OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
35 - 42

Unveiling Vulnerabilities: Development IoT-Enabled Health Bracelets Without Security Measures

Mohamad Adrian Mohd Fuaad[1], Qairel Qayyum Muhamad Ridhuan[1], Wan Muhammad Alif Firdaus Wan Hanapi[1], Shelena Soosay Nathan*[1,2],
[1]Center for Diploma Studies, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
[2]ITecH Focus Group, Center for Diploma Studies, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
***shelena@uthm.edu.my**

ARTICLE INFO

Article History
Received 30 Jan 2024
Received in revised form 31 Jan 2024
Accepted 26 Jun 2024

Keywords:
Wearable device; healthcare, internet of things; security, privacy

ABSTRACT

The integration of Internet of Things (IoT) technology to strengthen the health bracelets intended for senior citizens is the subject of this study. It seeks to thoroughly evaluate the efficiency of these wristbands in tracking physical activity and vital signs, evaluating their influence on health outcomes, and pointing out any potential drawbacks. The project uses an agile methodology to construct a unique Arduino device that uses sensors and IoT to monitor vital signs. It also integrates data analysis to identify the capacity of the device to response to user health issues. The device, named LifeGuardian, detects temperature and heart rate, giving important information about a person's general health. However, in the IoT, security and privacy for wearable devices are largely disregarded. It is essential to apply a systematic approach for security and privacy safeguards in the context of healthcare and remote health monitoring. This study adds knowledge on security and privacy of wearable smart health device of these IoT-enabled health bracelets for the elderly besides offers solutions for security and privacy.

I. INTRODUCTION

Inadequate health monitoring increases the likelihood of unanticipated health risks, which include unanticipated risks associated with undetected illnesses, postponed medical interventions, insufficient monitoring capacities, and a deficiency in health education [1]. Without routine monitoring, a number of health issues may go undiagnosed and have serious repercussions, including life-threatening events like heart attacks or abrupt cardiac arrests [1]. Utilizing the Internet of Things (IoT) and other rapidly developing technologies, smart health monitoring applications are made possible, allowing people to proactively monitor their health.

When it comes to IoT for medical device integration, the focus is shifted towards the consumer ends, such as Continuous Glucose Monitoring (SGM), blood pressure cuffs, ingestible sensors, connected inhalers and other devices designed to record data on patient vital signs however these wearable devices are lacking in terms of security and privacy which are paramount for patient safety of their personal health details and other related information's.

As many security breaches and data privacy issues are becoming common in medical sector [2] where these data collected over IoT devices are threatened by malwares and other interventions. Besides that, current state of IoT devices is also not adopting security measures which results concern on privacy data breaches and concern by user. Study by the Aruba research agency [3] states, IoT related security breaches exceeds 84% in 2019. As such, security measures should be investigated serious when adapting IoT related devices [4].

ISSN 2636-9680
eISSN 2682-9266

This study basically focuses on the development of smart health care for elderly users and how user acceptance towards lesser or no security measure IoT devices. Besides, this study also examines current states of security and privacy in terms of technical and challenges of implementing the health-related device.

The goal of this study is to develop an Internet of Things technology to create a health monitoring wristband which can improve personal health monitoring by elderly people however with no security measurements been taken into consideration and present the result on how user accept the devices besides discussing on the security measurement that should be included in any IoT device in near future.

II. RELATED WORK

Critical health issues are addressed by the LifeGuardian, which was created especially to meet the healthcare needs of senior citizens in an aging population that is at risk for heart disease [5]. An accelerometer, temperature sensor, heart rate sensor, emergency button, and other sensors are integrated into this user-friendly wearable to allow for continuous health monitoring and early health issue detection [6]. The goal of the gadget is to improve safety and offer immediate health insights, giving wearers access to real-time vital sign data so they can act quickly in an emergency. The addition of an emergency button, which makes calling for help simple, further guarantees wearer safety.

LifeGuardian and related products share fundamental ideas in the field of smart health bracelets. But to set itself apart, this initiative does extensive comparisons with the goal of developing a special and enhanced health monitoring gadget. The proposed bracelet emphasizes proactive health monitoring by aligning with IoT technological improvements, hence solving the shortcomings of traditional health monitoring methodologies outlined in the introduction.

TABLE 1: Differences between existing projects

Previous Project	Advantages	Disadvantages
MyBotic Durian UNO - Smart Patient Monitoring System [7]	Contains LCD display for displaying user health metrics.	Does not have an emergency button.
	Includes SpO2 sensor for blood oxygen level monitoring, including BPM monitoring.	Large.
	Includes LM35 Temperature Module, enabling body temperature tracking.	Lacks a battery to be fully portable and worn.
Pulse Oximeter! Measure Heart Rate and Oxygen Saturation using Max30102, Arduino and OLED Display [8]	Contains a similar LCD display to the MyBotic system.	Lacks temperature sensor.
	Tracks and measures BPM and SpO2 levels.	Push button can be seen as unnecessary and should've been used as an emergency button.
	Includes a push button that acts as a display navigator.	Unable to be worn, lack of a proper strap.
Heartbeat monitoring wrist band. Is it possible to make using MAX30102 module [9]	Comes with similar heartbeat sensing capabilities as other Arduino projects.	No SpO2 sensor for blood oxygen level monitoring.
	Smaller LCD display that project current wearer's readings.	Lack of an emergency button.

	Smallest size footprint amongst the bunch.	Similar to the other Arduino projects, with no distinguishing feature.

Table 1 shows that most of the project used similar items in the realm of Arduino projects, health monitoring systems have gained significant popularity. This is to provide a comparative analysis of three such Arduino projects: MyBotic Durian UNO, MountDynamics Health Monitoring System, and UT Go Health Monitoring Wristband. The analysis focuses on their advantages and disadvantages, enabling readers to make informed decisions when choosing a suitable health monitoring solution, whilst also giving the project team a foundation to base the initials ideas upon. However, based on the study, it revealed that no security measures have been included or taken into consideration.

Although the LifeGuardian's user-friendly design and continuous health monitoring features help older persons with important health problems [2], it is crucial to expand this attention to the security aspect. Strong security and privacy safeguards are required as IoT-enabled devices like LifeGuardian become more commonplace and potential vulnerabilities surface.

The significance of wearable device security is emphasized by research in the field of IoT security and privacy. It is crucial to guarantee the availability, confidentiality, and integrity of the data transferred and stored by health bracelets [4]. Big data collected from millions of IoT devices provide an impact on devices associated with medical care for data analytics. However, most security breaches and data privacy issues are reported in the medical sector [3]. For example, two Austrians meddled with the pain management infusion pumps and the overdose caused respiratory problems but could be fatal [10]. In another study, it is revealed that the FDA warned on pacemaker programmer models are at risk as outsiders can adjust the pacemaker setting in a patient through internet [10].

Therefore, it is imperative to adopt sufficient security measures to secure the medical systems, infrastructure, and protect the privacy of patient's sensitive personal data.

These studies highlight the necessity of adopting secure communication protocols and raising user knowledge of security and privacy in the context of wearable health monitoring devices to prevent data breaches and unwanted access to private health information [6]. To maintain user confidence and guarantee the safe and secure operation of these wearables, security elements must be incorporated into their design [7].

Another extensive survey conducted by Quadri et al. [1] that the security and privacy of IoT applications were overlooked, solutions prone to attacks and doesn't prescribe a robust security solution for healthcare IoT spectrum. It is also clear less research was carried out in the healthcare IoT in the past.

Strong security protections should be given top priority in the creation of the suggested health monitoring bracelet, which includes LifeGuardian, considering these observations. However, this security and privacy is what Lifeguardian failed to implement as well as much as many other studies on IoT in healthcare misses which impacted the need of using the device securely.

III. METHODOLOGY

The methodology that is used for the development of LifeGuardian is the Agile methodology as shown in **Fig 1**, which is an iterative and incremental approach to project development that prioritises adaptability, collaboration, and continuous improvement [11]. Unlike traditional waterfall methods, agile methodologies emphasise user collaboration, frequent feedback, and the delivery of working software in short development cycles called sprints. Agile projects are divided into phases, each with its specific objectives and deliverables.

ISSN 2636-9680
eISSN 2682-9266

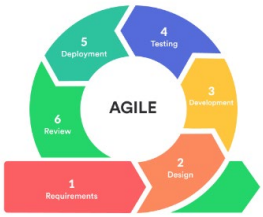

Fig. 1. Agile Methodology

This section explains the research methodology used and among others, on how the research data are being collected or generated. In addition, this section should also explain how the data collected are analyzed.

A. Requirements

The requirement phase serves as a crucial starting point for the project. The phase involves gathering essential knowledge to create a main framework of ideas for the LifeGuardian project. This phase is key to setting the stage of a successful development journey in revolutionizing the wearable devices that have emerged as valuable tools for monitoring and improving personal health.

B. Design

During the design phase, requirements are obtained and collected to begin creating an innovative health tracking bracelet. This phase also acts as the architectural stage, which follows a top-down technical approach. Various diagrams, such as the context circuit diagram, and flowchart, are used in this scenario to describe how the LifeGuardian bracelet would work, from receiving input to processing and providing the final output.

Fig 2 shows function circuit diagram is a simplified graphical representation of how different components in a circuit are connected. The diagram details the wiring and connections that are connected to create the circuit of the LifeGuardian bracelet.

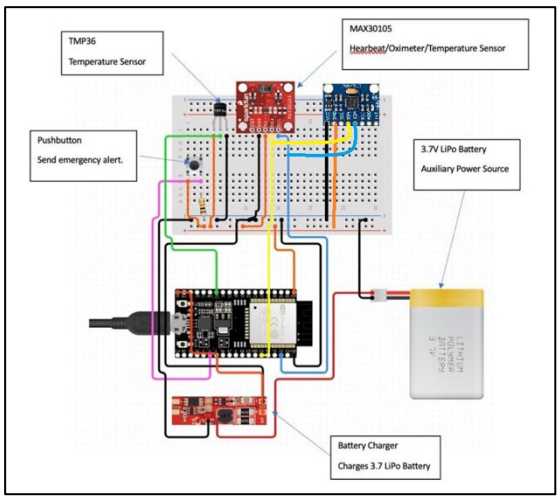

Fig. 2. Circuit Diagram

The ESP32 Arduino board acts as the main board that all sensors are connected to transmit data, whilst the main power source is from the 3.7 LiPo battery. After succesful connection, the ESP32 reads data from all sensors, and transmit the data to the Blynk API. Comparisons are done with the data readings to ensure theres no abnormalities, otherwise emergency alerts are sent to Blynk. Lastly, the health metrics data are displayed on connection mobile phones.

C. Development

After the design phase, the project is set to be developed. All planning, component specifications, and desired functionalities of the project are developed following increments for each separate functionality including the heart rate tracker, body temperature tracker, emergency button, impact and fall detection, mobile application synchronization, and notification functionalities. Development consists of creating the main code that interfaces with all components and synchronizes with a mobile phone for sensor readings to be interpreted and displayed. The LifeGuardian bracelet will be implemented feature by feature, tested to assure functionality, and then integrated and combined into a cohesive, fully functional wearable bracelet band.

D. Testing

The testing phase of LifeGuardian development is crucial for ensuring its accuracy, reliability, and performance in

measuring health data. This phase involves functional testing to validate the functionalities of the bracelet, including its sensors and features such as temperature, heartbeat, emergency button, and notifications. The high accuracy sensor of the Apple Watch provides readings like those of the LifeGuardian, while being significantly more expensive.

Performance testing is conducted to ensure the accuracy and dependability of these sensors, comparing their readings with calibrated devices of similar functions. Compatibility testing is also conducted to ensure the bracelet works seamlessly across end devices, uncovering any issues related to data synchronization, connectivity, or performance. Thorough testing is done to identify and uncover future issues that may arise and take pre-active actions to eliminate further anomalies which guarantee precise and trustworthy data. However, security and privacy has been ignored which is a serious measure that must be avoided by any cost during IoT devices development process especially on health care monitoring.

E. Deployment

The deployment phase of the project follows an iterative approach. Iterative deployment involves small, frequent releases based on user feedback and priorities. User acceptance testing validated integration and deployment, with feedback driving further improvements. Deployment procedures assisted in completing the process, and continuous monitoring provided real-time data for ongoing enhancements. Through Agile methodology, LifeGuardian achieved seamless integration and deployment into successfully creating and delivering a high-quality bracelet that tracks the wearers health metrics and provides a warning system for guardians.

F. Review

The primary objective of the review phase is to assess the implemented features, identify any gaps or discrepancies, and validate their alignment with the project's requirements. During review meetings, the team presents the completed work, demonstrating the functionality and usability of the LifeGuardian. Feedback and suggestions from the target scope are gathered, and necessary adjustments or improvements are noted for implementation in subsequent sprints.

IV. RESULTS AND ANALYSIS

Fig 3 shows the main dashboard that displays the current health metrics of the wearer. The wearer's heart rate (BPM), and body temperature (Celcius) are displayed as a gauge for the current readings, in addition to a chart that shows the patterns of the readings.

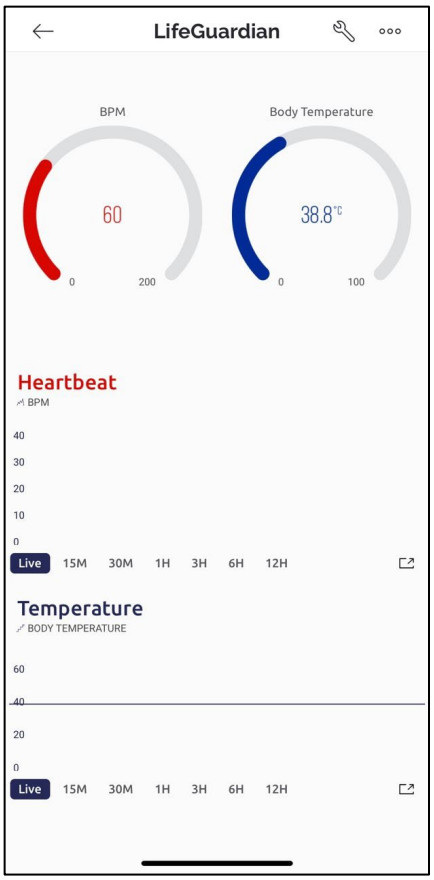

Fig. 3. Main Dashboard

Summarize the findings in text and illustrate them. Where appropriate, use figures and tables. In text, describe each of the results, pointing the reader to observations that are most relevant to the problem. Analyze the data and prepare the analyzed (converted) data in the form of figures (graph), table, or in text form.

Fig 4 showcases when the emergency button on the wearer's bracelet is pressed, a notification is triggered and sent to the Blynk API. This

ISSN 2636-9680
eISSN 2682-9266

notification act as an alert, indicating that the wearer is in danger or requires immediate assistance. The Blynk API shows this notification by sending the emergency alert to wearer close contact and triggering predefined actions, ensuring a prompt response to the wearer's emergency.

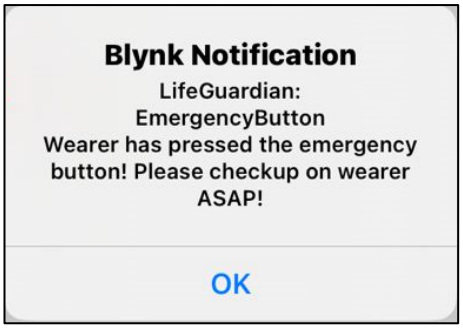

Fig. 4. Emergency Alert

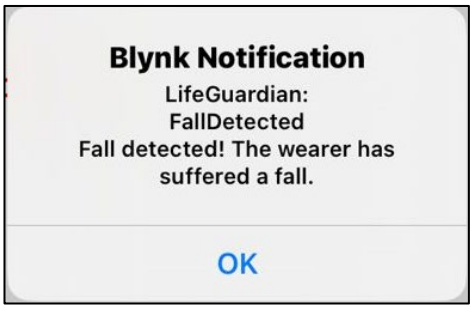

Fig. 5. Fall Detection Alert

While **Fig 5** showcases when the wearer experiences a fall, the sensor triggers a notification within the Blynk system. This notification act as an alert to inform the wearer close contact about the incident. By leveraging the sensor's capabilities, the Blynk API ensures prompt detection of falls and facilitates immediate communication to ensure the wearer's safety.

From the development process, it is clearly shown that no security nor privacy was included in any phases of the methodology. This might result in the acceptance of such devices as user are concern on their personal health information is on the internet and easily can be share or misused if these security measure are not conformed into the device and during development process.

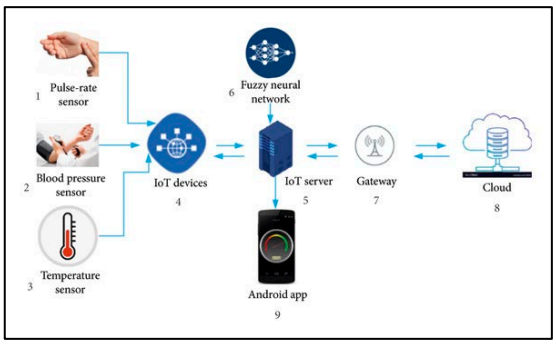

Fig. 8. Smart health Architecture

Wearables and sensors Healthcare devices use WiFi, Bluetooth, and Zigbee to transmit medical data to a gateway via cloud services and edge or node computing. The processing layer of wide-area communication technologies like 4G LTE, LoRaWAN, and NB-IoT subsequently carries this farther to the data center. The data center processes and analyzes this massive volume of data before sharing specific information with each patient [12].

The major challenge in implementing security measures for IoT in healthcare is the devices that enter through various channels to the network systems. Open WiFi or personal hotspots networks are used to connect a huge number of diverse devices—without encryption or passwords—to the internet. Hackers may target specific people to disable their device and prevent access to life-saving care, begin a general attack on a specific type of device, or steal data. According to [12], the key security measure must be considered in IoT for healthcare is that data confidentiality, integrity, authentication, and authorization besides adapating ISO security and privacy standards ISO 25237:2017 in which standard provides various techniques including pseudo randomization to anonymize the data in the health domain. Adapting the standards allows the patients to trust in e-Healthcare enterprises while also allowing for healthcare record sharing for research without compromising privacy.

V. DISCUSSION

As such in this development study, potential improvements may include the integration of additional health metrics, such as oxygen saturation or stress levels, or the exploration of advanced machine learning techniques to provide personalized health insights. The device does not complete the evaluation on public as its concern on security and privacy that was failed to be adapted as the study does not want to collect any personal data without knowing the consequences it can bring to the user.

Machine learning (ML), deep learning (DL), blockchain, or nanotechnologies, and fog computing are a few of the novel solutions that could fill the gaps and enhance the existing security architecture of IoT of healthcare devices [12].

By envisioning and discussing these future improvements, the project group aims to lay the groundwork for continuous innovation, ensuring that the LifeGuardian remains at the forefront of innovating the health monitoring technology and continues to make a positive impact on the lives of individuals susceptible to heart disease.

VI. CONCLUSION

In conclusion, the objective to develop a health product that uses the IoT concept was achieved by producing a new model of wearable device which can give many benefits for people to keep track of their health. Through the testing, this project was proven to reach the expected outcome which fulfilled the objective of this project. The devices must be added security and privacy measurement before being tested for its accuracy or other variables that might produce good result for future use and benefits many especially the healthcare system. However a deep review on past studies regarding this security and privacy to support the need of such devices and user acceptance.

VII. ACKNOWLEDGEMENT

The authors would also like to thank the Centre for Diploma Studies, Universiti Tun Hussein Onn Malaysia for its support.

VIII. REFERENCES

[1] M. A. Martínez-González, A. Gea, and M. Ruiz-Canela, “The Mediterranean Diet and Cardiovascular Health,” Circulation Research, vol. 124, no. 5, pp. 779–798, Mar. 2019, doi: 10.1161/circresaha.118.313348.

[2] Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V. Vasilakos, and S. W. Kim, “The Future of Healthcare Internet of Things: A Survey of Emerging Technologies,” IEEE Commun. Surv. Tutorials, vol. 22, no. 2, pp. 1121–1167, 2020

[3] Aruba Networks, “IoT Heading for Mass Adoption by 2019 Driven by Better-Than-Expected Business Results,” arubanetworks.com, 2017. [Online]. Available: https://news.arubanetworks.com/press-release/arubanetworks/iotheading-mass-adoption-2019-driven-better-expected-businessresults. [Accessed: 28-Jul-2020]

[4] P. A. H. Williams and V. McCauley, “Always connected: The security challenges of the healthcare Internet of Things,” in 2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016, 2017, pp. 30–35

[5] Larnyo, E.; Dai, B.; Larnyo, A.; Nutakor, J.A.; Ampon-Wireko, S.; Nkrumah, E.N.K.; Appiah, R. Impact of Actual Use Behavior of Healthcare Wearable Devices on Quality of Life: A Cross-Sectional Survey of People with Dementia and Their Caregivers in Ghana. Healthcare 2022, 10, 275.

[6] D. Martinho, J. Carneiro, J. M. Corchado, and G. Marreiros, “A systematic review of gamification techniques applied to elderly care,” Artificial Intelligence Review, vol. 53, no. 7, pp. 4863–4901, Feb. 2020, doi: 10.1007/s10462-020-09809-6.

[7] Arduino IOT Smart Patient Monitoring system with BLYNK Durian UNO (Enhancement Of Arduino UNO),” Arduino IOT Smart Patient Monitoring system with BLYNK Durian UNO (Enhancement Of Arduino UNO). https://mybotic.com.my/arduino-iot-smart-patient-monitoring-system-with-blynk-durian-uno-enhancement-of-arduino-uno

[8] “Pulse Oximeter! Measure Heart Rate and Oxygen Saturation using Max30102, Arduino and Oled Display,” YouTube, Jun.

ISSN 2636-9680
eISSN 2682-9266

14, 2021. https://www.youtube.com/watch?v=W_3ljVlt7Sk

[9] "Heart beat monitoring wrist band. Is it possible to make using MAX30102 module ? | Ut Go," YouTube, May 12, 2020. https://www.youtube.com/watch?v=qI_456UPf5Y

[10] FDA, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," FDA Guid., p. 6, 2018.

[11] V. Venkatesh, J. Y. L. Thong, F. K. Y. Chan, H. Hoehle, and K. Spohrer, "How agile software development methods reduce work exhaustion: Insights on role perceptions and organizational skills," Information Systems Journal, vol. 30, no. 4, pp. 733–761, Mar. 2020, doi: 10.1111/isj.12282.

[12] Karunarathne, Sivanarayani M., Neetesh Saxena, and Muhammad Khurram Khan. "Security and privacy in IoT smart healthcare." *IEEE Internet Computing* 25.4 (2021): 37-48.