

New design of lightweight authentication protocol in wearable technology

Galih Bangun Santosa*¹, Setiyo Budiyanto²

¹Sekolah Tinggi Sandi Negara, Bogor, Indonesia

²Department of Electrical Engineering, Universitas Mercu Buana, Jakarta, Indonesia

*Corresponding author, e-mail: genio.genio444@gmail.com¹, sbudiyanto@mercubuana.ac.id²

Abstract

Today, the use of wearable devices is becoming a thing inherent in the daily activities of urban communities. In practice, wearable communications may contain sensitive information regarding a user's health record, so authentication and confidentiality of data exchanged must be guaranteed. In addition, the success of authentication between users, wearable devices and smartphones is very important because there are various threats of attack on the authentication process. Based on previous studies, it was found that the security functionality of user impersonation attack is not owned by lightweight authentication protocols in the current wearable communication environment. So this research undertakes the design of a lightweight authentication protocol to be immune to user impersonation attacks to supplement the lack of security functionality in previous protocols with the support of performing a formal analysis using the Scyther Tool. The research method used is a Research Library supported by conducting protocol security test experiment. The developed protocol utilizes a modified and customized S-NCI key establishment protocol scheme to meet all targeted security functionality. The research resulted that the lightweight authentication protocol generated was immune to the impersonation attacks of users, then was able to add two new functionalities that added wearable devices and added smartphones.

Keywords: key establishment, lightweight authentication protocol, scyther tool, user impersonation attack, wearable device

Copyright © 2019 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

Wearable technology is an electronic technology or computer that is incorporated into items of clothing and accessories which can comfortably be worn on the body. These wearable devices can perform many of the same computing tasks as mobile phones and laptop computers; however, in some cases, wearable technology can outperform these handheld devices entirely. Wearable technology tends to be more sophisticated than handheld technology on the market today because it can provide sensory and scanning features not typically seen in mobile and laptop devices, such as biofeedback and tracking of physiological function [1].

The authentication process between WD and MT becomes very important. Authentication is very important because there are various threats of attack that can happen [2]. Based on [2, 3] comparative results of concise authentication protocol schemes in a wearable communication environment consisting of Liu et al [4], Sun et al [5], Liu et al [6], it was generated that the security features of mobile terminal stolen attack, wearable device stolen attack, replay attack, user/wearable device/mobile terminal impersonation attack and the use of non-tamper resistant are not supported by all three protocol schemes. In addition, a number of such attacks can be classified into unauthorized access activities where the required security requirement is with the key establishment and trust setup [7]. The comparative results of a number of lightweight authentication protocol schemes in wearable communication environments based on their security features are described in Table 1. Meanwhile, wearable device usage trends are illustrated in Figure 1. The problem in this research is how the resistance of lightweight authentication protocol in wearable communication environment is designed against mobile terminal stolen attacks, wearable device stolen attacks, replay attacks, and wearable device/mobile terminal/user impersonation attacks.

Following up on these conditions, the proposed solution in this study is designing a lightweight authentication protocol on a wearable communication environment that is immune to

mobile terminal stolen attacks, wearable device stolen attacks, replay attacks, and wearable device/mobile terminal/user impersonation attacks to complement feature deficiencies security on previous protocols supported by performing a formal protocol analysis using Scyther Tool [10-12].

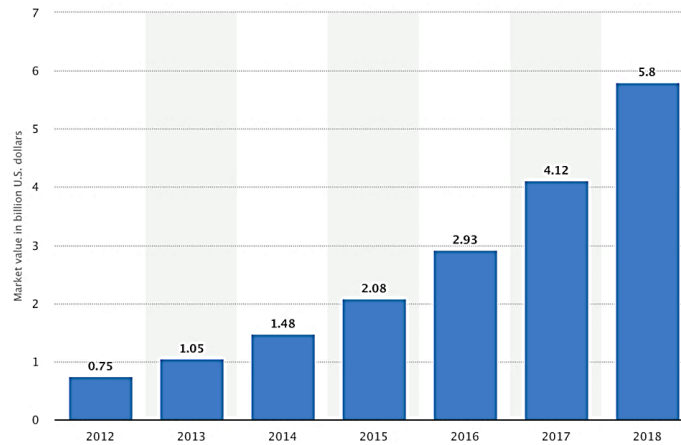


Figure 1. Forecasted value of the global wearable devices market from 2012 to 2018 [8]

Table 1. Analysis of Protocol Security Features [2], [9]

Feature	Liu et al. [4]	Sun et al. [5]	Liu et al. [6]
User/Wearable Device/Mobile Terminal Anonymity Preservation	V	x	V
Mobile Terminal Stolen Attack Protection	x	x	x
Wearable Device Stolen Attack Protection	x	x	x
Online/Offline Password Guessing Attack Protection	N/A	V	N/A
Privileged-Insider Attack Protection	V	V	x
Traceability Preservation	V	x	V
Replay Attack Protection	x	x	x
Man in the Middle Attack Protection	V	x	x
User/Wearable Device/Mobile Terminal Impersonation Attack Protection	x	x	x
Denial-of-Service Attack Protection	V	V	V
Use of Non-Tamper Resistant Wearable Device	x	x	x
Password Update Phase	V	x	x
Dynamic Users Addition Phase	V	x	x
Replacing Wearable Device Phase	V	x	x
Replacing Mobile Terminal Phase	V	x	x

2. Research Method

The research method used is a Research Library supported by conducting protocol security test experiment. Then, step research flowchart is described in Figure 2.

3. Results and Analysis

Based on the understanding of previous protocols, the characteristics of the lightweight authentication protocol can be explained in Table 2. In addition, the results of weakness analysis of previous protocols are Liu et al [4], Sun et al [5], Liu et al [6] and alternative development solutions described in Table 3.

In practice, key establishment protocols can involve trusted third-parties as initial system setup and online actions [13-19]. Currently the S-NCI key establishment protocol scheme has been developed. After performing formal analysis of S-NCI [20] protocol using Scyther Tool, it was found that the security characteristics of Alive and Weakagree are not owned by the protocol. So it is necessary to modify the S-NCI protocol by adding ID_T (identity T) and N_T (Nonce from T), and adding a step as a Step 5. Before and after modification of the S-NCI protocol is described in Table 4. Efforts to utilize and modify related protocols in various fields are also implemented on [21-26].

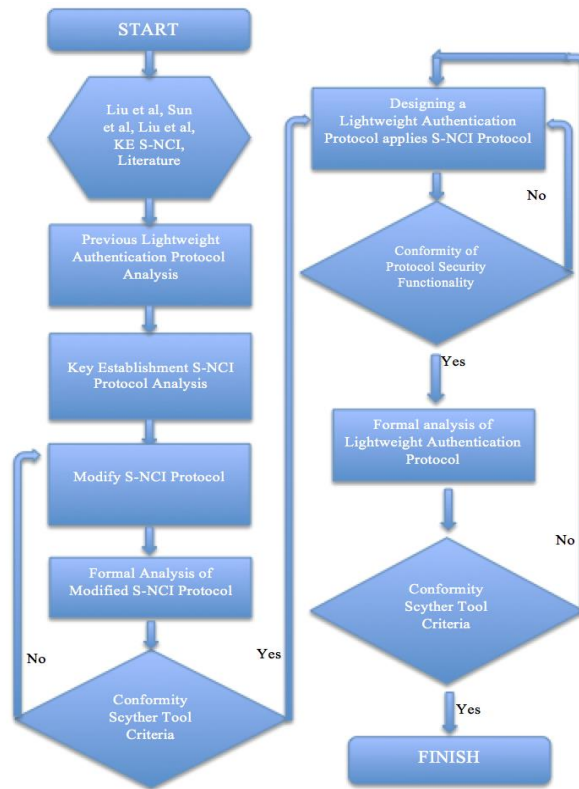


Figure 2. Step research flowchart

Table 2. Characteristics of Lightweight Authentication Protocols in a Wearable Communications Environment

No.	Characteristics
1.	Has a preparatory stage
2.	Has an encryption process to ensure data confidentiality
3.	Has a hash function to ensure the integrity of the data
4.	Has a challenge response process to ensure the authenticity of each entity
5.	Has a mutual authentication process
6.	Has the process of providing session key

Table 3. Weakness Analysis of the Protocol and Alternative Protocol Development Steps

No	Weakness Analysis	Alternative Development
1.	The user's fingerprint information assets and user wearable device passwords whose utilization has not been able to prevent the possibility of impersonation attacks both WD, MT and Users.	User fingerprint information and user wearable device passwords in protocol steps designed to prevent impersonation attacks both WD, MT and Users.
2.	There is user involvement in the role of witnessing and determining whether the WD and MT have been authenticated, but before that user has not performed any special authentication process for the user itself, which ensures that that person is indeed a legitimate user. So it still allows users to forge.	User involvement in determining the success of authentication between WD and MT should be supported by a protocol stage designed to accommodate that only authorized users who can encounter authentication conditions between the WD and the MT.
3.	There are protocol steps that are inconsistent with the design principles of cryptographic protocols according to Abadi and Needham.	In designing a lightweight authentication protocol, it is best to follow the design principles of cryptographic protocols according to Abadi and Needham.
4.	There are a utilization of key exchange protocols that are vulnerable to man-in-the-middle attacks.	A lightweight authentication protocol designed, in its key exchange step should be immune to replay attacks and man-in-the-middle attacks.
5.	Protocol assets that play an important role in determining the authenticity of each entity, are still stored in the device, allowing enemies to obtain the data with a power analysis attack, and can be used for further attacks.	The designed protocol allows all protocol assets that play an important role in determining the authenticity of each entity not stored in the device.

Table 4. Stages of the S-NCI Protocol Before and After Modification

Before Modification		After Modification	
$A \rightarrow T: E_{K_{AT}}(K_s ID_A ID_B t_1) H(K_s ID_A ID_B t_1)$	Step 1	$A \rightarrow T: E_{K_{AT}}(K_s ID_A ID_B ID_T t_1) H(K_s ID_A ID_B ID_T t_1)$	Step 1
$T \rightarrow B: E_{K_{BT}}(K_s ID_A t_2) H(K_s ID_A t_2)$	Step 2	$T \rightarrow B: E_{K_{BT}}(K_s ID_A ID_T N_T t_2) H(K_s ID_A ID_T N_T t_2)$	Step 2
$A \leftarrow B: E_{K_{BS}}(N_B t_3)$	Step 3	$A \leftarrow B: E_{K_{BS}}(N_B ID_T t_3)$	Step 3
$A \rightarrow B: H_{K_S}(N_B)$	Step 4	$A \rightarrow B: H_{K_S}(N_B ID_T)$	Step 4
		$B \rightarrow T: H_{K_S}(N_T)$	Step 5

3.1. Design of Lightweight Authentication Protocol

The proposed design consists of two stages, namely Registration Phase and Phase Pair and Mutual Authentication. In Phase Pair and Mutual Authentication is divided into three sub-stages. The proposed design begins with an Initialization System explanation.

3.1.1. Initialization System

The notation in the designed lightweight authentication protocol described in Table 5. Figure 3 describes the result of stage Initialization System. Figure 4 illustrates the proposed lightweight authentication protocol authentication model, which consists of four key entities: User, Smart Device (smart phone and smart watch), Cloud Server, and a Key Translation Center (KTC).

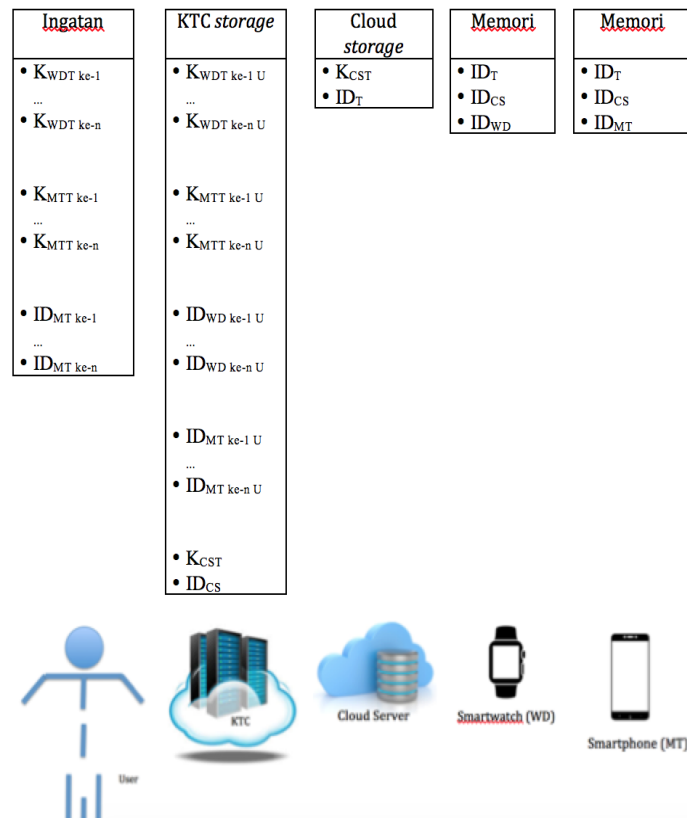


Figure 3. System initialization on the lightweight authentication protocol

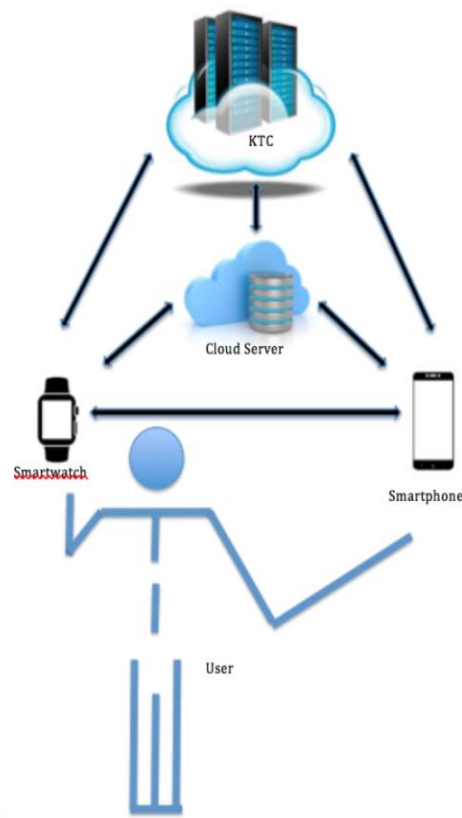


Figure 4. Lightweight authentication protocol authentication model

3.1.2. Registration Phase

At this Registration stage, a user registers by inputting important attributes required by the protocol through MT to be stored by the Cloud Server. Registration stages are described in Table 6 and Figure 5. Results of registration of the User by using MT, stored in CS, described in Table 7, are as follows.

Table 5. Notations and Definitions of the Lightweight Authentication Protocol

Notation	Definition	Notation	Definition
T	Trusted Third party as Key Translation Center (KTC)	PWD _{WD}	Password on WD set by the User
WD	Wearable Device	F_Inf _U	Fingerprint data on MT set by the User
MT	Mobile Terminal/ Smartphone	Rand _{CS}	The random number belongs to CS
CS	Cloud Server	Rand _T	The random number belongs to KTC
U	User	K _S	Session Key
Atr_P	A set of protocol attributes	H _K	MAC hash function (key uses K _S)
E _K ()	The encryption process uses the K key	H	Hash function
K _{WDT}	Encryption key between WD and T	t	Timestamp
K _{MTT}	Encryption key between MT and T	N	Nonce
K _{CST}	Encryption key between CS and T		Concat
ID _{WD}	WD identity	Insert	Description of activities to enter data (can be as a description of the Initial Registration, Adding Users, Adding WD, and Adding MT)
ID _{MT}	MT identity	Upd_WD	Description of activities to update the WD data
ID _T	T identity	Upd_MT	Description of activities to update the MT data
ID _{CS}	CS identity	Upd_pwd_WD	Description of activities to update the WD password
B_Addr _{WD}	WD bluetooth address	Temp_H_i	The temporary variable of the hash result calculated by CS
B_Addr _{MT}	MT bluetooth address	nCS	

Table 6. Explanation of the Registration Phase

Exchange messages on the Registration Phase	
MT → T: E _{K_{MTT}} (Insert K _S ID _{MT} ID _{CS} ID _T Atr_P t ₁) H(Insert K _S ID _{MT} ID _{CS} ID _T Atr_P t ₁)	Step 1
T → CS: E _{K_{CST}} (Insert K _S ID _{MT} N _T ID _T Atr_P t ₂) H(Insert K _S ID _{MT} N _T ID _T Atr_P t ₂)	
Step 2	
<ul style="list-style-type: none"> In this case, for example, CS gets "Insert" However, the description may consist of "Insert", "Upd_WD", "Upd_MT" dan "Upd_pwd_WD" Description "Insert" can be used in addition to user registration for the first time, also can be used to Add Users, Add WD and Add MT CS gets K_S, N_T, ID_{MT}, ID_T and Atr_P which contains (B_Addr_{WD} PWD_{WD} ID_{MT} B_Addr_{MT} F_Inf_U) 	
MT ← CS: E _{K_S} (N _{CS} ID _T t ₃)	Step 3
<ul style="list-style-type: none"> CS calculates H_{K_S}(N_{CS} ID_T) to be required in Step 4 MT gets N_{CS} and ID_T, so CS and T have been authenticated by MT 	
MT → CS : H _{K_S} (N _{CS} ID _T)	
Step 4	
CS → T : H _{K_S} (N _T)	
Step 5	
In Step 4, CS compares the previously computed MAC results, with results received from MT. If the result matches, then the MT has been authenticated by CS and the protocol is proceeded to Step 5, to authenticate CS by T. After all done, CS will process activities "Insert", "Upd_WD", "Upd_MT" and "Upd_pwd_WD".	
<ul style="list-style-type: none"> If "Insert" (can be used for Initial Registration/Adding Users/Adding WD/Adding MT) then: CS will add and store all Atr_P data in the tabel_Registrasi_User (Table 7), with the added value of H(Rand_{CS} H(PWD_{WD})) and H(Rand_{CS} H(F_Inf_U)) into the CsWd and CsMt columns. CS starts calculating and obtaining hash values of H(Rand_{CS} H(PWD_{WD})) and H(Rand_{CS} H(F_Inf_U)). Then, CS will do the following query: INSERT INTO tabel_Registrasi_User VALUES(B_WD=B_Addr_{WD},P_WD=H(PWD_{WD}),ID_MT=ID_{MT},B_MT=B_Addr_{MT},F_USR=H(F_Inf_U), CsWd=H(Rand_{CS} H(PWD_{WD})), CsMt=H(Rand_{CS} H(F_Inf_U))) CS successfully saved into tabel_Registrasi_User. If "Upd_WD" (Replacing Wearable Device) then: CS will update data related to WD (B_Addr_{WD}, PWD_{WD}) of User by F_Inf_U authentication. Then, CS will do the following query: UPDATE tabel_Registrasi_User SET B_WD= B_Addr_{WD}, P_WD= H(PWD_{WD}) WHERE (F_USR = H(F_Inf_U)) CS successfully saved into tabel_Registrasi_User. If "Upd_MT" (Replacing Mobile Terminal) then: CS will update data related to MT (ID_{MT}, B_Addr_{MT}) of User by F_Inf_U authentication Then, CS will do the following query: UPDATE tabel_Registrasi_User SET ID_MT=ID_{MT}, B_MT=B_Addr_{MT} WHERE (F_USR = H(F_Inf_U)) CS successfully saved into tabel_Registrasi_User. If "Upd_pwd_WD" (WD Password Update) then: CS will update data related to WD (PWD_{WD}) of User by F_Inf_U authentication Then, CS will do the following query: UPDATE tabel_Registrasi_User SET P_PWD= H(PWD_{WD}) WHERE (F_USR = H(F_Inf_U)) CS successfully saved into tabel_Registrasi_User. 	

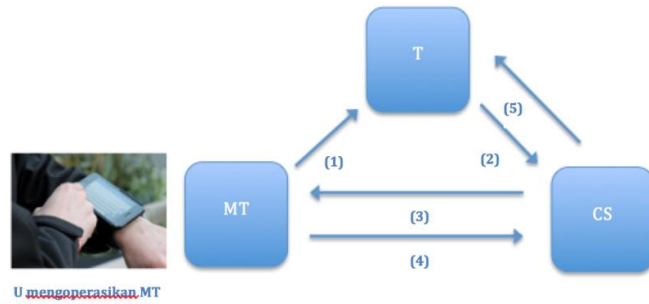


Figure 5. Lightweight authentication protocol registration phase

Table 7. Registration Result Stored in Table in CS (table_Registration_User)

No	B_WD	P_WD	ID_MT	B_MT	F_USR	CsWd	CsMt
1.	B_Addr _{WD}	h(PWD _{WD})	ID _{MT}	B_Addr _{MT}	h(F_Inf _U)	h(Rand _{CS} h(PWD _{WD}))	h(Rand _{CS} h(F_Inf _U))
2.	-	-	-	-	-	-	-
3.	etc	etc	etc	etc	etc	etc	etc

3.1.3. Phase Pair and Mutual Authentication

Phase Pair and Mutual Authentication consists of three sub-stages, namely Sub Stage 1 (WD Authentication by CS), Sub Stage 2 (MT Authentication by CS), and Sub Stage 3 (Authentication between WD and MT). All sub-stages are described in full in Figure 6, Figure 7, Figure 8, and Table 8.

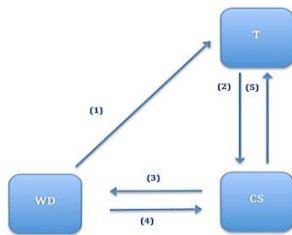


Figure 6. Sub stage 1 (WD authentication by CS)

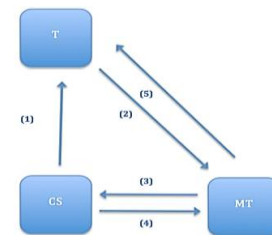


Figure 7. Sub stage 2 (MT authentication by CS)

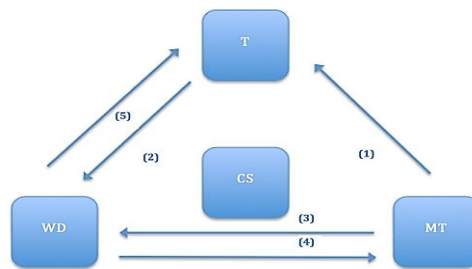


Figure 8. Sub stage 3 (authentication between WD and MT)

3.2. Lightweight Authentication Protocol Security Analysis

3.2.1. User/Wearable Device/Mobile Terminal Anonymity Preservation

The availability of user anonymity preservation, wearable devices and smartphones will be realized when protection from replay attacks and man-in-the-middle attacks can materialize. Due to the attacker trying to get important data that play a role in the success of device authentication/users, from tapping results that can be used to perform replay attacks and man-in-the-middle. However, it can not be attackers doing because the lightweight authentication protocol designed is proven to be immune to replay attacks and man-in-the-middle attacks, so the taping results will also not be useful.

3.2.2. Mobile Terminal Stolen Attack Protection

An attacker can steal or get a legitimate User's Smartphone. Then attacker can perform a power analysis attack to get the data stored on the smartphone. It will not be useful because the data stored on the smartphone are IDT, IDCS, and IDMT where those items do not play an important role in determining the success of the authentication process between devices/users. So the attacker will not be able to use it for a variety of subsequent attacks.

3.2.3. Wearable Device Stolen Attack Protection

An attacker can steal or get a legitimate User's wearable device. Then attacker can perform a power analysis attack to get the data stored on the device. It will not be useful because the data stored on the device are IDT, IDCS, and IDWD where those items do not play an important role in determining the success of the authentication process between devices/users. So the attacker will not be able to use it for a variety of subsequent attacks.

3.2.4. Online/Offline Password Guessing Attack Protection

This activity cannot be done by the attacker because when the wearable device or smart phone is stolen and carried out attack power analysis, which can be obtained by the attacker is an item that is not useful or no effect in the process of authenticating the device or the user, so it can not be used as data that can support a password dictionary attack. In addition, the protocol has also been shown to be immune to replay and man-in-the-middle attacks so the attacker is unable to tap into the communication between the parties.

3.2.5. Privileged-insider Attack Protection

In this protocol, especially at the registration stage, the registration process involved only the legitimate User only. This means there will be no other party who can represent or have the same authority as the actual User. Because in the registration stage, there are biometric data inquiries, and only eligible or legitimate Users have WD and MT pairs alone that can populate the biometric data themselves. In addition, suppose if a legitimate User feels the need to be assisted in the registration, then there are other parties who can help, and for example theft MT, then it is also useless, because the thief if it can do power analysis, and the data obtained nothing useful in the success of the authentication process.

3.2.6. Traceability Preservation

Traceability of the sender's source of messages is something that can be done on a security protocol that is still vulnerable to replay and man-in-the-middle attacks. In this concise authentication protocol, the tapping results will not work because the attacker does not have its encryption key. So the attacker cannot get the actual message and cannot browse the message source. It also supported earlier analysis that the concise authentication protocol designed was immune to replay and man-in-the-middle attacks.

3.2.7. Replay Attack Protection

This protocol has been shown to be resistant to replay attacks based on test results using a Scyther tool.

3.2.8. Man in the Middle Attack Protection

This protocol has been shown to be resistant to man-in-the-middle attacks based on test results using a Scyther tool.

3.2.9. Wearable Device/Mobile Terminal Impersonation Attack Protection

An attacker to be able to forge WD or MT must have items that play an important role in determining the success of each device/user authentication process. However, even though the attacker has stolen WD/MT and performs a power analysis, the attacker still does not get any useful items to attack authentication success, so the attacker's attempt to falsify identity against the device/user will not work either. In addition, the designed protocol has to scenario that in the Phase Pair and Mutual Authentication stage it can only run with the obligation of a legitimate User to operate it, as K_{WDT} , K_{MTT} , PWD_{WD} , and F_{inf_u} in the protocol are required, and only legitimate Users have it. So there is no chance for an attacker to fake WD/MT, because running the protocol cannot. In addition, the process of comparing the hash value $h(Rand_{CS}||h(PWD_{WD}))$ and $h(Rand_{CS}||h(F_{Inf_U}))$ occurs within the cloud, where the attacker will not be able to encounter that phase let alone manipulate it.

Table 8. Explanation of the Phase Pair and Mutual Authentication

Exchange messages on the Phase Pair and Mutual Authentication	
Sub Stage 1 (WD Authentication by CS)	
WD → T: $E_{K_{WDT}}(K_S H(PWD_{WD}) B_Addr_{WD} ID_{WD} ID_{CS} ID_T t_1) H(K_S H(PWD_{WD}) B_Addr_{WD} ID_{WD} ID_{CS} ID_T t_1)$	
Step 1	
T → CS: $E_{K_{CST}}(K_S H(PWD_{WD}) B_Addr_{WD} N_T ID_{WD} ID_T t_2) H(K_S H(PWD_{WD}) B_Addr_{WD} N_T ID_{WD} ID_T t_2)$	
Step 2	
<ul style="list-style-type: none"> ▪ T calculates the value of $H_{K_S}(N_T)$, to be used in Step 5 ▪ CS gets K_S, hash value of $H(PWD_{WD})$, B_Addr_{WD}, N_T, ID_{WD}, and ID_T. ▪ CS will authenticate WD if it is registered on the Registration, and also to obtain a valid MT pair in accordance with table_Registration_User, in the following way: SELECT ID_MT, B_WD FROM tabel_Registrasi_User WHERE B_WD=B_Addr_WD AND P_WD=H(PWD_WD) AND CsWd=H(Random_Cs H(PWD_WD)) ▪ If the result does not exist, then the protocol stops and authentication stages on Sub Stage 1 fails. ▪ If the result is there, then with sourced from table_Registrasi_User, CS will get valid data that is ID_MT (ID_{MT}) and B_WD (B_Addr_{WD}) which is a legitimate WD pair. ▪ Then, the protocol proceeds to Step 3. 	
WD ← CS: $E_{K_S}(N_{CS} ID_T t_3)$	
Step 3	
<ul style="list-style-type: none"> ▪ CS calculates $H_{K_S}(N_{CS} ID_T)$ to be required in Step 4. ▪ WD gets N_{CS} and ID_T, so that CS and T have been authenticated by WD. 	
WD → CS : $H_{K_S}(N_{CS} ID_T)$	Step 4
CS → T : $H_{K_S}(N_T)$	Step 5
<ul style="list-style-type: none"> ▪ In step 4, CS compares the previously computed MAC results, with results received from WD. If the result is the same, then the WD has been authenticated by CS and the protocol is proceeded to step 5, to authenticate CS by T. After all done, then the protocol can proceed to Sub Stage 2. 	
Sub Stage 2 (MT Authentication by CS)	
CS → T: $E_{K_{CST}}(K_S B_Addr_{WD} ID_{WD} ID_{CS} ID_{MT} ID_T t_1) H(K_S B_Addr_{WD} ID_{WD} ID_{CS} ID_{MT} ID_T t_1)$	Step 1
<ul style="list-style-type: none"> ▪ ID_{WD}, B_Addr_{WD} and ID_{MT} are obtained from table_Registration_User in CS, which took place on the previous Sub Stage 1 	
T → MT: $E_{K_{MTT}}(K_S B_Addr_{WD} ID_{WD} N_T ID_{CS} ID_T t_2) H(K_S B_Addr_{WD} ID_{WD} N_T ID_{CS} ID_T t_2)$	Step 2
<ul style="list-style-type: none"> ▪ T calculates the value of $H_{K_S}(N_T)$, to be used in Step 5. ▪ MT gets K_S, B_Addr_{WD}, ID_{WD}, N_T, ID_{CS}, and ID_T. 	
CS ← MT: $E_{K_S}(N_{MT} H(F_Inf_U) ID_T t_3)$	Step 3
<ul style="list-style-type: none"> ▪ MT calculates $H_{K_S}(N_{MT} H(F_Inf_U) ID_T)$ to be required in Step 4 ▪ CS gets N_{MT}, hash value $H(F_Inf_U)$ and ID_T. ▪ Next, CS will authenticate the MT if it is listed in table_Registration_User, by doing the following: SELECT CsMt FROM tabel_Registrasi_User WHERE F_USR= H(F_Inf_U) AND CsMt=H(Rand_Cs H(F_Inf_U)) ▪ If the result does not exist, then the protocol stops and authentication on Sub Stage 2 fails. Then, MT will display on screen "Refuse". ▪ If the result is there, then MT and T have been authenticated by CS and protocol can proceed to Step 4. 	
CS → MT : $H_{K_S}(N_{MT} H(F_Inf_U) ID_T)$	Step 4
MT → T : $H_{K_S}(N_T)$	Step 5
<ul style="list-style-type: none"> ▪ In Step 4, MT compares the previously computed MAC results, with results received from CS. If the result is the same, then CS has been authenticated by MT. Then, MT will display on the "Accept" screen. Then, the protocol proceeds to Step 5, to authenticate MT by T. After all done, then the protocol can proceed to Sub Stage 3. 	
Sub Stage 3 (Authentication between WD and MT)	
MT → T: $E_{K_{MTT}}(K_S B_Addr_{WD} ID_{MT} ID_{WD} ID_T t_1) H(K_S B_Addr_{WD} ID_{MT} ID_{WD} ID_T t_1)$	Step 1
<ul style="list-style-type: none"> ▪ ID_{WD} and B_Addr_{WD} were previously obtained from CS, which took place on the previous Sub Stage 2. 	
T → WD: $E_{K_{WDT}}(K_S B_Addr_{WD} N_T ID_{MT} ID_T t_2) H(K_S B_Addr_{WD} N_T ID_{MT} ID_T t_2)$	Step 2
<ul style="list-style-type: none"> ▪ T calculates the value of $H_{K_S}(N_T)$, to be used in Step 5. ▪ WD gets K_S, B_Addr_{WD}, N_T, ID_{MT} and ID_T ▪ To authenticate that MT is the right smartphone pair of WD, then WD will compare the Bluetooth address on WD with the B_Addr_{WD} earned. ▪ If the value of B_Addr_{WD} compared of the WD Bluetooth address is not the same, then the protocol stops and Sub Stage 3 fails. Then, WD will display on screen "Refuse". ▪ If the value of B_Addr_{WD} compared of the WD Bluetooth address is the same, then the protocol can proceed to Step 3. 	
MT ← WD: $E_{K_S}(N_{WD} ID_T t_3)$	Step 3
<ul style="list-style-type: none"> ▪ WD calculates $H_{K_S}(N_{WD} ID_T)$ to be required in Step 4. ▪ MT can get N_{WD} and ID_T, so that WD and T have been authenticated by MT. 	
MT → WD : $H_{K_S}(N_{WD} ID_T)$	Step 4
WD → T : $H_{K_S}(N_T)$	Step 5
<ul style="list-style-type: none"> ▪ In step 4, WD compares the previously computed MAC results, with results received from MT. If the result is the same, then the MT has been authenticated by WD. Then, WD will display on the "Accept" screen. Then, the protocol proceeds to Step 5, to authenticate WD by T. ▪ Once all is done, the Phase Pair and Mutual Authentication successful, then WD and MT have K_S used in secret communications. ▪ The user immediately executes local authentication by checking the screen results on WD and MT. If all screen displays Accept results, then User immediately makes a pairing Bluetooth between WD and MT. 	

3.2.10. User Impersonation Attack Protection

The lightweight authentication protocol designed has already demonstrated that the Phase Pair and Mutual Authentication stage can only work with legitimate Users operating it, as K_{WDT} or K_{MTT} , PWD_{WD} , and F_{inf_u} inputs are required in the protocol, as a requirement for the protocol to function. Then it is only the legitimate User who owns it. So with the existence of such specification, forgery of User cannot be done.

3.2.11. Denial-of-Service Attack Protection

A DoS attack can be done with the condition that an attacker can insert certain steps into the protocol to prevent the protocol from failing or unable to provide service. However, these conditions cannot be attackers do, because the attacker can only insert if the protocol has man-in-the-middle weakness, but it has been proven that this lightweight authentication protocol is immune to replay and man-in-the-middle attacks. So the attacker can not do the DoS attacks.

3.2.12. Use of Non-Tamper Resistant Wearable Device

Not discussed in this study.

3.2.13. Support of Password Update Phase

The activity description of "Upd_pwd_WD" allows this protocol to have the feature of Password WD Update, which occurs at the registration stage.

3.2.14. Support of Dynamic Users Addition Phase

The activity description of "Insert" allows this protocol to have the feature of adding User, which occurs at the registration stage.

3.2.15. Support of Replacing Wearable Device Phase

The activity description of "Upd_WD" allows this protocol to have the feature of Replacing WD, which occurs at the registration stage.

3.2.16. Support of Replacing Mobile Terminal Phase

The activity description of "Upd_MT" allows this protocol to have the feature of Replacing MT, which occurs at the registration stage.

3.2.17. Support Adding Wearable Device

The activity description of "Insert" allows this protocol to have the feature of adding WD, which occurs at the registration stage.

3.2.18. Support Adding Mobile Terminal


The activity description of "Insert" allows this protocol to have the feature of adding MT, which occurs at the registration stage. Thus, based on the designs performed and the resulting security analysis, the proposed lightweight authentication protocol has the functionality described in Table 9, as follows:

Table 9. Results of Protocol Security Functionality

Feature	Liu et al. [4]	Sun et al. [5]	Liu et al. [6]	The Proposed Protocol
User/WD/MT Anonymity Preservation	V	x	V	V
Mobile Terminal Stolen Attack Protection	x	x	x	V
Wearable Device Stolen Attack Protection	x	x	x	V
Online/Offline Password Guessing Attack Protection	N/A	V	N/A	V
Privileged-Insider Attack Protection	V	V	x	V
Traceability Preservation	V	x	V	V
Replay Attack Protection	x	x	x	V
Man in the Middle Attack Protection	V	x	x	V
User/WD/MT Impersonation Attack Protection	x	x	x	V
Denial-of-Service Attack Protection	V	V	V	V
Use of Non-Tamper Resistant Wearable Device	x	x	x	x
Password Update Phase	V	x	x	V
Dynamic Users Addition Phase	V	x	x	V
Replacing Wearable Device Phase	V	x	x	V
Replacing Mobile Terminal Phase	V	x	x	V
Adding Wearable Device	x	x	x	V
Adding Smartphone	x	x	x	V

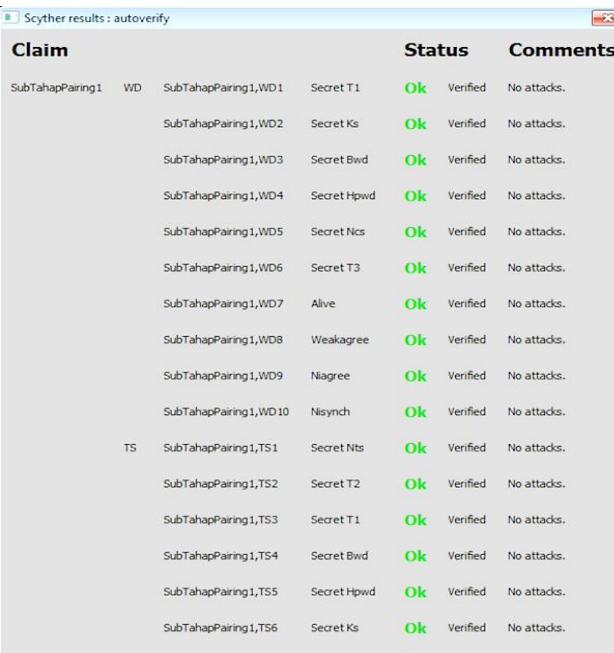
3.3. Formal Analysis

Formal analysis is performed with a Scyther Tool, which results in all stages of the protocol being shown to be immune to Replay Attacks and Man-in-The-Middle Attacks and meeting the criteria Alive, Weakagree, Niagree, and Nisynch. The results of the formal analysis using Scyther Tools on Registration Phase, Sub Stage 1 (WD Authentication by CS), Sub Stage 2 (MT Authentication by CS) and Sub Stage 3 (Authentication between WD and MT) are explained sequentially in Figure 9, Figure 10, Figure 11 and Figure 12.



Claim	Status	Comments
Registrasi, MT	Ok	Verified No attacks.
Registrasi,MT1	Ok	Verified No attacks.
Registrasi,MT2	Ok	Verified No attacks.
Registrasi,MT3	Ok	Verified No attacks.
Registrasi,MT4	Ok	Verified No attacks.
Registrasi,MT5	Ok	Verified No attacks.
Registrasi,MT6	Ok	Verified No attacks.
Registrasi,MT7	Ok	Verified No attacks.
Registrasi,MT8	Ok	Verified No attacks.
Registrasi,MT9	Ok	Verified No attacks.
Registrasi,MT10	Ok	Verified No attacks.
Registrasi, TS	Ok	Verified No attacks.
Registrasi,TS1	Ok	Verified No attacks.
Registrasi,TS2	Ok	Verified No attacks.
Registrasi,TS3	Ok	Verified No attacks.
Registrasi,TS4	Ok	Verified No attacks.
Registrasi,TS5	Ok	Verified No attacks.
Registrasi,TS6	Ok	Verified No attacks.
Registrasi,TS7	Ok	Verified No attacks.

Figure 9. Scyther result: verify (registration phase)



Claim	Status	Comments
SubTahapPairing1, WD	Ok	Verified No attacks.
SubTahapPairing1,WD1	Ok	Verified No attacks.
SubTahapPairing1,WD2	Ok	Verified No attacks.
SubTahapPairing1,WD3	Ok	Verified No attacks.
SubTahapPairing1,WD4	Ok	Verified No attacks.
SubTahapPairing1,WD5	Ok	Verified No attacks.
SubTahapPairing1,WD6	Ok	Verified No attacks.
SubTahapPairing1,WD7	Ok	Verified No attacks.
SubTahapPairing1,WD8	Ok	Verified No attacks.
SubTahapPairing1,WD9	Ok	Verified No attacks.
SubTahapPairing1,WD10	Ok	Verified No attacks.
SubTahapPairing1, TS	Ok	Verified No attacks.
SubTahapPairing1,TS1	Ok	Verified No attacks.
SubTahapPairing1,TS2	Ok	Verified No attacks.
SubTahapPairing1,TS3	Ok	Verified No attacks.
SubTahapPairing1,TS4	Ok	Verified No attacks.
SubTahapPairing1,TS5	Ok	Verified No attacks.
SubTahapPairing1,TS6	Ok	Verified No attacks.
SubTahapPairing1,TS7	Ok	Verified No attacks.

Figure 10. Scyther result: verify (WD authentication by CS)

Claim	Status	Comments
SubTahapPairing2 CS SubTahapPairing2,CS1 Secret T1	Ok Verified	No attacks.
SubTahapPairing2,CS2 Secret Ks	Ok Verified	No attacks.
SubTahapPairing2,CS3 Secret Bwd	Ok Verified	No attacks.
SubTahapPairing2,CS4 Secret IDwd	Ok Verified	No attacks.
SubTahapPairing2,CS5 Secret Hfi	Ok Verified	No attacks.
SubTahapPairing2,CS6 Secret Nmt	Ok Verified	No attacks.
SubTahapPairing2,CS7 Secret T3	Ok Verified	No attacks.
SubTahapPairing2,CS8 Alive	Ok Verified	No attacks.
SubTahapPairing2,CS9 Weakagree	Ok Verified	No attacks.
SubTahapPairing2,CS10 Niagree	Ok Verified	No attacks.
SubTahapPairing2,CS11 Nisynch	Ok Verified	No attacks.
TS SubTahapPairing2,TS1 Secret Nts	Ok Verified	No attacks.
SubTahapPairing2,TS2 Secret T2	Ok Verified	No attacks.
SubTahapPairing2,TS3 Secret T1	Ok Verified	No attacks.
SubTahapPairing2,TS4 Secret Bwd	Ok Verified	No attacks.
SubTahapPairing2,TS5 Secret IDwd	Ok Verified	No attacks.
Done. SubTahapPairing2,TS6 Secret Ks	Ok Verified	No attacks.

Figure 11. Scyther result:
verify (MT authentication by CS)

Claim	Status	Comments
SubTahapPairing3 MT SubTahapPairing3,MT1 Secret T1	Ok Verified	No attacks.
SubTahapPairing3,MT2 Secret Ks	Ok Verified	No attacks.
SubTahapPairing3,MT3 Secret Bwd	Ok Verified	No attacks.
SubTahapPairing3,MT4 Secret Nwd	Ok Verified	No attacks.
SubTahapPairing3,MT5 Secret T3	Ok Verified	No attacks.
SubTahapPairing3,MT6 Alive	Ok Verified	No attacks.
SubTahapPairing3,MT7 Weakagree	Ok Verified	No attacks.
SubTahapPairing3,MT8 Niagree	Ok Verified	No attacks.
SubTahapPairing3,MT9 Nisynch	Ok Verified	No attacks.
TS SubTahapPairing3,TS1 Secret Nts	Ok Verified	No attacks.
SubTahapPairing3,TS2 Secret T2	Ok Verified	No attacks.
SubTahapPairing3,TS3 Secret T1	Ok Verified	No attacks.
SubTahapPairing3,TS4 Secret Bwd	Ok Verified	No attacks.
SubTahapPairing3,TS5 Secret Ks	Ok Verified	No attacks.
SubTahapPairing3,TS6 Alive	Ok Verified	No attacks.
SubTahapPairing3,TS7 Weakagree	Ok Verified	No attacks.
Done. SubTahapPairing3,TS8 Niagree	Ok Verified	No attacks.

Figure 12. Scyther result:
verify (authentication between WD and MT)

4. Conclusion

This study has the following conclusions: a) The lightweight authentication protocols in the wearable communication environment generated in this study are immune to mobile terminal stolen attack, wearable device stolen attack, replay attack, user/wearable device/mobile terminal impersonation attack to supplement the lack of security functionality in previous lightweight authentication protocols; b) The lightweight authentication protocols in the wearable communication environment generated in this study have been shown to be safe against replay attacks and man-in-the-middle attacks and meet all formal analysis criteria in the Scyther Tool; c) The lightweight authentication protocol in the wearable communication environment generated in this study has two new functionalities that add wearable device and add smartphone.

References

- [1] Tehrani K, Michael A. Wearable Technology and Wearable Devices: Everything You Need to Know. 2014. [Online]. Available: <http://www.wearabledevices.com/what-is-a-wearable-device/>. [Accessed: December 1, 2017].
- [2] Das AK, Zeadally S, Wazid M. Lightweight authentication protocols for wearable devices. *Computers & Electrical Engineering*. 2017; 63: 196–208.
- [3] Gope P, Lee J, Quek TQS. Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks. *IEEE Sensors J*. 2017; 17(2): 498–503.
- [4] Liu S, Hu S, Weng J, Zhu S, Chen Z. A novel asymmetric three-party based authentication scheme in wearable devices environment. *Journal of Network and Computer Applications*. 2016; 60: 144–154.
- [5] Sun DZ, Huai JP, Sun JZ, Zhang JW, Feng ZY. A new design of wearable token system for mobile device security. *IEEE Transactions on Consumer Electronics*. 2008; 54(4): 1784–1789.
- [6] Liu W, Liu H, Wan Y, Kong H, Ning H. The yoking-proof-based authentication protocol for cloud-assisted wearable devices. *Personal and Ubiquitous Computing*. 2016; 20(3): 469–479.
- [7] Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*. 2017; 18(2): 113–122.

- [8] U.S. Global wearable technology market 2012-2018|Statistic Forecasted value of the global wearable devices market from 2012 to 2018 (in billion Statista Accounts : Access All Statistics . Starting from \$588/Year Global wearable technology market 2012). 2018. [Online]. Available: <https://www.statista.com/statistics/302482/wearable-device-market-value/%0A>. [Accessed: 12-May-2018].
- [9] Adrian D, Bhargavan K, Durumeric Z, Gaudry P, Green M, Halderman J A, Heninger N, Springall D, Thomé E, Valenta L, Vandersloot B, Wustrow E, Paul S Z. *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015: 5–17.
- [10] Cremers CJF. Scyther : Unbounded Verification of Security Protocols. *Technical report/Swiss Federal Institute of Technology Zurich, Department of Computer Science*. 2011; 572: 1–18.
- [11] Pavel O. Analysis of authentication protocols with scyter: Case study. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*. 2011: 359–365.
- [12] Dalal N, Shah J, Hisaria K, Jinwala D. A Comparative Analysis of Tools for Verification of Security Protocols. *International Journal of Communications, Network and System Sciences*. 2010; 3(10): 779–787.
- [13] AJ Menezes, PC Van Oorschot, and SA Vanstone, Handbook of Applied Cryptography. 1997. 106.
- [14] B Colin and M Anish. Information Security and Cryptography Texts and Monographs Springer-Verlag Berlin Heidelberg GmbH. 2003.
- [15] RM Needham and MD Schroeder. Using encryption for authentication in large networks of computers. *Commun ACM*. 1978; 21(12): 993–999.
- [16] Z Cheng and R Comley. Attacks on an ISO/IEC 11770-2 key establishment protocol. *Int. J. Netw. Secur.* 2006; 3(3): 290–295.
- [17] DE Denning and GM Sacco. Timestamps in key distribution protocols. *Commun ACM*. 1981; 24(8): 533–536.
- [18] SG Stubblebine and VD Gligor. *On message integrity in cryptographic protocols*. Proc. 1992 IEEE Comput. Soc. Symp. Res. Secur. Priv. 1992: 85–104.
- [19] W Mao and C Boyd. *On The Use of Encryption in Cryptographic Protocols*. Proc. 4th IMA Conf. Cryptogr. Coding. 1995.
- [20] Sadikin MALI, Windarta S. *S-NCI: Protocol Design of Key Establishment (in Indonesian: S-NCI: Desain Protokol Key Establishment)*. Proc. Semin. Nas. Mat. Univ. Indonesia. 2017: 1–10.
- [21] Budiyo S, Asvial M, Gunawan D. Performance Analysis of Genetic Zone Routing Protocol Combined With Vertical Handover Algorithm for 3G-WiFi Offload. *Journal of ICT Research and Applications*. 2014; 8(1): 49–63.
- [22] Asvial M, Budiyo S, Gunawan D. *An intelligent load balancing and offloading in 3G-WiFi offload network using hybrid and distance vector algorithm*. IEEE Symposium, Wireless Technology and Applications (ISWTA). 2014: 36–40.
- [23] Budiyo S, Nugroho A. A New Model of Genetic Zone Routing Protocol (GZRP): The Process of Load Balancing and Offloading on The UMTS-IEEE 802.11g Hybrid Networks. *TELKOMNIKA Telecommunication, Computing, Electronics and Control*. 2017; 15(2): 598–605.
- [24] Adiputra RR, Hadiyoso S, Hariyani YS. Internet of Things : Low Cost and Wearable SpO2 Device for Health Monitoring. *International Journal of Electrical and Computer Engineering (IJECE)*. 2018; 8(2): 939–945.
- [25] Weng OT, Isaak S, Yusof Y. Low Power CMOS Electrocardiogram Amplifier Design for Wearable Cardiac Screening. *International Journal of Electrical and Computer Engineering (IJECE)*. 2018; 8(3): 1830–1836.
- [26] Karthik RAN, Parvathy AK. Physicians' and Users' Perceptions Towards Wearable Health Devices. *Indonesian journal of electrical engineering and computer science*. 2017; 5(1): 48–57.