UNDERSTANDING SECURITY RISKS AND USERS PERCEPTION TOWARDS ADOPTING WEARABLE INTERNET OF MEDICAL THINGS

[Sanjit Jung Thapa]

[Master by research]

[Dr Abubakar Bello and Professor Alana Maurushat]

Faculty of Social Sciences

Western Sydney University

2021

Abstract

This thesis examines users' perception of trust within the context of security and privacy of Wearable Internet of Medical Things (WIoMT). WIoMT is a collective term for all medical devices connected to internet to facilitate collection and sharing of health-related data such as blood pressure, heart rate, oxygen level and more. Common wearable devices include smart watches and fitness bands. WIoMT, a phenomenon due to Internet of Things (IoT) has become prevalent in managing the day-to-day activities and health of individuals. This increased growth and adoption poses severe security and privacy concerns. Similar to IoT, there is a need to analyse WIoMT security risks as they are used by individuals and organisations on regular basis, risking personal and confidential information. Additionally, for better implementation, performance, adoption, and secured wearable medical devices, it is crucial to observe users' perception. Users' perspectives towards trust are critical for adopting WIoMT. This research aimed to understand users' perception of trust in the adoption of WIoMT, while also exploring the security risks associated with adopting wearable IoMT. Employing a quantitative method approach, 189 participants from Western Sydney University completed an online survey. The results of the study and research model indicated more than half of the variance ($R^2 = 0.553$) in the Intention to Use WIoMT devices, which was determined by the significant predictors (95% Confidence Interval; $p < 0.05$), Perceived Usefulness, Perceived Ease of Use and Perceived Security and Privacy. Among these two, the domain Perceived Security and Privacy was found to have significant outcomes. Hence, this study reinforced that a WIoMT user intends to use the device only if he/she trusts the device; trust here has been defined in terms of its usefulness, easy to use and security and privacy features. This finding will be a steppingstone for equipment vendors and manufacturers to have a good grasp on the health industry, since the proper utilisation of WIoMT devices results in the effective and efficient management of health and wellbeing of users. The expected outcome from this research also aims to identify how users' security and perception matters while adopting WIoMT, which in future can benefit security professionals to examine trust factors when implementing new and advanced WIoMT devices. Moreover, the expected result will help consumers as well as different healthcare industry to create a device which can be easily adopted and used securely by consumers.

Table of Contents

List of Figures

List of Tables

List of Abbreviation

- IoT=Internet of Things
- IoMT=Internet of Medical Things
- WIoMT=Wearable Internet of Medical Things
- ECG= Electrocardiogram
- EEG= Electroencephalogram
- HER= Electronic Health Record
- RFID= Radio-Frequency Identification
- TAM= Technology Acceptance Model
- HMD= Head-Mounted Display
- RAM=Random Access Memory
- PDA=Personal Digital Assistant
- ICD= Industrial Clothing Division
- ARPANET= Advance Research Project Agency Network
- GPS= Global Positions System
- SMS= Short Message Service
- HTTP= Hypertext Transfer Protocol
- FDA= Food and Drug Administration
- SPSS=Statistical Package for Social Science
- ANOVA= Analysis on Variance

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature: 

Date: 27 December 2021

Acknowledgement

This master by research thesis has helped me understand every aspect of the survey and how users' perspectives on technology affect adopting such technology. The outcome was successful because of continuous advice and support from various people.

I want to express my gratitude to my supervisors, Dr Abubakar Bello and Professor Alana Maurushat, for providing me with the opportunity to comprehend from their current ongoing research and offering me all the guidance I required to accomplish this research. They demonstrated a great method for acquiring the result analysis and structuring all documentation parts. I am truly grateful to have all of those supportive hands with me until completing this dissertation.

I would also like to thank the human ethics committee of Western Sydney University for continuously supporting getting ethics approved. Also, I am thankful to all the participants from Western Sydney University and those who helped me through spreading the survey among the participants.

I must express my heartfelt thanks to my friends and family for their guidance and moral support as I venture on this eminent MRes path.

1. Introduction

1.1 Background

Technology influences our lives daily, so much so that we cannot imagine our everyday operations without it. Starting from the morning and ending to the evening, we cannot go without technology, specifically, smartphones and other innovative technologies, including some health monitoring and tracking devices generally known as Wearable Internet of Medical Things (WIoMT). These are now an integral part of our routine monitoring of various medical and health concerns. For instance, they help keep track of changes to the body, such as monitoring sleep to heart rates, calories burned, and distance travelled. Health is of a great concern, and technology has backed it up well with different versions and variations of WIoMT (Li et al., 2016).

WIoMT has enabled several individual devices to connect via the internet through a network. WIoMT is described as interconnected individual medical devices that communicate over the internet to enable data collection and sharing (Dimitrov, 2016). Most commonly used WIoMT are Wearable Fitness Trackers such as fitness bands, patches and smartwatches with health monitoring functions. Other forms include Wearable ECG Monitors, Wearable Blood Pressure Monitors, Biosensors, Smart Patches and Ingestible Sensors.

Wearable Fitness Trackers are the device to monitor steps, heart rates, sleep hours and burnt calories. (Majumder et al., 2017) Likewise, Wearable ECG Monitors gather and share ECG data using Wi-Fi. (Yang et al., 2016) Wearable Blood Pressure Monitors are non-invasive and cuffless devices measuring blood pressure. (Ganti et al., 2021) Biosensors detect specific analytes in a biological sample, and Smart Patches monitor various physiological measures such as pulse. (Pateraki et al., 2020; AG, 2021) Ingestible Sensors measure temperature, pressure and various other chemical and physical parameters. (Molteni, 2018)

WIoMT evolved from the Internet of Things (IoT) and the Internet of Medical Things (IoMT). Internet of Things (IoT) is an encompassing term for all connected devices with the internet, such as devices from simple sensors to smartphones (Burgess, 2018). They are further described as interconnected devices that communicate over the internet to enable data collection and sharing. (Dimitrov, 2016) They have been widely used in various areas such as personal home use, the medical sector, automation for industry and manufacturers, smart environment, traffic management, and several more.

Internet of Medical Things (IoMT) is a group of health devices and products which connect with the healthcare system via networks (Dimitrov, 2016). Medical devices accessing Wi-Fi allow machine-to-machine networking that is the establishment of IoMT (Shin and Hwang, 2017). Related aspects of IoMT include active monitoring of the patient with long-term or chronic conditions, recording requests for medical attention and the status of hospitalized patients, and wearable patient care devices transferring data to hospitals(Shin and Hwang, 2017). Health devices that can be transformed into or integrated as IoMT technology are infusion drives that connect to analytics supports and hospital beds fitted with devices that monitor fundamental signs of patients (Shin and Hwang, 2017).

Further, IoT usage in healthcare for the very purpose of health assistance is known as IoMT. In other words, when IoT is integrated with medical devices, enabling improved patient comfort, cost-effective medical solutions, quick hospital treatments, and even more personalized healthcare, such are collectively identified as IoMT (Razdan and Sharma, 2021). They also help diagnose certain diseases, mainly without a health professional (Suresh et al., 2020). The IoMT industry is made up of smart devices like medical/vital sensors and wearables that are solely used for health care on the body, in the community or at home, healthcare settings, as well as related real-time location, community health, and other services, and they are termed as WIoMT devices. (Frost and Sullivan, 2017).

As the WIoMT industry evolves, so do potentially the security and privacy concerns. They should be treated as a high privacy risk device because they constantly acquire the user's personal health information in real-time, and personal health information is more vulnerable than other types of information like demographic or basic customer data (Bansal et al., 2010). Since the use of wearables medical devices requires the disclosure of personal medical information, the decision to adopt such technology implies a privacy analysis that considers the distinction between significant gains and perceived privacy risks (Xu et al., 2009). Security and privacy issues play a role with user adoption and trust of these devices.

There is a need for exploring user’s security and perception regarding WIoMT regarding their adoption, and this is the very purpose of this study, which is to understand understand the user’s perception of trust in the adoption of WIoMT and find out security risks associated with this adoption. These are portrayed research questions mentioned below:

1. What factors influence trust and adoption of WIoMT?
2. What are the security risks associated with adoption WIoMT?

1.2 Architectural Context

The architectural basis of IoT is built on three different layers, as illustrated in Figure 1, which is followed by IoMT and WIoMT devices.

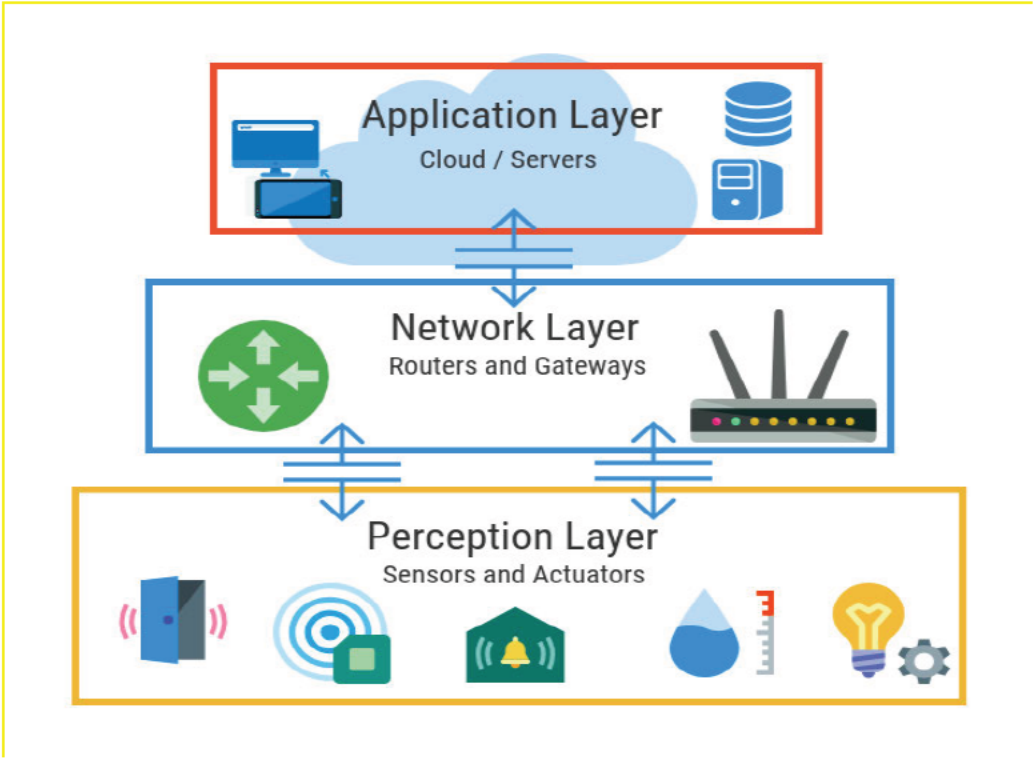

Figure 1: Fundamental architecture of IoT (Dutta Pramanik et al., 2018)

The perception layer consists of sensors that collect information from the physical environment. The network layer connects various objects, servers and network devices and processes and transfers the information received through the sensors. Finally, the application layer provides users with specific application services such as cloud and servers (Dutta Pramanik et al., 2018).

The application layer includes clouds and servers where the device from the perception layer is connected through the network layer and stored in an abstract space, and easily retrieved when required or necessary. The Network layer is the component commonly known as routers and gateways. So, they act as a bridge between the application and the perception layers. The perception layer is 'the tangible things' that users use. The perception layer consists of various devices and instruments with sensors and actuators. Architecture can visualise where the perception and network layers are physical and work as coding agents and application layer, an intangible and abstract component where all information regarding network and perception is stored and operates overall operation. IoMT and WIoMT follow a similar architectural model where sensors, RFID, and smartphones are connected through various networks and operated from various application domains. Although the structure is similar for IoMT and WIoMT, the only difference lies in the Perception layer devices.

Healthcare service providers are growing their medical practices to include both IoMT and Wearable IoMT, which have become increasingly important as efficient methods to monitor patient health (Microchip, 2020). These have given rise to new architectures, applications, and standards related to addressing current health challenges, which have further enhanced the development of individualised and single-user based WIoMT (S Rubí and L Gondim, 2019).

1.3 Benefits

WIoMT has become significant in providing different benefits to the medical sector, such as minimising patients' travel time and expenses, delivering medical care in places with limited accessibility and enhancing the delivery of critical knowledge to health personnel from distant places. For instance, the beneficial use of WIoMT devices has ensured monitoring and consciousness about individual health status among users (Islam et al., 2015).

WIoMT connects sensors, smartphones, and other WIoMT devices via wireless communication. It collects data from such devices and sends it across a wireless network to be stored in the cloud or on servers. Modern WIoMT promises personalised and enhanced healthcare services by using mobile technology. In the current scenario, increasing portable medical apps are shifting hospitals to domestic healthcare monitoring (for example, wearable devices and glucose meters). Such wearable applications, enabled by Bluetooth and close-field connectivity, change the precautionary medicine domain and the lives of chronic disease individuals by providing continuous health surveillance, detection, and even care (Shin and Hwang, 2017).

1.4 Concerns

Though there are various benefits of WIoMT, certain drawbacks have also surfaced. The most significant concern of WIoMT usage is personal data. Information spreading through the internet from devices has created a sense of insecurity among IoMT users, who fear that their data may be shared and exploited without their permission, making them feel threatened. As a large amount of data is collected and exchanged via the internet, there are several methods to be replicated and altered.

As suggested by Yan et al. (2014), trust is a complex concept influenced by numerous variables that may be assessable and non-assessable. *Trust* is defined as the assumption that a system has all of the required components to work as expected under various circumstances (McKnight et al., 2011a). Because consumers must interact safely, reliably, and simply with connected WIoMT devices and systems, trust may be seen as vital for consumer adoption in the WIoMT because it can cope with two critical circumstances of IoT systems, namely ambiguity and the danger of vulnerability (AlHogail, 2018, Belanche et al., 2012a, Gefen et al., 2003b). Similarly, Mayer et al. (1995) have related trust with security, in a sense that if the user feels their shared information is

private and not disclosed to others, then the trust on the device is attained (Mayer et al 1995, Alhogail, 2018)

Therefore, this study aims to understand the security risks and users' perception of adopting WIoMT, as trust issues generate towards the devices and services providers. This study is to understand the existing challenges and further explore how users' perception contributes to the adoption of WIoMT.

1.5 Significance and Scope

As WIoMT is becoming prevalent and accessible, mistrust and insecurity concerning users' data are equally prevailing (AlHogail, 2018, Ometov et al., 2021). Hence, this study can be considered substantial in attaining updated knowledge about the trust and perception of WIoMT users. The findings from this study will be of interest to WIoMT manufacturers, retailers, and business marketers as they will allow for deeper insights into the role of perceptions of security, privacy, trust and utility play in the decision making of purchasing and use of WIoMT. Thus, this type of study is essential.

From a medical and health standpoint, because these gadgets are depicted as portable "health managers," they may be put to more use in order to improve people's health and fitness (Zhang et al., 2017). That helps to explain why people are attracted to the use of WIoMT.

This study will serve as a source of secondary information for future researchers working in similar domains, particularly where it will help obtain insights into users' perceptions of WIoMT. As security and privacy concerns escalate and give more media notice, users perceptions of such risks will play an essential role in future technical development, market advantage (should security and privacy move in importance) and use of WIoMT in general.

The value of this study lies in its scope, which is limited to WIoMT. Specially, in the present context, where health of the citizens is of the utmost priority and the governments are striving to enhance public health, these devices come in handy. These devices help people monitor their health from time to time and thus, help manage the overall wellness. Also, these are well-known to most of the public and they are user-friendly in contrast to other technologies requiring much technical knowledge to utilise them properly. Therefore, WIoMT devices help reduce costs of medical services and improve efficiency in disease diagnosis and treatment (Alraja et al., 2019).

1.6 Thesis Outline

The thesis outline is essential for research. In this sense, this thesis organises into following chapters for a better general understanding:

Chapter 1. Introduction

This chapter starts with the basic introduction and background of WIoMT and the context of this study. Similarly, the purpose of this study, its significance and the scope of the present circumstances are highlighted.

Chapter 2. Literature Review

This chapter deals with the various dynamics and innovations concerned with the evolution of WIoMT devices, an overview of wearable technology, its significance. Furthermore, challenges in WIoMT adoption, security and privacy risks associated with WIoMT are mentioned. This chapter concludes with the theoretical framework, TAM model and development of hypothesis for this study.

Chapter 3. Methodology

This chapter includes the methodology of this research, which discusses the study participants, instruments, methods, data analysis, and ethical considerations.

Chapter 4. Results

This chapter illustrates the results of the data analysis, followed by the chapter on the discussion of the results, the study's theoretical and practical implications, and strengths and limitations.

Chapter 5. Discussion

This chapter discusses results, analysis and justification of hypothesis and research questions based on results obtained.

Chapter 6. Conclusion

This chapter includes conclusion remarks for this study.

Finally, all the references have been indicated as per the requirement of the study, along with appendices.

2. Literature review

2.1 Historical perspectives of Wearables and WIoMT

Technology has evolved throughout centuries to get to WIoMT devices that we are using today.

In a study by Ometov et al. (2021), the authors have visualised the historical milestones of wearable technologies, the illustration is provided below:

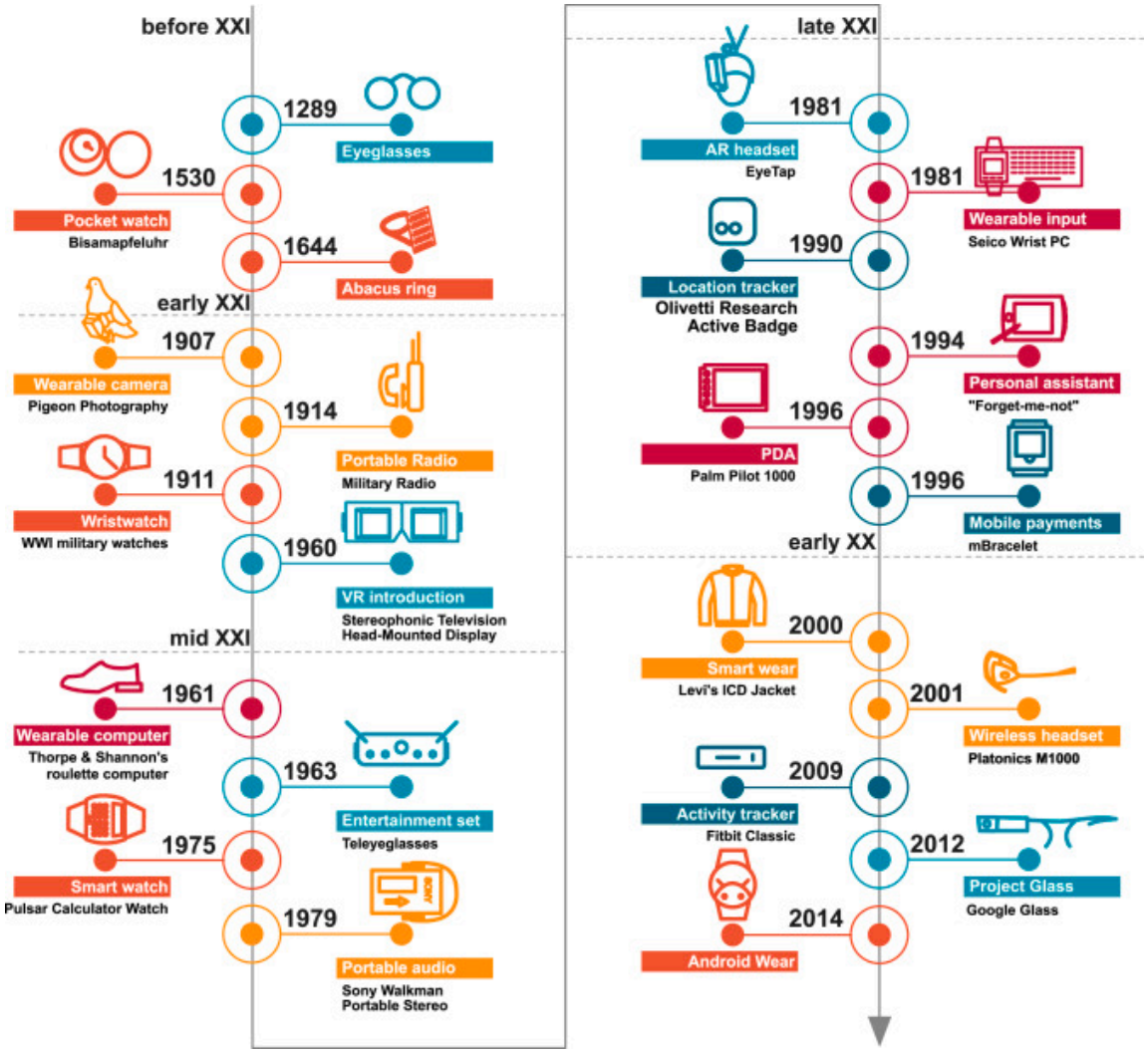

Figure 2: Historical milestones of wearable technologies (Ometov et al., 2021)

Before the 20th century

The period of wearables began with the development of eyeglasses by British monk Roger Bacon in the 13th century (Roman, 1993). In his accomplishments, Bacon developed the scientific concepts that followed the operation of corrective lenses. Before Bacon's innovation, there was

evidence of spherical glass pieces for reading purposes where letters were amplified. In terms of concrete wearables, those were dubious. As a result, Bacon's glass became renowned as the first smart wearable glasses(Roman, 1993).

The Pomander watch is the earliest pocket mechanical watch that could be carried around(Leuenberger, 2002). It goes back to the early 16th century. Peter Henlein designed it in 1505 as a portable but inaccurate clock. This design sparked a trend in creating wearable watches, followed by more than ten other variants throughout the following century. Pocket watches evolved substantially over time as miniaturisation progressed, leading to the notion of strapping the gadget to the wrist in the twentieth century (Leuenberger, 2002). At the time, the improvements were driven mainly by military requirements (Friedman, 2015).

The Abacus Ring, which originates from the early 17th century under the Qing Dynasty, is the first known smart ring (Zolfagharifard, 2014). Back then, a traditional abacus was created out of parallel wires running between two boards on a frame, each with nine beads. It was designed primarily as a small, smart trading item. At the same time, it cleared the path for today's wearable computers and smart rings (Ometov et al., 2021).

Around the 20th century

The Pidgeon camera, designed by German scientist Julius Neubronner in 1907, is the first milestone in the history of portable cameras (Wilkinson, 2013). Unlike most other technological advances of the century, the camera was created to photograph Neubronner's pigeon flights. It is commonly misattributed to military purposes because pigeon photography and aircraft were often used for aerial surveillance during the 1st World War (DenHoed, 2018).

During World Wars I and II, the military was responsible for many wearable advancements (Ometov et al., 2021). The earliest held wireless systems were intended for ground communications in the first instance. Those were large and bulky, and military horses initially carried them. In 1937, Donald Hings designed a "packet" device, which eventually became known as a "walkie-talkie," which was a triumph in portable radio (Leer, 1989).

Wristwatches were essential for mission communication and preparation, allowing wearables to be widely used in the significant military sector and, as a result, marketing teams to adopt wristwatches globally (Myre, 2017). Simultaneously, the first wired hands-free devices combined with flying helmets were developed for the navy and pilots (Stamp, 2013).

Morton Heilig, who invented "Stereophonic Television Head-Mounted Display" in 1960, took the next important step in the evolution of wearable technology after World War II recovery(Ticknor, 2018). It was quickly followed by another claim for the "Sensorama Simulator," an improved version of the first device (Heilig, 1962). The gadget was the first to have a cold air blower, binocular display, an odour generator, vibrating seat, and stereophonic speakers (Rhodes, 1997).

MIT researchers Claude Shannon and Edward O. Thorpe built a timing device in a shoe that could perfectly predict the placement of a roulette ball on a table in 1961 (Thorp, 1966). This Timing device was the first wearable computer hidden inside a shoe. Later, in 1998, the actual story behind

the invention was revealed (Thorp, 1998). Hugo Gernsback created TV eyeglasses only a few years later (Kurland, 2017). Those glasses weighed approximately 140 gm and were fashioned around two battery-powered cathode-ray tubes, providing the stereoscopic sensation, which was revolutionary in 1963 (Ackerman, 2016).

Following that, in 1968, Ivan Sutherland invented the "Sword of Damocles," which is regarded as the first VR Head-Mounted Display (HMD) device, allowing users to engage themselves in a three-dimensional world(Ackerman, 2016). The prototype was partially see-through and allowed for head tracking, which took nearly ten years to build (Ackerman, 2016).

n 1972, Alan Lewis created the digital camera-case computer to predict roulette wheels. Following Thorpe's lead, he built a radio link between the information's receiver and the individual. The recipient used a computer to predict the roulette wheel and uttered his or her guess to the hearing aid radio antenna via a radio connection (Guler et al., 2016b).

The Pulsar Calculator Watch, which debuted in 1975, was an essential step forwards in the evolution of smartwatches. The first calculator watches to hit the market were sold higher (UniqueWatch, 2015).

Hewlett Packard introduced its first logical calculator watch in 1977. The HP-01 was a slight and brilliant design brilliance, with 28 keys on the clock display (Sasaki, 1982). 4 keys have been elevated for the convenience of usage (memory, alarm, amount, time), and two have been implanted. However, they can still be accessed with the fingers. The remaining keys were critical to pushing with a pen, which rapidly clamps the bracelet into the fastening (Hicks, 2007). The cheaper models, manufactured mainly by CASIO, maintain the calculator's clock architecture.

The first camera-to-tactile vest was built for the impaired by the enterprise "Smith-Kettlewell" in 1977. A decade of the investigation was required. The technology employed a head-mounted camera to generate a tactile simulation on a 10 inch and 1024-point grid on the user's clothing (Popat and Sharma, 2013).

Portable Stereo, another advancement in wearable technologies, might bring the mid-twentieth century to a conclusion. The Sony Walkman, which debuted in 1979, was the first commercially available portable personal stereo tape player with headphones. It was the first luxury wearable with a leather cover and a sophisticated appearance, and two jack outputs for privacy (Harrison, 2018).

Late 20th century

Wearable technology progressed quickly in the 1980s, with advancements in prior years' technology and a new AR wave. In 1981, Steve Mann finalised the Eye Tap project. He created the first backpack-style computer capable of processing data from a camera situated close to the eye and displaying it on a monitor in front of the sight (Mann et al., 2005). That was the precursor to Google Glasses and the first step towards contemporary AR glasses (Peltola, 2017).

The creation of The Active Badge, the first portable home automation tracker, 1990 brightened the start of the 1990s. It was developed by Olivetti Research and was capable of transmitting unique Identifiable Infrared (IR) signals to convey a person's position, marking the beginning of the Smart Room idea (Want et al., 1992, Greaves, 2000).

In 1994, the initial steps for personalised and portable electronic aides were taken. "Forget-Me-Not," a continuous personal recording system (Lamming and Flynn, 1994), was created by Mik Lamming and Mike Flynn. It was a device that captured people's interactions and saved the data in a database for later use.

Palm released the PalmPilot 1000, the first consumer personal digital assistant (PDA), in March 1996. It contains 128 kB of Random-access memory (RAM) and up to 12 MB of storage because it is effectively a single-chip computer. A 160 by 160-pixel screen and a stylus-based text input were included in these devices (Knight, 2016).

The year 1998 might be considered the start of the wearable payment era, now available on Apple Watch and Android Wear (Ometov et al., 2021). The mBracelet was the enabling device. It has three spaces for iButton buttons that could be swapped out. A three-colour Light-emitting diode (LED) grid was used to linkage the mBracelet to the client. Users might exchange messages by cross-shaking their hands using the mBracelet plug-in interface (Ometov et al., 2021).

The 21st century

The Levi's Industrial Clothing Division (ICD) Jacket, developed by Massimo Osti in cooperation with Philips, ushered in the 21st century (Kim, 2007). The jacket was composed of technology material and included an internal network connecting electrical devices. For its time, the concept was new, and it encouraged the development of businesses like Acronym(Kim, 2007).

Eric Friedman and James Park invented Fitbit in the early 2000s (Marshall, 2018) . Fitbit Classic was the first wireless activity tracker to integrate data with the internet and provide the same information available on a mobile phone when it was released (Marshall, 2018). In 2009, Samsung S9110 Smart Watch was introduced, which was the first smartwatch having a music player, full-colour touch screen, Bluetooth connectivity and voice recognition (Marshall, 2013). Around 2010, they were enhanced with texting, calling and email abilities(Guler et al., 2016a). With the development of Personal activity trackers around 2014, which collected data such as heart rate, calorie ingestion, sweat, skin temperature and several sleep levels using body IQ technology, the era of WIoMT began (Nguyen, 2016).

If we only look at IoT and its evolution, the leading technology started with Advanced Research Project Agency Network (ARPANET), which was used in academics and research studies to share work and connect with peers(Sharma et al., 2019).Then, it evolved with Radio-Frequency Identification (RFID) and embedded computer system(Sharma et al., 2019). The early use of IoT was on a coke machine to report the availability and temperature of the drink (Ornes, 2016).

Then came the limited use of the internet in the business and market in the early 90s, followed by pervasive computing (Weiser, 1999) and sensor nodes, which was the focal idea for IoT (Khan et al., 2012) Then, with the introduction of the device to device communication, the term "Internet of Things" came into existence (Ashton, 1999).

IoMT came into existence when sensor-based devices were incorporated with IoT and integrated with mobile technologies. These were then connected with Electronic Health Records in hospital settings, which grew the scope of IoMT (Frost and Sullivan, 2017).

Park and Jayaraman have also mentioned the development of user-friendly devices integrated into garments for the collection of body and environment information as one of the significant leads to the evolution of WIoMT (Park and Jayaraman, 2017). For instance, the Cyberia survival suit created by and registered under Remia was an innovative wearable with electronic heart rate, temperature and humidity measuring features along with communication ability (antenna, Global positions System (GPS) Short Message Service (SMS)), and positioning devices (motion sensors, posture, movement impacts) (McCann et al., 2009).

2.2 Wearable Technology and Internet of Medical Things (IoMT)

Wearable Technology is part of the Internet of Things (IoT). Wearables, wearable devices, or wearable technology refers to small mobile and digital devices, as well as computers with wireless communications capabilities, integrated into gadgets, accessories, or clothing that can be worn on the human body, or even invasive versions such as microchips or smart tattoos(Ometov et al., 2021).

IoT in healthcare is often termed as IoMT, Internet of Medical Things. IoMT is understood as a device of medical equipment, software applications, and health systems and services connected to the internet designed for people with medical assistance(Steger, 2020). It can also be defined as "the application of the fundamentals, principles, tools, techniques and concepts of the well-recognized with Internet approach particularly for the medical and healthcare sectors and domains"(Pratap Singh et al., 2020). IoMT provides tremendous advantages to people's well-being through improving quality of life and lowering medical costs.

In healthcare, the providers use IoT applications for various reasons: "embedded context prediction; embedded gateway configuration; indirect emergency treatment; semantic medical access; wearable device access; health information regarding children; community healthcare; and adverse drug reactions" (Alraja et al., 2019). These have indeed lowered healthcare costs, increased user satisfaction and served more people with limited resources (Alraja et al., 2019).
However, such devices have become a commodity of daily life for many. It indicates the importance of health, as many individuals wish to monitor their health indicators periodically.

Thus, the adoption of IoMT is considered "a growing pool of IoT technologies that is benefiting many industries" as it is a wave of sensory devices, including wearables (Steger, 2020).

Wearable devices are handy, seamless, portable, and may provide hands-free access to gadgets, despite their battery limitations (Ometov et al., 2021). They may be worn in any setting, and they provide customized data and the ability to connect to communication networks, allowing for remote monitoring (Godfrey et al., 2018). They may perform various monitoring and scanning tasks, including biofeedback and other sensory physiological functions like biometry(Ometov et al., 2021). They provide affordable, clinically sensitive data for more informed patient assessment (Godfrey et al., 2018).

Some of these wearable devices with their functions are mentioned below in a table (Ometov et al., 2021):

Device	**Functions**
Activity trackers	To monitor everyday activity such as the number of steps, basic heart rate, and body temperature to increase the overall physical activity of the user.
E-Skin (or nano patches)	Artificial skin with mechanical properties of human skin providing various sensing functions, close-to-human perception abilities
EEG and ECG belts	To monitor the user's health state from fitness, medical, and professional sports perspectives without specialized medical equipment.
Haptic suits	To capture both motion and biometrics
Ingestible and insertable	like medicine capsule packed with sensors, controllers and microprocessors to diagnose a disease or monitor the body internally
Personal notification devices	To signal the user about the incoming call or received messages
Smart Bands	To recognize gestures, detect stress/mood and monitor ECG
Smart clothes	regular clothes with invisibly embedded features, such as heating, charging or displaying
Smart contact lenses	Boost vision and monitor physiological parameters that help track blood glucose levels from the body fluid
Smart footwear	To monitor a person's posture, gait, and the number of steps mainly utilized to train professional athletes or monitor children

Device	Functions
Smart gloves	For gesture recognition, rehabilitation, or providing better haptic feedback
Smart necklaces	Jewellery with activity tracking, health monitoring, posture correction, or safety functionality
Smart patches	Utilized in sports and healthcare monitoring
Smart rings	For notifications regarding physical activity of the user
Smart watches	For health monitoring, activity tracking and many other similar functions. The most widely adopted wearables after the activity tracker. Generally, it provides almost the same functionality as a smartphone. However, most smartwatches' energy efficiency is still challenging without the gateway node due to the small form factor.

Table 1: Example Wearable devices with functions

There is a spectrum of devices under WIoMT such as Wearable Fitness Trackers, Wearable ECG Monitors, Wearable Blood Pressure Monitors, Biosensors, Smart Patches and Ingestible Sensors (Majumder et al., 2017). Wearable Fitness Trackers or Activity Trackers are IoT-based devices to monitor activity parameters of the wearer, and these indicators can be anything from the number of steps taken, distances covered, average speed, calories burned, hours of sleep and heart rates. The advanced and integrated versions of these trackers would be smartwatches with additional features of setting goals and being accountable for one's health (Kao et al., 2019). It is synchronized continuously wirelessly to a computer or smartphone (Lee et al., 2016, Kaewkannate and Kim, 2016).

Figure 3: Wearable Fitness Trackers (Rear, 2021)

Similar is Wearable ECG and Blood Pressure monitors. In the former, a wearable monitoring node gathers and transmits ECG data directly to the IoT cloud using Wi-Fi(Yang et al., 2016).

These can be worn on the wrist like a watch, wrist band, or bracelet, or they can be patches, clothes, necklaces, or straps for the chest that monitor either single-lead or multichannel ECG(Mizuno et al., 2021). On the other hand, the other type measures blood pressure and are wearable, non-invasive and cuff-less (Ganti et al., 2021).

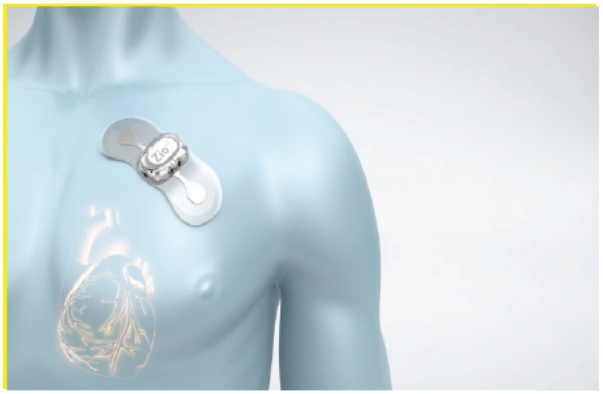

Figure 4: Wearable ECG Monitor (Lovett, 2018)

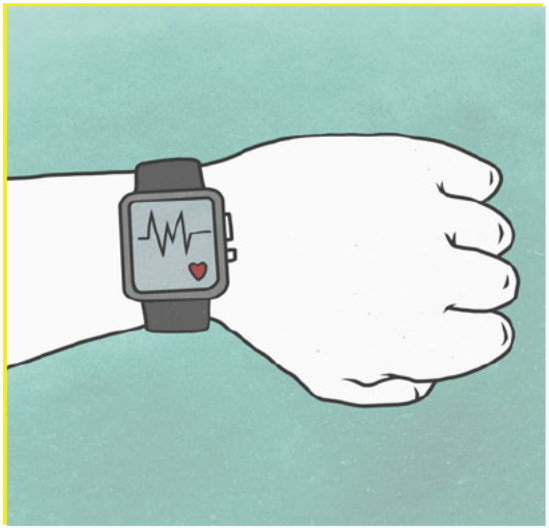

Figure 5: Wearable Blood Pressure Monitor (Alger, 2019)

Correspondingly, there are biosensors, smart patches and ingestible sensors, among a few of the other types of WIoMT devices. Biosensors are whole analytical devices in which a receptor, an active biological system such as an enzyme, antibody, or other similar systems, is placed on top of a transducer and can detect the presence of a specific analyte (Pateraki et al., 2020). Smart biosensors may be useful for those who require medical assistance or care and older persons who are experiencing a progressive loss of physical, cognitive, and other skills as they age(Pateraki et al., 2020). Smart systems can create a reactive living and working environment by continuously

monitoring bio-signals and combining them with environmental sensing to give suitable and timely suggestions, act preventively, and minimise health concerns (Pateraki et al., 2020).

Likewise, smart patches are a type of wearable sensor that is commonly utilised in the medical field. They have foam components and embedded electronics that monitor the patient's physiological indicators, such as their pulse(AG, 2021). Also, there are ingestible sensors which are electronic pills that, when swallowed, measure pH, temperature and pressure, and also monitor if a person has taken her/his medications (Molteni, 2018).

Some real examples of WIoMT devices are mentioned in the table below:

WIoMT devices type	**Real examples**
Wearable Fitness Trackers	Fitbit, Jawbone, Polar loop
Wearable ECG Monitors	Fitbit sense, Fitbit Versa 3
Wearable Blood Pressure Monitors	BPM Connect, Omron platinum
Biosensors	Vital Patch, Philips wearable biosensor
Smart Patches	Bio-patch, skin patch
Ingestible Sensors	ingestible sensing capsules

Table 2: Practical examples of WIoMT

2.3 Benefits of WIoMT

According to Deloitte's Centre for Health Solutions, the market for connected medical devices is predicted to grow from $14.9 billion in 2017 to $52.2 billion in 2022, with close to 70% of all medical devices being connected" (HD, 2021). It means that IoMT is a matter of concern for many users, with or without comprehending its necessity (HD, 2021).

Wearable technology allows users to access information on health, fitness, food and aging in real-time(Kaewkannate and Kim, 2016). The tracking and recording of daily activities or fitness can be computerized and integrated onto a wearable device, which displays the information on-screen or a smartphone (Kaewkannate and Kim, 2016). Further, it is quite useful in medical information systems, where it aids in the diagnosis, treatment and care of the patient (Godfrey et al., 2018). It is cost-effective as it consistently collects relevant data, which can be further used to predict clinical outcomes (Godfrey et al., 2018).

Furthermore, patients can see any doctor they desire in any part of the world in the future using wearable medical things. Physical constraints and distances that currently limit a specialist's field of practice will be removed, resulting in a global network of "specialty" centres where each hospital can focus on one discipline of healthcare rather than competing in all fields of expertise (Park and Jayaraman, 2003).

When medical services are needed in certain remote regions, the suggested IoMT technologies are vital. As a result, the use of IoMT principles and technologies has fundamentally transformed healthcare, medical procedures, and services (Pratap Singh et al., 2020).

Moreover, the IoMT industry produces smart devices like medical/vital sensors and wearables, which have become part of primary healthcare at home or community, and healthcare settings are also linked with real-time location, community health, and other services (Frost and Sullivan, 2017). These wearables in IoMT are given a specific term, Wearable Internet of Medical Things (WIoMT), and they have become one of the prevalent domains of IoMT (Frost and Sullivan, 2017). Athletic watches, activity trackers, wristbands, smart clothing and consumer-grade gadgets for personal wellbeing are some of the consumer wearable medical devices, like, for example, Apple Watch, Fitbit, Samsung Gear and Mi Band (Frost and Sullivan, 2017).

2.4 WIoMT Adoption Challenges and Risks

Healthcare wearables should be considered high-privacy and security risk gadgets since they continually collect the user's personal health information in real-time. Personal health information is more susceptible than other forms of data such as demographic or basic consumer data(Bansal et al., 2010). The choice to embrace such technology requires a security and privacy assessment that weighs the trade-offs between major benefits and perceived security/privacy hazards because the use of such devices involves the exposure of personal medical data (Xu et al., 2009). When a user believes that the anticipated advantages of using a wearable system outweigh the risks, the user will prefer to use healthcare wearable technology.

Initially, society had concentrated on the negative consequences of sharing personal data, such as security flaws, forgeries, and data theft. Angst and Agarwal (2009) did a preliminary investigation to see if individuals considered the costs and advantages of possibly surrendering some privacy in exchange for using Electronic Health Records (EHR). They found a substantial need for research on evaluating the effect of the user's perspective whenever technology is used to exchange personal information (Angst and Agarwal, 2009).

In addition, these wearables are typically conceived as consumer items, which may restrict their utility as health apps, as they are easily accessible and available to everyone who may not have bought them for health management in the first place itself (Azodo et al., 2020). Also, they have

the potential to alter healthcare delivery methods and the acquisition and transmission of sensitive personal information (Azodo et al., 2020). For all these reasons, these devices tend to complicate the matters related to privacy, security, sharing, autonomy, permission, ownership, access and valuation of data (Mittelstadt, 2017).

One of the major security and privacy issues in WIoMT is clear text login information and clear text HTTP data processing (Putta et al., 2020). It implies login and passwords of these devices are recorded in log files as plaintext (Putta et al., 2020). The data shared among different domains is sent as plain text, and no security measures such as encryption are used while transmitting the data(Putta et al., 2020).

In a study by Nanayakkara et al. (2019) , it was found that sensor tracking is the most commonly identified threat in the perception layer. Further, tag cloning, side channel, physical harm, and jamming threats were identified as potentially significant threats in the perception layer (Nanayakkara et al., 2019).

Further complications arise with preserving robust security and privacy of sensitive data (Nanayakkara et al., 2019). Unauthorised access to the medical data of the users and patients have been reported quite often (Nanayakkara et al., 2019). These security and privacy issues result in the deterioration of the effectiveness of WIoMT and adversely impact individuals' sensitive health information (Nanayakkara et al., 2019).

Another major vulnerability that WIoMT has been facing is cyber-attack. Cybercriminals can target devices that usually have less security protection. For example, MyFitness Pal was hacked in 2018, exposing the data of up to 150 million users and subsequently sold on the dark web. Recently 94% of health care organisations have been the victim of a cyber-attack (Williams and Woodward, 2015). It includes attacks on medical devices and infrastructure (Williams and Woodward, 2015). The international standards community has taken a lead role in developing and modifying existing standards to address issues related to malware infections, vulnerability and cyber-attacks (Slight and Bates, 2014). The proprietary nature of previously non-interoperable medical devices has limited integration between vendors' products (Slight and Bates, 2014) leading to errors in communication when integration is achieved. It means security is not achieved as interoperability and integration do not equate (Slight and Bates, 2014).

Similarly, various recommendations have been published by national regulatory bodies in order to address the serious issues of cyberattacks and the associated vulnerabilities and complications related to Health Care information of patients and WIoMT users (Yuan et al., 2018). The Food and Drug Administration (FDA) has issued two guideline publications on the management of cybersecurity in medical devices. Manufacturers should integrate risk management into the creation of medical devices, according to the initial FDA advice, and furnish the FDA with specified papers when submitting for clearance. The second FDA advisory advises producers to

keep an eye on cybersecurity for existing goods to adjust for new risks and vulnerabilities(Yuan et al., 2018). The FDA's guidelines does not analyse the risk assessment method used by manufacturers to assess the cyberthreats that their goods face, nor does it give criteria for manufacturers to determine the ability of countermeasures(Yuan et al., 2018). Though such recommendations are non-binding, they acknowledge that the shift in the operating environment of WIoMT needs urgent attention (Yuan et al., 2018). A debate also exists over the definition of medical devices and under what kind of circumstances any software shall be called medical devices (Yuan et al., 2018).

In light of the above, the security and privacy risks considerations in WIoMT and their impact could be summarised as follows: (Table 3)

WIOMT Security and Privacy Risks	**Impact**
Lack of Security Measures such as encryption while transmitting data	Data shared in different domains is recorded as plain text, which leads to compromised user login details.
Sensor tracking	Potential threats such as tag cloning, side channel, physical harm, and jamming threats
Poor Signal communication between medical devices such as Pacemaker and insulin pumps	Users rely on such devices but are at risk of cyber-attacks.
Unauthorised access	Deterioration of the effectiveness of WIoMT and adversely impact on individual's sensitive health information
Lack of standards, limited integration between devices	Errors in communication when integration is achieved.
Lack of regulation and compliance	Exposing medical devices towards cyber attacks

Table 3. Security and privacy risks impact

2.5 Theoretical framework

Recent research has focused on technical requirements and devices and improving IoT through connectivity and performance(Alraja et al., 2019). In 2017, Park et al. (2017) proposed a remote IoT monitoring system for home patients, evaluated based on effective system performance and efficient functioning for the IoT environment. Similarly, a study was done by Li and Pan (2017) where smartphones played a key role and sensors and microprocessors were integrated into a single device. Smartphone, emergency detection and online analysis was used to monitor vital signs, and it was linked with a telemedicine centre. These studies have only indicated the technological elements of IoT that will enhance service efficiency but lack processing of data (Li and Pan, 2017, Park et al., 2017). Ahmad, Rathore, Jeon, Anisetti and Paul proposed an intelligent care framework focused on IoT-based integration of big data across all devices in the medical system (Christensen et al., 2019) . This system has an innovative function in collecting data from different sensors, such as wearable devices for calculating health parameters that would be transmitted to a key mobile device. Later, the data obtained will be thoroughly analysed to determine whether or not there is a serious health issue. Using the same approach, Rathore et al. (2016) suggested a real-time medical emergency response system using IoT-based medical sensors installed on the user's body. Collected data were analysed for further decision making.

These researchers highlighted the significance of the technical requirements of IoT and the aspects in which health data could be assessed. However, they failed to address how the system could implement any potential architectures or alternatives for IoT adoption in the healthcare sector. In terms of user needs, Prayoga and Abraham (2016) explored variables that could anticipate the future user's decision to use an IoT health device and incorporated them into an understandable model. Researchers used the Technology Acceptance Model (TAM) model to observe the user's acceptance of technology and found out that the user's perception of IoT devices influences a user's intention to use such devices. Most of the studies relied on the TAM model and identified trust as one factor for technology adoption (Belanche et al., 2012a, Gao and Bai, 2014). Thus, there are differing views, and a general and concrete conclusion may not be derived.

2.5.1 TAM model

The technology acceptance model (TAM) is a widely used theory in information systems that describes how users accept and use technology. TAM (Davis 1989) is an extension of the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1980) and the Theory of Planned Behavior (TPB)(Ajzen, 1991). It mainly focuses on the effect of attitude on behaviour, and according to this theory, a user's intention to utilise a new information system determines his acceptance of the system (Lallmahomood, 2007). Researchers have confirmed and validated the TAM as a conceptual approach for technological adoption (Cho and Sagynov, 2015). The TAM suggests

that many variables influence users' decisions about how and when to utilise a recently introduced system (AlHogail, 2018). Further, it proposes that perceived ease of use and utility are the two fundamental factors of behavioural intention to utilise new technology. The proposed model's factors correspond to the TAM factors in two main ways. Firstly, in the TAM, the user intention to adopt technology is usually affected by external factors. In this model, the trust that leads to adoption is based on several external factors. Moreover, the two major factors from TAM, namely perceived ease of use and perceived usefulness, were employed as the starting points to collect other factors influencing trust towards adoption.

There are two key determinants in the traditional TAM model: perceived usefulness (PU) and perceived ease of use (PEU).

The degree to which a person feels that utilising a certain technology would improve his or her job performance is PU. This aspect is mostly used to assess a person's opinion of whether the desired objective can be reached with a certain technology (Davis, 1989). Usefulness is an important notion to consider while assessing the practicality of technology, such as IoT-based wearable fitness monitors (Kao et al., 2019).

On the other hand, PEU refers to how confident a person is that utilising a technology would be simple(Davis, 1989), and this is associated with the individual's ability and capacity to use relevant technology's functional components(Nielsen, 1993). PEU implies that something works well and that a person of ordinary ability may use the technology without annoyance for the intended objectives (Kao et al., 2019). Users' attitudes toward adopting and using a certain technology or product are determined by both PU and PEU (Kao et al., 2019). Most extended models for forecasting human behaviour in terms of technology adoption include two key assumptions, which substantially influence the technology adoption model (Kao et al., 2019).

2.5.2 Trust

Trust is a complex matter driven by various measurable and non-measurable factors(Yan et al., 2014). It is interrelated to security, as it is critical to ensure system security and user safety to build trust. According to Mayer et al. (1995), trust is "the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party". The most recent study on technology acceptance has emphasised trust as a key determinant of technology user behaviour (Tams et al., 2018).

In IoT, trust is a mechanism undertaken in the context of the user's perception and assumption of the competence of the IoT product. It implies the user was deciding to rely on the trusted entity to achieve the desired objective(AlHogail, 2018). The user would be aware of all the hazards

associated with being susceptible in this trust relationship (Lin and Dong, 2018). Trust is substantial for user's acceptance as it deals with the risk of vulnerability and uncertainty. Users need to interconnect with interconnected devices reliably and safely (Belanche et al., 2012b). Despite all potential risks and uncertainty associated with devices, trust is the factor that makes people use such devices. Gaining trust from users helps users decide on using only trustworthy devices and systems (Falcone and Sapienza, 2018).

Trust is vital for users to decide and adopt advanced technology without considering its consequences easily. The study conducted by Gao and Bai (2014) found a significant effect of trust on behavioural intention to adopt any IoT devices.

Though WIoMT is popularly used, they are considered a medium for data tampering. Due to various reasons such as insecure Web Interface, insufficient and invalid authorisation, lack of encryption and inadequate software protection, IOTs have severe vulnerabilities. These are the vulnerabilities of more than 70% of present IoT systems (Smith and Miessler, 2014). It became a major concern for WIoMT users and thus, creating trust issues among users.

A wide range of stakeholders is involved in the use of WIoMT. They are connected to the complexities of technological, social and policy considerations (Aldowah et al., 2020). WIoMT adoption is a trend that will remain. Thus, institutions, governments, and industries must manage, mitigate, and reduce the threats of using such devices (Aldowah et al., 2020). Trust requirements are difficult to meet concerning access control and identity management (Sicari et al., 2015). User needs and rights are of major concern in processing and manipulating data (Sicari et al., 2015). Control over one's virtual presence is necessary and should be ensured, but that is not the case now. Users are kept from creating a mental map of their virtual world (Sicari et al., 2015).

As WIoMT devices have benefits such as helping track sleep, calorie intake, movement etc., users gain a better understanding of their body and the ways to keep healthy (Prayoga and Abraham, 2016). However, benefits do not immediately equal users' acceptance. A study conducted by Prayoga and Abraham (2016) showed that Perceived Usefulness predicts behavioural intention to use. Nevertheless, trust should be considered essential for user acceptance as it can resolve two crucial circumstances in WIoMT systems such as vulnerability risk and uncertainty (Belanche et al. (2012a).

Gefen deduced that users, must be able to communicate with interconnected WIoMT systems and devices more securely (Gefen et al., 2003a) otherwise trust will be impeded. Besides, trust enables users to differentiate trustworthy devices and technology from harmful ones (Falcone and Sapienza, 2018). Trust is important to allow people to quickly adopt new technologies in unexpected situations since trust helps people understand the digital social world and eliminates

insecurity (Mayer et al., 1995). (Gao and Bai, 2014) and (Han et al., 2014) have shown the significance of trust in the adoption of IoT devices. Therefore, for the adoption of modern technology, especially WIoMT, trust plays a vital role in developing such devices.

2.5.3 Hypothesis Development

A study conducted on 489 IoT users by Hsu and Lin (2018) exposed that perceived usefulness and enjoyment significantly affect behavioural intention through the perceived value of IoT services. Similarly, it was also found that IoT adoption is significantly determined by perceived privacy risk (Hsu and Lin, 2018).

In another study, some of the major factors influencing and significant predictors in adopting IoT are performance expectancy, effort expectancy, social influence, hedonic motivation, and price value (Aldossari and Sidorova, 2020). Trust and security risk further play a vital role in determining IoT adoption (Aldossari and Sidorova, 2020).

According to Dong et al., many researchers have used experience theory and TAM to explore the general perceptions of users through the usage of IoT. In contrast, the finding that users embraced IoT systems through healthcare is constrained (Dong et al., 2017). There is a need for exploring users' security and perception of WIoMT.

This research aims to understand the user's perception of trust in the adoption of WIoMT. Exploring the security risks associated while adopting WIoMT is also crucial. Therefore, this study aims to contribute to the body of knowledge in this field by addressing this research gap and specifying the factors that influence users trust decisions.

Lee and Turban (2001) classified trust-related findings into three categories based on their different theories:

- Trust is defined in personality theory as a belief founded in conduct, which emerges early in the personality's psychological growth.
- Trust is defined in sociology and economics as a process that occurs inside and between communities, organisations, and individuals who trust them.
- In social psychology, trust is defined as the intentions and desires of the innocent party in a transaction, the concerns arising from that transaction and the various components that aid or obstruct the creation and maintenance of that trust.

This study adopts asocial-psychological viewpoint for examining variables impacting users trust and intentions in using WIoMT as it focuses on transactions and risk associated with WIoMT transactions.

To better understand the significance of the trust factors on the adoption of WIoMT, a conceptual model has been proposed that draws from the diverse understanding of trust and is based theoretically on the Technology Acceptance Model (TAM). The TAM is a prominent theory in

information systems that explains how a user adopts and uses technology. The TAM has been examined and validated by researchers, and it has been proved to be acceptable as a theoretical underpinning for technological adoption (Cho and Sagynov, 2015). There are numerous theoretical foundations for technology adoption, according to the TAM. According to the TAM, various variables influence users' decisions about how they will use a newly given system and factors that influence consumers' decisions about how they will use a recently suggested system. According to the TAM, the two most important criteria in behavioural intention to use technology are perceived ease of use and perceived utility (Gao and Bai, 2014).

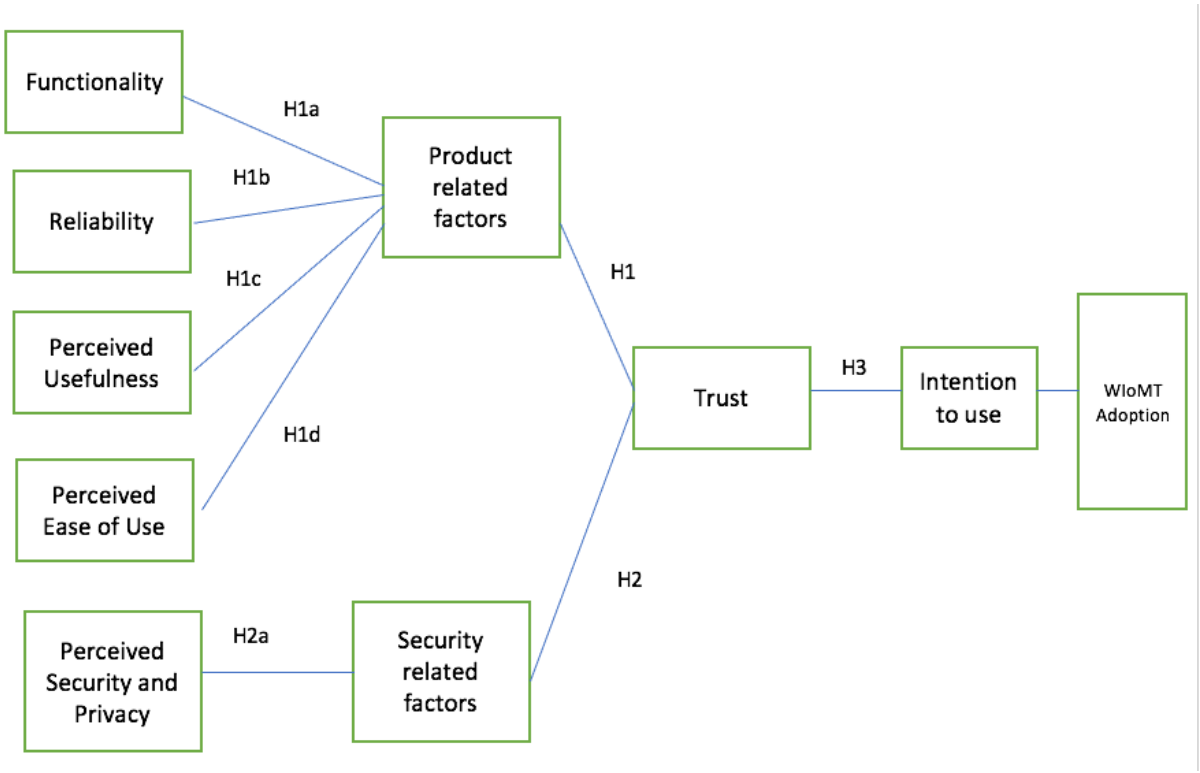

Figure 6. Conceptual Model

WIoMT device should have higher adoption rates to simplify it for consumers. The acceptance of WIoMT devices must be analysed from the users' perspective. Therefore, the following research questions and hypotheses will be considered in this study.

A. What factors influence trust and adoption of WIoMT?

B. What are the security risks associated with adopting WIoMT?

Numerous quantifiable and non-quantifiable factors impact WIoMT trust. The research model classified the factors into two main dimensions: product-related factors and security-related factors. Each dimension consists of several factors.

2.5.3.1 Product-related factors

Several product-specific factors may affect users' decision to trust a WIoMT product. Various models and studies have suggested a variety of factors affecting confidence that influence the adoption decision. These are:

Functionality and reliability: refer to whether technology has the ability or capacity to accomplish a specified task by having the required characteristics; and will function correctly and reliably in a consistent manner (Mcknight et al., 2011b).

Trust in the functionality of a technology depends on the capacity of that technology to perform properly. It is noted that users' trust is based on the perception that the service or product will carry out it is expected and requested function(Lai et al., 2011). Because errors are not acceptable to users on any technology, there is a huge impact of the absence of errors on trust toward WIoMT adoption, similar to IoT devices (Bart et al., 2005). Hence, the following hypothesis will be considered.

H1a: The functionality of WIoMT devices has an effect on trust towards WIoMT adoption.

H1b: The reliability of WIoMT devices has an effect on trust towards WIoMT adoption.

Perceived Usefulness: is defined as the degree to which one believes that using the technology will enhance his/her performance (Mcknight et al., 2011b).

Numerous studies have demonstrated the positive relationship between IoT products or services adoption rates and user perception that it could facilitate their everyday lives. Therefore, the Perceived Usefulness of the *WIoMT* devices must be advocated to achieve successful adoption.

H1c: Perceived usefulness has an impact on trusting WIoMT devices.

Ease of Use: refers to the degree to which one believes that using the technology will be effort-free. According to the ease of use of technology plays a significant role in building up consumers' trust towards a technology.

H1d: Perceived ease of use has an impact on trusting WIoMT devices.

2.5.3.2 Security related factors

In this context, security indicates the degree to which a person believes it will be risk-free to use a WIoMT product. When introducing new technology, security is a major user concern and directly affects the trust of the user of a particular product or service and thus the acceptance of technology (Al-Momani et al., 2016).

Perceived Security and Privacy: this factor is concerned with the ability of the trustee to achieve major security goals such as confidentiality which assures that only authorised users can have access to sensitive data, availability which guarantees the resilience of systems even though attacks occur, integrity assures to protect an original form of data and authenticity which eases any interaction between confirmed devices. Security is always a critical issue to which users are concerned regarding trust towards adoption. The level of security and privacy are critical characteristics of IoT technology that affect the development of users confidence in them as it assures users that they will be safe (Lai et al., 2011).

According to (Køien, 2011), users tend to trust IoT devices that use credible entities for authentication and access control. Such devices that show ability and willingness to protect themselves are w noted as trusted devices. Therefore, it can be deduced that there is a positive relationship between trust and WIoMT product security level.

H2: Perceived security and privacy has an impact on trusting WIoMT devices.

Trust may be considered as a major factor affecting behavioural intention to use any IoT technology (Yildirim and Ali-Eldin, 2019). Therefore, Trust plays a significant role in users' perception and adoption of WIoMT.

H3: Trust has a direct impact on behavioural intention to use WIoMT devices.

3. Methodology

This study adopted quantitative methods using a non-experimental cross-sectional design in a questionnaire. The reason for employing a questionnaire is to benefit from insights and perceptions to allow for correlation and regression analysis to be employed. Further, the participants fill the questionnaire directly, without any influence. So, genuine findings may be achieved.

The questionnaire consisted of two sections. The first section used demographic information to segment data and compared respondents. This section collected information regarding age group, gender and level of technical proficiency in using computers.

The objective of the second section was to assess the factors affecting trust based on the conceptual model in Section 2.6.3.

For the validity and reliability of the questionnaire, the questions were adapted from existing survey instruments and WIoMT risks and control gaps identified from the above literature. The questionnaire represented mainly two dimensions of factors with a hypothesis set for each factor. The table below illustrates the survey questions' description and their significance based on the hypothesis.

Dimension Hypothesis	**Domain Hypothesis**	**Description of Survey Questions**	**Question**
Product-related factors have a positive influence on trust towards WIoMT technology.	H1: The functionality and reliability of the WIoMT technology have positive effects on trust in its adoption.	To examine the impact of specific details about the functionality and reliability of WIoMT products on consumer trust. Furthermore, it assesses the impact of user expectations of product features, functionality, and capabilities on user decision to adopt.	Q29, Q30
	H2: Perceived ease of use has an important impact on trust in the adoption of WIoMT technology.	To investigate the impact of device ease of use and design on growing device trust and influencing customer decisions	Q18, Q19, Q20, Q21, Q22, Q23

		regarding device acceptance.	
	H3: Perceived usefulness has a strong impact on trust in the adoption of WIoMT technology.	To evaluate the influence of users' perceptions that using WIoMT technologies would make their lives easier and smarter, as well as save them time and effort, on their decision to adopt.	Q9, Q10, Q11, Q12, Q13, Q14, Q15, Q16, Q17
Security-related factors have a positive influence on trust towards WIoMT technology.	H4: Perceived security and privacy has a positive impact on trust in WIoMT technology adoption.	To investigate the significance of WIoMT system security and privacy in affecting user trust and acquire decisions.	Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q46, Q47, Q48, Q49, Q50, Q51

Table 4: Survey Questions' description

3.1 Participants

This study included 189 participants associated with Western Sydney University (WSU). The participants belonged to diverse cultures, backgrounds and age groups. Confirmation of the applicable and effective number of participants was done with implementing the rule set by Tabachnick and Fidell, which is $N \geq 50+8m$, where m is the number of predictors. Similarly, Stevens (2002) states that 15 participants per predictor are appropriate for sampling. This study meets the assumptions for both, with 189 participants.

To determine the user's perception towards WIoMT regarding consumer wearable device, the questionnaire was created based on the research questions and hypothesis stated in Table 4.

IoT is an extensively researched area that allows for the acceptance of previously used scales. Although the scales are created precisely for addressing specific IoT challenges, these can be adapted to address the identification and understanding of security risks and user perception of

WIoMT adoption. Each part of the questionnaire in this study was adapted from a previously used scale and literature.

3.2 Instruments

A structured questionnaire was created to collect primary data from the determined participants. The questionnaire included demographics, Perceived usefulness, Perceived ease of use, Functionality and Reliability, Perceived Security and Privacy, and Behavioural Intention to Use.

Each category of questions has been derived from a separate scale measuring the mentioned attribute.

- VSM International Questionnaire (2013) suggested by Hofstede and Minkov (2013) for demographics was followed. It included questions concerning age, gender, technical proficiency in using computers, perceived significance of technology, familiarity and usage of WIoMT, and if they were aware of any WIoMT from the list given in the questionnaire.

- Age was divided into five age groups: 18 to 24 years, 25 to 34, 35 to 44, 45 to 54, and above 55 years. Gender was categorized as "Male", "Female", "Non-binary/Third Gender", and "Prefer not to say" to be inclusive of all genders and also for those who do not prefer to answer this question. Technical proficiency in using computers was categorized ordinally that ranged from "Far Above Average" to "Far Below Average" with three other categories as "Somewhat Above Average", "Average" and "Somewhat Below Average". It is a self-reported perceived measure of technical proficiency rather than an objective measurement of competency of computer use.

- The perceived significance of technology was assessed via a statement affirming the significance of technology in everyday lives, for which the possible ordinal options were "Definitely Yes", "Probably Yes", "Might or Might Not", "Probably Not", and "Definitely Not". Similarly, familiarity and usage were evaluated by Yes/No statements.

- About various WIoMT the respondents were aware of, the list contained options: Wearable Fitness trackers, Wearable ECG Monitors, Wearable Blood Pressure Monitors, Biosensors and Smart Patches.

- Likewise, another section measured Perceived Usefulness, in which the questions were referred from studies by Prayoga and Abraham (2016) and Gao and Bai (2014).

- Here, there were nine statements related to Perceived Usefulness which were given ordinal ranks as: "Definitely Yes", "Probably Yes", "Might or Might Not", "Probably Not", and "Definitely Not".

- For Perceived Ease of Use, the statements were extracted from studies AlHogail (2018) and Lallmahomood (2007). Here also, there were six statements with the same ordinal ranks: "Definitely Yes", "Probably Yes", "Might or Might Not", "Probably Not", and "Definitely Not".

- Correspondingly, there were two statements assessing Functionality and Reliability which were obtained from the studies by AlHogail (2018) ,which had the same ordinal ranks as Perceived Ease of Use and Perceived Usefulness.

- Then, there were 26 more questions related to Perceived Security and Privacy in the same assertion format as the domains mentioned above, based on the surveys by Lallmahomood (2007) , Huang et al. (2007) and Alraja et al. (2019), which included the factors that influence user perception on the security of information. In this domain though, the ordinal ranks varied according to what is mentioned in the statement. For some set of questions, there was little pre-information given on the topic, so that the respondent is clear about how to rank the statement. Within these 26 questions, six answered the security risk perception, which answer one of our research questions.

- Lastly, there were four statements measuring Behavioural Intention to Use derived from studies by Alraja et al. (2019), AlHogail (2018) and Lallmahomood (2007) with the same ordinal ranks as before (i.e. Perceived Ease of Use and Perceived Usefulness).

- Gao and Bai (2014), Lai et al. (2011) , Alraja et al. (2019) and AlHogail (2018) were referred to for deriving questions concerning Trust Perception towards the security of WIoMT.

3.3 Methods and Procedure

All ethical approvals necessary for this project were considered. The first step towards collecting data confirmed that the study had ethics approval from the Western Sydney University ethics committee. For ethical approval, the ethics application was submitted online. In addition to this, a project description, participant information sheet, consent forms, and recruitment documents were developed. Once all these documents were in order, the application was sent for approval by the ethics board.

The questionnaire collated was uploaded onto Qualtrics and then advertised to current Western Sydney University students and staff.

3.4 Analysis

The collected data were exported to Microsoft Excel from Qualtrics for cleaning, screening and coding. It was further exported to Statistical Package for Social Science (SPSS) for statistical analyses.

At first, for descriptive statistics, frequency, percentage, mean, median and standard deviation were calculated, as appropriate. The frequency and percentage were calculated for all the categorical variables such as age groups, gender, technical proficiency in using computers, perceived significance of technology, and each domain's statement.
Mean, median and standard deviation were calculated for all the numerical variables such as age and scores for each domain and dimension. Graphical and tabular presentations were used where needed.

For inferential statistics, correlation analyses were tested between domains and dimensions at a 95% Confidence Interval with a p-value less than 0.05 being statistically significant. Pearson Correlation analysis was utilized when the association between two numerical variables are to be determined if they are non-Normal variables (Campbell (1995)). This study calculated scores for all domains based on their ordinal categories. These scores were correlated in pairs for each respondent to determine a significant association between two domains in the pair.

Moreover, regression analysis was conducted to determine the factor that has the most influence on the outcome variable of this study. Also, regression analysis calculated the per cent variation of the outcome variable (Behavioural Intention to Use) represented by the independent/input variables (Perceived usefulness, Perceived ease of use, Functionality and Reliability, and Perceived security and privacy). The regression model generated was also tested if it predicted the outcome variable, and if it did, to also determine which variable had the highest power to predict the outcome variable.

According to Iustina-Cristina and Gheorghe (2019), correlation analysis with a series of regression analyses between variables can display significant outcomes and precisely find factors that influence consumers' decision to accept WIoMT devices.

IBM SPSS software for statistical analysis was used to analyse the data in this study. Based on Correlation analysis, it was expected that there might be a correlation between security and perceived usefulness towards Trust and a correlation of intention to use that leads to attitude. Regression analysis was expected to find the strongest relationship between factors leading towards Trust and how they affect users' perception.

3.5 Ethics and Limitation

The ethical approval (H14191) for this study was obtained from the Ethics Committee of Western Sydney University, which included the project description and rationale, participant information

sheet and consent forms (see Appendix 4). After the ethical approval was received, the data collection commenced via Qualtrics.

Further, only data from those who gave online consent were collected. Before obtaining consent, participants were provided with a Participant Information Sheet, which contained information on the research, its objectives and possible risks and benefits. The beginning of the questionnaire ensured that respondents were above 18 years of age. Participants that were less than 18years were excluded from the study. All data collected was downloaded and stored in a password-protected cloud server.

4. Results

This study was conducted using Qualtrics with 55 questions involving 243 participants. Initial data screening revealed 32 blank surveys and 1 case of ineligible participant, which were removed before exporting to Microsoft Excel and SPSS for data cleaning and analysis. Then, the missing value analysis in SPSS showed 21 cases had incomplete responses with more than 50% questions unanswered, and the remaining others with at least 1 question unanswered. The former 21 cases were deleted as per suggestion by Kang (2013) and for the latter ones, regression imputation was conducted to replace the missing data with estimated values. Ultimately, the study included 189 responses. The analyses based on the responses provided by the participants were conducted through SPSS software, version 21, with the following outputs noted as findings/results.

4.1 Demographics

The first set of questions were related to demographics and other related information. Starting with age, more than half (42.9%) belonged to the 25 to 34 years age group, followed by 37% of those between ages 18 and 24, 9.5% between 35 and 44 and 6.9% between 45 and 54. There were 7 respondents of age 55 or above. (Table 5)

A little more than half of the respondents identified themselves as female. Males comprised 46.6% of the total respondents.

When asked about one's technical proficiency in using computers, almost half (45%) indicated they were at "Somewhat Above Average" level, 40.2% at "Average" level and 13.8% at "Far above Average" level of technical proficiency. Only 1.1% stated they had "Somewhat below Average" level of technical proficiency.

Likewise, when asked about technology having great significance in their lives, the majority

(88.4%) affirmed with "Definitely Yes", 11.1% answered with "Probably Yes" and only 0.5% gave the answer "Might or might not".

Also, more than half (65.6 %) of them responded they were familiar with WIoMT devices, and among them, 77 mentioned they used such devices and 47 said they did not. Similarly, when those who used such devices were asked if they were aware of any of the listed WioMT devices, only one-fourth (23.8%) selected Wearable Fitness Trackers, 3.2% selected Wearable ECG Monitors, 6.9% Wearable Blood Pressure Monitors, 2.1% Smart Patches and 4.8% mentioned they were aware of none of the listed devices.

Variables	Categories	Frequency	Percent (%)
Age Group	18-24	70	37.0
	25-34	81	42.9
	35-44	18	9.5
	45-54	13	6.9
	Above 55	7	3.7
Gender	Male	88	46.6
	Female	101	53.4
Level of technical proficiency	Far Above Average	26	13.8
	Somewhat Above Average	85	45.0
	Average	76	40.2
	Somewhat Below Average	2	1.1
Technology has great significance in your life	Definitely Yes	167	88.4
	Probably Yes	21	11.1
	Might or might not	1	0.5
Familiar with WioMT devices	Yes	124	65.6
	No	65	34.4
Use WioMT devices (n = 124)	Yes	77	40.7
	No	47	24.9
Aware of WioMT devices (n = 77)	Wearable Fitness Trackers	45	23.8
	Wearable ECG Monitors	6	3.2
	Wearable Blood Pressure Monitors	13	6.9

	Smart Patches	4	2.1
	None	9	4.8
Total		**189**	**100**

Table 5: Demographic and other characteristics of the respondents (N=189)

4.2 Security Risks

There were six statements related to security risks within Perceived Security and Privacy domain, which are: unauthorised access to data; malware infections and vulnerabilities; lack of regulation and compliance; unsecured network connectivity; lack of encryption; and lack of patching and device updates. (Table 4)

Taking descriptive look at each risk, for unauthorised access to data, more than two-thirds of the respondents agreed on its effect on WIoMT, while 23.2% gave neutral reply and only 6.4% denied its effect on the performance of such technologies.

Similarly, for all other security risks, more than sixty percent of the respondents affirmed the effect of those risks on the WIoMT devices. Only less than 10% of the respondents felt these risks did not affect the performance of WIoMT devices.

If we observe the proportions of participants responding to the statements related to security risks, most of them felt "unauthorised access to data" to be the most prominent risk for these devices, followed by "unsecured network connectivity" and "malware infections and vulnerabilities".

Statement	**Response n (%)**				
	Definitely Yes	**Probably Yes**	**Might or might not**	**Probably Not**	**Definitely Not**
Indicate your level of agreement on the security risk of "**unauthorised access to data**" impact on Wearable Internet of Medical Things.	64 (33.9)	69 (36.5)	44 (23.2)	3 (1.6)	9 (4.8)

Indicate your level of agreement on the security risk of "**malware infections and vulnerabilities**" impact on Wearable Internet of Medical Things.	59 (31.2)	68 (36.1)	49 (25.9)	5 (2.6)	8 (4.2)
Indicate your level of agreement on the security risk relating to "**lack of regulation and compliance**" impact on Wearable Internet of Medical Things.	56 (29.6)	69 (36.5)	48 (25.4)	7 (3.7)	9 (4.8)
Indicate your level of agreement on the security risk of "**unsecured network connectivity**" impact on Wearable Internet of Medical Things.	59 (31.2)	69 (36.5)	51 (27.0)	3 (1.6)	7 (3.7)
Indicate your level of agreement on the security risk of "**lack of encryption**" impact on Wearable Internet of Medical Things.	56 (29.6)	66 (34.9)	54 (28.7)	5 (2.6)	8 (4.2)
Indicate your level of agreement on the security risk of "**lack of patching and device updates**" impact on Wearable Internet of Medical Things.	52 (27.5)	75 (39.7)	46 (24.3)	9 (4.8)	7 (3.7)

Table 6: Security Risks of WIoMT

4.3 Reliability and Validity

Cronbach's alpha value was used to test the internal consistency within each domain and dimension.

Among the domains, the internal consistency was calculated for Perceived Usefulness, Perceived Ease of Use, Functionality and Reliability, Perceived Security and Privacy, and Intention to Use due to the multiple numbers of questions in each. It was found that the internal consistency in all five domains (Perceived Usefulness, Perceived Ease of Use, Functionality and Reliability, Perceived Security and Privacy, and Intention to Use) was higher than the acceptable value of 0.7 (Hair et al. 2010), thus, indicating a reasonable and acceptable level of reliability and validity as recommended by Hair et al (2010).

Domains	**Cronbach's alpha value**	**Cronbach's alpha value analysis**
Perceived Usefulness	0.911	Excellent
Perceived Ease of Use	0.892	Excellent
Functionality and Reliability	0.853	Excellent
Perceived Security and Privacy	0.917	Excellent
Security Risk*	0.943	Excellent
Intention to Use	0.866	Excellent

* "Security Risk" is the sub-domain of "Perceived Security and Privacy" domain.

Table 7: Internal Consistency of the Domains

Among three dimensions, the internal consistency was calculated for Product-related factors and Security-related factors, and the internal consistency for both dimensions are in the acceptable range (i.e., above 0.7). (Table 8)

Dimensions	**Cronbach's alpha value**	**Cronbach's alpha value analysis**
Product-related factors	0.929	Excellent
Security-related factors	0.917	Excellent

Table 8: Internal Consistency of dimensions

4.4 Correlation

a. Correlation between Product and Security-related factors

i. Functionality vs. Perceived Security and Privacy

There is a weak positive correlation between Functionality and Perceived Security and Privacy, and it is significant at $p < 0.001$ (Table 9). This means that, with the increase in the functionality of WIoMT devices, there is a significant increase in the Perceived Security and Privacy of such devices among the consumers.

Coefficient of Correlation I	**p-value**	**Functionality mean**	**Perceived Security and Privacy mean**
0.473	**0.000***	2.67	2.29

*Correlation is significant at the 0.001 level (2-tailed).

Table 9: Correlation between Functionality and Perceived Security and Privacy

ii. Reliability vs. Perceived Security and Privacy

There is a moderate positive correlation between Reliability and Perceived Security and Privacy, and it is significant at $p < 0.001$ (Table 10). This means that, with the increase in the reliability of WIoMT devices, there is a significant increase in how consumers Perceive Security and Privacy of such devices.

Coefficient of Correlation I	**p-value**	**Reliability mean**	**Perceived Security and Privacy mean**

0.531	**0.000***	2.83	2.29

*Correlation is significant at the 0.001 level (2-tailed).

Table 10: Correlation between Reliability and Perceived Security and Privacy

iii. Perceived Usefulness vs. Perceived Security and Privacy

There is a moderate positive correlation between Perceived Usefulness and Perceived Security and Privacy, and it is significant at $p < 0.001$ (Table 11). This means that, with the increase in the Perceived Usefulness of WIoMT devices, there is a significant increase in the Security and Privacy perception of such devices among the consumers.

Coefficient of Correlation I	**p-value**	**Perceived Usefulness mean**	**Perceived Security and Privacy mean**
0.540	**0.000***	2.04	2.29

*Correlation is significant at the 0.001 level (2-tailed).

Table 11: Correlation between Perceived Usefulness and Perceived Security and Privacy

iv. Perceived Ease of Use vs. Perceived Security and Privacy

There is a moderate positive correlation between Perceived Ease of Use and Perceived Security and Privacy, and it is significant at $p < 0.001$. (Table 12). This means that, with the increase in the Perceived Ease of Use of WIoMT devices, there is a significant increase in the Perceived Security and Privacy of such devices among the consumers.

Coefficient of Correlation I	**p-value**	**Perceived Ease of Use mean**	**Perceived Security and**

			Privacy mean
0.645	**0.000***	2.12	2.29

*Correlation is significant at the 0.001 level (2-tailed).

Table 12: Correlation between Perceived Ease of Use and perceived Security and Privacy

b. Correlation between Product and Security-related factors, and Intention to Use

Correlation analysis shows that there is significant correlation between Product and Security-related factors, and Intention to Use. (Table 13)

Product and Security-related Factors	Correlation Coefficient (with Intention to Use)	p-value
Functionality	0.371	**0.000***
Reliability	0.364	**0.000***
Perceived Usefulness	0.565	**0.000***
Perceived Ease of Use	0.631	**0.000***
Perceived Security and Privacy	0.686	**0.000***
Security Risk**	0.312	**0.000***

*Correlation is significant at the 0.001 level (2-tailed).

** "Security Risk" is the sub-domain of "Perceived Security and Privacy" domain.

Table 13: Correlation between Product and Security-related factors and Intention to Use

Moderate positive correlation can be observed between Perceived Usefulness, Perceived Ease of Use and Perceived Security and Privacy with Intention to Use of WIoMT devices respectively. Additionally, there is a weak, yet positive correlation between the Functionality, Reliability and Security Risk of such devices with their Intention to Use. According to Table 14, all factors are found to be significantly associated with Intention to Use at $p < 0.001$ level.

The Correlation analysis indicates that all Product and Security-related factors have a positive influence on the Intention to Use WIoMT devices, which leads to the rejection of their null hypotheses and affirmation of their hypotheses.

As it was found that the functionality of WIoMT devices was significantly linked to use, H1a, "The functionality of WIoMT devices has an effect on trust towards WIoMT adoption" was

supported by this study. It means that the respondents were ready to adopt WIoMT devices provided that the devices have proper functionality. An increase in functionality was found to increase users' perception of security and privacy. It creates more awareness of the potential risks of the use of WIoMT. It leads to trust, which finally results in the high possibility of adopting WIoMT devices, as an intention to use becomes strong.

H1b, states “the reliability of WIoMT devices has an effect on trust towards WIoMT adoption”. Reliability and intention to use were found to have positive correlation in this study. Reliability of the WIoMT devices builds trust and gives way to an intention to use, resulting in the adoption of WIoMT. It shows that despite lacking knowledge about device reliability, users are still willing to trust and adopt WIoMT devices.

H1c, “Perceived usefulness has an impact on trusting WIoMT devices” was also supported by the study. It was found to correlate with the intention to use positively. It proves that if the respondents understand the usefulness of the WIoMT, they trust WIoMT devices.

“Perceived ease of use has an impact on trusting WIoMT devices” was indicated as H1d in this study. It was found to support this study as the perceived ease of use was significantly associated with the intention of use. It brings forth an insight that trust in WIoMT and their adoption is highly impacted by perceived ease of use.

H2, “Perceived security and privacy has an impact on trusting WIoMT devices” was also supported by this study as it was found to be significantly correlated to intention to use. Trusting WIoMT devices on these grounds ignited the intention to use among the respondents. Security and privacy always matter while trusting to adopt or use any WIoMT devices. It was found that the participants considered trusting WIoMT device companies and service providers in protecting their individual data. This hypothesis is further supported by the positive correlation of Security Risk and Intention to Use.

On the grounds of functionality, reliability, perceived usefulness, perceived ease of use and perceived security and privacy, H3, “Trust has a direct impact on behavioural intention to use WIoMT devices” was found to be supported by this study.

All the above variables are further explored in a multivariate analysis (Regression) to determine the variables and factors with the strongest relationship and relevance when adopting WIoMT. The results are given below.

4.5 Regression

The regression has been calculated in the tables below. The adjusted R square value shows that 54% of the variation in Intention to Use is represented by Reliability, Perceived Usefulness, Perceived Ease of Use, Functionality and Perceived Security and Privacy (Table 14).

The value for the threshold of F is 0, which tells us that the null hypotheses can be negated, and the research hypotheses can be accepted.

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	0.744[a]	0.553	0.541	0.57698	0.553	45.266	5	183	.000

a. Predictors: (Constant), Reliability, Perceived Usefulness, Perceived Ease of Use, Functionality, Perceived Security and Privacy
b. Dependent Variable: Intention to Use

Table 14: Regression Analysis

Further, Table 14 shows how well the regression equation fits the data, and in this case, the model predicts the dependent variable significantly, i.e., the regression model statistically and significantly predicts the outcome variable.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	75.348	5	15.070	45.266	.000[b]
	Residual	60.923	183	.333		
	Total	136.270	188			

a. Dependent Variable: Intention to Use
b. Predictors: (Constant), Reliability, Perceived Usefulness, Perceived Ease of Use, Functionality, Perceived Security and Privacy

Table 15: ANOVA results

Likewise, Table 16 below shows the results of the multiple regression test. Here, the t-value of Perceived Security and Privacy is the highest with significance at $p < 0.001$ and hence, has the

highest power to predict the outcome (Intention to Use WIoMT). This brings clarity that users depend on device security and privacy while trusting to adopt any WIoMT devices.

Based on power to predict, Perceived Security and Privacy is followed by Perceived Ease of Use and Perceived Usefulness in the prediction of Intention to Use WIoMT devices.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.324	.179		-1.812	.072		
	Perceived Usefulness	.244	.093	.186	2.612	**.010***	.482	2.075
	Perceived Ease of Use	.280	.097	.221	2.875	**.005***	.414	2.417
	Perceived Security and Privacy	.691	.102	.474	6.789	**.000****	.500	1.998
	Functionality	.066	.054	.091	1.217	.225	.437	2.290
	Reliability	-.097	.055	-.140	-1.768	.079	.391	2.557

a. Dependent Variable: Intention to Use

* Significant at the 0.05 level (2-tailed)

** Significant at the 0.001 level (2-tailed)

Table 16: Regression Analysis on the Intention to Use WIoMT devices

This implies that three of the considered independent variables (Perceived Usefulness, Perceived Ease of Use, and Perceived Security and Privacy) of this study are the significant predictors of the dependent variable (Intention to Use). The following findings can be stated as the regression results for each of the three domains:

- Another significant aspect of WIoMT devices adoption by the users found in this study was WIoMT devices' security and privacy. It was found that WIoMT device adoption was affected by the perception of the user on this ground. It was found that if the user perception indicated the compromising of one's privacy and security, the user is less likely to adopt WIoMT devices. Therefore, it became clear that concerns about privacy and security are of high consideration in terms of users while trusting to adopt WIoMT devices.

  In terms of evaluating the influence of users' perceptions that using WIoMT technologies would make their lives easier and smarter, some enquiries were put forth. It was found that

the users who believe and understand the time and effort saving nature of WIoMT devices influenced their decision to adopt them. With respect to the questions regarding ease of use and device usefulness, results indicate a positive attitude towards adoption if WIoMT devices are easy to use and able to demonstrate device usefulness. Perceived usefulness and ease of use are inter-related aspects and affect user's perception towards trusting to adopt any WIoMT devices.

Likewise, the regression analysis shows that Intention to Use of WIoMT devices is also determined by the user's Perceived Security and Privacy. When the user's Perceived Security and Perceived Privacy are ensured by WIoMT, then the user gains trust in the device and intend to use the device.

This study was also geared towards investigating the significance of trust in affecting behavioural intention to use towards WIoMT adoption. It was found that trust generated in the user plays an important role in affecting the behavioural intention to use towards WIoMT adoption. This implies that any user's behavioural intention to use is influenced by trusting WIoMT devices.

5. Discussion

This study aimed to find the factors influencing trust and intention to use WIoMT devices. The results confirmed that the two dimensions and five domains predict consumers' intention to use WIoMT devices. These two dimensions were product-related factors and security-related factors, whereas five domains were Functionality, Reliability, Perceived Usefulness, Perceived Ease of Use and Perceived Security and Privacy. The study showed that these factors were significantly associated with Intention to Use WIoMT devices. Perceived Security and Privacy was the greatest predictor of the dependent variable, Intention to Use. Each of the factors and variables studied in this research is discussed below regarding the research questions and hypothesis of this study.

This study comprised of individuals who aged mostly between 25 to 34 years old, followed by those of 18 to 24 years of age, which is similar to the studies by AlHogail (2018), Lallmahomood (2007) , Kao et al. (2019) , Hsu and Lin (2018) and Zhang et al. (2017). This study can be explained by the fact that it took place in a university context where young adults comprise most of the population. In the other mentioned studies, online surveys were also utilised, mostly accessed by young people, not older individuals (Kelfve et al., 2020).

Similarly, there were more female respondents than males, which was opposite to the studies by Lallmahomood (2007) , Kao et al. (2019) and Smith (2008). However, this finding was similar to other studies by Hsu and Lin (2018) and Zhang et al. (2017). It may be explained by a study on the influence of gender on online survey participation, which showed that females are more likely to contribute to online surveys than males (Smith, 2008).

When asked about the familiarity with WIoMT devices, in this study, more than half of the respondents mentioned they were familiar with such devices. Among them, 40.7% of the total sample had used them, which is quite different from the study by AlHogail (2018) which mentioned 81% of their sample had used at least 1 to 5 IoT devices, and from the studies by Kao et al. (2019) and Hsu and Lin (2018), which have 100% of the sample using IoT devices. It is an interesting finding for a sample extracted from a specific population belonging to an educational institution. It lets us predict the usage of such devices in the general population, and this information can be useful for promoters and marketers of such technology.

In this study, the reliability measure across the dimensions shows accuracy in the measurement to the extent that even if the respondent answers the questions multiple times, she/he answers the same way every time. It is determined' by Cronbach's alpha higher than 0.7 for both dimensions. Similar values were also obtained in studies by AlHogail (2018) and Lai et al. (2011) the reference articles for this study.

Likewise, the reliability across the domains is also high, i.e., more than 0.7 for all domains. This is in coherence with other studies (AlHogail, 2018, Kao et al., 2019, Lai et al., 2011, Lallmahomood, 2007, Kowatsch and Maass, 2012) where the reliability measure is above satisfactory for the concerned domains of the Intention to Use WIoMT devices, such as Perceived Usefulness, Perceived Ease of Use, Perceived Security and Privacy, Functionality, and Reliability. There were similar results in the pilot study, which incorporated the same dimensions and domains.

All product-related and security-related factors are significantly associated in this study. They have a positive correlation, which means that with an increase of one, there is a subsequent and significant increase in the other. For example, if the functionality of WIoMT devices perceived by the consumer increases, then their perception of privacy and security of such devices also increases. Similarly, if these devices are perceived to be reliable, useful and easy to use, their view regarding the privacy and security of using such devices also increases. This finding is also coherent with studies by AlHogail (2018) and Lallmahomood (2007).

Likewise, in this study, it was found that all Product and Security-related factors were significantly and positively correlated with the dependent variable, Intention to Use. This result was similar to Kowatsch and Maass (2012) and Lallmahomood (2007). It illustrates that the theoretical framework for this study is in alliance with the findings derived from the analyses. It, in fact, also validates the hypotheses we had set before commencing the study, which stated that the Product-related and Security-related factors (Perceived Usefulness, Perceived Ease of Use, Perceived Security and Privacy, Functionality and Reliability) all have an impact on trusting WIoMT devices which in turn affect the intention to use them.

Similarly, the sub-domain Security Risk was also significantly correlated with the dependent variable Intention to Use. In this study, the security risks identified were

1. Unauthorized access to data
2. Malware infections and vulnerabilities
3. Lack of regulation and compliance
4. Unsecured network connectivity
5. Lack of encryption
6. Lack of patching and device updates

In this study, most of the participants felt "unauthorised access to data" to be the most prominent security risk for WIoMT devices, followed by "unsecured network connectivity" and "malware infections and vulnerabilities".

There was a significant correlation with Intention to Use. When users perceive security risks in using the devices, their tendency to use such devices is affected, which is significant and not merely due to chance. According to the findings from this study, the security risk mentioned had an impact on the intention to use such devices. It showed that intention to use was affected when it agreed more on the impact of the security risk.

Furthermore, the regression analysis has shown all domains to predict factors of the dependent variable, Intention to Use WIoMT devices. These domains are the independent variables: Perceived Usefulness, Perceived Ease of Use Functionality, Reliability, and Perceived Security and Privacy. It is consistent with the studies by (Alraja et al., 2019, AlHogail, 2018) , Kao et al. (2019) , Hsu and Lin (2018) and Lallmahomood (2007). Among the predictors of Intention to Use, Perceived Security and Privacy was found to have the highest power to predict the outcome. This finding was similar to the studies by Kowatsch and Maass (2012) , AlHogail (2018) , Kim et al. (2017) , Kowatsch and Maass (2012) and the theory presented by Khan et al. (2016). It suggests that if users believe that the device protects their privacy and has security measures for their stored/shared information, they are more likely to use it. It is basic for any technology in the modern world, where people trust in the inanimate objects for their health and wellbeing. In other words, IoT service providers need to resolve security issues using various security controls such as encryption, data transparency and Public Key Infrastructure, and in general applying best data? management practices. (AlHogail, 2018)

However, this finding is different in studies by Yildirim and Ali-Eldin (2019), Lai et al. (2011), Kao et al. (2019), Gao and Bai (2014) , Alraja et al. (2019), Hsu and Lin (2018) and Lallmahomood (2007) where other factors turned out to be the powerful predictors other than Perceived Security and Privacy. Most of them concluded the product-related factor (mostly Perceived Usefulness) to be the most influential predictor of Intention to Use of WIoMT devices. It is also relevant because the consumer buys a product only when they perceive something to be useful. Similar is the case with WIoMT devices. If a person does not see any need for it, even though it has the best security

features and is very easy to use, he/she does not intend to use it, which in turn discourages him/her from buying it in the first place. However, our study showed that the privacy and security domain had the highest power to predict the intention to use such devices. In contrast, others such as Perceived Ease of Use and Perceived Usefulness had lower power to predict in comparison, but still, they were the other predictors.

This study had two research questions which were:

(a) What factors influence trust and adoption of WIoMT?
(b) What are the security risks associated with adopting WIoMT?

The results and findings indicated that the factors that influence trust and adoption of WIoMT were mainly Perceived Security and Privacy, Perceived Ease of Use and Perceived Usefulness. Among these, Perceived Security and Privacy had the highest power to predict the adoption of WIoMT. All these predictors led the user to trust the devices and intent to use them. It means that the participants in our study looked for security features in such devices before trusting them and intending to use them. After they are assured of their ability to keep information private and secure, they look for ease in using them and how useful they are for themselves. Yes, there was a positive correlation between their functionality and reliability with the intention to use WIoMT devices, but these became insignificant when adjusted with other factors.
As for the next question, the security risks identified in this study were: unauthorised access to data, malware infections and vulnerabilities, lack of regulation and compliance, unsecured network connectivity, lack of encryption and lack of patching and device updates.

These risks had been identified in the literature review of this study, and the findings from the survey showed that these risks were, in fact, significantly correlated with Intention to Use, which means they had a significant effect on the behavioural adoption of these technologies. These risks comprised the sub-domain part of the Security-related domain, the strongest predictor of the outcome variable.

5.1 Theoretical and Practical Implications

This study revealed that the proposed model predicted more than half of the outcome variable (R^2 = 0.54). The significant variables that affect the intention to use WIoMT devices were Perceived Security and Privacy, Perceived Ease of Use and Perceived Usefulness. Perceived Security and Privacy had the highest influence on the adoption of WIoMT than other domains (ß = 0.691, t = 6.789). This showed that if the consumers of these technologies do not perceive the devices to store and/or relay information securely and privately, they will not have intention to use it in the first place. This reflects that WIoMT devices need to have the best security and privacy features to be relevant in the market.

Also, these technologies need to be easy to use so that users do not get discouraged in using them. After all, these are built to be used voluntarily, as for many these have not become necessities, until and unless they have some health issues they want to manage on their own. Hence, these devices need to be easily comprehensible for all age-groups, especially older generations who need more utilization of these wearables that track their health and help maintain wellness.

Not only easiness in use, but also its actual usefulness determines it utilization among the users. They need to visualize what these devices can do to make their lives easier, and this can be done in various ways. One effective way can be bringing forth prominent people in the community who use these devices and can advocate for them to others. Hence the developers need to make these devices user-friendly and purposive with exciting features so that they have intention to use it.

Moreover, this study can be considered a good contribution to the body of knowledge in terms of understanding the perception as well as adoption of users towards WIoMT. This facilitates in understanding the usage and practicality of WIoMT in improving and facilitating good health among users, which is the main goal of such devices.

In terms of definition and usage, WIoMT basically are such devices that are small, digital and mobile devices that are either worn on clothes, or as wearable articles (such as watches, necklaces etc) or inserted in the body, with the motive of either monitoring one's body functions or providing aid to the body in order to reduce the effects occurred due to some bodily dysfunction. WIoMT need to be connected to the internet, either regularly or periodically and either directly or via smartphones. In saying so, it is to be understood that WIoMT are suitable mostly in such areas where the internet is accessible.

On the other hand, the users have certain considerations for the adoption and use of WIoMT such as trust and intention to use. Insurance of data privacy and security leads to the intention of use. Similarly, one of the most influential factors that leads to the adoption of WIoMT is the efficiency of them in saving time and efforts of medical attention or health monitoring.

This study narrowed the research on the wearable technology, which are much more prevalent and known among the general public than other IoT and IoMT devices and equipment. It has developed a better understanding of the trust factor in behavioural intention to use those products.

5.2 Strength and Limitations

This study's strength lies in its scope, which is WIoMT devices. Many studies before have utilised these models to discuss the adoption of IoT and IoMT, but this study is among very few that have stayed relevant to the present times, where wearable technologies have become a necessity for many with chronic and other diseases. This study provides insight to vendors, manufacturers and healthcare providers in understanding advanced technology from the user's perspective to contribute to this competitive global market. Also, most of the researchers from our findings have focused on considering technological aspects of the device rather than the user's perspective for adopting new technology, which has been the main focus of this study. The adoption of WIoMT by users will benefit various groups, including the government, advertising firms, manufacturers, and healthcare professionals. It will help users and the healthcare sector develop a device that is simple to use and secure for users. Understanding the user's perception of trust towards WIoMT from this study will contribute to new advances in the IoMT sector, such as robotic medical equipment and remote monitoring devices. Adopting technology over conventional techniques is difficult, especially in the health care industry. This study will help overcome the challenges of trust, security, and privacy in the usage of wearables to assist manufacturers and the healthcare sector in developing true consumer-centric technologies.

These results of this study come with limitations. First, this is a self-reported online survey, which may have resulted in information and selection biases, which is common with the nature of the study methodology.

The second is generalisability. The participants of this study are limited to Western Sydney University in Australia; hence the results may not be generalisable to populations of other countries, which may be very different from Australia in the economic, social and cultural context. The study has tried to minimise this by incorporating international students and staff, but the country's cultural context will influence consumer behaviour.

Third, the study is primarily quantitative, and hence, only objective views have been captured. Supplementary qualitative studies might provide more insight into the utility of such devices.

Lastly, in this study, a little more than half (54%) of the variance in the outcome variable was due to the independent variables considered in this study. However, the unexplained remaining 46% variance implies to some extent that there might be other possible domains that influence the

Intention to Use WIoMT devices and have been missed in this research model. This study can be a basis for further research on this arena.

Nonetheless, the study's results are consistent with those of other similar studies, indicating that it will benefit a wide range of people by providing information on users' behaviour and intentions to use WIoMT devices. It will help future researchers to work for better acceptance and usability of similar or advanced WIoMT devices.

6. Conclusion

The main purpose of this study was to investigate the factors that led to trust and eventually to the intention to use WIoMT devices, study the power of those independent variables on the outcome variable, and explore the security risks associated with adopting WIoMT. The independent variables/domains considered in this study were Perceived Usability, Perceived Ease of Use, Reliability, Functionality and Perceived Security and Privacy, mainly extracted from the TAM model.

The study had 189 responses subjected to quantitative analyses using SPSS version 21. First, the descriptive data was extracted, which showed more participants belonged to 25 to 34 years age group, more females, more with the above-average level of technical proficiency in using computers, more believing technology to be significant in one's life, more familiar with WIoMT devices, and more using such devices among those who knew about such devices.
Next, to check the reliability and validity of the study instrument, the internal consistency was calculated within each dimension and each domain. Cronbach's alpha value, which measures the internal consistency, was higher than the acceptable cut-off of 0.7. It showed that the study instrument was reliable and valid in accomplishing the research objectives.

The collected data was further subjected to correlation analysis, which looked for correlation coefficients among various domains and sub-domains and thus bivariate associations of one domain with another. It was found that all independent variables were correlated univariately with the dependent variable as all domains were found to be significantly associated with Intention to Use at $p < 0.001$ level. The correlation analysis helped validate the hypotheses mentioned at the beginning of this study. It means that when all Product and Security-related factors increase in their influence, the resulting Intention to Use of WIoMT devices also increases.

Then, regression analysis helped determine the factors with the strongest relevance when adopting WIoMT. Only three of them, i.e., Perceived Security and Privacy, Perceived Usability and Perceived Ease of Use, were found to have significantly predicted the outcome variable (Intention to Use). This finding is not merely by chance but a statistical backup to it. It means that if the user perceives that that device maintains security and privacy, if it is usable and easy to use, only he/she will intend to use it.

The highest power to predict the dependent variable was the Perceived Security and Privacy domain, even among these three. Also, the generated model predicted a 54% variation in the outcome variable to be credited to the study's independent variables, namely Reliability, Perceived Usefulness, Perceived Ease of Use, Functionality and Perceived Security and Privacy. These findings led to the answers to the research questions stated at the beginning of this thesis.

This study was also geared to explore security risks in the adoption of WIoMT devices. These security risks were unauthorized access to data, malware infection and vulnerabilities, lack of regulation and compliance, unsecured network connectivity, lack of encryption and lack of patching and device updates. The sub-domain of these risks was significantly correlated with Intention to Use. It means that if the users perceive these risks to be present during WIoMT devices, they will have less intention to use such technology.

This study contributes to the literature regarding adopting WIoMT devices in our daily lives in which usability, ease to use, security and privacy affect the trust of the consumer, which ultimately leads towards the behavioural intention to use such devices regularly and adopting these technologies in day-to-day lives.

Moreover, this study has highlighted that security and privacy factors have the most power to influence the use of WIoMT where manufacturers, healthcare providers and vendors need to focus on what users think if they have the vision to proliferate their technology in the world.
As found in this study, there were still potential consumers who were yet to be familiar with and use of WIoMT devices. There could be expansive marketing and public awareness strategies so that more people adopt these technologies and be proactive in building a healthier living.

Future Research

This study discovered interesting findings, such as the impact of security and privacy concerns on WIoMT device adoption. There were certain limitations, such as that this study only drew individuals from Western Sydney University. However, this work might serve as a starting point for further research in this area. It will aid future researchers in improving the acceptability and use of comparable or upgraded WIoMT devices in the future. Future researchers can obtain more individuals who have used WIoMT devices with more geographical location and understand more about users' perspectives towards adoption.

7. References

ACKERMAN, E. 2016. The Man Who Invented VR Goggles 50 years Too Soon. *IEEE Spectr*.

AG, C. 2021. *Wearable smart patches in medical monitoring and diagnosis* [Online]. Available: https://solutions.covestro.com/en/highlights/articles/cases/2021/sensor-based-wearable-smart-patches [Accessed 16 August 2021].

AJZEN, I. 1991. The theory of planned behavior. *Organizational behavior and human decision processes,* 50**,** 179-211.

AL-MOMANI, A. M., MAHMOUD, M. A. & AHMAD, M. 2016. Modeling the adoption of internet of things services: A conceptual framework. *International journal of applied research,* 2**,** 361-367.

ALDOSSARI, M. Q. & SIDOROVA, A. 2020. Consumer Acceptance of Internet of Things (IoT): Smart Home Context. *Journal of Computer Information Systems,* 60**,** 507-517.

ALDOWAH, H., REHMAN, S. & UMAR, I. 2020. Trust in IoT Systems: A Vision on the Current Issues, Challenges, and Recommended Solutions.

ALGER, K. 2019. Best heart rate monitors to track your heart health. Hearst UK
ALHOGAIL, A. 2018. Improving IoT technology adoption through improving consumer trust. *Technologies,* 6**,** 64.
ALRAJA, M. N., FAROOQUE, M. M. J. & KHASHAB, B. 2019. The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception. *IEEE Access,* 7**,** 111341-111354.
ANGST, C. & AGARWAL, R. 2009. Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly,* 33**,** 339-370.
ASHTON, K. That 'Internet of Thing' Thing. 1999.
AZODO, I., WILLIAMS, R., SHEIKH, A. & CRESSWELL, K. 2020. Opportunities and Challenges Surrounding the Use of Data From Wearable Sensor Devices in Health Care: Qualitative Interview Study. *J Med Internet Res,* 22**,** e19542.
BANSAL, G., ZAHEDI, F. M. & GEFEN, D. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decis. Support Syst.,* 49**,** 138–150.
BART, Y., SHANKAR, V., SULTAN, F. & URBAN, G. L. 2005. Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *Journal of Marketing,* 69**,** 133-152.
BELANCHE, D., CASALÓ ARIÑO, L. & FLAVIAN, C. 2012a. Integrating trust and personal values into the Technology Acceptance Model: The case of e-government services adoption. *Cuadernos de Economía y Dirección de la Empresa,* 15**,** 192–204.
BELANCHE, D., CASALÓ, L. V. & FLAVIÁN, C. 2012b. Integrating trust and personal values into the Technology Acceptance Model: The case of e-government services adoption. *Cuadernos de Economía y Dirección de la Empresa,* 15**,** 192-204.
BURGESS, M. 2018. *What is the Internet of Things? WIRED explains.* [Online]. WIRED UK. Available: https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot. [Accessed 12 August 2021].
CAMPBELL, M. J. 1995. *Statistics at Square One* [Online]. BMJ Publishing Group 1997. Available: https://www.bmj.com/about-bmj/resources-readers/publications/statistics-square-one [Accessed].
CHO, Y. C. & SAGYNOV, E. Exploring Factors That Affect Usefulness, Ease Of Use, Trust, And Purchase Intention In The Online Environment. 2015.
CHRISTENSEN, J., PONTOPPIDAN, N. H., ANISETTI, M., BELLANDI, V. & CREMONINI, M. 2019. *Improving Hearing Healthcare with Big Data Analytics of Real-Time Hearing Aid Data*.
DAVIS, F. D. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly,* 13**,** 319-340.
DENHOED, A. 2018. The Turn-of-the-Century Pigeons That Photographed Earth from Above. línea] Disponible en: https://www. newyorker. com/culture/photo-booth/the ….
DIMITROV, D. V. 2016. Medical Internet of Things and Big Data in Healthcare. *Healthcare informatics research,* 22**,** 156-163.
DONG, X., CHANG, Y., WANG, Y. & YAN, J. 2017. Understanding usage of Internet of Things (IOT) systems in China: Cognitive experience and affect experience as moderator. *Information Technology & People,* 30**,** 117-138.

DUTTA PRAMANIK, P., UPADHYAYA, B., PAL, S. & PAL, T. 2018. Internet of Things, Smart Sensors, and Pervasive Systems: Enabling the Connected and Pervasive Health Care.
FALCONE, R. & SAPIENZA, A. 2018. On the Users' Acceptance of IoT Systems: A Theoretical Approach. *Information (Switzerland),* 9.
FISHBEIN, M. & AJZEN, A. 1980. Understanding Attitudes and Predicting Social Behaviour. Preventive-Hall. *Inc., Englewood Cliffs*.
FRIEDMAN, U. 2015. A brief history of the wristwatch. *The Atlantic,* 27.
FROST & SULLIVAN. 2017. *Internet of Medical Things: Revolutionizing Healthcare* [Online]. Available: https://aabme.asme.org/posts/internet-of-medical-things-revolutionizing-healthcare [Accessed March 12, 2020].
GANTI, V., CAREK, A. M., JUNG, H., SRIVATSA, A. V., CHERRY, D., JOHNSON, L. N. & INAN, O. T. 2021. Enabling Wearable Pulse Transit Time-Based Blood Pressure Estimation for Medically Underserved Areas and Health Equity: Comprehensive Evaluation Study. *JMIR Mhealth Uhealth,* 9**,** e27466.
GAO, L. & BAI, X. 2014. A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics,* 26**,** 211-231.
GEFEN, D., KARAHANNA, E. & STRAUB, D. 2003a. Trust and TAM in Online Shopping: An Integrated Model. *MIS Q.,* 27**,** 51-90.
GEFEN, D., KARAHANNA, E. & STRAUB, D. W. 2003b. Trust and TAM in Online Shopping: An Integrated Model. *MIS Q.,* 27**,** 51-90.
GODFREY, A., HETHERINGTON, V., SHUM, H., BONATO, P., LOVELL, N. H. & STUART, S. 2018. From A to Z: Wearable technology explained. *Maturitas,* 113**,** 40-47.
GREAVES, D. 2000. Olivetti research active badge.
GULER, S., GANNON, M. & SICCHIO, K. A Brief History of Wearables. 2016a.
GULER, S. D., GANNON, M. & SICCHIO, K. 2016b. A brief history of wearables. *Crafting Wearables.* Springer.
HAN, B., WU, Y. & WINDSOR, J. C. 2014. User's Adoption of Free Third-Party Security Apps. *Journal of Computer Information Systems,* 54**,** 77 - 86.
HARRISON, B. 2018. *Design Moment: Sony Walkman, 1979: The Silver and Blue Portable Personal Stereo Sold beyond All Expectation* [Online]. The Irish Times (1979). Available: https://www.irishtimes.com/life-and-style/homes-and-property/interiors/design-moment-sony-walkman-1979-1.3465629 [Accessed December 2021].
HD. 2021. *Understanding the basics of the IoMT and Connected Devices* [Online]. Haughton Design. Available: https://haughtondesign.co.uk/understanding-iomt-connected-devices/ [Accessed 12 August 2021].
HEILIG, M. L. 1962. Sensorama simulator. Google Patents.
HICKS, D. G. 2007. The Museum of HP Calculators.
HOFSTEDE, G. & MINKOV, M. 2013. VSM 2013. *Values survey module*.
HSU, C.-L. & LIN, J. C.-C. 2018. Exploring Factors Affecting the Adoption of Internet of Things Services. *Journal of Computer Information Systems,* 58**,** 49-57.
HUANG, D.-L., RAU, P.-L. & SALVENDY, G. 2007. *A Survey of Factors Influencing People's Perception of Information Security*.

ISLAM, S. M. R., KWAK, D., KABIR, M. H., HOSSAIN, M. & KWAK, K. 2015. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access,* 3**,** 678-708.
IUSTINA-CRISTINA, C.-M. & GHEORGHE, M. 2019. Patients' attitudes toward the use of IoT medical devices: empirical evidence from Romania. *Proceedings of the International Conference on Business Excellence,* 13**,** 567-577.
KAEWKANNATE, K. & KIM, S. 2016. A comparison of wearable fitness devices. *BMC Public Health,* 16**,** 433.
KANG, H. 2013. The prevention and handling of the missing data. *Korean journal of anesthesiology,* 64**,** 402-406.
KAO, Y.-S., NAWATA, K. & HUANG, C.-Y. 2019. An Exploration and Confirmation of the Factors Influencing Adoption of IoT-Based Wearable Fitness Trackers. *International journal of environmental research and public health,* 16**,** 3227.
KELFVE, S., KIVI, M., JOHANSSON, B. & LINDWALL, M. 2020. Going web or staying paper? The use of web-surveys among older people. *BMC Medical Research Methodology,* 20**,** 252.
KHAN, R., KHAN, S. U., ZAHEER, R. & KHAN, S. 2012. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. *2012 10th International Conference on Frontiers of Information Technology***,** 257-260.
KHAN, W., AALSALEM, M. Y., KHAN, M. K. & ARSHAD, Q. Enabling Consumer Trust Upon Acceptance of IoT Technologies Through Security and Privacy Model. 2016.
KIM, J.-H. 2007. A study on the characteristics of modern fashion design for digital nomadic culture. *Fashion & Textile Research Journal,* 9**,** 6-14.
KIM, Y., PARK, Y. & CHOI, J. 2017. A study on the adoption of IoT smart home service: using Value-based Adoption Model. *Total Quality Management & Business Excellence,* 28**,** 1149-1165.
KNIGHT, D. 2016. *A history of palm part 2: Palm PDAs phones 1996 to 2003* [Online]. Available: https://lowendmac.com/2016/a-history-of-palm-part-2-palm-pdas-and-phones-1996-to-2003/ [Accessed December 2021].
KØIEN, G. 2011. Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet-of-Things Context. *Wireless Personal Communications - WIREL PERS COMMUN,* 61.
KOWATSCH, T. & MAASS, W. Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts. MCIS, 2012.
KURLAND, E. 2017. History of VR. *Virtual Reality Filmmaking.* Routledge.
LAI, I. K. W., TONG, V. W. L. & LAI, D. C. F. 2011. Trust factors influencing the adoption of internet-based interorganizational systems. *Electronic Commerce Research and Applications,* 10**,** 85-93.
LALLMAHOMOOD, M. 2007. An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce,* 12**,** 1-26.
LAMMING, M. & FLYNN, M. Forget-me-not: Intimate computing in support of human memory. Proc. FRIEND21, 1994 Int. Symp. on Next Generation Human Interface, 1994. Citeseer.
LEE, J., KIM, D., RYOO, H.-Y. & SHIN, B.-S. 2016. Sustainable Wearables: Wearable Technology for Enhancing the Quality of Human Life. *Sustainability,* 8**,** 466.

LEE, M. & TURBAN, E. 2001. A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce /Fall,* 6**,** 75-91.
LEER, S. D. 1989. Walkie talkie. Google Patents.
LEUENBERGER, C.-E. 2002. Wristwatch. Google Patents.
LI, H. & PAN, T. 2017. Development of Physiological Parameters Monitoring System using the Internet of Things. *International Journal of Online Engineering (iJOE),* 13**,** 87.
LI, H., WU, J., GAO, Y. & SHI, Y. 2016. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics,* 88**,** 8-17.
LIN, Z. & DONG, L. 2018. Clarifying Trust in Social Internet of Things. *IEEE Transactions on Knowledge and Data Engineering,* 30**,** 234-248.
LOVETT, L. 2018. Prompt monitoring with wearable ECG patch more frequently detects undiagnosed a-fib. MobiHealthNews HIMSS Media.
MAJUMDER, S., MONDAL, T. & DEEN, M. J. 2017. Wearable Sensors for Remote Health Monitoring. *Sensors (Basel, Switzerland),* 17**,** 130.
MANN, S., FUNG, J., AIMONE, C., SEHGAL, A. & CHEN, D. 2005. Designing EyeTap digital eyeglasses for continuous lifelong capture and sharing of personal experiences. Alt. Chi, Proc. CHI.
MARSHALL, G. 2013. Before iWatch: the timely history of the smartwatch. *TechRadar***,** 3-10.
MARSHALL, G. 2018. The story of Fitbit: How a wooden box became a $4 billion company.
MAYER, R. C., DAVIS, J. H. & SCHOORMAN, F. D. 1995. An Integrative Model of Organizational Trust. *The Academy of Management Review,* 20**,** 709-734.
MCCANN, J., BRYSON, D., MALMIVAARA, M., HURFORD, R., SAIFEE, F., RCA, L., KANE, D., MARTIN, A., LAM, P., MIN, G., MORSKY, S., DONG, X., AGNUSDEI, I., TAYLOR, A., TREADAWAY, D., TIMMINS, M., UNDERWOOD, S., BIRRINGER, J., DANJOUX, M. & STAHL, W. 2009. *Smart Clothes and Wearable Technology*.
MCKNIGHT, D., CARTER, M., THATCHER, J. & CLAY, P. 2011a. Trust in a specific technology: An Investigation of its Components and Measures. *ACM Transactions on Management Information Systems,* 2**,** 12-32.
MCKNIGHT, D. H., CARTER, M., THATCHER, J. B. & CLAY, P. F. 2011b. Trust in a specific technology: An investigation of its components and measures. *ACM Trans. Manage. Inf. Syst.,* 2**,** Article 12.
MICROCHIP. 2020. *Intelligence and the Internet of Medical Things (IoMT)* [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/00003668.pdf [Accessed August 31 2021].
MITTELSTADT, B. 2017. Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology,* 19**,** 157-175.
MIZUNO, A., CHANGOLKAR, S. & PATEL, M. S. 2021. Wearable Devices to Monitor and Reduce the Risk of Cardiovascular Disease: Evidence and Opportunities. *Annual Review of Medicine,* 72**,** 459-471.
MOLTENI, M. 2018. *Ingestible Sensors Electronically Monitor Your Guts* [Online]. Available: https://www.wired.com/story/this-digital-pill-prototype-uses-bacteria-to-sense-stomach-bleeding/ [Accessed 16 August 2021].

MYRE, G. 2017. *From Wristwatches To Radio, How World War I Ushered in the Modern World* [Online]. Available: https://www.npr.org/sections/parallels/2017/04/02/521792062/from-wristwatches-to-radio-how-world-war-i-ushered-in-the-modern-world?t=1568188507348 [Accessed December 12 2021].

NANAYAKKARA, N., HALGAMUGE, M. & SYED, A. 2019. *Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review*.

NGUYEN, M. 2016. The most successful wearable for consumers.

NIELSEN, J. 1993. *Usability Engineering*, Morgan Kaufmann Publishers Inc.

OMETOV, A., SHUBINA, V., KLUS, L., SKIBIŃSKA, J., SAAFI, S., PASCACIO, P., FLUERATORU, L., GAIBOR, D. Q., CHUKHNO, N., CHUKHNO, O., ALI, A., CHANNA, A., SVERTOKA, E., QAIM, W. B., CASANOVA-MARQUÉS, R., HOLCER, S., TORRES-SOSPEDRA, J., CASTELEYN, S., RUGGERI, G., ARANITI, G., BURGET, R., HOSEK, J. & LOHAN, E. S. 2021. A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges. *Computer Networks,* 193**,** 108074.

ORNES, S. 2016. Core Concept: The Internet of Things and the explosion of interconnectivity. *Proceedings of the National Academy of Sciences,* 113**,** 11059.

PARK, K., PARK, J. & LEE, J. 2017. An IoT System for Remote Monitoring of Patients at Home. *Applied Sciences,* 7**,** 260.

PARK, S. & JAYARAMAN, S. 2003. Enhancing the quality of life through wearable technology. *IEEE Eng Med Biol Mag,* 22**,** 41-8.

PARK, S. & JAYARAMAN, S. 2017. The wearables revolution and Big Data: the textile lineage. *The Journal of The Textile Institute,* 108**,** 605-614.

PATERAKI, M., FYSARAKIS, K., SAKKALIS, V., SPANOUDAKIS, G., VARLAMIS, I., MANIADAKIS, M., LOURAKIS, M., IOANNIDIS, S., CUMMINS, N., SCHULLER, B., LOUTSETIS, E. & KOUTSOURIS, D. 2020. Chapter 2 - Biosensors and Internet of Things in smart healthcare applications: challenges and opportunities. *In:* DEY, N., ASHOUR, A. S., JAMES FONG, S. & BHATT, C. (eds.) *Wearable and Implantable Medical Devices.* Academic Press.

PELTOLA, O. 2017. Introduction to Wearable Healthcare Technology.

POPAT, K. A. & SHARMA, P. 2013. Wearable computer applications a future perspective. *International Journal of Engineering and Innovative Technology,* 3**,** 213-217.

PRATAP SINGH, R., JAVAID, M., HALEEM, A., VAISHYA, R. & ALI, S. 2020. Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications. *Journal of Clinical Orthopaedics and Trauma,* 11**,** 713-717.

PRAYOGA, T. & ABRAHAM, J. 2016. Behavioral Intention to Use IoT Health Device: The Role of Perceived Usefulness, Facilitated Appropriation, Big Five Personality Traits, and Cultural Value Orientations. *International Journal of Electrical and Computer Engineering,* 6**,** 1751-1765.

PUTTA, S. R., ABUHUSSEIN, A., ALSUBAEI, F., SHIVA, S. & ATIEWI, S. 2020. Security Benchmarks for Wearable Medical Things: Stakeholders-Centric Approach.

RATHORE, M. M., AHMAD, A., PAUL, A., WAN, J. & ZHANG, D. 2016. Real-time Medical Emergency Response System: Exploiting IoT and Big Data for Public Health. *J Med Syst,* 40**,** 283.

RAZDAN, S. & SHARMA, S. 2021. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Technical Review*.
REAR, J. 2021. *The best fitness trackers and watches to help you reach your health goals.* [Online]. The Telegraph. Available: https://www.telegraph.co.uk/recommended/leisure/best-fitness-trackers-watches. [Accessed 12 August 2021].
RHODES, B. 1997. A brief history of wearable computing. *MIT Wearable Computing Project*.
ROMAN, F. 1993. The invention of spectacles. *The British journal of ophthalmology,* 77**,** 568.
S RUBÍ, J. N. & L GONDIM, P. R. 2019. IoMT Platform for Pervasive Healthcare Data Aggregation, Processing, and Sharing Based on OneM2M and OpenEHR. *Sensors (Basel, Switzerland),* 19**,** 4283.
SASAKI, K. 1982. Wristwatch. Google Patents.
SHARMA, N., SHAMKUWAR, M. & SINGH, I. 2019. The History, Present and Future with IoT. *In:* BALAS, V. E., SOLANKI, V. K., KUMAR, R. & KHARI, M. (eds.) *Internet of Things and Big Data Analytics for Smart Generation.* Cham: Springer International Publishing.
SHIN, D. & HWANG, Y. 2017. Integrated acceptance and sustainability evaluation of Internet of Medical Things. *Internet Research,* 27**,** 1227-1254.
SICARI, S., RIZZARDI, A., GRIECO, L. & COEN-PORISINI, A. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks,* 76.
SLIGHT, S. P. & BATES, D. W. 2014. A risk-based regulatory framework for health IT: recommendations of the FDASIA working group. *Journal of the American Medical Informatics Association,* 21**,** e181-e184.
SMITH, C. & MIESSLER, D. 2014. Internet of Things: HP Security Research Study. HP Fortify
SMITH, G. Does Gender Influence Online Survey Participation? A Record-Linkage Analysis of University Faculty Online Survey Response Behavior. 2008.
STAMP, J. 2013. A partial history of headphones. *Retrieved from*.
STEGER, A. 2020. *How the Internet of Medical Things Is Impacting Healthcare.* [Online]. Technology Solutions That Drive Healthcare. Available: https://healthtechmagazine.net/article/2020/01/how-internet-medical-things-impacting-healthcare-perfcon. [Accessed 12 August 2021].
SURESH, V., RAMSON, J. & JEGAN, D. 2020. *Internet of Medical Things (IoMT) - An overview*.
TAMS, S., THATCHER, J. B. & CRAIG, K. 2018. How and why trust matters in post-adoptive usage: The mediating roles of internal and external self-efficacy. *The Journal of Strategic Information Systems,* 27**,** 170-190.
THORP, E. O. 1966. *Beat the Dealer: a winning strategy for the game of twenty one*, Vintage.
THORP, E. O. The invention of the first wearable computer. Digest of Papers. Second international symposium on wearable computers (Cat. No. 98EX215), 1998. IEEE, 4-8.
TICKNOR, B. 2018. *Virtual Reality and the Criminal Justice System: Exploring the Possibilities for Correctional Rehabilitation*, Lexington Books.
UNIQUEWATCH. 2015. *Calculator watches* [Online]. Available: http://www.uniquewatchguide.com/calculator-watches.html [Accessed December 2021].
WANT, R., HOPPER, A., FALCAO, V. & GIBBONS, J. 1992. The active badge location system. *ACM Transactions on Information Systems (TOIS),* 10**,** 91-102.

WEISER, M. 1999. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.,* 3**,** 3–11.

WILKINSON, J. 2013. Animalizing the apparatus: Pigeons, drones and the aerial view. *Shift,* 6**,** 1-21.

WILLIAMS, P. A. & WOODWARD, A. J. 2015. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.),* 8**,** 305-316.

XU, H., TEO, H.-H., TAN, B. C. Y. & AGARWAL, R. 2009. The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems,* 26**,** 135-174.

YAN, Z., ZHANG, P. & VASILAKOS, A. 2014. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.,* 42**,** 120-134.

YANG, Z., ZHOU, Q., LEI, L., ZHENG, K. & XIANG, W. 2016. An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. *Journal of Medical Systems,* 40**,** 286.

YILDIRIM, H. & ALI-ELDIN, A. M. T. 2019. A model for predicting user intention to use wearable IoT devices at the workplace. *Journal of King Saud University - Computer and Information Sciences,* 31**,** 497-505.

YUAN, S., FERNANDO, A. & KLONOFF, D. C. 2018. Standards for Medical Device Cybersecurity in 2018. *Journal of diabetes science and technology,* 12**,** 743-746.

ZHANG, M., LUO, M., NIE, R. & ZHANG, Y. 2017. Technical attributes, health attribute, consumer attributes and their roles in adoption intention of healthcare wearable technology. *Int J Med Inform,* 108**,** 97-109.

ZOLFAGHARIFARD, E. 2014. Is this the first wearable computer? 300-year-old Chinese abacus ring was used during the Qing Dynasty to help traders. *Daily Mail*.

Appendix 1: SPSS Results

Demographics

1. Above 18 years old

I am above 18 years old.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	189	100.0	100.0	100.0

2. Age

What is your age group?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 24	70	37.0	37.0	37.0
	25 - 34	81	42.9	42.9	79.9
	35 - 44	18	9.5	9.5	89.4
	45 - 54	13	6.9	6.9	96.3
	Above 55	7	3.7	3.7	100.0
	Total	189	100.0	100.0	

3. Gender

What is your gender?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	88	46.6	46.6	46.6
	Female	101	53.4	53.4	100.0

	Total	189	100.0	100.0	

4. Level of tech prof

What is your level of technical proficiency in the use of computers?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Far above average	26	13.8	13.8	13.8
	Somewhat above average	85	45.0	45.0	58.7
	Average	76	40.2	40.2	98.9
	Somewhat below average	2	1.1	1.1	100.0
	Total	189	100.0	100.0	

5. Technology significance

Technology has become an integral part of our everyday lives. Technology now has a significant impact on how we live in the world today and how we interact with everything around us.

Do you agree that technology has great significance in your current life?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Definitely Yes	167	88.4	88.4	88.4
	Probably Yes	21	11.1	11.1	99.5
	Might or might not	1	.5	.5	100.0
	Total	189	100.0	100.0	

6. Familiarity

I am familiar with Wearable Internet of Medical Things devices.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	124	65.6	65.6	65.6
	No	65	34.4	34.4	100.0
	Total	189	100.0	100.0	

7. Use of devices

I use Wearable Internet of Medical Things devices.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	77	40.7	62.1	62.1
	No	47	24.9	37.9	100.0
	Total	124	65.6	100.0	
Missing	System	65	34.4		
Total		189	100.0		

8. Aware

I am aware of any of the following Wearable Internet of Medical Things devices.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Wearable Fitness Trackers	45	23.8	58.4	58.4
	Wearable ECG Monitors	6	3.2	7.8	66.2
	Wearable Blood Pressure Monitors	13	6.9	16.9	83.1
	Smart Patches	4	2.1	5.2	88.3
	None	9	4.8	11.7	100.0
	Total	77	40.7	100.0	
Missing	System	112	59.3		
Total		189	100.0		

Reliability and Validity

PU

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.911	.913	9

PEU

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.892	.894	6

FR

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.853	.853	2

PSP

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.917	.918	26

IU

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.866	.867	4

Product-related factors

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.929	.934	17

Correlation

Correlations

	Perceived Security and Privacy	Perceived Ease of Use	24 Wearable Internet of Medical Things helps to monitor health metrics for both personal uses and for sharing with healthcare providers. For example, BPM Connect can warn users about irregular heart rates as an early warning signs of serious health condit	25 Wearable Internet of Medical Things like Vital Patch which records user's physiological data such as heart rate and respiratory rates needs to be accurate without any error. I am willing to trust Wearable Internet of Medical Things devices without the	Perceived Usefulness	Behavioural Intention to Use

Perceived Security and Privacy	Pearson Correlation	1	.645**	.473**	.531**	.540**	.686**
	Sig. (2-tailed)		.000	.000	.000	.000	.000
	N	189	189	189	189	189	189
Perceived Ease of Use	Pearson Correlation	.645**	1	.400**	.439**	.694**	.631**
	Sig. (2-tailed)	.000		.000	.000	.000	.000
	N	189	189	189	189	189	189
24 Wearable Internet of Medical Things helps to monitor health metrics for both personal uses and for sharing with healthcare providers. For example, BPM Connect can warn users about irregular heart rates as an early warning signs of serious health condit	Pearson Correlation	.473**	.400**	1	.744**	.385**	.371**
	Sig. (2-tailed)	.000	.000		.000	.000	.000
	N	189	189	189	189	189	189

25 Wearable Internet of Medical Things like Vital Patch which records user's physiological data such as heart rate and respiratory rates needs to be accurate without any error. I am willing to trust Wearable Internet of Medical Things devices without the	Pearson Correlation	.531**	.439**	.744**	1	.467**	.364**
	Sig. (2-tailed)	.000	.000	.000		.000	.000
	N	189	189	189	189	189	189
Perceived Usefulness	Pearson Correlation	.540**	.694**	.385**	.467**	1	.565**
	Sig. (2-tailed)	.000	.000	.000	.000		.000
	N	189	189	189	189	189	189
Behavioural Intention to Use	Pearson Correlation	.686**	.631**	.371**	.364**	.565**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	
	N	189	189	189	189	189	189

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 2: Questionnaire

Project Title:

Understanding Security Risks and Users Perception Towards Adopting the Internet of Medical Things: Wearable IoMT

Project Briefing

Internet of Medical Things (IoMT) is a new term which is also referred as IoT in healthcare sector which is collections of medical devices connected to monitor and track individual's health. Some of the examples of IoMT are remote patient monitoring system, wearable medical devices, surgical robot arm, biosensors and ingestible sensors and many more.

Wearable IoMT (WIoMT) is part of the IoMT devices that are used for monitoring consumers health for blood pressure, sugar level, heart rate and ECG. Fitbit sense and Fitbit Versa 3 are an example of Wearable Internet of Medical Things which have advanced features for monitoring ECG to detect abnormal heart rate as well as oxygen level in blood. It will provide early warnings of serious health condition to the users. BPM Connect is another example of Wearable Internet of Medical Things that provides medically accurate measurement of your systolic and diastolic blood pressure as well as heart rate. Users can connect their device through WIFI or Bluetooth to connect with the vendor's health app through smartphones and can easily share blood pressure results with their doctors. Also, Vital Patch is an emerging wearable biosensor to monitor user's physiological data such as heart rate, electrocardiography (ECG), heartrate variability, respiratory rate and skin temperature, which can be transmitted wirelessly via the VitalConnect platform. Sensors collect data and store in the platform and have ability to notify healthcare professionals. Such devices are used by healthcare professionals and general users as an aid to diagnose ailments.

Due to this advancement, there is a significant need to understand users' perception regarding trust and security risks to adopt Wearable Internet of Medical Things devices. The purpose of this research is to understand existing Wearable Internet of Medical Things challenges, followed by exploring how user's perception contributes to the adoption of Wearable Internet of Medical Things.

The expected outcome from this research aims to identify how users' security and perception matters while adopting Wearable Internet of Medical Things, which in future can benefit security professionals to examine trust factors when implementing new and advanced Wearable Internet of Medical Things devices. The expected result is to help consumers as well as different healthcare industry to create a device which can be easily adopted and used securely by consumers.

- The demographics survey is an adapted version of the VSM International Questionnaire (2013) by Hofstede, G.

○ Survey questions are modified and adapted from "**Improving IoT Technology Adoption through Improving Consumer Trust"** by AlHogail, A. (2018).		
Question Type	**Questions**	**Answer options**
Demographic questions	Q1. I am above 18 years old	○ Yes ○ No (Exit Survey)
	Q2. Age Group	○ 18 - 24 ○ 25 - 34 ○ 35 - 44 ○ 45 - 54 ○ Above 55
	Q3. Gender	○ Male ○ Female ○ Non-binary / third gender ○ Prefer not to say
	Q4. What is your level of technical proficiency in the use of computers?	○ Far above average ○ Somewhat above average ○ Average ○ Somewhat below average ○ Far below average
	Q5. Technology has become an integral part of our everyday lives. Technology now has a significant impact on how we live in the world today and how we interact with everything around us. Do you agree that technology has great significance in your current life?	○ Definitely Yes ○ Probably Yes ○ Might or might not ○ Probably not ○ Definitely not
	Q6. I am familiar with Wearable Internet of Medical Things devices.	○ Yes (move to Q7) ○ No (automatically moved to Q 9)

	Q7. I use Wearable Internet of Medical Things devices?	o Yes (move to Q8) o No (automatically moved to Q9)
	Q8. I am aware of any of the following Wearable Internet of Medical Things devices.	o Wearable Fitness Trackers o Wearable ECG Monitors o Wearable Blood Pressure Monitors o Biosensors o Smart Patches o Ingestible sensors o None
Functionality and Reliability	Q29. Wearable Internet of Medical Things helps to monitor health metrics for both personal uses and for sharing with healthcare providers. For example, BPM Connect can warn users about irregular heart rates as an early warning signs of serious health conditions. I am willing to trust Wearable Internet of Medical Things devices without the knowledge of their functionality.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q30. Wearable Internet of Medical Things like Vital Patch which records user's physiological data such as heart rate and respiratory rates needs to be accurate without any error. I am willing to trust Wearable Internet of Medical Things devices	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	without the knowledge of their reliability.	
Perceived Usefulness	Q9. Wearable Internet of Medical Things could be useful in maintaining health.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q10. Using Wearable Internet of Medical Things could help me to keep track of my health.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q11. Using Wearable Internet of Medical Things could help to improve my health.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q12. Using Wearable Internet of Medical Things could help me to diagnose new or existing ailment.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q13. Using Wearable Internet of Medical Things could assist me in avoiding health risks.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q14. Using Wearable Internet of Medical Things could reduce time and effort required to monitor my health.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	Q15. Using Wearable Internet of Medical Things could help to improve my quality of life.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q16. I could use Wearable Internet of Medical Things to reduce clinical and hospital visits.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q17. Using Wearable Internet of Medical Things could ease healthcare professional's ability to monitor individual's health.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
Perceived Ease of Use	Q18. Learning to use Wearable Internet of Medical Things could be easy for me.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q19. I would find it easy to get Wearable Internet of Medical Things to function the way I want.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q20. My interaction with Wearable Internet of Medical Things would be clear and understandable.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q21. I would find Wearable Internet of Medical Things to be flexible to interact with.	o Definitely Yes o Probably Yes o Might or might not o Probably not

		o Definitely not
	Q22. It could be easy for me to become proficient at using Wearable Internet of Medical Things.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q23. Using Wearable Internet of Medical Things would not require a lot of mental/physical efforts.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
Perceived Security & Privacy	Q24. Using Wearable Internet of Medical Things devices would be secure.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q25. I would trust the ability of Wearable Internet of Medical Things devices to protect my privacy.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q26. As more consumers purchase wearable tech, they unknowingly expose themselves to potential security breaches. Some security breaches could include password hacking, malware attack using	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	phishing email and exploiting system vulnerabilities. Sharing personal information is associated with risks of getting leaked or compromised due to either human error or product-related issues. Matters on security would not influence my usage of Wearable Internet of Medical Things.	
	Q27. I am aware of security flaws associated with Wearable Internet of Medical Things application and services.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q28. I am aware of privacy issues with Wearable Internet of Medical Things application and services.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q31. I would still use Wearable Internet of Medical Things devices even if I am aware of any reputation of the devices being hacked.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q32. I am willing to trust manufacturers and vendors who provide Wearable Internet of Medical Things devices and services.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	Q33. In Wearable Internet of Medical Things, your data is shared with healthcare professionals. This data is collected and retrieved through the device, transmitted via network and stored in servers. Besides health and medical data, Wearable Internet of Medical Things also collects biometric data such as heart rate from human body which is valuable information to the health sector. Location of user monitored by Wearable Internet of Medical Things devices can also be considered as sensitive data. I would feel safe to share my personal information while using Wearable Internet of Medical Things devices.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q34. Wearable Internet of Medical Things such as BPM Connect and Vital Patch has access to sensitive data such as, heart rates, the user's position, locations and other health metrics. As we work to consolidate more and more personalised information, it is becoming increasingly difficult and important to ensure that the data in such wearable	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	devices remain safe and free from unauthorised access. I feel assured when using Wearable Internet of Medical Things devices despite the possibility of unauthorised access.	
	Q35. Data sharing with third parties should be restricted, and data collected should be secured against unauthorized access. The data can also be exchanged without disclosing the individual's real identity. Data can be only used, shared, transmitted to a third party only if formal consent is obtained from the user. If I have control over my personal information, I can trust Wearable Internet of Medical Things devices.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q36. If I believe that any Wearable Internet of Medical Things devices might compromise my privacy or access to my personally identifiable information, I will no longer use the devices.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q37. I am aware of the potential vulnerabilities and risks associated to my sensitive data being accessed by a third party or external entity when using	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	Wearable Internet of Medical Things devices.	
	Q38. It would be reasonable for me to take risks regarding my sensitive data for Wearable Internet of Medical Things devices that are trustworthy.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q39. When using Wearable Internet of Medical Things devices, I feel that privacy controls and policies related to personal data access and sharing must be clear and convenient.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q40. Cybercriminals can target devices that usually have less security protection. For example, MyFitness Pal was hacked in 2018, exposing the data of up to 150 million users and subsequently sold on the dark web. I would accept full liability in the event of my Wearable Internet of Medical Things device being compromised by hackers or cybercriminals.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	Q41. I think Wearable Internet of Medical Things vendor/manufacturers should accept full liability in the event of any security or privacy breach, or the devices being compromised.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q42. Wearable Internet of Medical Things Vendors/manufacturers should provide information about authentication and security measures and how and where Wearable Internet of Medical Things devices data is stored.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q43. I think Wearable Internet of Medical Things vendors/manufacturers should avoid using third party or external entity for storing and managing data.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q44. There should be a strong authentication method when my data is being shared through Wearable Internet of Medical Things devices.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q45. Privacy policies should be mandated for all Wearable Internet of Medical Things vendors.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not

	Q46. Indicate your level of agreement on the security risk of "unauthorised access to data" impact on Wearable Internet of Medical Things.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q47. Indicate your level of agreement on the security risk of "malware infections and vulnerabilities" impact on Wearable Internet of Medical Things.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q48. Indicate your level of agreement on the security risk relating to "lack of regulation and compliance" impact on Wearable Internet of Medical Things.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q49. Indicate your level of agreement on the security risk of "unsecured network connectivity" impact on Wearable Internet of Medical Things.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q50. Indicate your level of agreement on the security risk of "lack of encryption" impact on Wearable Internet of Medical Things.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
	Q51. Indicate your level of agreement on the security risk of "lack of patching and device updates" impact on Wearable Internet of Medical Things.	o Definitely Yes o Probably Yes o Might or might not o Probably not o Definitely not
Behavioral Intention to use	Q52. I intend to use Wearable Internet of Medical Things devices for assessing or managing my health.	o Definitely Yes o Probably Yes o Might or might not o Probably not

		○ Definitely not
	Q53. I would strongly recommend others to use Wearable Internet of Medical Things devices.	○ Definitely Yes ○ Probably Yes ○ Might or might not ○ Probably not ○ Definitely not
	Q54. If Wearable Internet of Medical Things devices are safe and secure, I intend to use them more frequently.	○ Definitely Yes ○ Probably Yes ○ Might or might not ○ Probably not ○ Definitely not
	Q55. If vendors/manufacturers could manage to keep my personal information protected, my interest to use Wearable Internet of Medical Things devices would be greater.	○ Definitely Yes ○ Probably Yes ○ Might or might not ○ Probably not ○ Definitely not

Appendix 3: Ethical Approval

24 August 2021
Doctor Abubakar Bello School of Social Sciences

Dear Abubakar,

HREC Approval Number H14191 Risk Rating Low

HUMAN RESEARCH ETHICS COMMITTEE

Project Title: "Understanding Security Risks and Users Perception Towards Adopting Internet of Medical Things: Robotic IoMT"

I am pleased to advise the above research project meets the requirements of the National Statement on Ethical Conduct in Human Research 2007 (Updated 2018).

Ethical approval for this project has been granted by the Western Sydney University Human Research Ethics Committee. This HREC is constituted and operates in accordance with the National Statement on Ethical Conduct in Human Research 2007 (Updated 2018).

Approval of this project is valid from 24 August 2021 until 24 August 2022. This protocol covers the following researchers

Abubakar Bello, Sanjit Thapa, Alana Maurushat Summary of Conditions of Approval

1. A progress report will be due annually on the anniversary of the approval date. 2. A final report will be due at the expiration of the approval period.

3. Any amendments to the project must be approved by the Human Research Ethics Committee prior to being implemented. Amendments must be requested using the HREC Amendment Request Form.

4. Any serious or unexpected adverse events on participants must be reported to the Human Research Ethics Committee via the Human Ethics Officer as a matter of priority.

5. Any unforeseen events that might affect continued ethical acceptability of the project should also be reported to the Committee as a matter of priority.

6. Consent forms are to be retained within the archives of the School or Research Institute and made available to the Committee upon request.

7. Approval is only valid while you hold a position or are enrolled at Western Sydney University. You will need to transfer your project or seek fresh ethics approval from your new institution if you leave Western Sydney University.

8. Project specific conditions

There are no specific conditions applicable.

Please quote the registration number and title as indicated above in the subject line on all future correspondence related to this project. All correspondence should be sent to humanethics@westernsydney.edu.au as this email address is closely monitored.

Yours sincerely

Associate Professor Gabrielle Weidemann

Presiding Member,
Western Sydney University Human Research Ethics Committee

[redacted]

Western Sydney University
ABN 53 014 069 881 CRICOS Provider No. 00917K
Locked Bag 1797 Penrith NSW 2751 Australia
westernsydney.edu.au

WESTERN SYDNEY
UNIVERSITY

Western Sydney University
ABN 53 014 069 881 CRICOS Provider No. 00917K
Locked Bag 1797 Penrith NSW 2751 Australia
westernsydney.edu.au

Appendix 4: Others

Participant Information Sheet

Project Title: Understanding Security Risks and Users Perception Towards Adopting the Internet of Medical Things: *Wearable Internet of Medical Things (WIoMT)*

Project Summary:
You are invited to participate in a research study being conducted by Sanjit Jung Thapa, Master by research student from Western Sydney University *under the Supervision of* Dr Abubakar Bello and Professor Alana Maurushat.
The research is based on understanding Security Risks and Users Perception Towards Adopting the Internet of Medical Things, particularly, Wearable Internet of Medical Things.

How is the study being paid for?
This study is funded and fully supported by Western Sydney University.

What will I be asked to do?
You will be asked to *complete an online survey.*

How much of my time will I need to give?
Approximately 20 minutes

What benefits will I, and/or the broader community, receive for participating?

Wearable Internet of Medical Things *usage from the users' perspective will contribute to various entities such as government, advertising agencies, manufacturers as well as healthcare providers. It will help consumers as well as different healthcare industry to create a device which can be easily adopted and used securely by consumers.*

Understanding the user's perception of trust in new technology will benefit users from new developments such as robotic and wearable medical devices. Accepting technology over traditional methods is very challenging, especially when technology is related to the health sector. Overcoming trust and safety issues in the adoption of new technologies will help manufacturers and the healthcare sector to create real consumer-oriented systems.

Will the study involve any risk or discomfort for me? If so, what will be done to rectify it?
No, this study will carry no risks above and beyond what you would expect from a survey task.
How do you intend to publish or disseminate the results?
It is anticipated that the results of this research project will be published and/or presented in a variety of forums. In any publication and/or presentation, the information will be provided in such

a way that the participant cannot be identified, except with your permission. Results may be published in reputable academic journals in the research discipline of Social Science.

Will the data and information that I have provided be disposed of?
Please be assured that only the researchers will have access to the raw data you provide. However, your data may be used in other related projects for an extended period of time. Besides, results after analysis of the non-identifiable data may be shared with other researchers or data repositories.

Can I withdraw from the study?
Participation is entirely voluntary and you are not obliged to be involved. If you do participate you can withdraw at any time without giving reason *(change this statement if it is not relevant).*
If you do choose to withdraw, any information that you have supplied may be used for research purposes unless otherwise notified by contacting Sanjit Jung Thapa (19881658@student.westernsydney.edu.au).

Can I tell other people about the study?
Yes, you can tell other people about the study.
What if I require further information?
Please contact Sanjit Jung Thapa, should you wish to discuss the research further before deciding whether or not to participate.
Main researcher: Sanjit Jung Thapa
Contact: 19881658@student.westernsydney.edu.au
Principal Supervisor: Dr Abubakar Bello
Contact: A.Bello@westernsydney.edu.au
Co-Supervisor: Alana Maurushat
Contact: a.maurushat@westernsydney.edu.au

What if I have a complaint?
If you have any complaints or reservations about the ethical conduct of this research, you may contact the Ethics Committee through Research Engagement, Development and Innovation (REDI) on Tel +61 2 4736 0229 or email humanethics@westernsydney.edu.au.
Any issues you raise will be treated in confidence and investigated fully, and you will be informed of the outcome.
If you agree to participate in this study, you may be asked to sign the Participant Consent Form. The information sheet is for you to keep and the consent form is retained by the researcher/s.
This study has been approved by the Western Sydney University Human Research Ethics Committee. The Approval number is **H14191**

Online Consent Statement

"**The project**
I understand that I am being asked to provide my data as part of the research project [Understanding Security Risks and Users Perception Towards Adopting the Internet of Medical Things: Wearable Internet of Medical Things].

I have read the information sheet and understand I can speak with a research team member if I have any questions.

I agree
I understand that I can withdraw from the research by not completing and submitting the survey.

I understand that if I do complete and submit the survey my data can't be withdrawn because the survey is anonymous.

Scope of consent

I understand that I am being asked to allow the data to be used for this project.

I consent for my data and information provided to be used in this project and other related projects for an extended period of time.

I understand that my involvement is confidential, and that the information gained during the study may be published and stored for other research use but no information about me will be used in any way that reveals my identity.

I understand that I can withdraw from the study at any time without affecting my relationship with the researcher/s, and any organisations involved, now or in the future.

Note: Following this statement there will be access to the survey questionnaire to those who have consented.