

An Analysis of IoMT Vital Signs Measurement Devices for Practical and Secure Remote Clinical Monitoring

Kerry Y. Fang¹^a, Quoc Lap Trieu¹^b, Heidi Bjerling¹^c, Steven Thomas²^d, Jim Basilakis¹^e,
and Jeewani Anupama Ginige¹^f

¹*School of Computer, Data and Mathematical Sciences, Western Sydney University, Sydney, Australia*

²*South Western Sydney Local Health District, Sydney, Australia*

Keywords: Vital Signs Measurement, Internet of Medical Things (IoMT), Remote Monitoring, Security, Interoperability.

Abstract: The increasing need to provide care outside of hospitals necessitates remote monitoring of basic vital signs of patients from places such as private homes and aged care facilities. While much exploratory research has been done on using Internet of Medical Things (IoMT) devices for remote monitoring, there is a requirement to examine the practicality associated with the mass use of affordable off-the-shelf devices in terms of usability, secure access to data, and integration into hospital-based information systems. This paper investigates various security aspects in nine vital signs sensor devices that can be purchased and used for homecare monitoring in Australia. Specifically, the security and privacy aspects of these devices and associated software, regulatory compliance, interoperability, and formats of the accessible data streams were investigated. It was found that the devices were not entirely secure, as personal health information could be accessed using appropriate tools. Only one vendor enabled encryption during data transmission and provided an API to access data. While the clinical use of these devices with integration into hospital systems for practical remote monitoring is not easily achievable, it is possible to use devices for day-to-day vital signs monitoring purposes in a home setting.


1 INTRODUCTION


With the continuous advancement in technologies such as the Internet of Medical Things (IoMT), cloud computing and sensor devices, the remote monitoring of health and well-being is becoming more common and convenient worldwide, especially in developed countries. In addition, integrating innovative technologies into smart homes and smart healthcare is positively changing how people live. However, security and privacy issues are still a major concern surrounding the adoption of IoMT devices in the health sector (Chacko & Hayajneh, 2018).


Threats of the network layer, support layer and application layer on IoT devices remain challenging when integrating IoMT devices (Pahlevanzadeh et al., 2021). Data tampering, eavesdropping, DoS (Denial-


of-Service) attack, unauthorised access, DDoS (Distributed Denial-of-Service) and sniffers are all examples of the three perception layer attacks (Leloglu, 2016). Furthermore, security risks increase with the growing number of IoMT devices connected to the Internet (Talwana & Hua, 2016).


This exploratory research aims to investigate regulatory compliance, interoperability, data format, security and privacy issues associated with a selected set of off-the-shelf Bluetooth-enabled vital signs sensor devices in the context of using the devices for homecare monitoring in Australia. The sensor devices investigated are designed for the remote measuring and monitoring of five vital signs measurements: body temperature, blood oxygen saturation, heart rate/electrocardiogram, blood pressure, and body weight. The selected devices ranged from low-cost to


^a <https://orcid.org/0000-0001-6989-4485>

^b <https://orcid.org/0000-0003-0678-374X>

^c <https://orcid.org/0000-0001-5925-3510>

^d <https://orcid.org/0000-0002-2416-0020>

^e <https://orcid.org/0000-0002-7440-1320>

^f <https://orcid.org/0000-0002-6695-6983>

expensive off-the-shelf products and included regulated and unregulated medical devices according to federal agencies such as the FDA (Food and Drug Administration of the USA) and TGA (Therapeutic Goods Administration in Australia). In addition, the mobile apps corresponding to these sensor devices were also investigated to ascertain the ease of setup, security and privacy of the patient data and measurement data stored and shared within the apps.

The security and privacy aspects of these sensor devices were inspected and compared using Node-RED¹ and ESP32² devices. Hence this paper aims to answer the following research question:

“In the Australian context, is it **practical** to use off-the-shelf vital signs measurement products for remote **clinical monitoring** of patients **securely**?”

There are several highlighted keywords in the above question that requires some contextual explanations as follows:

1. Practicality – practical usage of these off-the-shelf products has several aspects. Firstly, considering the potential mass use, these products should be affordable, user-friendly and easy to set up by an average consumer, including older adults. In addition, it should be possible to remotely integrate these devices to pull the data into clinical information management systems housed in the healthcare networks. In other words, the implementation should not depend on IT professionals visiting every household to set up. It should be doable by the average end-users with some guidance.
2. Clinical monitoring – In the clinical setting, it is imperative to use devices approved by regulatory authorities, such as TGA or FDA, to ensure that these devices comply with the standards expected in healthcare. When exploring the off-the-shelf vital sign measurement device market, it is unclear whether the available products are suitable for clinical use in this sense. Also, certain words used in marketing (e.g., FDA cleared vs approved) around regulatory compliance can be ambiguous and confusing for the average user.
3. Security – The ability to easily integrate devices into healthcare information systems essentially means sharing the data via Bluetooth/Wi-Fi and through the internet to locations beyond the patient's home setting. This can be a double-edged sword as it is likely that other motivated

yet uninvited parties (e.g., hackers) would also be interested in having access to such data when exposed through these technologies.

The major contribution of this paper is the evaluation of the possible security vulnerabilities of popular Bluetooth-enabled sensor devices used for vital sign measurements using third-party software (Node-RED¹) and instruments (ESP32²).

The remainder of this paper is organised as follows. First, the background section summarises the current research on security IoMT devices used in healthcare and followed by that, our methods in device selection and testing procedures are presented. The next section discusses the findings from four dimensions – usability and regulatory compliance; security and privacy at the end-user and mobile app level; data accessibility and integration; and sensor device data extraction, followed by a brief conclusion with an outline of possible future works.

2 BACKGROUND

Health care is moving beyond the hospital and into patients' homes with the aging population increase. This change is one of the main drivers behind the growth of innovative and smart healthcare IoMT devices. The word “smart” implies the combination of software, hardware, cloud, and sensor technologies to collect and share real-time health data, which can then be used to monitor health and aid decision-making (Papa et al., 2020). The IoMT environment supports this process through the creation and linkage of a network of smart devices, and it is estimated that the number of connected devices worldwide will reach 75 billion by the year 2025 (Nick, 2022). Smart healthcare is therefore considered an application of IoMT. The sensor technology used in smart healthcare is gradually being embedded into the daily lives of many people, especially the elderly and people with chronic diseases. Wearable sensors are devices patients can wear, and measurements can be transmitted to the smartphone via Bluetooth or Wi-Fi technology. It offers significant advantages to healthcare as it provides the ability for remote health monitoring, such as the monitoring of various vital signs.

The main challenges with IoMTs are security and privacy issues. Many of the existing IoMT devices in the market require connections from the sensor to a mobile app for displaying and storing results and

¹ <https://nodered.org/>

² <https://en.wikipedia.org/wiki/ESP32>

personal data. Bluetooth is one of the preferred ways of data communication, as it is economical and suitable for use in compact devices (Zubair et al., 2019). Bluetooth 4.0 is known as Bluetooth Low Energy (BLE), a low-energy variation widely used in IoMTs (Kandhare, 2019). However, when Bluetooth is used to connect and transfer results to an app, it can act as an attack surface, that may potentially compromise the integrity, availability and confidentiality of the transmitted clinical data. In addition, although people's health data privacy awareness is increasing, many still need to secure their smartphones (Grindrod et al., 2017). This can be an issue when the smartphone is lost or taken by others without consent, and all the valuable personal app data and phone data are at risk of malicious attack.

Some existing research looked at the security and privacy concerns of home monitoring technologies such as medical sensor devices. Gerke and colleagues (2020) discussed the security and privacy issue of home monitoring technologies during the COVID-19 pandemic. Another study conducted by Sivaraman and colleagues (2017) looked at the security and privacy threats for smart home IoMT devices, including smart switches, smart cameras, Amazon Echo, and smart light bulbs. Within the study, 20 IoMT devices were tested in total using data capturing and mock server techniques. The result showed that most devices were vulnerable to some malicious attack. The authors also provided some recommendations to manage these potential risks, which range from user education to regulation and legislation (Sivaraman et al., 2017). Another study looked at the significant security and privacy features of health tracker devices, including Fitbit, Jawbone and Google Glass, by investigating the devices' strength, communication methods, and Bluetooth pairing processes (Zhang et al., 2020).

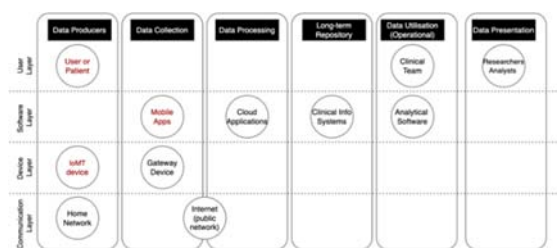


Figure 1: Points of security vulnerabilities adapted from Kim et al (2020).

Kim et al. (2020) present a model for security evaluation in telemedicine, in which they identify areas where telemedicine security could be

vulnerable to attacks. Based on Kim et al.'s (2020) Figure 1 summarises the areas of concern according to the architectural elements (in rounded rectangular boxes) and various layers – user, software, device and communication (separated by dotted lines).

However, none of the existing research utilised technologies and tools for data access to physically check/test the security and privacy of medical vital signs measurement devices and applications. In this paper, the security concerns related to end-user or patient, IoMT devices and Mobile Apps points of view (highlighted in red fonts in Figure 1) are discussed with respect to vital sign measurement devices used in homecare implementations. As previous examples show, most existing research discussed the overall security and privacy of health devices or sensors for general wellbeing and fitness, e.g., Fitbit or smart watches, thus not specific to vital medical signs measurement devices for clinical use. Moreover, most existing research focuses on health sensors and devices for managing certain health conditions or is limited to certain health devices or applications. For example, Hendricks-Sturup (2022) investigated the privacy of multiple pulse oximeter apps during the COVID-19 pandemic. Another study by Knorr and colleagues (2015) used a novel method that studied the files stored in the APK package of various Blood pressure and diabetes apps, the dynamic behaviour of the app and the app's privacy policy. Lastly, as far as the authors are aware, existing research could not be found on the security and privacy of vital medical signs measurement devices from both the device and mobile application (app) dimensions. The security and privacy aspects of the sensor devices and the related mobile applications can be especially crucial to the users, as both can be used to collect, store, and transfer sensitive personal health-related data. This means either one can become vulnerable to malicious attacks or privacy leaks, ultimately leading to patient risks. Therefore, our research aims to fill these gaps by utilising hardware and software solutions for examining more closely the processes and data involved in sensor information exchange, with tools such as Node-red and ESP32. These technologies allow us to analyse and compare the security and privacy aspects of existing medical vital signs measurement devices and their corresponding mobile applications.

3 METHODS

This study mainly consisted of four steps:

- (A) Vital signs measurement device selection;

- (B) Privacy policy inspection of the corresponding mobile applications;
- (C) Regulatory compliance investigation of the selected devices;
- (D) Checking the accessibility to low-level sensor data via Node-red and ESP32.

A total of nine (9) Bluetooth-enabled vital signs measurement devices were selected and tested; these consisted of three (3) oximeters, two (2) digital thermometers, two (2) blood pressure monitors, two (2) portable ECG/EKGs, and two (2) digital weight scales.

Table 1: Device list.

Vital sign measured	Device name	Local / International Company	Compliance Clearance Status	Online Retail Price in AUD (as of early 2022) excluding shipping costs
Temperature	Kinsa Smart Ear Thermometer	International	FDA-cleared	\$43.00
Blood pressure	iHealth Blood Pressure Monitor	Australian	TGA-approved	\$179.00
Blood pressure	Wellue Blood Pressure Monitor	International	FDA-cleared	\$65.00
ECG/EKG	SonoHealth EKG	International	FDA-cleared	\$159.00
ECG/EKG	AliveCor Kardia Mobile	Australian	TGA-approved	\$199.00
Blood oxygen	iHealth Wireless Pulse Oximeter	Australian	TGA-approved	\$120.99
Blood oxygen	Wellue OxySmart Fingertip Oximeter	International	FDA-cleared	\$53.32
Weight	A&D Weight Scale	International	None	\$98.05
Weight	Xiaomi Mi Smart Scale 2	Australia	None	\$24.30

(A) *Vital Signs Measurement Device Selection.*

Vital signs are the measurements of the human body’s basic functions and can be particularly useful in detecting or monitoring health issues. Four crucial vital signs are body temperature, blood oxygen saturation, heart rate/electrocardiogram, and blood pressure. In addition to the four crucial vital signs, body weight is an important measurement as it provides supporting information regarding a patient’s overall health and physical condition (NursingAnswers.net, 2018). Moreover, most treatment decisions and dosages depend on body weight measurement. These vital signs and body weight measurements are often measured through sensor technologies, which can be used in a variety of clinical settings, for instance in-home and hospitals. Results from the sensor devices are displayed almost immediately and can be sent to healthcare professionals or stored in the cloud for future reference.

A range of vital signs measurement devices was researched based on their price, functionality, and regulatory compliance clearance perspectives. Where possible, the authors made efforts to include at least one product from an Australian company. Table 1 lists the selected vital signs measurement devices for this research.

(B) *Privacy Policy Inspection of the Corresponding Mobile Applications.*

With the increased use of mobile devices worldwide, mobile applications have become popular for smartphone users as a platform for entertainment and personal use. mHealth (Mobile Health) uses apps, devices, and other wireless technology in medical care (Holman, 2022). mHealth apps are health applications available on mobile devices, offering users a wide range of medical and health-related services. This means various health data will be collected, analysed, and shared through the applications. As a result, mHealth apps accounted for the largest revenue share of 75.4% in the mHealth market in 2021 (Grand View Research, 2022). The innovation in mHealth apps brings many health and clinical benefits, such as real-time analysis and transmission of health data, remote health monitoring, promoting self-management, and promote health awareness. However, at the same time, mHealth apps also open up a portal to new privacy and security risks.

The corresponding mHealth apps to the sensor devices used in this research were inspected by examining the device organisations’ privacy policies, terms and services, and inspection of the mobile traffic using Fiddler Everywhere. Fiddler Everywhere is a secure web debugging proxy (Fiddler Everywhere, 2022). For this research, Fiddler Everywhere were used to inspect the traffic from the mHealth apps used on iOS mobile devices.

(C) *Regulatory Compliance Investigation of the Selected Devices.*

Various Acts and regulations exist to protect the collection and transmission of these sensitive health data, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. It is also important for IoMT device manufacturers to clarify the secondary use of data to the users (Muzny et al., 2020), either through the product manual or the company website. Gerke and colleagues (2020) further explored the regulatory aspect of medical technologies, such as the emergency use authorisations for medical devices in the USA and Europe. Healthcare professionals and medical device companies in the US should ensure that they comply with HIPAA in order to protect the privacy of the patient’s data. A similar regulation in Europe is the General Data Protection Regulation (GDPR), which prohibits using and processing of personal health and genetic data (Gerke et al., 2020). Besides issues with

privacy and security of health-related data, there are concerns regarding the accuracy and safety of medical IoMT devices and sensors. Regulations helped to govern medical devices sold in the market. However, many devices that can be bought online are still largely unregulated. In the US, for a medical device to be sold legally, it must be approved by the Food and Drug Administration (FDA) to prove that the device is safe to use. Similar regulation exists in Australia, where the Therapeutic Goods Administration (TGA) uses a four-tiered classification system to govern the supply and usage of medical devices in Australia. Nowadays, buyers are becoming more aware of various medical device regulations. Therefore, formal approvals from these regulatory bodies will give the buyers a sense of security.

In this study, the authors closely inspected the regulatory compliance status of the devices and various data collected and transmitted using the devices and associated software.

(D) *Checking the Accessibility to Low-level Sensor Data via NODE-RED and ESP32*

Sensor data from the chosen health sensor devices were gathered and analysed using Node-RED and ESP32. Node-RED is a browser-based visual tool for programming a device. It is used for wiring different hardware devices, APIs and online services. It is a mature framework that's been around for about nine years and can be applied on any machine or platform running Node.js. Furthermore, node-RED is simple to understand with the easy-to-use drag-and-drop components user interface, which makes it ideal to represent the flow of communication compared to many other frameworks such as Eclipse Kura.

ESP32 is a dual-core microcontroller with WiFi and Bluetooth communication and is a simplified version of what the industry has been using for years. In addition, ESP32 provides stability and reliability with its powerful dual-core CPU. Regarding connectivity, the Bluetooth and WiFi capabilities make ESP32 a more suitable microcontroller for IoMT projects compared to other microcontrollers in the market, such as the Arduino development boards. It is also less costly and can achieve ultra-low power consumption with its power-saving features.

Experimental Setup

There are two types of Bluetooth communication protocols: BLE (Bluetooth Low Energy) and Classic Bluetooth. Only iHealth Blood Pressure (BP5) uses Classic Bluetooth. The rest of the devices use the BLE Bluetooth protocol. In order to handle these

Bluetooth protocols, Node-RED uses two Bluetooth modules. The first module is node-red-contrib-generic-ble to handle BLE protocol and the second module is node-red-contrib-bluetooth-serial-port to handle Classic Bluetooth protocol. The authors used Node-RED v2.1.6 for the testing environment, which is installed on MacBook Pro (16-inch, 2019), 16 GB 2667 MHz DDR4, 2.3 GHz 8-Core Intel Core i9, running macOS Big Sur 11.5.2 (20G95). The MacBook Pro uses the Bluetooth chipset 4364B3 from Broadcom with firmware version v65 c4188.

For testing on ESP32, MicroPython (MicroPython, 2022) was used, which is an implementation of Python3 and is optimised for microcontrollers. Moreover, it has a Python library aioble to work on both types of Bluetooth protocols (Github, 2022).

It is important to identify the service and characteristic UUIDs of the sensor device. They are unique strings representing the information the sensor can provide. There are various ways to identify the service and its characteristics. Node-RED module node-red-contrib-generic-ble has the method for scanning the Bluetooth devices and provides the information related to the connection, such as services, characteristics, name, manufacturer, and peripheral identifier of the device. In macOS, an application named BlueSee was also used, which allowed users to scan and obtain similar information.

After obtaining UUIDs, the Bluetooth connection to the device were established by specifying the service UUID. It was essential to determine the attributes of the characteristics to be used. It was a read attribute or notify attribute in our case. The former allowed the client to read the data from the connected sensor device. The latter allowed the client to subscribe to the characteristic and be notified whenever data was available.

After connecting and subscribing to the sensor device, the data that was transmitted were able to be retrieved. However, some sensor devices, such as iHealth devices and EKGraph from SonoHealth, require extra steps before the devices can send the data over. In that case, it was necessary to understand the authentication process for each device to get the data from those sensor devices. For example, each iHealth device requires a key to encrypt and decrypt the buffer string sent over by the device when the connection was initiated. EKGraph device required the client to initiate the connection by sending a static buffer array.

It was necessary to understand the data structure stored in the buffer data of each sensor device in order to read the data received by the sensors. Some devices

can store lots of information in the buffer data, including timestamps, user values and more. The relevant information was extracted from the data by understanding the parsing structure and then converting the hex numbers with different character lengths to meaningful numbers.

4 FINDINGS/RESULTS

The apps corresponding to the chosen sensor devices were carefully researched and tested to identify the various privacy and security features that have been incorporated to protect personal and health-related information. Section 4.1 to Section 4.3 provides a detailed summary of the usability, security, accessibility and integration of the apps and devices. The Apps were tested on iOS smartphones, and the individual researchers tested the devices in real-life scenarios. Section 4.4 explained the back-end testing done using Node-Red and ESP32. Furthermore, section 4.5 provides an overall discussion of the findings.

4.1 Usability and Regulatory Compliance

As shown in Table 1, Section 3, most of the devices tested were either FDA or TGA approved/cleared for clinical use. This provides a certain level of assurance that these devices have undergone standard development and testing and may provide more accurate results compared to those that were not approved by such regulatory bodies. Within the list of devices selected for this research, only the Kardia (TGA-approved), Kinsa (FDA-cleared), and iHealth (TGA-approved) devices require a password when setting up the device through the app.

All the devices were relatively easy to set up and use. The devices required either insertion of batteries or charging via the provided charging cord before use. Clear instructions are given in the user manuals that are supplied with the devices. Three of the devices required installation and set-up of a mobile app before the devices could be used. These included the two iHealth devices and the Karida mobile ECG/EKG monitor. Both the iHealth devices connect to the same app. Although the remaining devices could be used without first connecting to the app, all the devices did have the ability to connect to apps. The apps had good usability overall, with user interfaces that are simple to understand.

4.2 Security and Privacy at the End-User and Mobile App Level

There are several points of concern regarding the security and privacy of remote patient care. As shown in Figure 1, the security and privacy concerns associated with this testing are presented under three sub-headings: Patient/User level, Device-level and Mobile app Level.

4.2.1 Data Privacy Policies

Australian regulations mandate that all digital data collection products (e.g., Apps and websites) should have a laid out privacy policy associated with the product that details the collection, usage, management and disclosure of personal information collected through the products (OAIC, 2022b). In addition, there are special provisions made for the collection, primary & secondary usage, and management of health-related data (OAIC, 2022a). The main requirement is that apps have a clearly laid out privacy policy on usage, storage and sharing of the collected information, in particular with parties outside Australia – for which the end user's explicit consent is required.

All apps analysed in this study had a set of Terms and Conditions (T&C) that the users had to agree to at the setup stage. These T&C statements included clauses around privacy, use of the collected information, conditions on access to services and applications, and any disclaimers surrounding diagnoses or other medically related matters.

Our analysis found that Kardia, SonoHealth, Oxysart and Wellue provided the most detailed privacy policies regarding data collection and usage. Since iHealth provides a platform to cater for a range of products, their privacy policy is set an overarching policy that apply to all devices and cloud accounts that link to the device. There were no specific details provided on the collection, usage and dissemination of the data on the iHealth thermometer app. However, iHealth provided terms and conditions around data privacy for their blood pressure monitor and pulse oximeter. The other entities, Kinsa and A&D, provided low-level details about the data collection and usage in their privacy policies.

The types of data collected varied between devices. However, email, date of birth, name, and sex details were collected by almost all Apps in addition to the intended measurements (e.g., blood pressure, weight) collected through the device. In addition to these, height and weight were collected by iHealth

pulse oximeter & blood pressure monitor and Kardia ECG monitor.

4.2.2 Data Security

The Australian Signals Directorate (ASD) provides an Information Security Manual, in accordance with the Intelligent Services Act 2001⁸³, that is to be followed by any software vendor⁴. The security principles outlined in this manual mandate that all software vendors take adequate measures to safeguard the data collected, stored and communicated through their platforms. In this regard, the authors explored the measures taken by the selected vendors of the off-shelf vital sign measurement devices analysed in this study. The findings are detailed below:

- **Cloud Set-Up -**

Most modern mobile applications use cloud locations to store and process data collected via the devices. In the analysis of the set of devices and the associated applications, the authors investigated which vendor saved the data on cloud locations.

Among the vendors studied Kinsa, Wellue, and A&D did not send the data to a cloud location but provided the capability to link to Apple Health⁵, which essentially transferred the data to the Apple cloud. The vendors iHealth and Kardia had their own cloud locations on which data was saved and processed. While the iHealth cloud was included as part of the device purchase, KardiaCare cloud required users to pay a monthly or equivalent annual subscription fee to have their data stored on the cloud for future usage.

- **Connection Security -**

Most devices connected to the App via Bluetooth, except for Kardia which used audio signals to push the measurement data onto the mobile device.

Information on the mechanisms to ensure secure connectivity were only provided by SonoHealth and Kardia. SonoHealth detailed what data is communicated and stored in server environments, while Kardia explained the encryption techniques deployed to assure connection security. The other vendors did not mention any aspect concerning connection security.

- **Password Policy (App security) –**

A weak password length can open up security vulnerabilities in any application setting. Therefore,

the password policies used by the vendors concerning App security were explored. In this exploration, it was found that Kardia has the most comprehensive password requirements of 8-20 characters (no space) length, at least one upper case letter, one lower case letter, and one number. Kinsa, iHealth, Wellue, and SonoHealth had only password length requirements of 6 characters or more. A&D did not require a password to access the App.

Forgotten password recovery methods also can create a security loophole if not properly managed. In exploring this aspect, it was found that all vendors sent emails to the nominated email address to recover the passwords.

- **Login Attempts (App security) –**

In best security practices, it is recommended to restrict login attempts if the right credentials are not provided, as this will eliminate brute-force attacks. However, none of the vendors had implemented any restrictions on login attempts, and users could make any number of attempts.

- **Two-Factor Authentication (App security) -**

Two-factor authentication was invented in 1967 and used as early as 1986. Google popularised it in 2010 in response to China's attacks on Gmail accounts (Petsas et al., 2015). Since then, many vendors have adopted the use of this technology. However, none of the vendors in the focus of this study did use two-factor authentication in their app implementation, possibly due to the perceived non-sensitivity of the collected data.

4.3 Data Accessibility and Integration

Personal data relating to the users are collected and stored in the apps that are linked to the sensor devices. For example, personal data such as first name, last name, date of birth (DOB), gender, email address and phone number are required and collected when first registering for an account in most apps. Two exceptions are the apps for the A&D weight scale and Wellue blood pressure monitor, where entering these personal data is optional. In addition, the iHealth app requires more personal data, such as the users' weight and height information.

The results taken by the sensor devices are transmitted to the mobile apps via Bluetooth. However, some devices can work without the app by displaying the results on the LCD screen, which

³ <https://www.legislation.gov.au/Series/C2004A00928>

⁴ <https://www.cyber.gov.au/acsc/view-all-content/ism>

⁵ <https://www.apple.com/au/ios/health/>

means these results will not be transmitted and stored in the app. Data accessibility is the degree to which other people can access and use the data stored in the device or the app. As shown in Table 2, most apps have integrated access control in the form of username and password during the device and app setup process. This protects personal health data from unauthorised access. However, no access control was in place for the apps where the collection of personal data is optional.

Table 2: Summary of the data collection requirements and access control for the apps.

Apps	Personal data collection	Mandatory/Optional data collection	Data access control	Cloud storage	In-app storage
Kinsa App	Yes	Mandatory	Yes	No	Yes
iHealth App	Yes	Mandatory	Yes	Yes	Yes
Wellue ViHealth App	Yes	Optional	No	No	Yes
SonoHealth App	Yes	Mandatory	Yes	No	Yes
Kardia App	Yes	Mandatory	Yes	Yes	Yes
A&D Connect App	Yes	Optional	No	No	Yes
Xiaomi Mi Smart Scale 2	Yes	Mandatory	Yes	No	Yes

All apps provide in-app storage of results, with a few also providing cloud storage. Wellue’s ViHealth App and Kardia App enable connection to Apple Health, where they transfer and sync the data and results. For example, Kardia’s app allows connection to Apple Health to sync health metrics automatically, and users can send Apple Watch ECGs for review by a clinician.

4.4 Sensor Device Data Extraction

This section briefly explains the process of accessing the considered sensor devices. One of the important steps to gaining access to the Bluetooth device is understanding the Bluetooth communication

protocol. Depending on the manufacturer, each device can have a different communication protocol. It could either require a key to authenticate like iHealth devices or trigger the communication by sending over a unique command. Data could also be captured directly from some sensor devices without authentication.

Figure 2 shows the Node-RED diagram of the communication between the client and the iHealth Pulse Oximeter PO3 device using Bluetooth BLE protocol. From the diagram, the first step (Step 1) for communication is to initialise the Bluetooth connection from the client by scanning and connecting to the sensor.

After connecting to the sensor, the next process is to determine whether the device needs to authenticate. By using the Wireshark⁶ tool, the authors were able to identify the characteristic value and the overall protocol to determine what the sensor device requires to communicate. In Step 2, to get the buffer key for authentication, reverse engineering the iHealth Android app allowed extraction of the static buffer key for each type of iHealth device from the iHealth Android SDK library. A buffer string can then be sent with a timestamp to the PO3 device to authenticate. Another buffer string can then be sent back for authentication. The authors used the key to decrypt that string and sent it back to the sensor device. Once successfully authenticated through the light on the sensor device, real-time data can be received through subscription to services. The received data is parsed depending on each type of device. At the end of the process, all received data are converted to a hexadecimal format for consistency.

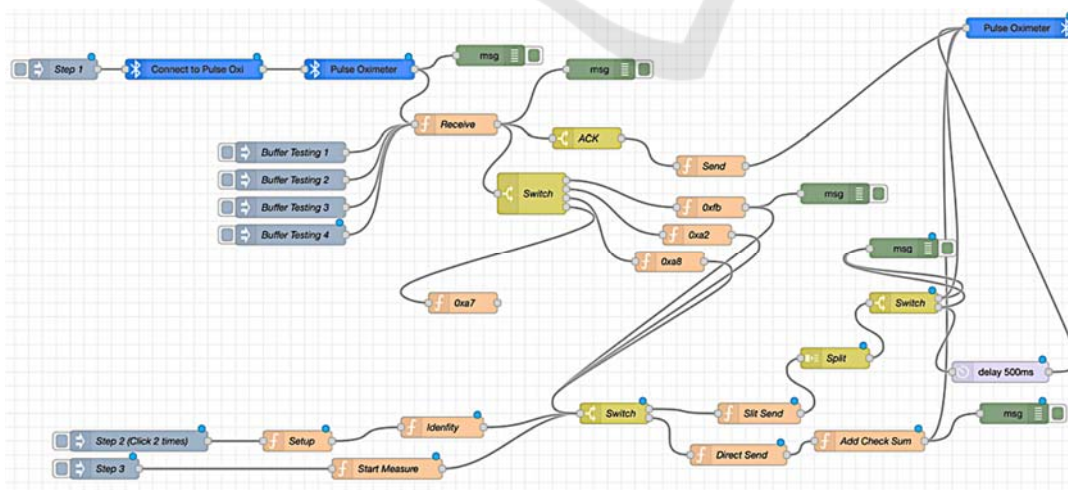


Figure 2: Node-RED diagram of iHealth Pulse Oximeter (PO3).

⁶ <https://www.wireshark.org/>

Table 3 shows examples of parsing the samples of raw data received from different sensor devices. Each device has a different method of parsing raw data to actual values. For example, the iHealth Pulse Oximeter PO3 device represents blood oxygen level using the first hexadecimal value and pulse rate measure with the second hexadecimal value in the received data transmission.

Table 3: Examples of parsing raw data samples.

Category	Brand	Raw Data Sample
Pulse Oximeters	Oxy Smart Bluetooth	Raw data in hexadecimal: aa 55 0f 08 01 63 4c 00 25 02 80 b2 aa 55 0f 03 03 02 a8 Oxy value is the 5 th byte: 0x63 = 99 P value is the 6 th byte: 0x4c = 76 Parsed data: Oxy=99, P=76
Pulse Oximeters	iHealth (PO3) Bluetooth	Raw data in hex: 61 4e 05 de 12 74 7b fd 0a 39 1f 0a Oxygen: first position 0x61 (97) Pulse Rate: second position 0x4e (78) Parsed data: Oxygen: 97, Pulse Rate: 78
Weight Scale	Xiao Mi Bluetooth	Raw data in hex: 02 96 00 e6 07 06 09 0c 2a 04 Read the first 2 bytes starting from the offset 2 in the little-endian order: 0x00 0x96 (value: 150) Divide the value by 100 and then by 2: 150/100/2 = 0.75 Parsed data: 0.75 kg
Weight Scale	A&D Bluetooth	Raw data in hex: 02 64 00 e6 07 05 0c 0f 06 19 Read 2 bytes starting from the second index in little endian order: 0x00 0x64 (value: 100). The value is then divided by 10: 100/10 = 10 kg
BPM	Wellue - Bluetooth (BP2)	Raw data received from the result: 6f 00 39 00 4e 00 49 00 00 81 94 03 00 58 3a 00 20 00 00 ab SYS value: first position 0x6f (111) DIA value: third position 0x39 (57) Parsed data: SYS:111, DIA:57
BPM	iHealth (BP5) - Bluetooth	Raw result data received after measuring in hex: 24 46 4c 00 00 Low pressure: second position 0x46 (70) High Pressure: first position + second position (106) Pulse: third position 0x4c (76) Parsed data: High Pressure: 106, Low Pressure: 70, Pulse: 76
Temp	Kinsa - Bluetooth	Raw data in hexadecimal: 43 03 0d b6 00 b7 c8 16 04 15 0b 31 21 Read the first 2 bytes starting from the offset 2 in the big-endian order: 0x0d 0xb6 (value 3510). Divide the value by 100: 3510/100 = 35.1 C degree

5 DISCUSSION

Vital signs measurement devices are becoming more commonly used in people's homes. In this study, the authors aim to find out the practicality of using these devices in remote clinical monitoring in a secure manner. In this regard, 9 devices that could be purchased in Australia, including online, were investigated. These devices could measure four vital signs: body temperature, blood oxygen saturation, heart rate/electrocardiogram, and blood pressure, plus

body weight as an additional measure. An overall summary of the privacy- and security-related features examined for all 9 sensor devices, together with their associated apps and online platforms, can be found within the link: '<https://tinyurl.com/5n87x9ht>'.

Based on the findings, it was identified that most devices could be used for clinical purposes, as these devices had regulatory clearances. However, it was unclear whether the associated software (mobile App) had clearance under 'software as a medical device' (Therapeutic Goods Administration, 2022). When selecting devices, the authors found that the non-regulated devices were relatively cheaper than those with regulatory clearances. Sometimes the regulated devices were \$100 (AUD) or more expensive than the non-cleared devices. These high prices may create access inequalities in implementing remote monitoring solutions.

It was relatively easy for the end-users to set up and use the devices. In that regard, most devices were suitable for practical use. However, integrating the data collected from these devices in hospital-based information systems would be difficult as most of these systems are closed systems that work with their own App and cloud solutions. Hence, the practical implementation of remote clinical monitoring would require medical device vendors and healthcare information system providers to work together - in other words, these were not simple 'plug and play' devices that could be used for implementing practical integrated solutions with other clinical information systems. However, it is worth noting that one vendor organisation, iHealth, provided a promising API in building interoperability between healthcare software systems and devices. Significant effort would be required to link individual patient readings correctly into their medical records and to overcome the appropriate authentication and validation measures.

The most alarming finding of this research is that despite the lack of legitimate access to collected data through an API, data stream transfers could still be intercepted through Bluetooth using either Node-RED, ESP32 or both. This may pose some privacy risk to individuals who have concerns about their sensor information and metadata being intercepted and leaked. In addition, most devices transmit data in clear formats. iHealth is the only vendor that provided encryption of the transmitted data, but an individual static key was used to access the transmitted data of each of the two iHealth devices tested. Overall, iHealth devices had the most promising results regarding practical and secure use.

6 CONCLUSIONS AND FUTURE WORK

Motivated by the increasing need for remote monitoring of patients, in this paper, the authors investigate whether it is practically possible to use off-the-shelf vital sign measurement devices for remote clinical use in a secure manner. A set of devices (9 in total) were selected to measure the four vital signs and weight. The devices and software associated with them (Apps) were examined in detail. In addition, usage terms and conditions and regulatory compliance status were explored. With the help of Node-Red and ESP32, the authors attempted to intercept the data streams that were communicated through Bluetooth.

Following review of the selected medical devices in this paper, the practical use off-the-shelf vital signs measurement products for remote clinical monitoring of patients securely appears to be a difficult prospect to achieve. This is due the fact that the reviewed products are predominantly closed systems that have regulatory challenges in terms of integration with other clinical information systems. Despite this fact, data from these sensor devices were able to be intercepted relatively easily, thereby posing some risk to individual privacy. The authors note there are promising products in the market, but these still require significant efforts to achieve practical solutions.

As for future work, there is the plan to investigate Bluetooth range testing to measure how far the devices can maintain connectivity with Node-RED or ESP32, providing a clearer indication of the proximity requirements of these sensor devices in their susceptibility to data interception or other attacks.

REFERENCES

- Chacko, A., & Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, 4(14), e2-e2.
- Fiddler Everywhere. (2022). <https://www.telerik.com/fiddler/fiddler-everywhere>
- Gerke, S., Shachar, C., Chai, P. R., & Cohen, I. G. (2020). Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nature medicine*, 26(8), 1176-1182.
- Github. (2022). *GitHub - Micropython*. <https://github.com/micropython/micropython-lib/tree/master/micropython/bluetooth/aioble>
- Grand View Research. (2022). *mHealth Market Size, Share & Trends Analysis Report By Component, By Services (Monitoring Services, Diagnosis Services), By Participants (Mobile Operators, Devices Vendors), By Region, And Segment Forecasts, 2022 - 2030*. <https://www.grandviewresearch.com/industry-analysis/mhealth-market>
- Grindrod, K., Boersema, J., Waked, K., Smith, V., Yang, J., & Gebotys, C. (2017). Locking it down: The privacy and security of mobile medication apps. *Canadian Pharmacists Journal/Revue Des Pharmaciens Du Canada*, 150(1), 60-66.
- Hendricks-Sturup, R. (2022). Pulse Oximeter App Privacy Policies During COVID-19: Scoping Assessment. *JMIR mHealth and uHealth*, 10(1), e30361.
- Holman, T. (2022). *mHealth (mobile health)*. <https://www.techtarget.com/searchhealthit/definition/mHealth>
- Kandhare, A. (2019). *Bluetooth Vs. Bluetooth Low Energy: What's The Difference?* <https://medium.com/@akash.kandhare/bluetooth-vs-bluetooth-low-energy-whats-the-difference-74687afcedb1>
- Kim, D.-w., Choi, J.-y., & Han, K.-h. (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making*, 20(1), 1-14.
- Knorr, K., Aspinall, D., & Wolters, M. (2015). On the privacy, security and safety of blood pressure and diabetes apps. IFIP International Information Security and Privacy Conference.
- Leloglu, E. (2016). A review of security concerns in Internet of Things. *Journal of Computer and Communications*, 5(1), 121-136.
- MicroPython. (2022). *MicroPython*. <https://micropython.org/>
- Muzny, M., Henriksen, A., Giordanengo, A., Muzik, J., Grøttland, A., Blixgård, H., Hartvigsen, G., & Årsand, E. (2020). Wearable sensors with possibilities for data exchange: Analyzing status and needs of different actors in mobile health monitoring systems. *International journal of medical informatics*, 133, 104017.
- Nick, G. (2022). *How Many IoT Devices Are There in 2022? [All You Need To Know]*. Tech Jury. <https://techjury.net/blog/how-many-iot-devices-are-there/#gref>
- NursingAnswers.net. (2018). *Health Observation Lecture: Measuring and Recording the Vital Signs*. <https://nursinganswers.net/lectures/nursing/health-observation/3-detailed.php>
- OAIC. (2022a). *Health and medical research*. <https://www.oaic.gov.au/privacy/the-privacy-act/health-and-medical-research>
- OAIC. (2022b). *Read the Australian Privacy Principles*. <https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles>
- Pahlevanzadeh, B., Koleini, S., & Fadilah, S. I. (2021). Security in IOT: Threats and vulnerabilities, layered architecture, encryption mechanisms, challenges and solutions. International Conference on Advances in Cyber Security,

- Papa, A., Mital, M., Pisano, P., & Del Giudice, M. (2020). E-health and wellbeing monitoring using smart healthcare devices: An empirical investigation. *Technological Forecasting and Social Change*, 153, 119226.
- Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015). Two-factor authentication: is the world ready? Quantifying 2FA adoption. Proceedings of the eighth european workshop on system security,
- Sivaraman, V., Gharakheili, H., & Fernandes, C. (2017). Inside Job: Security and privacy threats for smart-home IoT devices. *Australian Communications Consumer Action Network, Sydney*.
- Talwana, J. C., & Hua, H. J. (2016). Smart world of Internet of Things (IoT) and its security concerns. 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData),
- Therapeutic Goods Administration. (2022). *Regulation of software based medical devices*. <https://www.tga.gov.au/how-we-regulate/manufacturing/medical-devices/manufacture-guidance-specific-types-medical-devices/regulation-software-based-medical-devices>
- Zhang, C., Shahriar, H., & Riad, A. K. (2020). Security and Privacy Analysis of Wearable Health Device. 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC),
- Zubair, M., Unal, D., Al-Ali, A., & Shikfa, A. (2019). Exploiting bluetooth vulnerabilities in e-health IoT devices. Proceedings of the 3rd international conference on future networks and distributed systems,

SCIENCE AND TECHNOLOGY PUBLICATIONS