by avoiding hospital stays and treatments for example, rich user experience and increasing the quality of life (Islam et al., 2015), so it motivates people to use smart devices HIoT environment. There are numerous number of devices and systems contributes in different way for introducing this environment for HIoT.

There are medical devices to monitor different health conditions continuously and provide data for prediction of future health conditions (Sebestyen et al. 2014), and the expert systems are applied to

HIoT for patients to receive medical advice without going to doctor. As a result, the HIoT is predicted to reach a network of 26 billion devices with $117 billion market share in year 2020 (McCue, 2015; Williams & McCauley, 2016).

The present HIoT evolution is supported by different other technological approaches, and those are enhancement as improvement of following use of healthcare;

- **Telehealth** attempts to distribute the services related on health and required information through telecommunication technologies by means of electronic data. It allows new innovations to be introduced. For example;
    - **Tele-Home Healthcare** – the delivery of healthcare services to patient in home using telecommunication technologies; voice, video, healthcare data
    - **Tele-Medicine** – the clinical healthcare is provided remotely using telecommunication and information technology. It addresses the poor medical services in rural areas.
- **M-health** refers to use of mobile devices and wireless technologies in medical care, however m-health is effectively used for treatment support, disease surveillance, chronic disease management and epidemic outbreak tracking. This approach is increasingly popular with the increased performance of mobile devices.

Connected health is a socio-technical model for healthcare management and delivery, and technology is used to provide remote healthcare services (Islam et al., 2015). The connected health environment maximises healthcare resources facilitating useful chances for people to involve with clinicians and better self-manage of their healthcare, when the require care is needed outside the hospital. However, no standard definition can be found for connected health. It is an umbrella term introduced for reducing the misunderstanding of the definition of tele-medicine, tele-health and m-health.

Smart medical devices are unique as source of generating data of temperatures, glucose level, and heart rate for decision making for future health condition of patients by the hospitals or themselves for better care. More specifically, the Personal Monitoring Devices (PMDs) have some specific features. The sleep patterns, exercise patterns are also monitored implicitly. Those are attached with various nonintrusive sensors according to purpose and application available (Islam et al. 2015). Wearable devices must match with available HIoT architecture for intercommunication in between other devices and applications. The PMD specific details are discussed in the following section.

A **device** can be an instrument, machine, apparatus, implanted sensor (Williams & Woodward, 2015). There are many devices available in the market to facilitate healthcare requirement of people, and a device is attractive point for third party interception. Legacy operating system installed with devices are much more vulnerable, so it is necessary to update device software accordingly. Technical knowledge required for introducing intercommunication at the initial setup between devices must be done under supervision of technical person to avoid introducing common vulnerabilities; not having password, using default password, sharing password, sharing devices or unattended devices.

As discussed in the above section under the IoT, the **wireless technologies** are a significant supporting factor for enabling the mobility and data transmission needs of the HIoT environment, as a result, caregivers can arrange the required treatments (Castillejo et al. 2013). The transmission of sensitive healthcare information over wireless environment is always a risk, however the vulnerabilities in such environment has properly identified in some research, and alternative mechanisms have been introduced (Costantin, Sansurooah, & Williams, 2017). The Wi-Fi Protected Setup (WPS) protocol introduces four different authentication mechanisms for authentication; Personal Identification Number (PIN), Near Field Communication (NFC), Push Button, Universal Serial Bus (USB).

PMDs are vulnerable for **cybersecurity** too, due to the increased connectivity, and it is not a solely a technical problem. Better understanding of the complex of environment prevents cybersecurity incidents (Williams & Woodward, 2015). For that technical controls, regulation, standards and governance are required. Not only medical devices, cybersecurity incorporates with networks, operating systems, software applications leading to broad understanding. Different stakeholders' involvement is necessary for assuring secured environment. US Food and Drug administration is an example for one such authority responsible for quality effective service (Darshan & Anandakumar, 2015).

The introduction of Cloud computing influenced the evolution of HIoT due to the anytime-anywhere access. The public cloud architecture is more useful over private cloud with respect to the availability of access, however the private cloud architecture is much better for sensitive data (Lupşe, Vida, & Tivadar, 2012). Moreover, these devices are connected to cloud services in different ways considering limited storage and processing power available with devices themselves (Doukas & Maglogiannis 2012), and it facilitates anytime access of data for identified group of people. The centralized nature enhances risk of being vulnerable, since every accessing point is equally open for third party interception unless security practices are considered with priority. Encryption is used to send data over a public network to facilitate secure transmission, and storage services are also secured with encrypted data storage (Aberer & Hauswirth, 2006).

The PMD is uniquely identified among the devices in HIoT due to the specific use of PMD, and the details of PMD is discussed in next section.

2.3 Personnel Monitoring Devices (PMDs) on HIoT

There are many innovative medical devices in present world enhancing healthcare facilities (Hao & Foster, 2008). Even though there are many technological overlaps among them, there are four distinct group as in Figure 6 (Healey, Pollard, & Woods, 2015). This research focuses on the first segment; consumer product for health monitoring in figure 6. The PMDs are used for monitoring personal health condition in regular basis over long period of time, and the present HIoT infrastructure facilitates PMDs to interact with some other devices to store the personal healthcare data for evaluating to maintain health, diagnose a disease, or to monitor present health condition of patient in regular for example. With the motivation among consumers to maintain their health regular basis, PMDs add value for healthcare sector by improving quality of life through maintaining physical health.

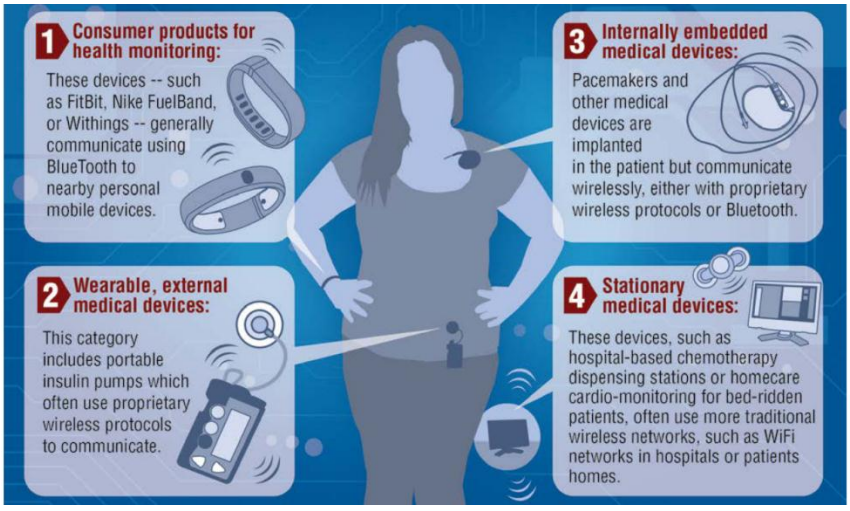


Figure 6 :Four categories of Networked Medical Devices (Healey et al., 2015)

There is documented history for the evolution of PMD. The conventional mechanical pedometer was introduced by Abraham-Louis Perrelet in Switzerland in year 1780 for military purpose to count the steps and distance while walking (Doukas & Maglogiannis, 2012). It was based on power a self-winding watch. The activity monitoring devices for personal use evolve from 1920 as per research findings (Mancuso, Thompson, Tietze, Kelk, & Roux, 2014).

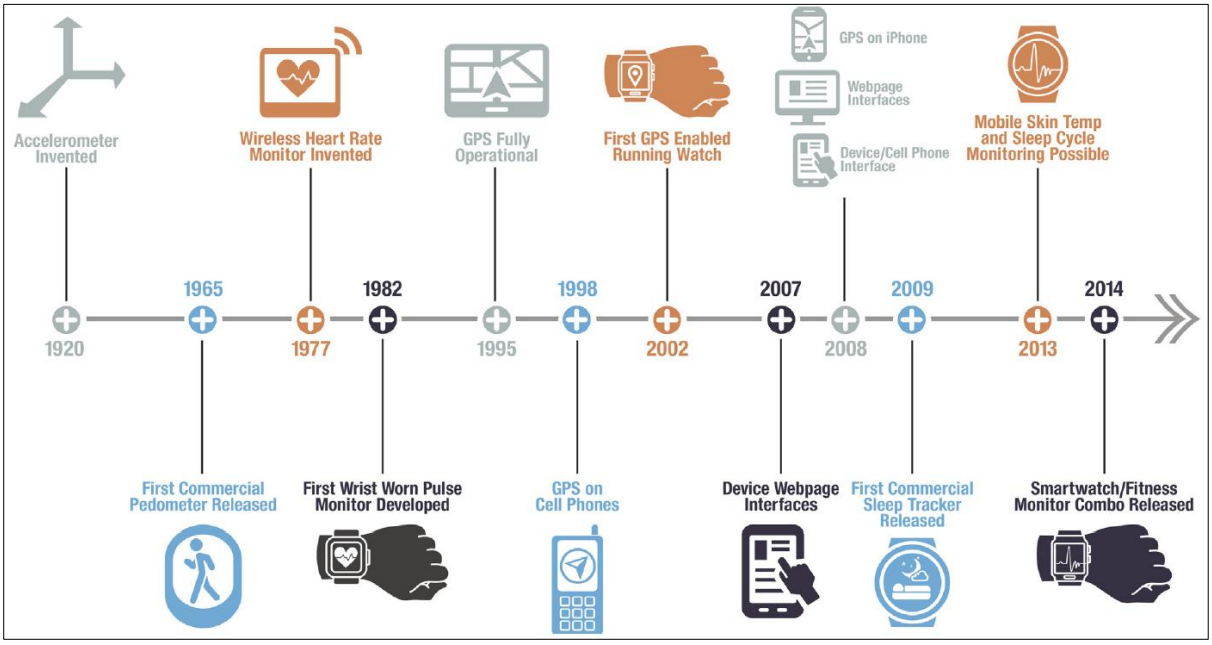


Figure 7: Personal Activity Monitoring Device evolution (Mancuso et al., 2014)

The conventional mechanical pedometer is obsolete approach with the introduction of electronic devices, further the evolution of HIoT introducing the platform for PMDs to interact with other computing devices seamlessly is also highly impactful on present use of PMDs (Mancuso et al., 2014). The PMDs are used for monitoring personal health status in regular basis to avoid having treatments, and the treatment for the patients are also based on PMDs to arrange required treatments with no delay. The first case is highly encouraged practice, since the quality of the life is maintained, and the cost for the treatments is significantly reduced (Aberer & Hauswirth, 2006).

A use of PMD for tracking physical activities is in practice for maintaining the quality of life with 'active living' by encouraging and enabling habitual physical activities (Altamimi & Skinner, 2016). There is a risk of becoming obesity and overweight due to the sedentary behaviour such as working with computer, playing video game, watching television, because those link with some health problems ultimately, and it is very common for children this generation (Gallo et al., 2017; Sallis et al., 2014). It is due to the technological enhancement, because the children are engaging with some activity otherwise (Sallis et al., 2014), however there are some technological solutions to overcoming such situations (Hnatiuk, Salmon, Hinkley, Okely, & Trost, 2014).

The technological solution is the pathway for introducing some physical activities as habitual actions. The PMD provides the good indicator for regular involvement of physical activities, then people acknowledge the need of physical activities to maintain their health.

There are different type of Physical Activity Monitoring Technologies (PAMT) for introducing PMDs; wristbands, waist-clips, and mobile applications, since the different vendors are using different approaches to record the same activity (Altamimi & Skinner, 2016). There are some research to demonstrate the accuracy of monitoring health of those different approaches (Altamimi & Skinner,

2016; F. Guo, Li, Kankanhalli, & Brown, 2013). Those research findings disclosed that minimising the time spent on sedentary activities may help in decreasing the risk of poor health. As a result, there are social, emotional and intellectual benefits (Hao & Foster, 2008).

There are set of guidelines for minimum level of physical activities for children and adolescents to have 60 minutes of physical activities in average per day, and the people in the age between 18 and 64 should accumulate 150 to 300 minutes of physical activities in average per week (Straker et al., 2016; Tremblay et al., 2011).

However there is research findings on decreasing relationship for participating in physical activity across age groups between childhood and adolescence (Brodersen, Steptoe, Boniface, & Wardle, 2007). There are different barriers due to such finding like unsafe neighbourhood, poor weather condition, a lack of parental time, energy (Gordon-Larsen, McMurray, & Popkin, 2010).

The recommendation for the number of steps are specified 12,000 steps for girls and 15,000 steps for boys for a day in general (Tudor-Locke et al., 2014) , however the adult is recommend to have 10,000 steps within a day in another research (Choi, Pak, & Choi, 2007). Furthermore that research is convinced, the large number of steps is an indicator for better health. There is rough consideration on daily steps and exercises, such that 60 minutes of exercise is equivalent to 10,000 -14,000 steps within a day for preschool children, 13,000 – 15,000 steps within a day for male, 11,000 – 12,000 steps per day for girls, and 10,000 – 11,700 steps within a day for adolescents (Olds et al., 2011).

These steps count can be accomplished during office activities, domestic activities, traveling, playing, so there should be mechanism to count steps at different scenarios automatically, and it must be accurate enough. There are many PAMT from earliest pedometer to latest Fitbit, however it is necessary consider the accuracy of the device before making the choice. There are some consideration in previous researches on the accuracy when the PAMT device is affected by the intensity of the activity and walking speed (Giannakidou et al., 2012; Lee & Gorelick, 2011).

Moreover, there is a research finding on low walking speeds, that distance is not accurately measured which leads to generate wrong statistics for consumer, medical practitioner for example (Takacs et al., 2014). There are many PAMT in the market at present with growing variations, and Fitbit is popular in the market due to the latest technology used for affordable price (Takacs et al., 2014), and the same study shows that the valid and reliable step counts are measured by Fitbit for multiple walking speeds. Moreover, good sleep is a direct influence on better health, so the quality of the sleep and the heart rate during the sleep is measured (de Zambotti et al., 2016).

Another approach is measuring blood pressure, monitoring heart rate and numerous other indices of health, and the present day evolution supports recording those indices of health constantly, and making them sync electronically with centralised system, and allowing the health care provider to monitor remotely (Altamimi & Skinner, 2016). The vendors and health care providers are confident on these technological evolutions helps on reducing the cost for the healthcare treatments (Reilly et al., 2006), so there is significant growth of manufacturing such devices, and the government of United State of America has reduced the cost for the treatment due to this impact (Sungmee & Jayaraman, 2013). In this research, the both approaches are considered in detail.

The BLE is the communication protocol addressing the energy constrains of PMDs, however it leads some other issues, and BLE protocol details are discussed at next.

2.3.1 Bluetooth Low Energy (BLE) Protocol

The Bluetooth is very common near field communication approach, and it has evolved into BLE to address the energy requirement constraints (Bluetooth, 2016; Gomez, Oller, & Paradells, 2012). More importantly, some devices have to be compatible with both platform to communicate, which is introduced as dual mode.

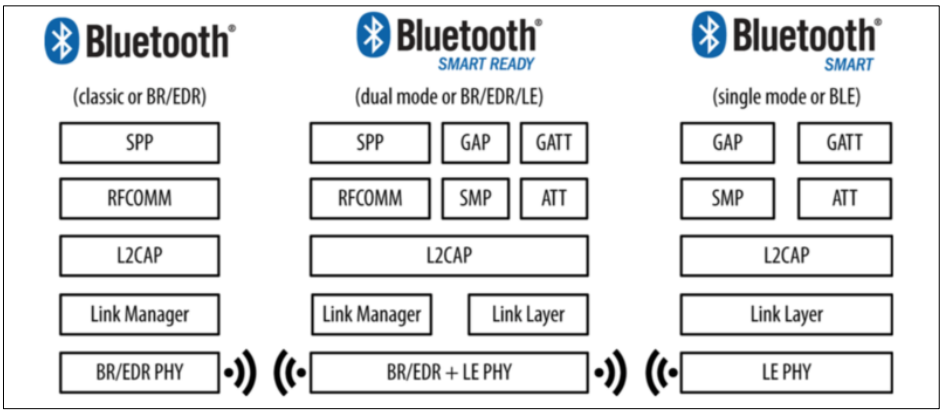


Figure 8: Bluetooth Protocol Structures (Bluetooth, 2016)

The communication in between PMDs and mobile/computer application software is based on BLE protocol (Bluetooth, 2016; Gomez et al., 2012). The experiment in this research focuses on technical aspects of communication. The Bluetooth and BLE are two different protocols, and both operate in the 2.4GHz ISM band. Bluetooth was designed originally for continuous streaming data applications, whereas BLE was introduced in year 2011 as Bluetooth 4.0 with low power consumption. BLE is positive approach considering communication among mobile devices, because applications may run for many years on a small battery with BLE.

In this context, BLE is the communication protocol due to that reason, however the information security consideration has not addressed adequately on BLE relative to Bluetooth. As a result, the possibility of intercepting BLE is relatively easy. In such situation, the experiment was considered for evaluating present information security implementation on BLE.

The following diagram illustrates the link layer operations in terms of states in a state machine of BLE (Bluetooth, 2016). Only one state is held by the Link Layer of BLE protocol structure as in figure 8. The advertising channel packets are used to transmit advertise state. Further, advertising state responses triggered by these advertising channel packets (Yan & Wen, 2012). The inherent delay is available in-between these states (Gomez et al., 2012), and it provides opportunity for third party involvement seamlessly.

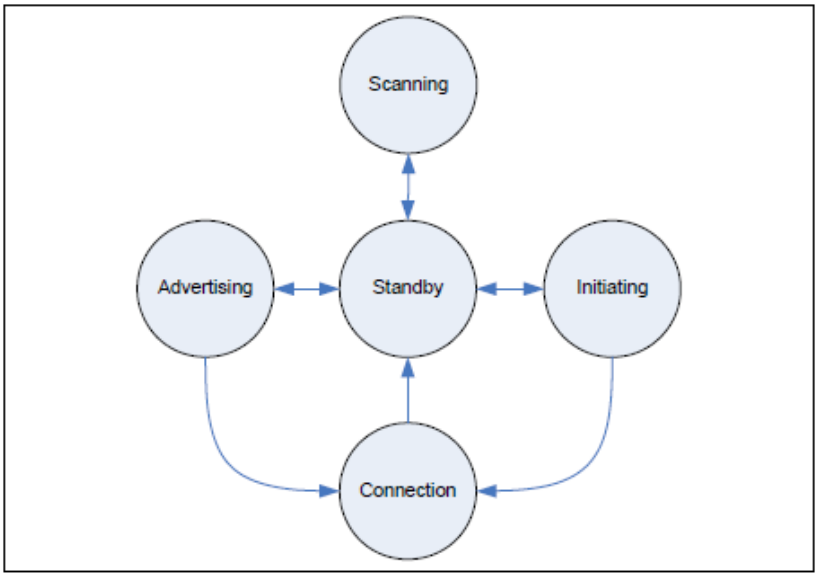


Figure 9: The Link Layer State Machine of BLE (Bluetooth, 2016)

BLE is not only low energy consumer, it is based on new development framework using generic attributes (Bluetooth, 2016). The BLE protocol stack consists two main part; the host and controller (Sungmee & Jayaraman, 2013). The controller includes the Physical Layer as small System of Chip with an integrated radio. The upper layer functionalities are in the host part; Logical Link Control and Adaptation Protocol (L2CAP), the Attribute Protocol (ATT), the Generic Attribute Profile (GATT), the Security Management Protocol (SMP), the Generic Access Profile (GAP) (Bluetooth, 2016). Further the Host Controller Interface (HCI) facilitates communication in between two main segments (Bluetooth, 2016).

The SMP of BLE facilitates device authentication, authorisation, integrity, confidentiality and privacy (Bluetooth, 2016). The SMP uses five keys for facilitating required functionalities; Temporary Key (TK), Short-Term Key (STK), Long-Term Key (LTK), Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK) (Bluetooth, 2016). Those keys are involved in pairing process of BLE in three steps; exchange of pairing information, authentication of the link and distribution of the keys (Sungmee & Jayaraman, 2013).

In first step, pairing request and pairing response SMP message are used, and the content of those messages introduce as per the device capability. In second step, authentication of the paring procedure is performed based on the information captured in the first step. The TK is generated in this stage in three ways; Just works, Passkey Entry, Out of Bond as describe in following table. There are flags to choose a method to pair at both ends; OOB flag and MIMT flag. In third step, keys are distributed using specific SMP packets and keys are encrypted with the STK.

Table 1: Temporary Key Approaches (Bluetooth, 2016)

Pairing Method	Just Works	Passkey Entry	Out of Band
Temporary Key (TK)	No use of TK	Six decimals	128 bit
MITM Protection	No	Yes	Yes
Notes	No authentication	Authenticated	Authenticated

The BLE does not support for strong security implementation (Gomez et al., 2012). As a result, security of use of PMD is always challenge due to the limited technical implementation, so the non-technical

aspects are also considered deducing the available literature in the field of HIoT. The countermeasures are introduced based on those understandings and following consideration on security in relevant field.

2.4 Security of IoT

The IoT is based on the Internet, sensor network and mobile communication network, so the security concerns of those areas are reflected in the IoT environment as fundamentals (Miorandi et al., 2012; Zanella et al., 2014). Additionally due to the great potential of IoT; wider deployment, huge generation of information, use of wireless technologies in public locations, increasing number of software/network attacks, device mobility and dynamic changing environment the security of IoT is an increasingly challenging factor (Xu et al., 2014), and there are many research projects focusing in that area (Xu et al., 2014). Further, the evolution of the field of IoT is challenged due to the security concerns, or the development of IoT is a threat to the information security of IoT (Xu et al., 2014).

An exceptional wide scope is introduced for security of IoT with five dimensions; trusted sensing, communication, privacy, digital forgetting and computation (Xu et al., 2014). The traditional security is almost obsolete facing the increasing complexity of communication system and attacks, because they are overwhelming limited resources to sustain the essential level of security (Sungmee & Jayaraman, 2013). The overhead cost reaches high rate and the security is automatically inefficient and inappropriate. As a result, new mechanisms must be introduced by addressing the nature of IoT to preserve security.

The IoT security needs have been addressed in two manner; consists of required security tasks and related to design metrics such as latency, cost, size and energy requirement (Xu et al., 2014). The devices in IoT environment are mostly mobile devices and they consumes battery power (Wander, Gura, Eberle, Gupta, & Shantz, 2005), and present use of application; like geo localisation, real time processing, consume much battery power. One use of real-time processing of security mechanism influences on limited resources available and power. As a result, a minimum level of security mechanisms are implemented, however it does not facilitate absolute level of security. This results in some attack to be successful.

Moreover, **cryptography** is most commonly used approach for securing information, however many IoT devices are not capable of supporting encryption due to performance issues (Yan & Wen, 2012). The initial configuration is done securely using encryption, but synchronisation of data is not encrypted in many scenarios. As a result, efficient algorithms are introduced for reducing energy cost to facilitate encryption in IoT environment. On the other hand, cryptography is not capable to assure the security alongside new attacks such as information leak due to jamming over WSNs (Yan & Wen, 2012).

Identity management is an important factor of a security model, and each IoT device has a unique identifier (Mahalle, Babar, Prasad, & Prasad, 2010). Moreover, the shared system must be monitored enabling mechanism for authentication for authorisation for the resources. Further, these identifiers are important to identify the device user for accountability and auditing requirement.

The trade-off among **security mechanisms and performance** are utterly important for investigation of new techniques (El Maliki & Seigneur, 2010). For example, the overprovisioning of security wastes additional processing and transmission resources. The adaptive security mechanisms are also introduced for wireless IoT environments based on security architecture and context aware access control by prompting completely reconfigurable architecture (Lacoste, Privat, & Ramparany, 2007).

Cloud computing has enhanced the use of IoT by incorporating sensors, smart devices, networks together. Further, the use of cloud computing introduces new set of security consideration for IoT environment from the perspectives of end-user, tenants, provider, wide scale context and cross platform functionality (Yan & Wen, 2012).

However, still there are many more challenges to be addressed in both sociological and technical aspects which are going to be addressed in this research. The fully interoperability among interconnected devices for high degree of smartness by empowering autonomous behaviour of them and adoption. The security consideration of HIoT is discussed in next section separately.

2.5 Security of HIoT

Though the HIoT facilitates a new environment with interoperability, each endpoint is a probable point of vulnerability for complete network (Williams & McCauley, 2016). The security of HIoT has different security considerations than IoT due to the sensitivity of healthcare data(Williams & McCauley, 2016). The conventional static security is almost obsolete facing the increasing complexity of communication system and attacks, further the healthcare environment has unique nature. As a result, there should be additional consideration for achieving principle of adaptation for the healthcare environment.

The complexity of security in HIoT increases due to many reasons; limited processing and storage capabilities, low power design and lack of standard interfaces (Williams & McCauley, 2016). Furthermore, the use of outdated hardware, operating systems and application software are well known vulnerabilities for any system (Yan & Wen, 2012). The influence of sensitive healthcare information is significant against all other information, because it is leading to wrong treatment leading to death. Also, there are regulatory issues inherent in the heterogeneous connectivity of the environment, as endpoints are possible access points for attacker (Williams & McCauley, 2016).

Though there are many advantages for healthcare sector by adopting IoT, the information security adaptation is not adequate. The technology implementation for information is limited due to the resource constrains, so HIoT relies on trust between people including consumers, operators and institutes. The use of PMD's makes the situation more complex, and next section talks about significance in such environment.

2.6 Security of PMDs

The security of PMDs is far more specific over security of HIoT considerations in line for the available limited resource of PMDs and the unsecured public environment (Kirby, Kirby, & Birch, 2016). Furthermore, the technology with weak security implementation is a challenge for healthcare information security. The PMDs have limited internet connectivity, however the available techniques of PMDs for assuring information security is lacking during collection, transmission and storing especially dealing with personal health information. As a result, the influence of people is considered with priority to reduce the risk of unauthorized access on information. Nevertheless, there is a significant risk for the information security as unsecured endpoints are more vulnerable; outside a controlled environment (Scheffler & Hirt, 2004). In that environment, it is not recommended to synchronise captured data from mobile device to the storage space using wireless network, because a third party is able to compromise wireless networks. It results leakage of sensitive information (Yan & Wen, 2012).

Moreover, the sensors in PMDs capture healthcare information and synchronise with different applications using different techniques such as Bluetooth, Bluetooth Low Energy (BLE), NFC and Zigbee

(Cyr, Horn, Miao, & Specter, 2014). Of course, the security of PMDs is additionally constrained in comparison to HIoT, due to the very limited resource available on wearable devices (El Maliki & Seigneur, 2010). Nevertheless, the technology with weak security is a challenge for healthcare information security. Whilst PMD connections can use different communication protocols (e.g. Zigbee, Bluetooth, BLE), the security functionality of PMD across the protocols is variable and inconsistent. This makes such protocols problematic for the secure transfer of personal health information (Yan & Wen, 2012). The available literature specific for PMDs is not sufficient, so alternative research to identify the issues for IoT is needed to understand the possible vulnerabilities.

2.7 Vulnerability of PMDs

The list of vulnerabilities is introduced as shown in table 2. The vulnerabilities are significant enough to introduce potential damage as per the findings in the literature. The description focuses in the use of PMDs in HIoT environment.

Table 2 – The List of Vulnerabilities.

Vulnerability	Description
Non-Technical Vulnerabilities	
Theft	Intentional and subsequent impact / damage high.
Lost	Unintentional but subsequent impact / damage may high.
Unattended Device	The device information can be captured, and the stolen information used for intercepting device communication.
Enable Bluetooth Always	The third-party Bluetooth receiver may be listening to information to capture sensitive information.
Enable GPS Always	This allows to violate privacy of the information, so it is necessary to identify the need of GPS for reducing the influence.
Eavesdropping	The user's credentials for application access may captured.
Human Error / Failure	The user error may lead to information leakage.
Missing, Inadequate Policy	Insufficient policy implementation advising the user about the significance and sensitivity of their health information.
Missing Security Methods and Tools	There is no enough use of security methods and tools to assure information security. For example, mobile devices does not use password.
Social Engineering	Social communications with the potential impact of stealing sensitive information.
Social Networking	Sharing personal health information over social networks may violate and put at risk an individuals' privacy.
Technical Vulnerabilities	
No Use of Encryption	Some devices do not use encryption due to the additional processing power.
No Use of Authentication	The authorisation is based on a 4-digit pin code in most of the cases, but no use of other authentication for the device.
Technological Obsolescence	People use devices over several years, and new technological evolution may make the devices and security measures obsolete.
Multiple Connectivity	The PMD uses NFC to communicate with application, and application synchronise data on storage space over IP network: introducing standards is complex in such environments.

Inherent Latency of BLE	The inherent latency of BLE introduces opportunity for attacker to represent legitimate traffic.
Software Attack	Mobile applications and web communications can present risks due to a software attack focusing configuration change, and capturing data.
Quality of Services	The endpoints are not capable of buffering traffic for the handshaking process to assure effective quality of service.
Man in the Middle	Third parties can intercept the communication media to listen passively. Brute force attack is also possible.
Communication Medias	Bluetooth and BLE are popular among PMD, whilst Zigbee, WiFi, and GSM are possible, more secure alternatives.
Denial of Services	Legitimate traffic is interrupted by introducing false traffic into the communication pathway, creating a jamming effect.
Tampering	Intercept the communication to insert unauthorised configuration into the device to forward legitimate traffic through unauthorised pathway.
Phishing	The use of email must be handled with strong attention without disclosing sensitive information for unauthorised parties.
Pharming	Device generates data, but it might be synchronised into third party before syncing into the legitimate device.
Web Application Attack	The web application is entry point for personal health data, so multiple factors involves in web application attack.
Spoofing	The use of email may mislead the user introducing entry point for sensitive personal healthcare data.

The above list of vulnerabilities identifies the possible vulnerabilities in the use of PMDs. The non-technical approaches to security are common for the IoT environment, however some of the technical vulnerabilities are unique for PMDs due to the resource constrains (Darshan & Anandakumar, 2015). Furthermore, technical experimentation has not been conducted to evaluate the issues associated with PMDs on the capture of BLE communication, so this research initiates something for future researchers to consider on evaluating BLE communication. Moreover, both technical and non-technical aspects are equally important for close consideration to introduce a socio-technical impact framework to address the research question.

3 METHODOLOGY

3.1 Theory Supporting the Study

People are more and more concerned with their personal health. Subsequently, the healthcare sector is evolving progressively to use and embrace IoT infrastructure (Hao & Foster, 2008). Moreover, the personal health related information is very sensitive due the privacy, and there is a need to address information security concerns in the complex IoT environment. The use of PMDs in the HIoT is a sub set of that information security consideration, and this research is concerned with how the use of PMDs is influenced by the security of HIoT.

Healthcare information flow is complex due to the contribution of many stakeholders. Data is generated in some devices, and stored in other storage devices/platforms, and accessed via smart phone or computer. This environment introduces the involvement of different sub-systems which is crucial. The influence of people on information security when they interact with subsystem of information systems, has not been addressed adequately, even though technical considerations are at a satisfactory level. Moreover, the inhibiting good security practices based on trust is the primary tool considering the poor performance of personal monitoring devices to introduce advanced technical implementation.

As a result, this research can be introduced as information system research. The field of information system researches consists of different research as shown in the Figure 10 from experiment to conceptual studies, whereas positivist focuses on observable phenomena and interpretivist considers analysing specific environment by observing the people of environment in situation (Williams, 2006).

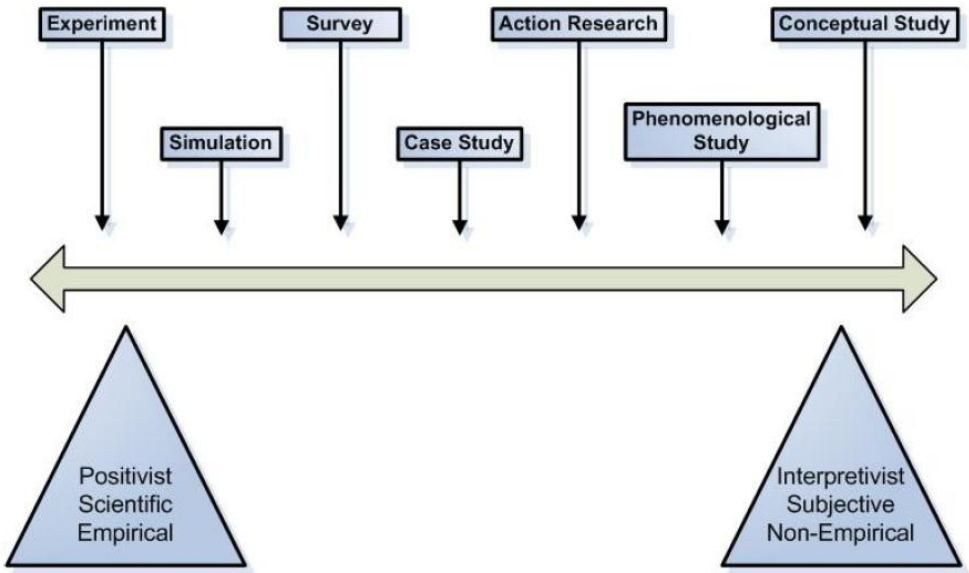


Figure 10: A Continuum of Approaches to Information System Research (Williams, 2006)

Positivist approach focus on positive aspect and observable phenomena to reject fundamental nature of reality and theism (Williams, 2006). It is focusing the interrelationships between elements in the environment under review. However, number of variable in the environment influencing research consideration, the outcome of the research is arguable.

Interpretivist approach is based on social interaction (Williams, 2006), which is against to the positivist approach, since there is no pure consideration on social interaction. Here, people, affect and are

affected by, is influenced in the social behavioural environment, and interpretivist approach addresses such situation qualitatively.

3.2 Methodology Selection

This research is addressed in different approaches in three phases. The case study is the first approach for having thorough understanding of the field of IoT and HIoT, and it is followed by specific understanding of PMDs in IoT environment. Then the security consideration of all the aspects is analysed using the available literature. The further research is continued to address the issues identified to improve the present level of security in the Healthcare environment in the use of PMDs. It is interpretivist approach rather than positivist.

The involvement of the experiment is the most appropriate approach for better understand of security concerns as per the factors find in the case study. The experiment is purely positivist approach; however, the experiment is for finding details of identified vulnerabilities. As a result, experiment provides some reflection, this research can be introduced as information system research, which is identified as interpretivist study after overall consideration. The fundamental approach of doing information system research is shown in Figure 11.

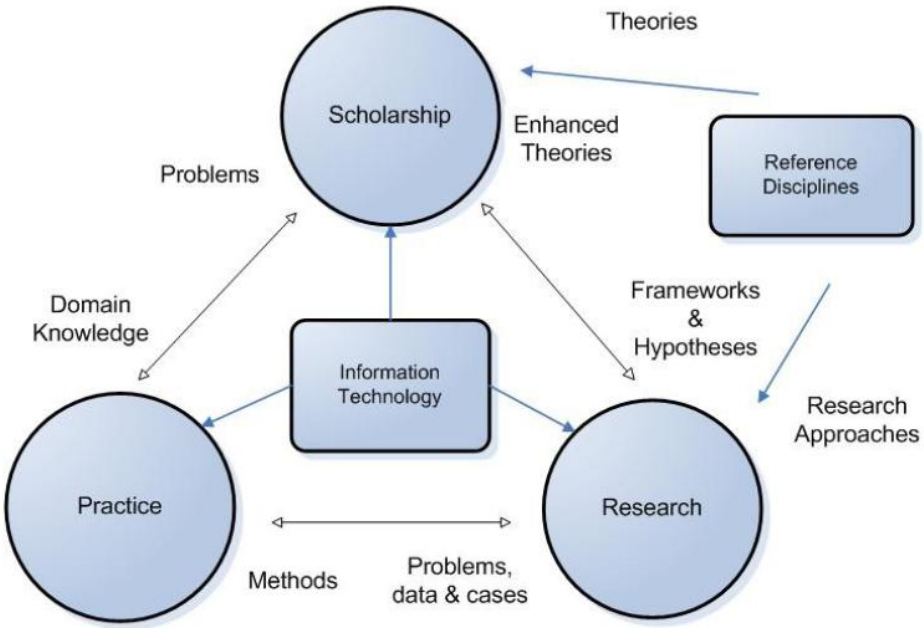


Figure 11: A Model of Discipline of Information Systems (Shanks, Arnott, & Rouse, 1993)

"Information systems is concerned with the effective use of information technology by people and organizations" (Shanks et al., 1993), and Figure 11 illustrates how an information system research model is developed. In this research, the thorough domain knowledge helps to find research question. Then different methods; case study and supplementary experiment accessing actual data, are planned for the research. The research outcome is a framework enhancing theories for someone to consider for implementation. The IoT, HIoT disciplines are referred for developing case study as reference.

3.3 Methodology

The methodology introduces the approach to achieve the ultimate objective of the research. The research question considers the possibility to improve socio-technical impact on security in the use of personal medical devices by introducing a framework for the secure use of PMDs. Further guidelines

for the PMD users are introduced focusing the present understanding of importance of assuring information security.

Firstly, in the literature review, there are two sections; better understand of the specific environment and security considerations of all aspects of the environment. At the end, it introduces a list of vulnerabilities and some solutions available at present. Those involvements are qualitative.

Secondly, a supplementary experiment is conducted to verify the influence of PMDs on secure environment for evaluating technical impact focusing the identified vulnerabilities, which is quantitative. The non-technical vulnerabilities are evaluated further in the domain of use of PMDs qualitatively. Then, the countermeasures are identified for assuring the information security in a qualitative manner.

Thirdly, a framework will be introduced for introducing policy to improve the security of information based on the human security factors of HIoT. That framework will help to communicate the challenges to be addressed in the use of PMDs in HIoT environment. As a result, the likelihood of exploiting on vulnerability resulting in a reduction of risk to information security. Finally, the guideline for the PMD users is introduced for their consideration. The both framework and guidelines are qualitative approaches.

3.4 Research Design

The research design has been introduced considering the methodology of the research, and three phases are introduced for the research as shown in following Figure 12. Each phase introduces an outcome, and it is input for the next phase.

In phase 1, the case study is conducted for detail information of HIoT and security consideration of HIoT by evaluating the literature, however these aspects only focus of using PMDs. The analysis is conducted synthesising the available literature for the conclusion considering both aspects. The use of PMD in HIoT environment evaluates for identifying vulnerabilities.

In phase 2, the experimentation is considered for design requirement with the exact understand of findings in the case study, and the Fitbit and Garmin are used for experimentation to represent PMDs, since those are popular among consumers. Nevertheless the present researches had not focused on use of Fitbit and Garmin in this perspective of information security. The Fitbit is Fitbit Charge 2 special edition, and the Garmin is Garmin vivosmart HR. Those fitness trackers capture some data automatically through the sensors, but it is essential to enter some data manually; drinks, foods, encouraging the consumer to maintain personal health with positive health habits such as calories in. The following steps are considered for the experiment;

1. A device; Fitbit/Garmin, is configured for Android smart phone
2. The smart phone is configured to capture Bluetooth communication
3. The active communication between a device and a smart phone is introduced to capture Bluetooth communication into log file
4. The Bluetooth sniffer log is collected for analysing it for specific information over Wireshark

Even though there is no exact outcome as a result, the meaningful information for consumer/medical practitioner can be visualised with relevant to the exercise, heart rate, diet and sleep facilitating physical, mental and cognitive well-being to the society. The captured health data is synchronised with the mobile device over BLE protocol, and that communication can be captured; the Bluetooth Sniffer Log, which generates from Android operating system of a mobile phone to evaluate BLE

communication. In addition, android applications are also used to capture device information; BLE Scanner, BlueScanner. The countermeasures are introduced at the end of this phase to assure better security.

In phase 3, the mitigation approaches are identified for the countermeasures identified in the second phase. It addresses the secure use of PMDs in HIoT environment. The user must contribute to the preservation of security while using PMDs, so the guidelines for the usage of PMDs are also introduced. The following diagram illustrates what the actual research is about in details steps.

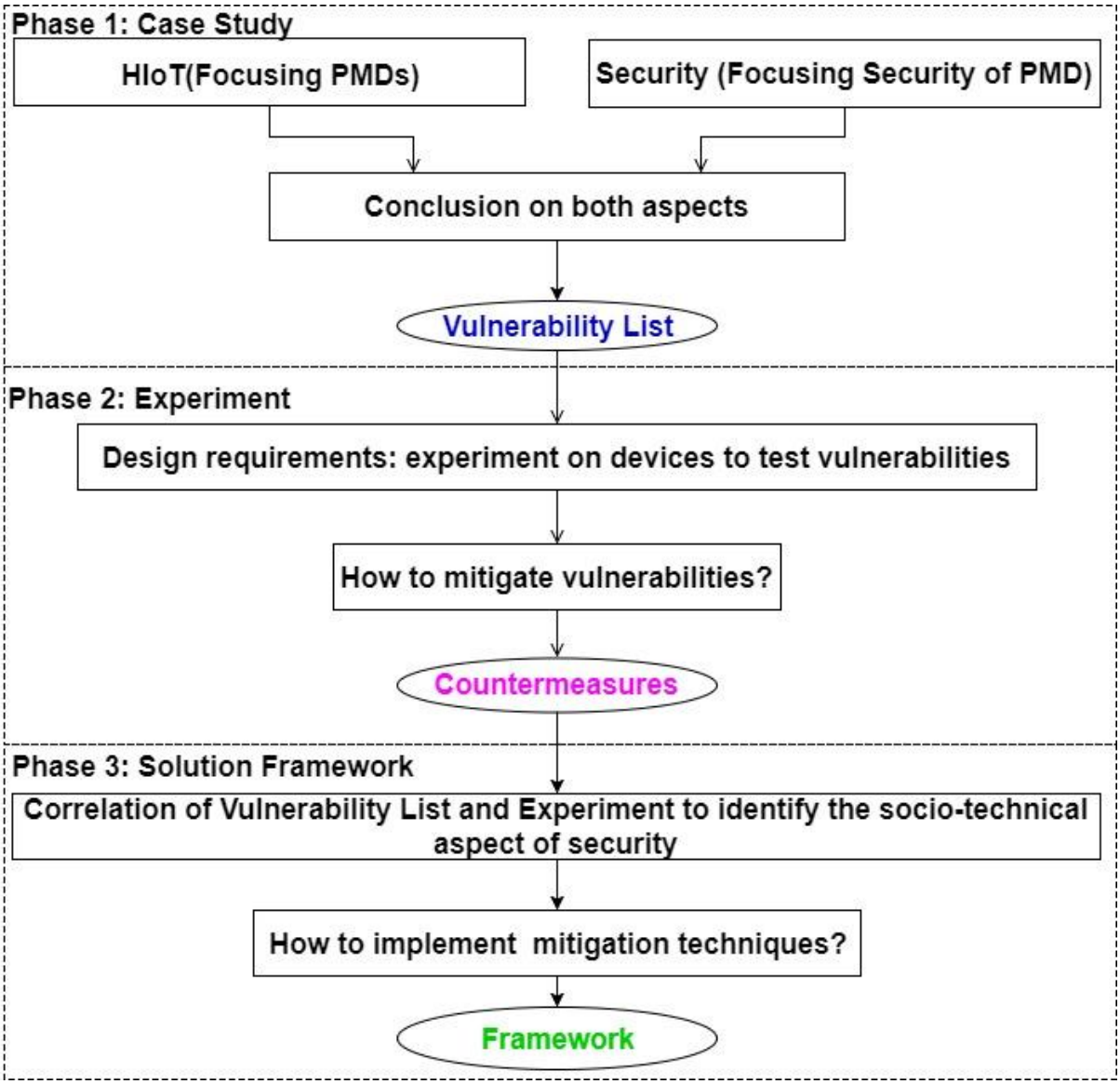


Figure 12: Research Design

3.5 Expected Outcomes

As discussed in the literature, with the evolution of IoT, healthcare industry has developed by introducing convenient use of HIoT. Enough technological implementations, such as devices, connectivity technologies, applications, are available, but people and organizations are reluctant to adopt them considering the sensitivity of healthcare information mainly (Darshan & Anandakumar, 2015). Furthermore poor understand and trust also significantly influence to embrace PMD. On the other hand, some people use those technologies due to their interest, but they do not have enough knowledge about the approaches to assure information security by considering information security

violation incidents. Emphasising people that about the importance of using the PMDs in the HIoT environment and approaches to assure sensitive healthcare information are utterly important. This research would be able to address such issues to encourage people to use HIoT securely with better understand of guidelines.

As part of the ongoing research on security of HIoT research, this research focuses the influence of PMDs for the security of HIoT. Further, a framework is introduced for avoiding such happenings to preserve security. The framework guides information security experts to start with some solution to assure the information security. Moreover, guidelines for the user are also introduced.

3.6 Limitations of the Study

The research focus is the socio-technical impact on the secure use of PMDs, and there is a lack of previous research in this area. Further, there has been no experiments conducted with the PMDs which use the BLE protocol for communication in the literature, so an experiment conducted in this research provides some initiative for experiment. Nonetheless, this research does not provide a comprehensive perspective on the experimentation, only a preliminary one. Furthermore, the security of HIoT is popular topic, and its scope is vast, so relevant details are gathered to develop literature on use of PMD.

This research uses the Bluetooth Sniffer Log generated by Android platform, however there was no opportunity to capture some important information from Bluetooth Sniffer Log due to the nature of its representation; log does not show the device identities. As a solution, the different Android applications are used against that; BLE Scanner, BlueScanner, to capture device information.

Whilst it would have been ideal to also capture user experience data in this research, the limitations on project size meant that this is an aspect to be considered for future research. The limitation of the case study method, is that the formulation of the resulting framework is a summation of the existing literature and experimentation, and is representative of existing knowledge only.

Lastly, use of Fitbit and Garmin devices for the experiment do not give a wide representation for a general conclusion, since there are various PMDs out in the market. Nevertheless, the influence of a manufacturer on research misleads the outcome, as a result the developed literature might not valid.

4 RESULT

This section includes the experiment to evaluate on some vulnerabilities and threats, and the list of countermeasures are leading to the framework implementation.

4.1 Phase 1: Case Study

The case study is a part of the literature review, and the list of vulnerabilities are the outcome of this phase as shown in the Table 2. The vulnerabilities have been identified in two categories; technical and non-technical in that table.

4.2 Phase 2: Experiment

As mentioned in the research design, the experiment is focused on two fitness trackers as PMDs considering the recent popularity for people to use fitness trackers; Fitbit and Garmin. The list of vulnerabilities and threats are listed below with the approaches; technical/non-technical, to evaluate and with relevant outcome. The Bluetooth Sniffing Log is the main source for the experiment for technical measurement, however there is some limitations due to the parameters disclosed in the log; does not discloses MAC addresses. Further, the captured data is not readable, however there is no exact understanding of use of either encoding or encryption although data is not in understandable form. The flow of the communication does not show any key sharing approach, so it should be encoding which is not acceptable for sensitive health data. The encoding is easy to extract health information, then it is recommended to use light weight encryption. Appendix A and appendix B include examples of captured communication, such that Bluetooth Sniffer Log is opened in the Wireshark.

As a result, experiment was not success as planed due to the limitation of Bluetooth Sniffer Log introduced in Android platform; it does not disclose device information. However, some other android applications were used to capture additional information of the PMDs; hardware address, memory, processing power. It could be better finding of this research, since future researchers will not plan their research based on Bluetooth Sniffer Log of Android.

The other approach to capture the Bluetooth traffic is the recent open-source project named “Ubertooth”. The “ubertooth-btle” utility tool of Ubertooth suite can capture Bluetooth communication for evaluating captured data with better findings. This would influence present outcome of the research with the use of the Bluetooth Sniffer Log of Android.

Then, the non-technical considerations are evaluated adapting the available literature towards the nature of use of PMDs. The outcome describes the influence for exploiting vulnerability and threat in action. The overall understand of the experiment is summarised into the Table 3 which leads for introducing countermeasures.

Table 3: Vulnerabilities and Threats

	Technical	Non-Technical	Approach to evaluate	Outcome
Vulnerabilities				
V1 - BLE Connectivity		x	The BLE has introduced for low energy consumption, so there is no comprehensive security implementation has considered.	There must be additional consideration in the use of BLE due to the poor security implementation.
V2 - Use of Encryption for Pairing Key/Data	x		**Bluetooth Sniffing Log** is analysed focusing the initiating data to verify the nature.	No use of encryption for data, however encoded date is used.
V3 - Use of Identifier	x		**Bluetooth Sniffing Log** is analysed focusing the streaming data to verify the nature.	No use of identifier.
V4 - Latency	x		**Bluetooth Sniffing Log** is analysed focusing captured the timestamps for observing latency.	There are inherent latencies allowing enough time for third party access allowing MIM.
V5 - Enable Bluetooth Always		x	The established Bluetooth connection transmits sensitive health data in public area allowing third party receiver to capture sensitive information as per the literature.	The sensitive health data leaks to third party.
V6 - Availability		x	PMD is used for continuous monitoring of health, but it is possibly not available due to some reason.	It is necessary to introduce situation specific countermeasures to address such concerns.
V7 - Energy Requirement		x	Many PMDs facilitates with BLE for transmitting data, so it allows reasonable life time for device.	PMD must be selected considering the energy requirement to have continuous service.
V8 - Multiple Connectivity	x		One Master may maintain multiple Slaves introducing data loses for overloaded processing.	The overloaded master may drop sensitive data leading for wrong treatment.
V9 - Use of GPS		x	The GPS enables consumer to track jogging pathways, however it allows to track consumer.	It influences on privacy allowing someone else to know consumer's location.
V10 - Technological Obsolescence	x		Monitor the hardware/software are used in the PMD and mobile application.	It allows opportunity for third party interception influencing on the security.

V11 - Missing, Inadequate, Incomplete Policy or Planning		x	The vendor specific policies are available; however the context of consumer use has not considered.	Consumer has no understand about the secure use of PMDs due to that, so it is necessary to introduce context specific policies.
V12 - QoS Deviation from the BLE Device	x		The delay in-between devices and variation of the delay, the provided bandwidth and packet loss are essential to maintain.	The BLE facilities acceptable services, once QoS are assured. Otherwise, there is data loose which is not acceptable due to retransmission.
V13 - QoS Deviations of Wireless Communication Provider	x		The QoS of WiFi or some other technology facilitates communication through the Internet to synchronise with data storage.	It is essential to maintain QoS to assure the effective communication is taken place avoiding retransmission.
V14 - Database Server	x		At present, there is no idea where data is stored, so this is for future consideration.	It is essential to introduce an approaches to access data for the owner of them.
V15 - Mobile Application	x		The sensitive health data is frequently accessed over this application, so the influence of the mobile application is considered.	The mobile application is updated automatically over the Internet to avoid any obsolete, however use of device is influenced.
V16 - Web Server	x		The sensitive health data is accessible over the web, so influences of the webserver must be considered.	The manufacturer is responsible for maintaining security at that end.
Threat				
T1 - Theft / Stolen Device		x	Available literature discloses the significance of losing device.	The policy must be addressed to acknowledge the significance of impact.
T2 - Data Theft		x	Available literature discloses the significance of losing data. Alternate treatment is offered.	The policy must be addressed to acknowledge the significance of impact.
T3 - Tamper with PMD	x		The unauthorised access can happen for changing configuration to redirect data channel for unauthorised party.	**This is not focused** in this research, but it is important aspect to consider.
T4 - Tamper with Mobile/ Laptop	x		The unauthorised access can happen for changing configuration to redirect data channel for unauthorised party.	**This is not focused** in this research, but it is important aspect to consider.
T5 - Eavesdropping		x	The leak of credentials allows unauthorised access to health data introducing many alternations.	The policy must be addressed to acknowledge the significance of impact.

T6 - Signal Interception	x		The Bluetooth uses frequency hopping techniques for assuring information security, catering additional complexity	**This is not focused** in this research, but it is important aspect to consider.
T7 - Espionage and Trespass		x	Third part may interest to capture sensitive data.	The devices must be used with extra attention.
T8 - Software Attacks	x		The de-compilation of software is necessary for evaluating weaknesses against the attacks.	**This is not focused** in this research, but it is important aspect to consider.
T9 - Human Errors or Failure		x	The consumer has poor intention to assure information security due to poor knowledge.	It is necessary to educate consumer to avoid such errors.

4.2.1 Countermeasures

The countermeasures have been introduced in the Table 4 against the identified vulnerabilities and threats followed by the experimentation outcome in the Table 3. The main outcome of second phase is the list of countermeasures in Table 4, and description for each countermeasure and includes the relevant adaptation for threats and vulnerabilities. It is essential to note, that one countermeasure might not able to address identified threat or vulnerability.

Table 4: List of Countermeasures

Countermeasures	Description	Associate Threat/ Vulnerability
Non-Technical Countermeasures		
C1 - User Policies	The user policies are introduced identifying possible human control to assure information security assuming consumer has no knowledge about secure use of PMDs. Further, delegating responsibilities to the consumer is required, when there is no solution technologically. It is tool to enhance the awareness of consumers.	V1, V4, V5, V6, V7, V8, V9, V12, V13, V15, V16, T1, T2, T5, T7, T9
C2 - Monitoring and Maintaining	The policy implementation is crucial due to the continued evolution of the technology. The context of policy implementation is change constantly, and it must be taken into account.	V1, V10, V11, V12, V13, V15, V16, T1, T2,
C3 - Social Awareness	The consumers of the PMDs may have heard about the available user policies, however they lack the understanding of the wider impacts. The Education and Training sessions for awareness are important for effective implementation of user policies.	V1, V5, V12, V13, V15, V16, T1, T2, T5, T7, T9
Technical Countermeasures		

C4 - Security Policies	It is necessary to officially address required technical implication for assuring security in the policy for acknowledging relevant parties. All the threats are considered here for future concerns.	V1, V3, V4, V8, V10, T3, T4, T6, T8
C5 - Technical Awareness	The secure implementations are essential to share among consumer through education and training sessions. The present limitation of addressing mentioned threats must acknowledge the user.	V1, V3, V4, V8, V10, T3, T4, T6, T8
C6 - Introducing Light Weight Encryption	The present use of encoding for data transmission is not secure. However, encryption is more secure, being unable to understand captured data without the key. It discourages third party interception.	V1, V2, V3
C7 - Introduce Multiple MAC Addresses for a Device	In theory, a MAC address is unique for a device. But multiple MAC addresses can be introduced for reducing the possibility to track a device assuring privacy and security as shown in Figure 13. It is known as LE Privacy, and that concept is already implemented in Apple fitness tracker, even though it conflicts the common understand of MAC address. However, many PMDs, including Fitbit and Garmin devices, are not implemented with this concept.	V4, T1, T2
C8 - Assuring QoS	It is required to maintain QoS technically to avoid retransmission in BLE protocol, even though user policy can manage at present.	V12
C9 - Clear & Informative User Interfaces	The PMD device interface is compact, and non-technical consumer are discouraged from using the device due to that. The flexibility of using device is very limited; for example, there is no way to disable use of BLE in some devices.	T2, T5, T7, T9
C10 - Tools for Managing Data	The present implementation introduces ways to use the data, but there is no control over the data. However, the consumer is owner of the data, so it is essential to have pure control on data for the consumer.	V14, T2

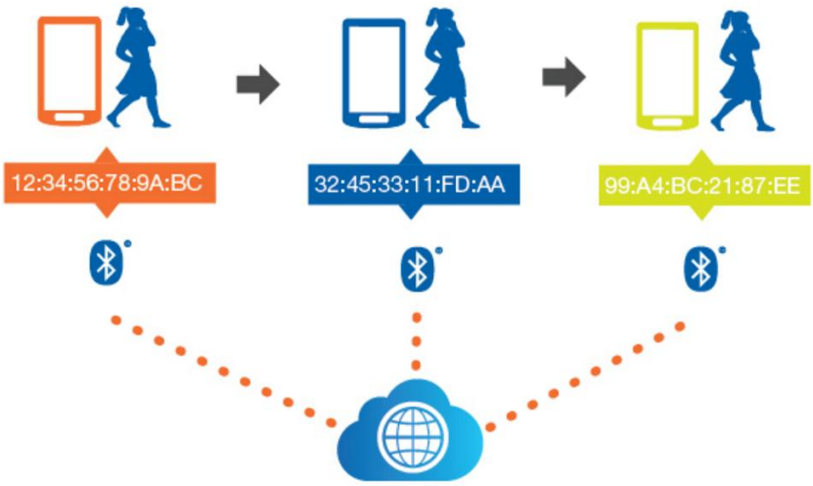


Figure 13: LE Privacy (Ogunu & Anokhuagbo, 2016)

4.3 Phase 3: Solution Framework

The countermeasures to mitigate the potential vulnerabilities are provided in Table 4. Categorising the countermeasures and assigning them to specific groups based in the similarity of the countermeasure as per Table 5, as the resultant framework shows in Figure 14. At the highest level, the framework makes a distinction between the technical and social factors. The social factors are important for the consumer behaviour on social aspects, whereas technical factors are important for the consumer contribution on technical aspects. The social layer is divided into three areas: User Policies, Monitoring and Maintenance, and Social Awareness. The technical layer is divided into Security Policies, Secure Implementation Policies, Tools to Manage Data, and Technical Awareness.

The policy implementation is one major consideration in any secure environment. Here, the identified vulnerabilities can be addressed by introducing environment specific User Policies, Security Policies and Implementation Policies of the framework. The technological evaluation and consumer's need influence on the secure environment, as a result monitoring the environment to maintain security requirement is essential as shown in Monitoring for Maintenance of the framework.

The user must be acknowledged about the importance of required social behaviour by conducting either education or training as required, and it is included in Social Awareness of the framework. The Tools to Manage Data focus on user's privilege on controlling data as owner of data using tools, finally the Technical Awareness focuses on acknowledging the importance of available security implementation by conducting either education or training as required. However, conserving the resources constrains of PMDs, the social aspect is considered with priority over technical aspects at present.

Table 5: Framework Consideration

Element	Description	Associated Countermeasures
Social		
1. User Policies	User policies are applicable for introducing best practices avoiding issues, further impact due to the inherent technological weaknesses can be reduced.	C1
2. Monitoring for Maintenance	It is essential to monitor the environment periodically to assure an expected level of security.	C2

3. Social Awareness	The consumer must have better understand about all the non-technical implementation available.	C3
Technical		
4. Security Policies	The consumer, manufacturer and stakeholders are educated about security using policies for shared understand.	C4
5. Secure Implementation Policy	The necessary implementation has been identified for better secure environment.	C6, C7, C8, C9
6. Tools to Manage Data	It is necessary for data owner to have full control over the data, however there is no such implantation for Fitbit and Garmin.	C10
7. Technical Awareness	It is a challenge to educate non-technical consumer on technical stuff, however it is worth to convince the significance of technical implementation.	C5

There is no perfect approach for secure use of PMDs, however the understanding behind this framework may guide to maintain accepted level of information security.

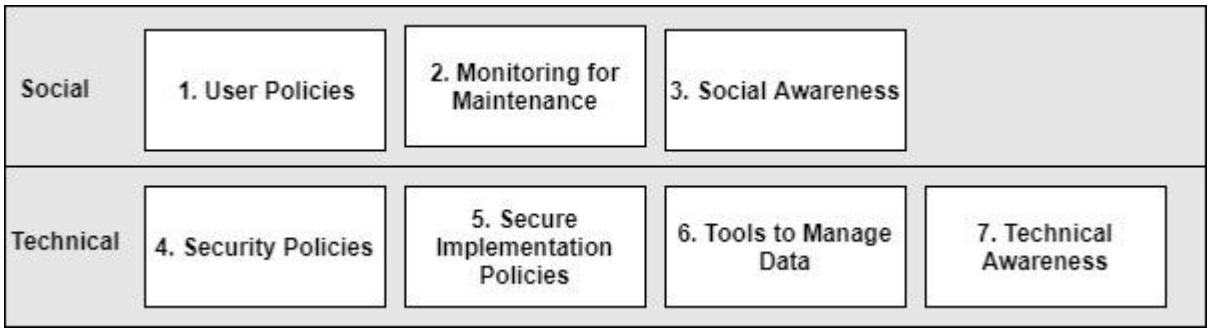


Figure 14: The Socio-Technical Impact Framework

This framework is initiation point for the regularity body, manufacturer to consider for implementing secure use of PMDs for the user. Further, this framework can be used for evaluating present environment for identifying the gaps to introducing information security.

4.4 Guideline for the PMD Consumers Using the Framework

The guideline for the PMD users is listed considering the factors identified over the research. The present environment is considered to survive with current technical implementation. The guideline shares some understanding about the importance of assuring the sensitive healthcare information security for consumers. It is introduced according to the elements identified in the framework, and each element deliver some responsibility for consumer to assure information security. The details are derived based on present understanding on the field in general.

Table 6: Guidelines

Social

1. User Policies
The device must not be unattended due to any reason; keep device lockable place once it is not used due to any reason. The mobile phone is also protected in equally important manner.
The captured data of PMD is synchronised with the application in a private environment assuring no third-party interception; turn off Bluetooth every other time in the mobile.
The sensitive healthcare data and device information must not be shared with someone who has no direct relationship with Medicare like a medical practitioner.
The GPS must not be enable if it is not essential. It does not allow someone else to capture consumer location.
It is not recommended to share device generated health information, since this may introduce some clues for social engineering group to deal with you.
The device battery must be charged as practice to avoid unavailability of the device.
Consumer must find the user policy introduced by the manufacturer or institute to practice.
2. Monitoring for Maintenance
It is necessary follow-up updates available for non-technical considerations to cope with the technological enhancement.
3. Social Awareness
Consumer must have better understanding about available user policies and their updates for effective secure implementation.
Technical
4. Security Policies
The mobile phone, as peripheral, must be password protected with better understand of sensitive data is stored in the mobile.
Consumer must find the security policy introduced by the manufacturer or institute to practice.
5. Secure Implementation Policies
Consumer must aware about available security implementation with the device before making decision to perches; encoding, encryption, LE privacy, QoS parameters, flexibility of user interface.
Consumer must have better understand about available security policies for effective secure implementation; updates for the mobile, utilise Bluetooth as required.
6. Tools to Manage Data
Consumer must use a tool to control its own data if available, however consumer has no option in most of the cases, so it is a responsibility of manufacturer to make them available.
7. Technical Awareness
The operating systems and application software must be updated on regular basis to avoid obsolesce.
It is essential to make sure the use of Bluetooth in present environment due to any other communication before synchronising data with application to avoid signal jamming.
Consumer must have better understand about available security policies, security implementation policies for effective technical awareness.

5 DISCUSSION

A socio-technical impact framework has been introduced to assist users with the secure use of PMDs, and it provides overall understand of the environment in two layers based on theoretical foundation. That framework helps to critically evaluate the present situation of any environment of use of PMDs.

All seven approaches in the socio-technical impact framework have been considered as in the Table 7 for evaluation, and each approach introduces three level with the literal meaning of each aspect; low, medium and high. Those three levels use to distinguish the environment in broad level as guidance to understand the level of present environment. The description for each level of approaches mentions the requirement for that level. This can be introduced as a tool of the framework.

Table 7: Framework Description

Approach	Level	Description
Social Approaches		
1. User Policies	Low	No user policy for use of PMD.
	Medium	User policy inherent from general artefacts only.
	High	User policy specific to the use of PMDs.
2. Monitoring and Maintenance	Low	No monitoring or maintenance.
	Medium	No pre-defined frequency for monitoring and maintenance
	High	Pre-defined frequency for monitoring and maintenance.
3. Social Awareness	Low	No education and training.
	Medium	Informal and ad-hoc education and training only.
	High	Formalised education and training.
Technical Approaches		
4. Security Policy	Low	No user security policy for use of PMD.
	Medium	Security policy inherent from general artefacts only.
	High	Security policy specific to the use of PMDs.
5. Security Implementation Policy	Low	No implementation policy for use of PMD.
	Medium	Ad-hoc implementation policy.
	High	Formalised implementation policy.
6. Tools to Manage Data	Low	No tool to manage data.
	Medium	Constrained tools to manage data only.
	High	Comprehensive tools to manage data.
7. Technical Awareness	Low	No education and training.
	Medium	No official education and training.
	High	Official education and training.

6 CONCLUSION

The use of PMD is becoming more prevalent due to the important benefits for maintaining health and managing chronic health conditions, however the sensitive health information protection and secure practices are not matured due to the poor consideration of PMD specific environment. Further, the technical implementation of PMDs is not enough for assuring the security of sensitive health information, because there are resource constraints, and the impact of social practices to implement mature technical solutions. As a result, the user of PMDs has significant responsibilities for assuring the protection of their sensitive health information. These initiatives are encouraged to involve with security consideration in the use of PMD. The different aspects are evaluated over case study and supplementary experiment to introduce the socio-technical impact framework addressing information security concerns. The regulators do not always keep pace with technological progress as they would like to be, as a result there is poor consideration in the use of PMDs. This research provides the fundamental understanding of the use of PMDs and the associated issues as an initiative for the researchers. It forms the basis for further investigation into the design of advice and education.

The model of the discipline of Information systems by Shanks in Figure 11 is addressed in this research as follows:

- Scholarship is addressed by introducing new knowledge in the form of a framework which enhances current user security theory. It would be an effective initiative for future researchers to consider about security use of PMD. Moreover, this research introduces some guidelines for the user contributing for practices in that model. Further, future work would develop this framework further;
- Research is addressed through the process of undertaking the case study and experimentation, and the identification of the need for more complex and thorough experimentation techniques for security testing of PMD devices; and
- Practice is addressed by providing guidelines for users to follow, and for application developers and device manufacturers to consider in design and production.

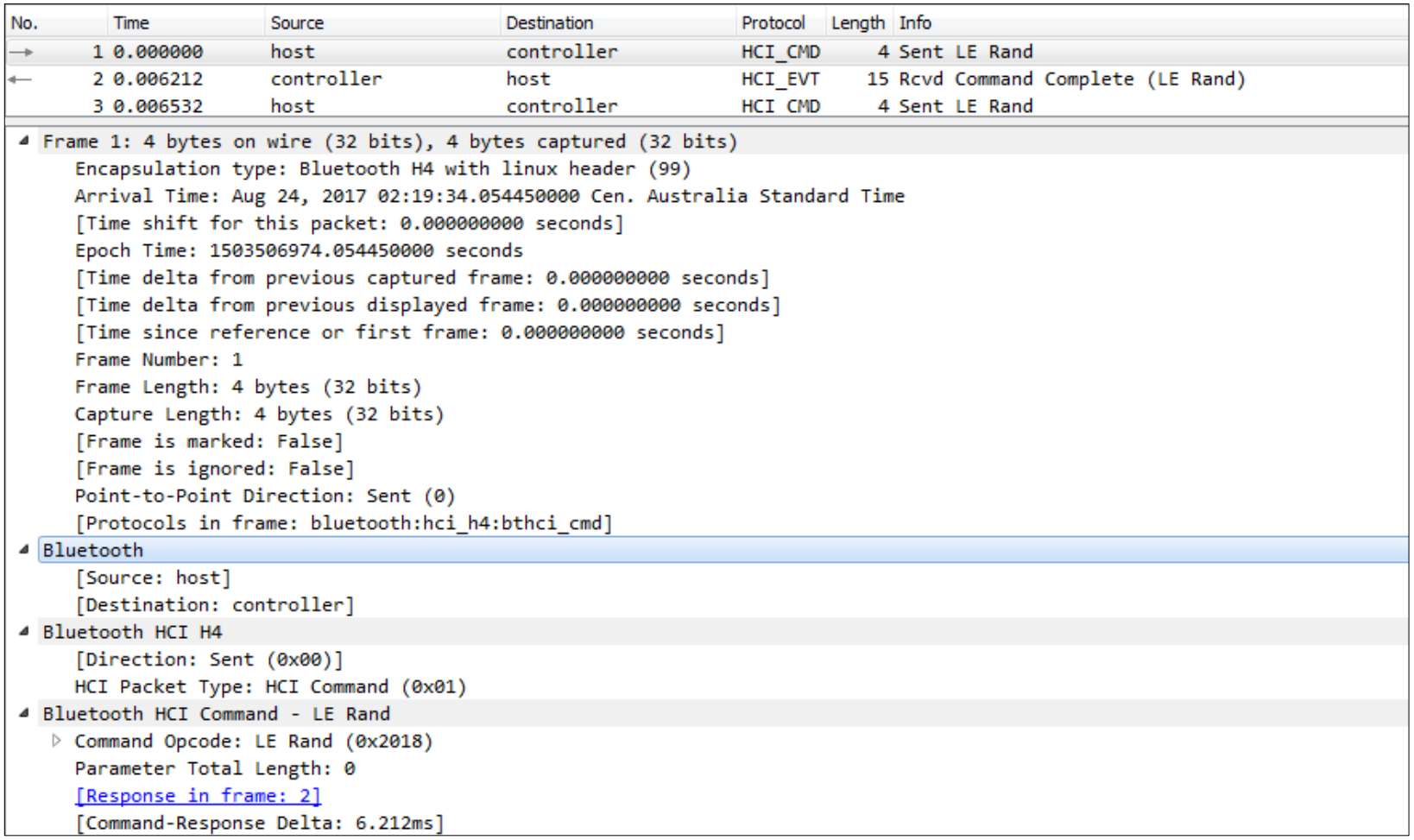
In answering the research question, “Can a socio-technical impact framework be developed to assist users with the secure use of Personal Monitoring Devices?” a socio-technical impact framework and associated user guidelines was developed.

The impact of this is that this framework guides implementation of usable information security mechanism for the users of PMDs. The framework is a tool for the security experts to introduce context specific policy for secure use of PMDs, so it is necessary to implement policy for practical benefits of effort for this research. Also, it provides an insight for application developers and manufacturers to consider in new development of PMDs.

To fulfil the research question by introducing comprehensive socio-technical impact framework to assure secure use of PMDs, it is essential to continue this research. Research have shown that systems developed with significant user input are more widely accepted and consistently used. It is highly recommended to interview people who are using PMDs for their contribution. In addition, the contribution of the manufacturer was not planned in this research, but it adds value for the final framework. Further, thorough experiment can be conducted using smoother technique addressing the identified limitation of Bluetooth Sniffer Log of Android in this research.

7 APPENDICES

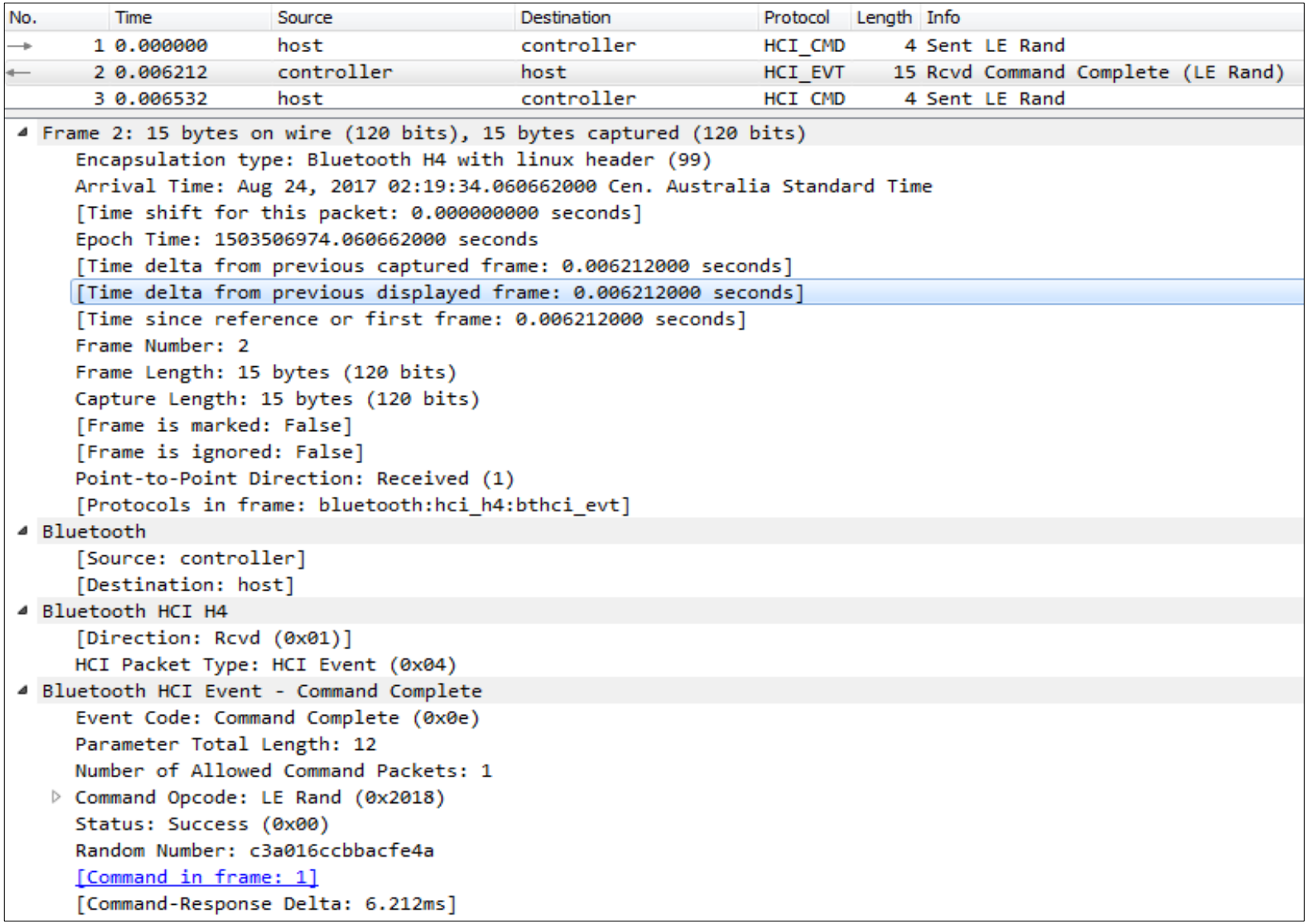
Appendix A: Bluetooth Sniffer Log analysis in Wireshark: Host to Controller



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	host	controller	HCI_CMD	4	Sent LE Rand
2	0.006212	controller	host	HCI_EVT	15	Rcvd Command Complete (LE Rand)
3	0.006532	host	controller	HCI_CMD	4	Sent LE Rand

```
Frame 1: 4 bytes on wire (32 bits), 4 bytes captured (32 bits)
    Encapsulation type: Bluetooth H4 with linux header (99)
    Arrival Time: Aug 24, 2017 02:19:34.054450000 Cen. Australia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1503506974.054450000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 4 bytes (32 bits)
    Capture Length: 4 bytes (32 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    Point-to-Point Direction: Sent (0)
    [Protocols in frame: bluetooth:hci_h4:bthci_cmd]
Bluetooth
    [Source: host]
    [Destination: controller]
Bluetooth HCI H4
    [Direction: Sent (0x00)]
    HCI Packet Type: HCI Command (0x01)
Bluetooth HCI Command - LE Rand
  ▷ Command Opcode: LE Rand (0x2018)
    Parameter Total Length: 0
    [Response in frame: 2]
    [Command-Response Delta: 6.212ms]
```

Appendix B: Bluetooth Sniffer Log analysis in Wireshark: Controller to Host



No.	Time	Source	Destination	Protocol	Length	Info
→	1 0.000000	host	controller	HCI_CMD	4	Sent LE Rand
←	2 0.006212	controller	host	HCI_EVT	15	Rcvd Command Complete (LE Rand)
	3 0.006532	host	controller	HCI_CMD	4	Sent LE Rand

```
▲ Frame 2: 15 bytes on wire (120 bits), 15 bytes captured (120 bits)
    Encapsulation type: Bluetooth H4 with linux header (99)
    Arrival Time: Aug 24, 2017 02:19:34.060662000 Cen. Australia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1503506974.060662000 seconds
    [Time delta from previous captured frame: 0.006212000 seconds]
    [Time delta from previous displayed frame: 0.006212000 seconds]
    [Time since reference or first frame: 0.006212000 seconds]
    Frame Number: 2
    Frame Length: 15 bytes (120 bits)
    Capture Length: 15 bytes (120 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    Point-to-Point Direction: Received (1)
    [Protocols in frame: bluetooth:hci_h4:bthci_evt]
▲ Bluetooth
    [Source: controller]
    [Destination: host]
▲ Bluetooth HCI H4
    [Direction: Rcvd (0x01)]
    HCI Packet Type: HCI Event (0x04)
▲ Bluetooth HCI Event - Command Complete
    Event Code: Command Complete (0x0e)
    Parameter Total Length: 12
    Number of Allowed Command Packets: 1
  ▷ Command Opcode: LE Rand (0x2018)
    Status: Success (0x00)
    Random Number: c3a016ccbbacfe4a
    [Command in frame: 1]
    [Command-Response Delta: 6.212ms]
```

8 REFERENCES

Aberer, K., & Hauswirth, M. (2006). Middleware support for the" Internet of Things".

Altamimi, R. I., & Skinner, G. D. (2016). Validation of Contemporary Physical Activity Tracking Technologies through Exercise in a Controlled Environment. *World Academy of Science, Engineering and Technology, International Journal of Medical, Health, Biomedical, Bioengineering and Pharmaceutical Engineering, 10*(1), 31-42.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, 6-9 July 2015). *Internet of Things: Security vulnerabilities and challenges.* Paper presented at the 2015 IEEE Symposium on Computers and Communication (ISCC).

Andreini, F., Crisciani, F., Cicconetti, C., & Mambrini, R. (2010). *Context-aware location in the internet of things.* Paper presented at the GLOBECOM Workshops (GC Wkshps), 2010 IEEE.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49-69.

Bluetooth. (2016). Bluetooth Core Specification v 5.0: Bluetooth SIG Proprietary.

Botta, A., Donato, W. d., Persico, V., & Pescapé, A. (2014, 27-29 Aug. 2014). *On the Integration of Cloud Computing and Internet of Things.* Paper presented at the 2014 International Conference on Future Internet of Things and Cloud.

Brodersen, N. H., Steptoe, A., Boniface, D. R., & Wardle, J. (2007). Trends in physical activity and sedentary behaviour in adolescence: ethnic and socioeconomic differences. *British journal of sports medicine, 41*(3), 140-144.

Castillejo, P., Martinez, J. F., Rodriguez-Molina, J., & Cuerva, A. (2013). Integration of wearable devices in a wireless sensor network for an E-health application. *IEEE Wireless Communications, 20*(4), 38-49. doi:10.1109/MWC.2013.6590049

Choi, B. C., Pak, A. W., & Choi, J. C. (2007). Daily step goal of 10,000 steps: a literature review. *Clinical & Investigative Medicine, 30*(3), 146-151.

Costantin, D., Sansurooah, K., & Williams, P. A. (2017). *Vulnerabilities associated with wi-fi protected setup in a medical environment.* Paper presented at the Proceedings of the Australasian Computer Science Week Multiconference.

Cyr, B., Horn, W., Miao, D., & Specter, M. (2014). Security analysis of wearable fitness devices (fitbit). *Massachusets Institute of Technology*, 1.

Darshan, K. R., & Anandakumar, K. R. (2015, 17-19 Dec. 2015). *A comprehensive review on usage of Internet of Things (IoT) in healthcare system.* Paper presented at the 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT).

de Zambotti, M., Baker, F. C., Willoughby, A. R., Godino, J. G., Wing, D., Patrick, K., & Colrain, I. M. (2016). Measures of sleep and cardiac functioning during sleep using a multi-sensory commercially-available wristband in adolescents. *Physiology & behavior, 158*, 143-149.

Dong, Z., Yian, Z., Wangbao, L., Jianhua, G., & Yunlan, W. (2010). *Object service provision in Internet of Things.* Paper presented at the e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E'10. International Conference on.

Doukas, C., & Maglogiannis, I. (2012, 4-6 July 2012). *Bringing IoT and Cloud Computing towards Pervasive Healthcare.* Paper presented at the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.

El Maliki, T., & Seigneur, J.-M. (2010). *A security adaptation reference monitor (SARM) for highly dynamic wireless environments.* Paper presented at the Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on.

Gallo, L. C., Roesch, S. P., McCurley, J. L., Isasi, C. R., Sotres-Alvarez, D., Delamater, A. M., . . . Buelna, C. (2017). Youth and caregiver physical activity and sedentary time: HCHS/SOL Youth. *American journal of health behavior, 41*(1), 67-75.

Giannakidou, D. M., Kambas, A., Ageloussis, N., Fatouros, I., Christoforidis, C., Venetsanou, F., . . . Taxildaris, K. (2012). The validity of two Omron pedometers during treadmill walking is speed dependent. *European journal of applied physiology, 112*(1), 49-57.

Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors, 12*(9), 11734-11753.

Gordon-Larsen, P., McMurray, R. G., & Popkin, B. M. (2010). Determinants of adolescent physical activity and inactivity patterns. *Pediatrics, 105*(6), e83-e83.

Guinard, D., Trifa, V., Mattern, F., & Wilde, E. (2011). From the internet of things to the web of things: Resource-oriented architecture and best practices. *Architecting the Internet of things*, 97-129.

Guo, B., Yu, Z., Zhou, X., & Zhang, D. (2012). *Opportunistic IoT: Exploring the social side of the internet of things.* Paper presented at the Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on.

Guo, F., Li, Y., Kankanhalli, M. S., & Brown, M. S. (2013). *An evaluation of wearable activity monitoring devices.* Paper presented at the Proceedings of the 1st ACM international workshop on Personal data meets distributed multimedia.

Hao, Y., & Foster, R. (2008). Wireless body sensor networks for health-monitoring applications. *Physiological measurement, 29*(11), R27.

Healey, J., Pollard, N., & Woods, B. (2015). The Healthcare Internet of Things: Rewards and Risks. *Atlantic Council*.

Hiremath, S., Yang, G., & Mankodiya, K. (2014, 3-5 Nov. 2014). *Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare.* Paper presented at the 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH).

Hnatiuk, J. A., Salmon, J., Hinkley, T., Okely, A. D., & Trost, S. (2014). A review of preschool children's physical activity and sedentary time using objective measures. *American journal of preventive medicine, 47*(4), 487-497.

Huang, Y., & Li, G. (2010). *A semantic analysis for internet of things.* Paper presented at the Intelligent computation technology and automation (icicta), 2010 international conference on.

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. doi:10.1109/ACCESS.2015.2437951

James, A., Cooper, J., Jeffery, K., & Saake, G. (2009). Research directions in database architectures for the internet of things: a communication of the first international workshop on database architectures for the internet of things (DAIT 2009). *Dataspace: The Final Frontier*, 225-233.

Josyula, S. K., & Gupta, D. (2016, 24-24 Oct. 2016). *Internet of things and cloud interoperability application based on Android.* Paper presented at the 2016 IEEE International Conference on Advances in Computer Applications (ICACA).

Kawsar, F., Kortuem, G., & Altakrouri, B. (2010). *Supporting interaction with the internet of things across objects, time and space.* Paper presented at the Internet of Things (IOT), 2010.

Kirby, B., Kirby, A., & Birch, J.-L. (2016). *Wearable tech: why architectures matter.* Paper presented at the Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion!

Kodali, R. K., Swamy, G., & Lakshmi, B. (2015, 10-12 Dec. 2015). *An implementation of IoT for healthcare.* Paper presented at the 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS).

Koshizuka, N., & Sakamura, K. (2010). Ubiquitous ID: standards for ubiquitous computing and the Internet of Things. *IEEE Pervasive Computing, 9*(4), 98-101.

Lacoste, M., Privat, G., & Ramparany, F. (2007). Evaluating confidence in context for context-aware security. *Ambient Intelligence*, 211-229.

Lee, C. M., & Gorelick, M. (2011). Validity of the Smarthealth watch to measure heart rate during rest and exercise. *Measurement in Physical Education and Exercise Science, 15*(1), 18-25.

Liu, J., Li, X., Chen, X., Zhen, Y., & Zeng, L. (2011). *Applications of internet of things on smart grid in China.* Paper presented at the Advanced Communication Technology (ICACT), 2011 13th International Conference on.

Lupşe, O.-S., Vida, M. M., & Tivadar, L. (2012). *Cloud computing and interoperability in healthcare information systems.* Paper presented at the The First International Conference on Intelligent Systems and Applications.

Macias, J. A. G., Alvarez-Lozano, J., Estrada, P., & Lopez, E. A. (2011). Browsing the internet of things with sentient visors. *Computer, 44*(5), 46-52.

Mahalle, P., Babar, S., Prasad, N. R., & Prasad, R. (2010). Identity management framework towards internet of things (IoT): Roadmap and key challenges. *Recent Trends in Network Security and Applications*, 430-439.

Mancuso, P. J., Thompson, M., Tietze, M., Kelk, S., & Roux, G. (2014). Can patient use of daily activity monitors change nurse practitioner practice? *The Journal for Nurse Practitioners, 10*(10), 787-793. e784.

McCue, T. (2015). $117 billion market for internet of things in healthcare by 2020. *Forbes Tech, April*.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516.

Ogunu, B., & Anokhuagbo, E. (2016). *A framework for user-centric privacy management in smartphones regarding bluetooth low energy beacons.* The University of North Carolina at Charlotte.

Olds, T. S., Tudor-Locke, C., Craig, C., Beets, M., Belton, S., Cardon, G., . . . Raustorp, A. (2011). How many steps/day are enough?: for children and adolescents.

Ostermaier, B., Römer, K., Mattern, F., Fahrmair, M., & Kellerer, W. (2010). *A real-time search engine for the web of things.* Paper presented at the Internet of Things (IOT), 2010.

Otterloo, S. v. (2017). Information security and PDCA (Plan-Do-Check-Act). Retrieved from https://ictinstitute.nl/pdca-plan-do-check-act/

Price, K., Bird, S. R., Lythgo, N., Raj, I. S., Wong, J. Y. L., & Lynch, C. (2017). Validation of the Fitbit One, Garmin Vivofit and Jawbone UP activity tracker in estimation of energy expenditure during treadmill walking and running. *Journal of Medical Engineering & Technology, 41*(3), 208-215. doi:10.1080/03091902.2016.1253795

Pujolle, G. (2006). *An autonomic-oriented architecture for the internet of things.* Paper presented at the Modern Computing, 2006. JVA'06. IEEE John Vincent Atanasoff 2006 International Symposium on.

Reilly, J. J., Kelly, L., Montgomery, C., Williamson, A., Fisher, A., McColl, J. H., . . . Grant, S. (2006). Physical activity to prevent obesity in young children: cluster randomised controlled trial. *Bmj, 333*(7577), 1041.

Sallis, J. F., Cutter, C. L., Lou, D., Spoon, C., Wilson, A. L., Ding, D., . . . Schmid, T. L. (2014). Active living research: creating and using evidence to support childhood obesity prevention. *American journal of preventive medicine, 46*(2), 195-207.

Scheffler, M., & Hirt, E. (2004, 1-5 Sept. 2004). *Wearable devices for emerging healthcare applications.* Paper presented at the The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society.

Shanks, G., Arnott, D., & Rouse, A. (1993). *A review of approaches to research and scholarship in information systems*: Department of Information Systems, Faculty of Computing and Information Technology, Monash University.

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Cloud security - Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal, 3*(3), 269-284.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Straker, L., Howie, E. K., Cliff, D. P., Davern, M. T., Engelen, L., Gomersall, S. R., . . . Tomkinson, G. R. (2016). Australia and other nations are failing to meet sedentary behaviour guidelines for children: implications and a way forward. *Journal of Physical Activity and Health, 13*(2), 177-188.

Sungmee, P., & Jayaraman, S. (2013). Enhancing the quality of life through wearable technology. *IEEE Engineering in Medicine and Biology Magazine, 22*(3), 41-48. doi:10.1109/MEMB.2003.1213625

Takacs, J., Pollock, C. L., Guenther, J. R., Bahar, M., Napier, C., & Hunt, M. A. (2014). Validation of the Fitbit One activity monitor device during treadmill walking. *Journal of Science and Medicine in Sport, 17*(5), 496-500.

Tremblay, M. S., Warburton, D. E., Janssen, I., Paterson, D. H., Latimer, A. E., Rhodes, R. E., . . . Zehr, L. (2011). New Canadian physical activity guidelines. *Applied Physiology, Nutrition, and Metabolism, 36*(1), 36-46.

Tudor-Locke, C., Pangrazi, R. P., Corbin, C. B., Rutherford, W. J., Vincent, S. D., Raustorp, A., . . . Cuddihy, T. F. (2014). BMI-referenced standards for recommended pedometer-determined steps/day in children. *Preventive medicine, 38*(6), 857-864.

Valera, A. J. J., Zamora, M. A., & Skarmeta, A. F. (2010). *An architecture based on internet of things to support mobility and security in medical environments.* Paper presented at the Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE.

Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005). *Energy analysis of public-key cryptography for wireless sensor networks.* Paper presented at the Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*: Cengage Learning.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274.

Williams, P. A. H. (2006). *Making Research Real: Is Action Research a Suitable Methodology for Medical Information Security Investigations?* Paper presented at the Australian Information Security Management Conference.

Williams, P. A. H., & McCauley, V. (2016, 12-14 Dec. 2016). *Always connected: The security challenges of the healthcare Internet of Things.* Paper presented at the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, NZ), 8*, 305.

Xu, T., Wendt, J. B., & Potkonjak, M. (2014). *Security of IoT systems: design challenges and opportunities*. Paper presented at the Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, San Jose, California.

Yan, T., & Wen, Q. (2012). A trust-third-party based key management protocol for secure mobile RFID service based on the Internet of Things. *Knowledge Discovery and Data Mining*, 201-208.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal, 1*(1), 22-32. doi:10.1109/JIOT.2014.2306328

Zhengxia, W., & Laisheng, X. (2010). *Modern logistics monitoring platform based on the Internet of things.* Paper presented at the Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on.

Zhou, W., & Piramuthu, S. (2014, 18-21 June 2014). *Security/privacy of wearable fitness tracking IoT devices.* Paper presented at the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI).