International Journal of Advanced Smart Convergence Vol.10 No.3 33-40 (2021)
http://dx.doi.org/10.7236/IJASC.2021.10.3.33

IJASC 21-3-5

Periodic Biometric Information Collection Interface Method for Wearable Vulnerable Users

Taegyu Lee[1]

[1]*Assistant Professor, Smart Contents Major, Division of ICT Convergence, Pyeongtaek University, Gyeonggi, Korea*
E-mail: tglee@ptu.ac.kr

Abstract

Recently, wearable computers equipped with various biosensors such as smart watches, smart bands, and smart patches that support daily health management of users as well as patients have been released. Users of wearable computers such as smart watches face various difficulties in performing biometric information processes such as data sensing, collection, transmission, real-time analysis, and feedback in a weak wireless and mobile biometric information service environment. In particular, the biometric information collection interface is an important basic process that determines the quality and performance of the entire biometric information service. So far, research has focused on sensing hardware and logic. This study intensively considers the interface method for effectively sensing and collecting raw biometric information. In particular, the process of collecting biometric information is designed and analyzed from the perspective of periodicity. Therefore, we propose an efficient and stable periodic collection method.

Keywords: *Wearable, Bio-information, Interface, Synchronization, Smart Watch*

1. Introduction

In recent years, wearable devices such as smart watches, smart patches, and smart bands are continuously growing. These wearable devices are creating various healthcare and medical information services based on the collection of user's biometric information [1-8]. Representative companies such as Google, Fitbit, Apple, and Samsung are adding various health information and management functions to users through smart watches and smart bands. In addition, continuous efforts are being made to collect various biometric information of users [2]. And, recently, legislation has been prepared to promote digital medical information sharing and application services based on personal information anonymization so that personal biometric information can be safely used while ensuring personal privacy [9-10].

Here, it is important to continuously and stably collect the user's accurate raw biometric information for optimal health management of users [1-2, 11-13]. Users of wearable devices such as smart watches face various

Manuscript Received: June. 27, 2021 / Revised: July. 3, 2021 / Accepted: July. 5, 2021
Corresponding Author: tglee@ptu.ac.kr
Tel: +82-31-659-8370, Fax: +82-31-659-8011
Assistant Professor, Smart Contents Major, Division of ICT Convergence, Pyeongtaek University, Gyeonggi, Korea

difficulties in performing biometric information processes such as data sensing, collection, transmission, real-time analysis, and feedback in a weak wireless and mobile biometric information service environment. In particular, the biometric information collection interface is an important basic process that determines the quality and performance of the entire biometric information service.

So far, research has focused on sensing hardware and logic [4]. Wearable sensing hardware is expanding around biosensors including position sensors, heart rate sensors, and breathing sensors. Sensing logic has focused on improving the quality and accuracy of signals and information, focusing on filtering, sampling, etc. based on analog and digital bio-signals.

As the development of many biometric information hardware and software continues to expand, the complexity of the biometric information collection and transmission interface is increasing. In order to effectively operate the wearable biometric information interface, the interface structure should be strengthened. The biometric information interface system should consider the synchronization process of the collected biometric information along with the division, independence, and integration of the data transmission interface module structurally.

Figure 1 shows the configuration of a feedback process that collects biometric information from various wearable devices and responds to the user's real-time environment. Here, the collected biometric information is built into a database, and a customized feedback service can be provided to the user through real-time analysis by a background process.

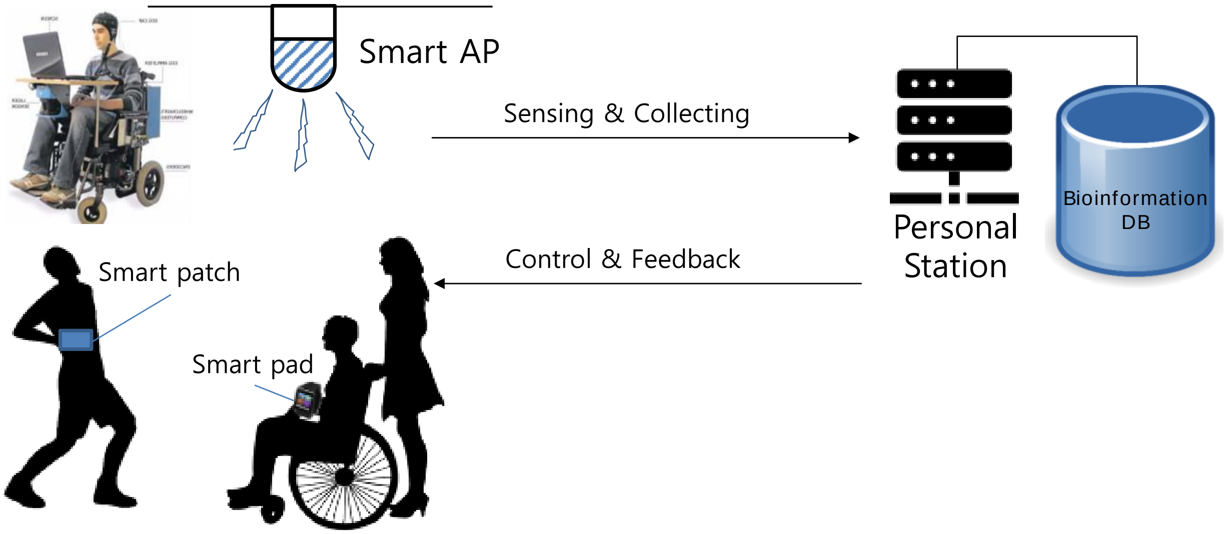

Figure 1. Bioinformation Transfer Organization on Wearable Devices Environments

In particular, a wearable biometric information device based on a free access environment (wireless Internet, etc.) may cause the following transmission failure due to weak resources. Such transmission failure causes include communication channel disconnection, power loss, power off, and interruption of user biometric information sensing. As a way to overcome such sensing failure, logging method and checkpointing method can be considered [14-15].

This study focuses on the transmission interface method for effectively sensing and collecting raw biometric information. In particular, the process of collecting biometric information is designed and analyzed from the perspective of periodicity. Therefore, we propose an efficient and stable periodic collection method. By analyzing the strengths and weaknesses of the existing aperiodic information collection method, we suggest a method to utilize the strength of periodic biometric information collection and suggest ways to strengthen its applicability.

This paper is described in the following order. Chapter 2 describes major issues related to a typical wearable user biometric information interface. Chapter 3 presents the biometric information transfer interface design and failure-recovery method for vulnerable wearable users proposed in this study, and Chapter 4 analyzes and evaluates the improvement points of the proposed interface method. Finally, Chapter 5 describes the conclusion and future research directions.

2. Wearable User Bioinformation Interface

The wearable user biometric information transmission interface digitizes the data collected from the client and supports real-time transmission to a remote PC or server based on local and wide area wireless networks.

The bio-information interface is an interface for collecting and transmitting bio-information from the human body, and accurately and effectively collects raw biodata sensed by the biosensor. In addition, biometric information collected from one device module is accurately and effectively transmitted to another device module.

The characteristics of the smart watch biometric information sensor and interface can support the following biometric information collection-related sensing and interface.

First, the lower layer in contact with the human body supports the skin and epidermal contact sensors and interfaces.

Second, as an intermediate layer, it supports extraction/sampling biometric information sensing and interface that removes noise from raw data of biometric data and controls the amount of data collection such as bit rate suitable for the collection environment.

Third, as the upper layer, it supports the bioinformation process and interface that optimizes or high quality bioinformation for various application environments.

Figure 2 shows the hierarchical structure of a smart watch and smart patch-based wearable user's biometric information system. In particular, the drug layer may be selectively configured for the purpose of treatment of the user.

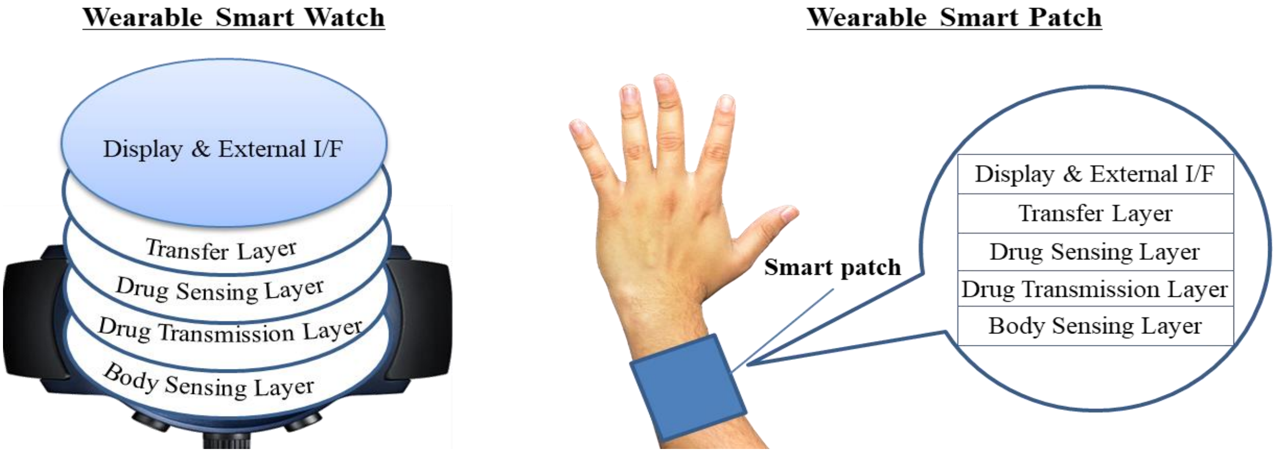

Figure 2. Example of Smart Watch/Patch based Wearable User and Bioinformation System Structure

In this study, the purpose of this study is to design an optimized biometric information interface in the wireless transmission and mobile transmission environments where the transmission environment of the transmission process is weak. This paper describes a transmission data synchronization method and a data recovery method to minimize data loss in a vulnerable transmission environment.

3. Vulnerable Wearable User Bioinformation Interface

The design and components of a smartwatch-based wearable biometric information collection and transmission platform as shown in Figure 1 are as follows. The wearable biometric information system shows a layered structure as shown in Figure 2. A key component of this hierarchical structure supports a biometric sensor, a transport layer, a display interface, and the like. In particular, the biometric information transmission module and transmission interface are collected and stored in the client's local memory, and support modules and interfaces for remote transmission and sharing.

In addition, compatible interfaces and libraries for collecting various biometric information may be supported. Such an interface may support a collection format compatibility of heterogeneous biometric information, thereby supporting a collection compatible interface platform of a biometric information terminal. In addition, the smart watch biometric information system provides a feedback interface that controls the client's functions in real time to build a user-customized biometric information service.

In the case of daily biometric activities, since biometric information shows periodicity in the same or similar pattern, periodic biometric data sampling is effectively performed, and even with a small amount of data collected, it can respond appropriately to grasp the user's biometric information status.

This periodic biometric information collection method plays an important role in establishing a user-customized daily health condition. In addition, it is possible to provide basic information for establishing a threshold value for more accurately evaluating an aperiodic singular state.

The amount of data transmission and collection of periodic monitoring and sampling is affected by the length of the cycle. Periodic monitoring and sampling can contribute to power optimization.

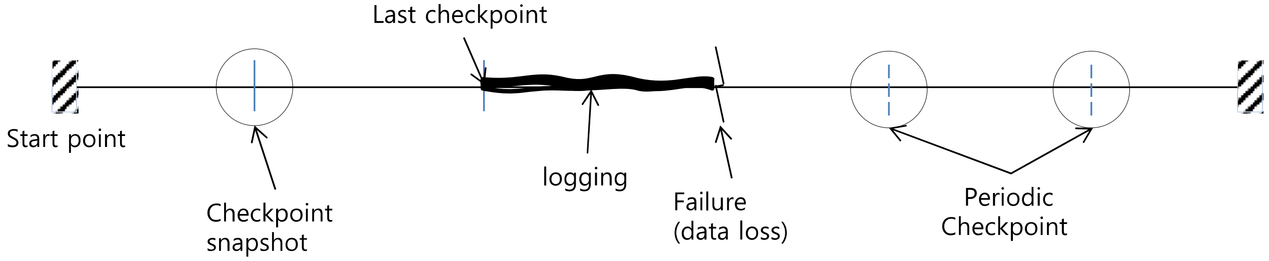

Figure 3. Periodic Checkpoints and Bioinformation Collection

In the periodic biometric information collection and transmission method, as shown in Figure 3, biometric information is collected and transmitted remotely according to the period set by the user or system. This real-time biometric information collection and transmission process causes aperiodic failure.

In order to effectively perform data recovery of transmission data of biometric information, a checkpoint snapshot, which is a periodic biometric memory image copy, is stored. The process of recovering from such a transmission failure rolls back to the most recent checkpoint period based on the failure point and restarts the transmission process. In addition, when the transmission process is logged from the most recent checkpoint period, transmission data loss can be minimized, thereby minimizing the recovery time.

Traditional real-time biometric data transmission methods do not pay attention to data loss recovery. This is because the real-time nature of the backup (periodic checkpointing and logging) or recovered data is compromised. Nevertheless, this study proposes a periodic checkpoint and logging method to improve the statistical accuracy and diagnostic information of the user's healthcare information.

Periodic checkpointing is a method that supports synchronization between user clients and servers while minimizing return points in case of failure. The periodic logging method may provide a method for minimizing the recovery process re-execution time due to an arbitrary transmission failure within the latest transmission period.

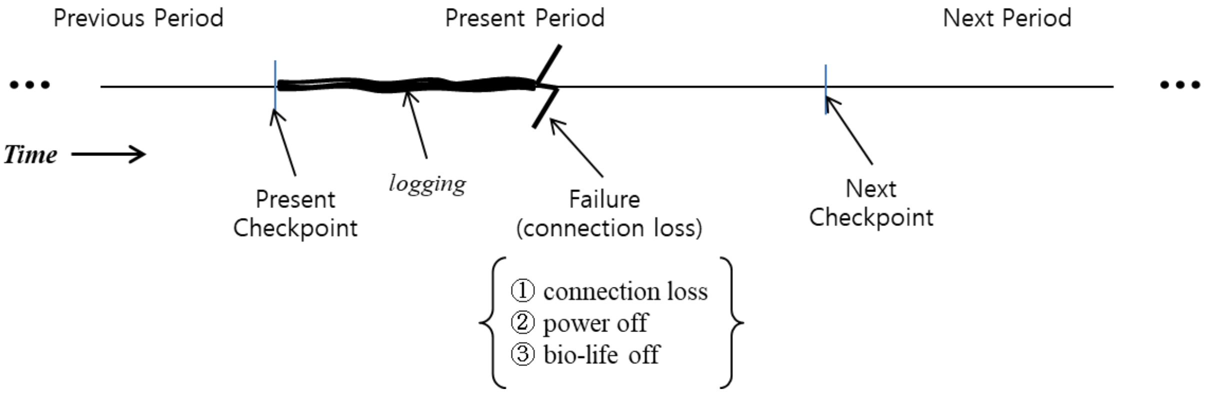

Figure 4. Communication Failure and Bioinformation Process Recovery

Figure 4 shows the logging backup process after the current checkpoint cycle and shows the process of returning and re-executing the transmission process due to a random transmission connection failure within the current transmission cycle. Causes of transmission failure may be divided into network disconnection, power off, and biometric information interruption. Depending on the cause of the failure of the biometric information transmission process, the interface can be selectively supported by external events such as backup recovery support, emergency power operation, and emergency medical service.

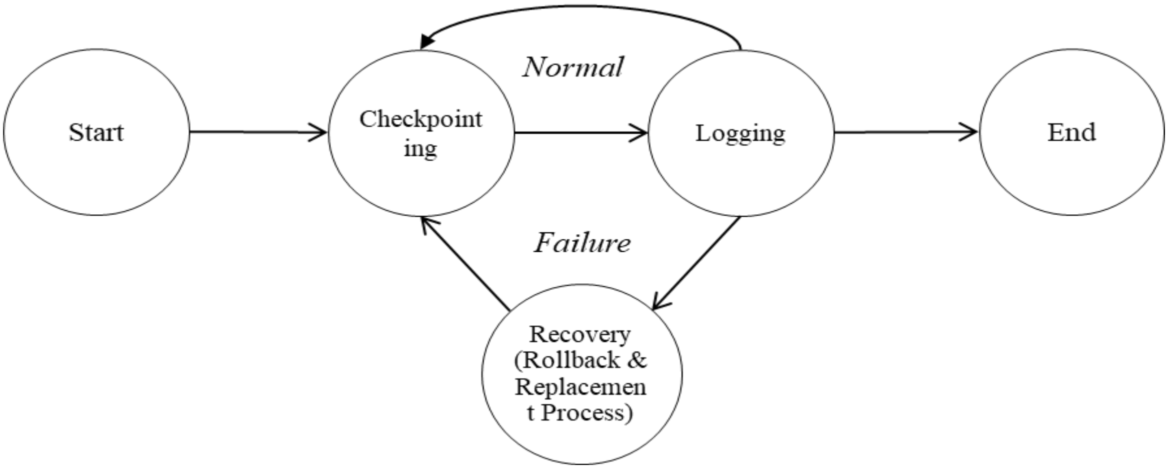

Figure 5. Bioinformation Communication and Resilience Processes

Another transmission process strategy may be to provide an aperiodic feedback process. In the case of an unpredictable and unusual biometric data event based on such a non-periodic collection process, the periodic bio data collection event cannot adequately respond because it shows aperiodicity in a pattern different from that of normal biometric data. Such a unique bioinformation phenomenon can be effectively dealt with through an aperiodic event checkpoint strategy based on a threshold value.

This aperiodic biometric information event may be linked to a user emergency medical response service. For aperiodic events, the amount of data transfer is proportional to the number of occurrences of the event. They are usually focused on unusual situations. When aperiodic events are based on constant monitoring, an effective power saving strategy is required for standby time.

4. System Analysis and Evaluations

The wearable smart watch and smart patch-based biometric information collection and transmission process in this study is based on the periodic process configuration. The data transmission analysis environment of this study assumes the following transmission models.

In this paper, we define various transmission models *X*, *Y*, and *Z* as shown in Figure 6 based on the following variables. If the start point of bioinformation transfer is T_s, the latest checkpoint time variable is T_c, the failure time variable is T_f, and the bit rate is R_{bps}, the analysis models of the data loss rate *LR* is defined as follows.

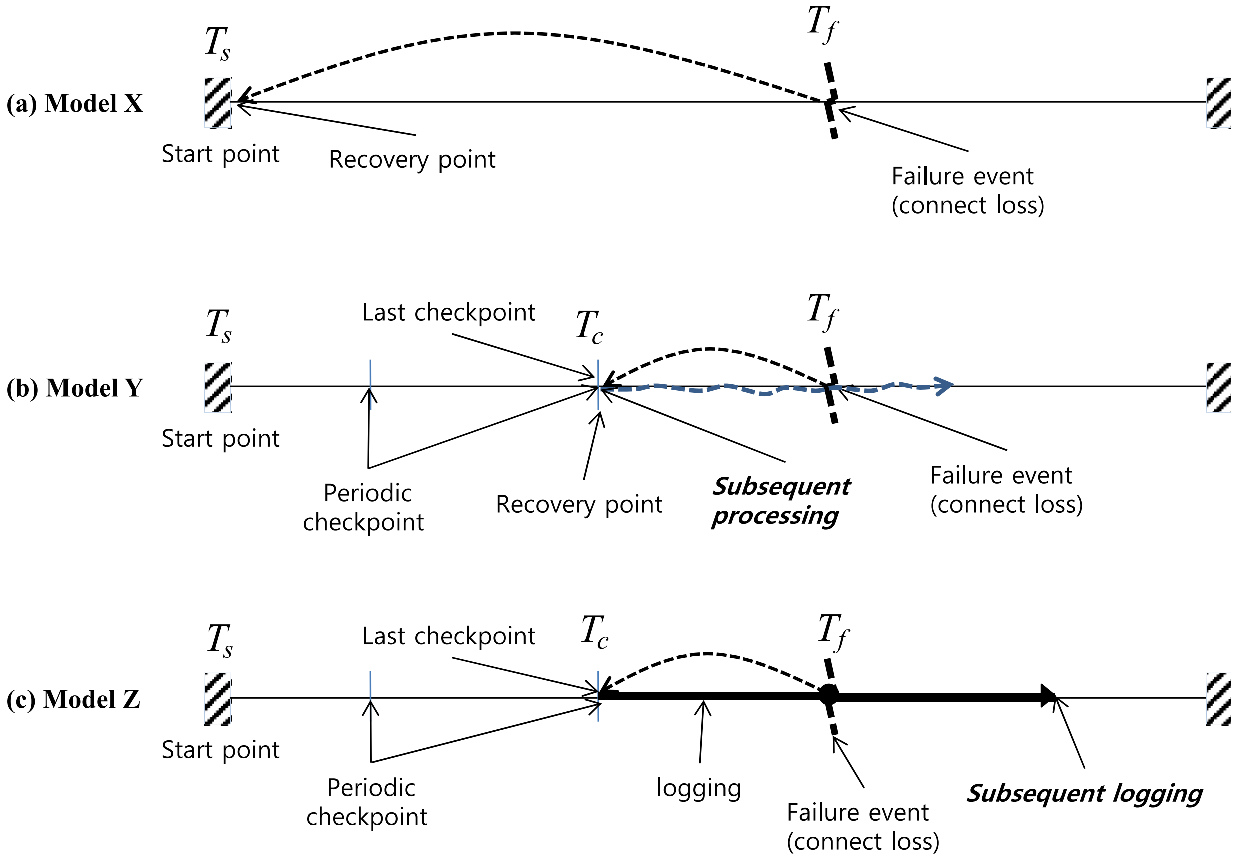

Figure 6. Bioinformation Transfer and Recovery Processes

Figure 6-(a) above shows a typical real-time biometric data transmission model, then 6-(b) and 6-(c) show the proposed models of this study. In 6-(a), in case of transmission failure, biometric information transmission is restarted from the recovery point T_s without backup and restore when the transmission channel is resumed.

From the failure point T_f to the recovery point T_s, the transmission data before the failure is lost. 6-(b) is a backup recovery transmission model based on checkpoints, in which data retransmission occurs from the latest checkpoint T_c on the sending side, and real-time performance is constrained by an arbitrary time delay. From the checkpoint point T_c of the latest transmission cycle to the failure point T_f, the transmission data before the failure point is lost. 6-(c) is a logging-based backup recovery transmission model. The overhead of the memory storage space on the transmission side can be minimized in recovery time and transmission time.

The data loss rate for model *X* is $LR(X) = (T_f - T_S) * R$, the data loss rate for model *Y* is $LR(Y) = (T_f - T_c) * R$, and the data loss rate for model *Z* is $LR(Z) = (T_f - T_f) * R = 0$. A comparison of the relative loss rates between the existing *X* model and the proposed *Y* model and *Z* model is in the order of magnitude of $LR(X) > LR(Y) > LR(Z)$. In the *Z* model, the loss rate is *0* because the data transmission recovery point is the same as the failure point T_f.

In addition, as an additional analysis, transmission time efficiency analysis requires less transmission recovery and retransmission time for the proposed *Y* model and *Z* model than for the existing *X* model. Here, in terms of backup space, model *Y* is more effective than model *Z*, and in terms of recovery time, model *Z* shows that model *Y* can respond effectively.

5. CONCLUSIONS

In this paper, we proposed an interface method for effectively sensing and collecting raw biometric information. In particular, the process of collecting biometric information was designed and analyzed from the perspective of periodicity. The periodic collection interface and method proposed in this study showed an efficient and stable transmission process.

The analysis results of the proposed models *Y* and *Z* in Chapter 4 show the strength of high transmission efficiency because the periodic biometric information collection and transmission data loss rate is lower than that of the existing model *X*. Therefore, it is possible to build a base data transmission environment for strengthening the applicability of wearable biometric information.

A comparison of the relative loss rates between the existing *X* model and the proposed *Y* model and *Z* model is in the order of magnitude of $LR(X) > LR(Y) > LR(Z)$. In the *Z* model, the loss rate is *0* because the data transmission recovery point is the same as the failure point T_f. Also, in terms of backup space, model *Y* is more effective than model *Z*, and in terms of recovery time, model *Z* shows that model *Y* can respond effectively.

Future research direction requires advanced research on intelligent bio-information prediction collection and transmission modeling, and disease prediction modeling can be developed through research on real-time and non-real-time semantic data sensing and extraction methods.

Acknowledgement

This paper was supported by the Research Fund, 2020, Pyeongtaek University in Korea’

References

[1] H. Jiang, X. Chen, S. Zhang, X. Zhang, W. Kong and T. Zhang, "Software for Wearable Devices: Challenges and Opportunities," *2015 IEEE 39th Annual Computer Software and Applications Conference*, 2015, pp. 592-597.
DOI: https://doi.org/10.1109/COMPSAC.2015.269.

[2] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne (2017),” A Survey of Wearable Devices and Challenges,” *IEEE Communications Surveys & Tutorials*. pp. 1-1,

DOI: https://doi.org/10.1109/COMST.2017.2731979.

[3] M. Kheirkhahan, S. Nair, A. Davoudi, P. Rashidi, A. A. Wanigatunga, D. B. Corbett, T. Mendoza, T. M. Manini, and S. Ranka, "A smartwatch-based framework for real-time and online assessment and mobility monitoring," *Journal of Biomedical Informatics*, Vol. 89, 2019, pp. 29-40,
DOI: https://doi.org/10.1016/j.jbi.2018.11.003.

[4] C. E. King, and M. Sarrafzadeh, "A Survey of Smart watches in Remote Health Monitoring." *Journal of healthcare informatics research*, vol. 2,1-2 (2018): pp. 1-24.
DOI: https://doi.org/10.1007/s41666-017-0012-7.

[5] D. Bonino, F. Corno and L. D. Russis, "dWatch: A Personal Wrist Watch for Smart Environments." *ANT/MobiWIS (2012). Procedia Computer Science*, Vol. 10, 2012, pp. 300-307.
DOI: https://doi.org/10.1016/j.procs.2012.06.040.

[6] B. Reeder, and A. David (2016). "Health at Hand: A Systematic Review of Smart Watch Uses for Health and Wellness," *Journal of biomedical informatics*. Vol. 63, pp. 269-276.
DOI: http://dx.doi.org/10.1016/j.jbi.2016.09.001.

[7] N. Anggraini, E. R. Kaburuan, G. Wang, and R. Jayadi (2019). "Usability Study and Users' Perception of Smartwatch: Study on Indonesian Customer," *Procedia Computer Science*. Vol. 161. pp. 1266-1274.
DOI: https://doi.org/10.1016/j.procs.2019.11.241.

[8] Jong-Yong Lee and Kye-Dong Jung, "Proposed Architecture for U-Healthcare Systems," The International Journal of Advanced Culture Technology, Vol. 4, pp. 43-46, June 2016.
DOI: 10.17703/IJACT.2016.4.2.43

[9] N. Liu (2013), "Bio-privacy: Privacy regulations and the challenge of biometrics," pp. 1-276.
DOI: https://doi.org/10.4324/9780203804087.

[10] C. Ebelogu, O. Amujo, O. Adelaiye, and F. Silas (2019). "Privacy Concerns in Biometrics," *IEEE-SEM*, Vol. 10, Issue 7, Jul. 2019, pp. 45-52.

[11] Jeong-Lae Kim, Gwan-Seok Kim, Jae-Yoon Kim, Han-Na Kim, and Eun-Yiu Jang, "A study of the communication transfer mode of physical signal (EKG, PPG)," The Journal of the Convergence on Culture Technology (JCCT), pp. 55-59, May 2017.
DOI: 10.17703/JCCT.2017.3.2.55

[12] Su-Jeong Yun, Sung-IL Hong, and Chi-Ho Lin, "An Efficient Smart Indoor Emotional Lighting Control System based on Android Platform using Biological Signal" Vol. 16, No. 1, pp. 199-207, Feb. 2016.
DOI: 10.7236/JIIBC.2016.16.1.199

[13] T. G. LEE (2019). "Data Pattern Modeling for Bio-information Processing based on OpenBCI Platform," The Journal of the Convergence on Culture Technology. The International Promotion Agency of Culture Technology, 5(4), pp. 451–456.
DOI: 10.17703/JCCT.2019.5.4.451

[14] W. Zhao (2021). "Logging and Checkpointing," *From Traditional Fault Tolerance to Blockchain*, pp. 21-62,
DOI: https://doi.org/10.1002/9781119682127.ch2.

[15] D. Johnson and W. Zwaenepoel, "Distributed system fault tolerance using message logging and checkpointing," (1990).