International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 11, No.1 (Jan-2022)

https://dx.doi.org/10.12785/ijcds/110121

An Improved User Anonymous Secure Authentication Protocol for Healthcare System Using Wireless Medical Sensor Network

M. F. Mridha[1], Md. Al Imran[2], Md. Anwar Hussen Wadud[1] and Md. Abdul Hamid[3]

[1]*Dept. of CSE, Bangladesh University of Business and Technology, Dhaka, Bangladesh*
[2]*Dept. of CSE, Bangladesh University of Professionals, Dhaka, Bangladesh*
[3]*Faculty of Computing and Information Technology, King Abdul Aziz University, Kingdom of Saudi Arabia*

Received 17 Mar. 2020, Revised 3 Jul. 2021, Accepted 8 Jul. 2021, Published 9 Jan. 2022

Abstract: Wireless Medical Sensor Network (WMSN) consists of biosensors connected with each other implanted within the human body. It transmits data to remote medical centers. Medical professionals can access the sensors of the human body to inquire about his health condition remotely. Transmitting patient data over insecure wireless channels is a major challenge because health data are very sensitive and must not be disclosed to unauthorized users, so ensuring secure authentication and preserving anonymity is very important. To address this issue, many researchers have provided many protocols for WMSNs. An anonymous patient monitoring system using WMSN presented by Amin et al. and demanded that their system preserves mutual authentication, user anonymity and security against stolen smart device attacks. By studying thorough and in-depth analyses, we found that this system is attackable to privileged insider attacks and stolen smart device attacks. In addition, it does not protect user anonymity. Additionally, it fails to protect denial of service attack. Furthermore, it has an error in the password modification stage. To overcome the above limitations of the existing systems we have proposed an advanced and mask identity-based secure mutual authentication protocol using WMSN. An informal security analysis is performed, which shows that our protocol is secure against different types of attacks. Furthermore, in our proposed protocol we have used the BAN logic model to prove the correctness of the mutual authentication feature. In addition, it offers ease login, secure authentication and strong password change phases.

Keywords: IoT, Wireless medical sensor network, Healthcare system, BAN logic, Secure authentication.

1. Introduction

Many small and embedded devices, low-power circuits, sensors, and IoT applications have been created based on the massive development of the Internet and wireless networks. These applications cover the areas of military applications, healthcare applications, vehicular applications, smart homes, office applications, etc. [1]. Normally, the IoT environment has different components, such as sensors, actuators, and smart devices, to collect the information transmitted by sensors and network infrastructure. This creates an integrated environment to provide easy access and better facility to human life [1]. Recently, applications of wireless medical sensor networks have become a point of fascination to academics and industry experts [2], E-healthcare monitoring systems using MobiHealth [3], CodeBlue [4], UbiMon [5], LiveNet [6], and SPINE [7] have been the focus of many researches works. Healthcare organizations are utilizing different technology such as wireless communication, IoT etc. to provide medical services to patients. Medical professionals can monitor patients' health conditions sitting anywhere in the world any time. Sensors implanted into the human body collect different information, such as ECG information, information on blood pressure, heart rate, body temperature, etc. and send this information to medical professionals through gateways. Then, medical professionals can monitor the patient's body condition using the information [8]. As information are transmitted through a wireless medium, a large security concern exists. User anonymity, mutual authentication and confidentiality of patient health data are very important. The potential disclosure of healthcare information is discussed and described in [3]. Due to the sensitiveness of these data, it is very inevitable to protect the communication channel and data [3], [4], [9]. Secure authentication protocols are being developed, and researchers have studied the security weaknesses of those protocols [5], [6], [7]. Preserving the confidentiality of the data encryption is an effective technology [10], [11], [12].

A. Architecture of the healthcare System using Wireless Medical Sensor Network

Wireless networks consist of low-power multifunctional sensor nodes. A sensor node is capable of sensing information, gathering information and communicating with

E-mail address: firoz@bubt.edu.bd, alimran13@gmail.com, mwadud@bubt.edu.bd, mabdulhamid1@kau.edu.sa

base stations and other connected nodes. Base stations are a prominent component of WSNs and act as gateways between sensor nodes and end users [13]. Presently, WSNs are broadly applied in different types of applications, for example, forest fire detection, air pollution monitoring, enemy intrusion monitoring, and healthcare monitoring. In this paper, we have provided a model for monitoring patient health using wireless sensor network in Figure 1. The newly introduced model was composed of three participants: medical professionals, such as doctors, patients, nurses, gateways and sensors. Sensors with less power and resources are placed into the human body, collect physical information from the patient body and send this information to gateway via router. The gateway has much more computation power, the core part of communication. It also acts as a secure registration and authentication medium between medical professionals and sensors. Before exchanging any information between the user and sensor, they need to register themselves with the help of a gateway. After authentication by the gateway, medical professionals can obtain health information from the sensor to monitor patient health conditions. Direct communication [1], [14], [15], [16] between sensors and medical professionals' costs higher energy and decreases the lifetime of sensor nodes. Some protocols have been described in [1], [14], [15], where sensor nodes send patient information directly to medical professionals. So, it incurs higher communication cost. For this reason, sensor node lifetime decreases gradually and becomes dead. We have addressed this issue in our proposed model and modified it in Figure 1, where the exchange of information occurs via the gateway node.

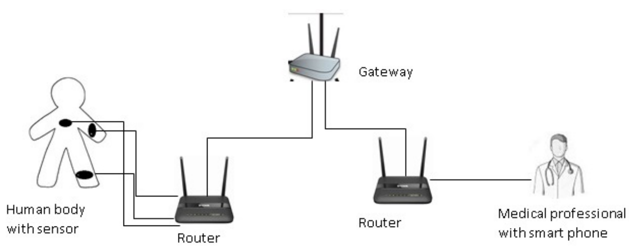

Figure 1. The proposed healthcare monitoring system architecture using WMSN. Sensor inside human body, gateway and medical professional, communicate through an access point called router.

B. Related works

We have studied the existing research works related to WMSNs focusing on security issues. The contributions and limitations of those protocols have been studied in detail. We know that the main property of security is the authenticity of the remote user and integrity of transmitted data [17], [18], [19], [20], [21], [22]. In 2009, Das proposed [23] a two-factor authentication process based on smart card devices. He claimed his protocol achieves protection against different security threats. However, the node camouflage invasions, user camouflage invasions, and guessing offline passwords have been found and described in [24]. In [25], the approach is risky in attacks of internal and parallel sessions where the process of mutual authentication has failed in its approach. A temporal credential-based authentication approach [26] was introduced by Xue et. al. in 2013. In the same year, cryptanalysis was performed in [27] on the Xue et. al. approach by Lie et. al. They demanded that the Xue et. al. approach is not protected against guessing offline password, stolen verifiers, privileged insiders, and stolen smart card attacks. We have found that ECC systems [28] [29], RSA cryptosystem [30], bilinierpairing [31], chaoric map [32] and hash function [17], [18], [33], [34], [35], [36], [37], [38] have been used to develop key agreement and user authentication protocols. A user authentication scheme for WMSN is presented in [14]. This scheme is not secure against privileged insider attacks and offline password guessing attacks [1]. They proposed an improved scheme to overcome the weakness of [14] in 2015. Later, a cryptanalysis was performed in [7] against this protocol and found several incorrectness and flaws in their design. Then, they [7] proposed a new scheme to remove the weakness of the [1] protocol. In 2016, R. Amin et. al. [39] found that their proposed security model is prone to internal attacks and sensor node capture attacks without revealing the username. A secure smart card-based anonymous user authentication protocol has been proposed by removing the drawback of the [7] protocol. In this paper, we have analyzed the paper and found that this protocol does not withstand privileged insider attacks, stolen mobile device attacks, denial of service attacks and fails to preserve user anonymity. Moreover, we have shown that there exists a flaw in the password change phase. To secure against the above security flaws, we have proposed an improved protocol that retains the original merits of [40]. Our scheme uses a one-way hash function and lightweight XOR operation.

C. Motivation and contribution

Our proposed architecture in Figure 1 provides a framework to monitor patient health data remotely. As patient data are very sensitive, security and privacy issues are a major concern here. Researchers have paid their attention in this field. They have also focused on different attacks, such as user anonymity, mutual authentication, and stolen device attacks. Several security protocols have been proposed in recent year to address these limitations, but we have observed in the related works section that those protocols still have weaknesses against known security attacks. For that reason, we are inspired to develop advanced user anonymous protocols in WMSN that is more efficient, and the main achievement of this article are given below:

1) We have proven that Amin et al.'s system has security flaws, such as stolen smart device attacks, privileged insider attacks, and denial of service attacks. It cannot preserve user anonymity. It also has weakness in the password change stage.
2) We have proposed a masked identity with hash function-based mutual authentication protocol to overcome this weakness.
3) We have analyzed and found that the proposed

protocol reduces the energy consumption of sensor nodes.

4) To prove the correctness of the mutual authentication feature, we have used the BAN model.
5) An informal defense analysis has been performed to show that it protects against various security attacks.

D. Construction of the paper

The rest of the paper is categorized as follows: section 2 provides security problems in the IoT for better understanding of the paper, security protocol [40] has been reviewed in section 3, and section 4 depicts the cryptanalysis of the protocol in [40]. The proposed protocol is explained in section 5. Section 6 gives an informal security analysis of the proposed protocol. The correctness of mutual authentication is proven in section 7, and section 8 concludes the paper.

2. SECURITY IN IOT ENVIRONMENT

The Internet of Things brings human life into a comfortable zone. It provides easy access to internet-using devices, smart phones, etc. Devices are connected through Wi-Fi, Bluetooth, radio frequency identification (RFID), etc. [41]. With the increase in different communication devices, security is a foremost concern because sensitive information is transferred using this network. Security threats and vulnerabilities are also increasing due to the increased number of embedded devices. This can compromise the privacy of the user. In addition, IoT environments have microprocessors, devices, sensors [42], and the devices are resource constraints. As a result, performance may vary due to the characteristics of IoT apparatus. The protocol should be developed by considering resource-constrained apparatus in the IoT environment [43].

One of the pressing concerns in IoT networks is to ensure the authenticity of the user and devices and key management among them. The IoT security requirement must provide the reliability of protection to the user [43]. Now, it becomes a challenge to deploy security in this environment. Cryptography plays an important role in ensuring security. User credentials are protected using the cryptographic technique. Identity management, key management, and user credential management are often maintained automatically, but it is still very challenging to deploy in the IoT environment [42].

A. Threat model

IoT devices are now used to operate many applications to provide better services. It is also used in many critical infrastructures, such as smart grids and healthcare organizations. In addition, IoT devices are generally portable in nature. Many security threats can hamper the activities of IoT environments. Therefore, we should be aware that it is not compromised by the adversary; otherwise, the loss encountered will be paramount. As devices use the internet to communicate with each other, they face the same security threats, which are as follows:

1) Privileged insider attack: One type of attack in which a user operates the activities of Gateway and has access to IoT devices. He can capture the information that an IoT device transmits to the gateway. In this way, he can compromise the operation and can do any modification to benefit from this environment.
2) Smart device/stolen mobile attack: The smart device is portable and can be lost or stolen. As these devices are tamper-resistant, if an intruder finds devices, the attackers can extract information from the stolen data using Power Analysis Attacks [44], [45]. From this information, intruders can extract more sensitive information that is communicated among different parties.
3) Denial of service attack: Denial of service attack occur where the operation of IoT devices is not available because of heavily consumed resources by intruders. People will not obtain services from this environment. As people are dependent on internet services, if it is unavailable, then human life will be hampered. It may cause different human life threat problems. Therefore, security against this type of attack is very important.
4) Password change attack: Password is an authentication parameter to prove a user's claim that he is a real user of the system. This password is needed to change after a certain period of time to make the system secure. If the password changing mechanism is not secure, then any adversary can change the password using a number of attempts and gain entry to the network. Once an opponent obtains entree to the system, he can modify any information that will reflect adverse effects on the system.

B. Security requirement

The security requirement is paramount when we develop any authentication protocol. Otherwise, the protocol will not be treated as secure. The essential requirements are discussed below.

1) Mutual authentication: Mutual authentication refers to the authentication where both entities are authenticated by each other. It is very important for any security protocol because the sender or receiver both needs confirmation that the message comes from a genuine source. Spoofing attacks can be protected using this parameter [42].
2) Confidentiality: Confidentiality means preventing unauthorized disclosure of information to unintended users. It is one of the basic security requirements for the IoT protocol because the IoT is used to support many applications, such as healthcare systems and smart grid systems. Therefore, if confidentiality is compromised, then much sensitive information will be lost. That is why we have to transmit the data securely. To achieve confidentiality, we can apply encryption with the aim of only genuine receivers to extract the information.

3) Availability: This term ensures that the services will remain available even if any disaster. People will receive services whenever they want. This requirement is very important because many sensitive applications are running using the IoT environment.
4) User anonymity: Anonymity means concealing the identity of users, such as doctors and patients. The importance of user privacy has been addressed in recent research papers. The user's identity is one of the most important personal information of the user because leaking this information can lead to the theft of that user's identity.

3. REVIEW OF AMIN ET AL.' S SCHEME

In [40], a patient monitoring system for a wireless medical sensor network was proposed. Their authentication and key negotiation scheme consist of five phases which we have discussed through sub-sections. In Table I, we described all the symbolizations used in the procedure.

TABLE I. SYMBOL USED IN PROCEDUE [40]

Symbol	Description
U_i	Medical professional
G_W	Gateway node
S_N_j	Sensor node
P_W_i	Password of U_i
U_ID_i	Identity of U_i
U_ID_{SNj}	Identity of S_N_j
S_K	Secret key of G_W
TU_ID_i	Unique Temporary Identity generated by G_W for U_i
RN_1	Random nonce created by U_i
RN_2	Random nonce created by G_W
RN_3	Random nonce created by S_N_j
$hf(.)$	Cryptographic one-way hash function
$\|\|$	Concatenation operation
$\oplus$	Bitwise XOR operation

A. Setup phase

In this segment, a long-term top-secret key S_K is generated by the registration center for gateway G_W and computes a secret key SK_{gw-snj} = hf($U\_ID_{SN_j}||S\_K$) for SN_j, where 1 ≤ j ≤ n, n denotes sensor node numbers. It also practices a lightweight cryptographic hash function which is prescribe as hf: $\{0,1\}^* \rightarrow \{0,1\}^l$, where l represents hf(.) output length.

B. Medical Professional registration phase

Here, medical professionals must be registered with G_W to provide health-care services. The steps are shown below:

Step 1: An individual user id U_ID_i and password P_W_i select by U_i, then apply HP_W_i = hf(U_ID_i $\oplus$P_W$_i$). then, user sends < U_ID_i , HP_W_i > to gateway G_W through TLS protocol.

Step 2: G_W calculates U_Reg_i = hf(U_ID_i || RN_i || HP_W_i), $AA_i = RN_i$ $\oplus$HP_W$_i$, AB_i = H(U_ID_i || RN_i || S_K), AC_i =AB_i $\oplus hf$(U_ID$_i$ $\oplus$RN$_i$ $\oplus$HP_W$_i$), $D_i = RN_i$ $\oplus hf$(TU_ID$_i$ || S_K), where RN_i and TU_ID_i are random numbers and temporary identities of U_i. G_W picks different TU_ID_i for each session to avoid traceability attacks.

Step 3: G_W uses a table to store < TU_ID_i , D_i > for future her use and forwards < TU_ID_i, U_Reg_i, AA_i, AC_i, hf(.) > to U_i. Then U_i stores < TU_ID_i, U_Reg_i, AA_i, AC_i, hf(.) > to user device after getting from G_W.

C. Patient registration phase

This stage is corresponding to Wu et. al [15] proposed phase with a similar name.

D. Login and authentication phase

At this stage, session key and mutual authentication discussions occur among the candidates engaged. The steps are described below:

Step 1: U_i enters U_ID_i and passwords P_W_i into smart device. Then, it computes $HP\_W_i^*$ = hf(U_ID_i $\oplus$P_W$_i$), RN_i =AA_i $\oplus$HP_W$_i^*$, $U\_Reg_i^*$= hf($U\_ID_i||RN_i^*||$ $HP\_W_i^*$). Then, it compares whether $U\_Reg_i^*$?= U_Reg_i. The smart device rejects the login invitation when input password is not same, else, it goes to the subsequent stage.

Step 2: It generates a arbitrary nonce RN_i and computes AB_i^*= AC_i $\oplus hf$(U_ID$_i$ $\oplus$RN$_i^*$|| HP_W_i *), CID_i =U_ID_i $\oplus hf$(TU_ID$_i$ || RN_i^*|| T_1), UM_1 = hf(U_ID_i|| $AB_i^*||RN_i||T_1$), UM_2 = hf(RN_i || T_1)$\oplus$RN$_i$. Then, sends < TU_ID_i, $U\_ID_{SN_j}$, CID_i, UM_1, UM_2, T_1 > to G_W over a doubtful network.

Step 3 : G_W searches the table TU_ID_i to retrieve U_ID_i and computes RN_i^*=U_ID_i $\oplus hf$(TU_ID$_i$ || S_K), $U\_ID_i^*$ = $CID_i \oplus hf$(TU_ID$_i$ ||$RN_i^*||T_1$), AB_i^*= hf($U\_ID_i^*||RN_i^*||S\_K$), RN_i^* = $UM_2\oplus$ hf($RN_i^*||T_1$), UM_1 = hf ($U\_ID_i^*$|| AB_i^* || RN_i^*|| T_1). Now, G_W verifies whether UM_1^* ?= UM_1. If UM_1^* ? = UM_1 is true, then G_W believes that U_i sent an authentic message, Otherwise stop the continuation.

Step 4: Subsequently scrutinizing the authenticity of U_i, G_W produces a arbitrary number RN_2 and computes SK_{gw-snj}= hf($U\_ID_{SN_j}$ || S_K), UM_3 = hf(hf(U_ID_i|| RN_i^*|| RN_2)|| 1)||SK_{gw-snj}|| RN_2), UM_4 = hf($U\_ID_i||RN_i||RN_2$)$\oplus$SK$_{gw-snj}$, UM_5 = RN_2 $\oplus hf$(SK$_{gw-snj}$). Then, G_W sends < UM_3, UM_4, UM_5 > to S_N_j through an insecure channel.

Step 5: S_N_j computes RN_2'=UM_5 $\oplus hf$(SK$_{gw-snj}$), UM_6' =UM_4 $\oplus$SK$_{gw-snj}$, UM_3' = hf(hf(UM_6' || 1)|| SK_{gw-snj}|| RN_2') and verifies whether UM_3' ?=UM_3 . If it is correct, S_N_j generates a random nonce RN_3 and computes SK

= hf(UM'_6 || RN_2|| RN_3), UM_7 = hf(SK || RN_3|| SK_{gw-snj}), UM_8 = hf(RN_2) ⊕RN$_3$. Finally, S_N_j sends < UM_7, UM_8 > to G_W through an insecure network.

Step 6: After receiving < UM_7, UM_8 >, G_W calculates RN'_3=UM_8 ⊕hf(RN$_2$), SK' = hf(U_ID_i ||RN_i || RN_2) || RN_2|| RN'_3), UM'_7 = hf(SK' || RN'_3|| SK_{gw-snj}) and verifies whether UM'_7 ?=UM_7 holds. If it is true, then G_W generates a unique identity $TU\_ID'_i$ (≠ TU_ID_i) and then calculates UM_9 =RN_2 ⊕hf(U_ID$_i$|| RN_i), UM_{10} = hf(U_ID_i|| SK' || RN'_3), and UM_{11} =$TU\_ID'_i$ ⊕hf(RN$_2$ ⊕RN$_3$). Then, G_W forwards < UM_8, UM_9, UM_{10}, UM_{11} > to U_i over a doubtful network.

Step 7: After getting < UM_8, UM_9, UM_{10}, UM_{11} >, U_i calculates RN^*_2 =UM_9 ⊕hf(U_ID$_i$|| RN_i), RN^*_3=UM_8 ⊕hf(RN$^*_2$), $TU\_ID'_i$ =UM_{11} ⊕hf(RN$^*_2$⊕RN$^*_3$), SK^* = hf(hf(U_ID_i|| RN_i || RN^*_2) || RN^*_2|| RN^*_3), UM^*_{10}= hf(U_ID_i||SK^* || RN^*_3). Now checks whether UM^*_{10} ? =UM^*_{10} holds. If it corrects, then U_i assumes that < UM_8, UM_9, UM_{10}, UM_{11} > is logical and G_W receives a confirmation. The mobile device then substitutes its old TU_ID_i with a new $TU\_ID'_i$. Similarly, the gateway computes the new value D'_i =RN_i ⊕hf(TU_ID'$_i$ ||S_K) and exchanges < TU_ID_i, D_i > with the new < $TU\_ID'_i$, D'_i >.

E. *Password change phase*

There is a detailed discussion at this stage on how to update passwords regularly.

Step 1: In the mobile device, U_i inputs U_ID_i and P_W_i. Then, it performs $HP\_W^*_i$ = hf(U_ID_i ⊕P_W$_i$), RN^*_i = AA_i ⊕HP_W$^*_i$, $U\_Reg^*_i$= hf(U_ID_i|| RN^*_i|| $HP\_W^*_i$) and checks whether $U\_Reg^*_i$? =U_Reg_i is correct or not. When the condition is incorrect, the password modification procedure will be canceled otherwise it will proceed to the subsequent step.

Step 2: Then the device requested a new password for the U_i after verifying the validity of the U_i.

Step 3: When U_i enters PW^{new}_i (original key), then it calculates HPW^{new}_i = hf(U_ID_i ⊕PW$^{new}_i$), Reg^{new}_i = hf(U_ID_i||RN^*_i|| HPW^{new}_i), A^{new}_i =RN^*_i ⊕HPW$^{new}_i$, AB_i= hf(U_ID_i|| RN_i ||S_K), C^{new}_i = A^{new}_i ⊕hf(U_ID$_i$ ⊕RN$^*_i$ ⊕HPW$^{new}_i$). Finally, it drops < U_Reg_i, AA_i, AC_i > and stores < Reg^{new}_i, A^{new}_i, C^{new}_i > into the mobile device.

4. Amin et al.'s Cryptanalysis protocol

Here, we demonstrate the security error of [40]. They claimed that their protocol [40] preserves user obscurity, which is the most significant security property in medical systems. Although, we have shown that they have failed to uphold it. We have observed that this procedure is penetrable to stolen mobile device attacks and privileged insider attacks; as a result, it also faces denial of service attacks. It also contains an error in the password change stage. A detailed explanation is given below:

A. *Privileged person attack*

In the medical recording stage of the procedure [40], user U_i sends < U_ID_i, HP_W_i > to G_W. Assume an insider who is a privileged user plays the role of an attacker. Thus, he can know the information U_ID_i and HP_W_i where HP_W_i = hf(U_ID_i⊕P_W$_i$). From this material, the invader can derive the password by executing the subsequent stages.

Step 1: Guess $P\_W^*_i$

Step 2: calculates $HP\_W^*_i$= hf(U_ID_i ⊕P_W$^*_i$). If $HP\_W^*_i$ matches HP_W_i, then the assumed $P\_W^*_i$ is the correct password. Therefore, this protocol has failed to protect against attacks against privileged internal users.

B. *Flaw in password change phase*

Suppose that the attacker knows the information U_ID_i and HP_W_i and derives P_W_i from this information. Assume that the insider attacker has stolen the smart device and extract all the information < TU_ID_i, U_Reg_i, AA_i, AC_i, hf(.) > using a power analysis attack [44], [45]. Using AA_i, he can calculate RN^*_i = AA_i ⊕HP_W$_i$ and $U\_Reg^*_i$ = hf(U_ID_i || RN^*_i || HP_W_i). If $U\_Reg^*_i$?=U_Reg_i holds, then it send a request to user U_i to enter a new password. Therefore, an attacker can initiate a new password. He can choose his own password $P\_W^*_i$ and consequently controls the mobile device with his own information.

TABLE II. SYMBOL USED IN THE PROPOSED PROCEDUE

Symbol	Description
U_i	Medical professional
GTW	Gateway node
SN	Sensor node
PW_u	Password of U_i
ID_u	Identity of U_i
ID_{gtw}	Identity of gateway node
K_u	Random nonce selected by U_i
SK_{gu}	Secret shared key between GTW and U_i
SK_{gns}	Secret shared key between GTW and SN
RN_u	Random nonce generated by GTW
RN_1	Random nonce created by U_i
RN_2	Random nonce created by GTW
RN_3	Random nonce created by SN
$hf(.)$	Cryptographic one-way hash function
||	Concatenation operation
⊕	Bitwise XOR operation

C. *Denial of service attack*

The attacker can initiate the password change phase and choose a new password. As a result, the original user cannot login into the system. This causes denial of service scenarios for authorized users.

D. Fails to preserve user anonymity

As this protocol transmits medical professionals' identity U_ID_i and sensors identity $U\_ID_{SN_j}$ clear text over an insecure channel, their identity can be exposed by hacker. This will fail to preserve user anonymity.

E. Stolen mobile device attack

User U_i stores $< TU\_ID_i, U\_Reg_i, AA_i, AC_i$, hf(.) $>$ to mobile devices. An attacker can extract all the data using a power analysis attack [44], [45] when the device is stolen. This information can be used to point the flaw in the password modification stage.

5. Proposed protocol

User anonymity and mutual authentication are immensely emergent for WMSNs. In this section, we have proposed an enhanced protocol to retreat the security defects remaining in [40] by introducing masked identity and hash function-based mutual authentication. Analogous to the protocol in [40], our protocol uses five phases: as Amin et. al. The explicit representation of the proposed protocol is described in Table II.

A. Setup

Initially, the recording center is a trusted unit in the system. It generates a secret shared key SK_gu for GTW and U. GTW and SN use SK_{gsn} shared key. RC uses a one hash function hf(.) where hf: $\{0, 1\} * \rightarrow \{0, 1\}l$, where l represents hf(.) output length.

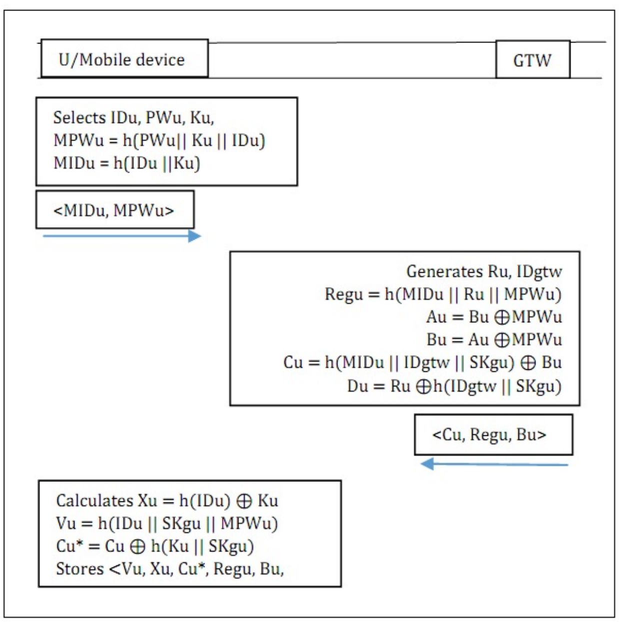

Figure 2. Medical professional registration phase

B. Medical professional registration stage

Health professional U_i first needs to register him/herself in the gateway to provide medical services to the patient. This phase is described in Figure 2. In this stage, U_i and GTW execute the following steps.

Step 1: U_i chooses an identity ID_u, password PW_u and a arbitrary nonce K_u. Then, MPW_u = hf($PW_u \| K_u \| ID_u$) and MID_u = hf($ID_u \| K_u$) are calculated. Now U_i sends $< MID_u, MPW_u >$ to GTW securely.

Step 2: On receiving $< MID_u, MPW_u >$, GTW selects a random number R_u . GTW calculates Reg_u = hf($MID_u \parallel RN_u \parallel MPW_u$), $A_u = RN_u \oplus \mathrm{MID}_u$, $B_u = A_u \oplus \mathrm{MPW}_u$, C_u = hf($MID_u \parallel ID_{GTW} \| SK_{gu}$) $\oplus \mathrm{B}_u$ and $D_u = RN_u \oplus hf(\mathrm{ID}_{GTW} \| SK_{gu}$). Then, he/she sends $< C_u, Reg_u, B_u >$ to U.S.

Step 3: Subsequently getting the information, U_i again calculates X_u = hf(ID_u) $\oplus \mathrm{K}_u$, V_u = hf($ID_u \| SK_{gu} \| MPW_u$) and $C^*_u = C_u \oplus hf(\mathrm{K}_u \parallel SK_{gu}$) and stores $< V_u, X_u, C^*_u, Reg_u$, hf(.) $>$into the mobile device.

C. Patient registration phase

This stage is similar like the [15] protocol. The steps are described below:

Step 1: The candidate first enters his/her name and sends to the registration point. The registration point picks the accurate detecting device and entitles a medical professional.

Step 2: At last, patient recognition and medical sensor data sent by the registration center to the mentioned professional.

D. Login and authentication phase

At this stage, session key and mutual authentication agreement among the parties involved in this procedure is achieved. The steps are depicted below:

Step 1: U_i inputs its uniqueness ID_u and password PW_u to the mobile. Following that, it measures $K^*_u = X_u \oplus hf(\mathrm{ID}_u)$, MID_u = hf($ID_u \parallel K^*_u$), MPW_u = hf($ID_u \parallel K^*_u \| PW_u$). It also calculates $A^*_u = B_u \oplus \mathrm{MPW}^*_u$, $RN^*_u = A^*_u \oplus \mathrm{MID}^*_u$, Reg^*_u = hf($MID^*_u \parallel RN^*_u \parallel MPW^*_u$) and V^*_u = hf($ID_u \parallel SK_{gu} \parallel MPW^*_u$). If Reg^*_u matches Reg_u and V^*_u matches V_u, then U_i inputs correct ID and password. Then, it generates RN_1 and calculates $CID_U = ID_u \oplus hf(\mathrm{RN}^*_u \parallel T_1$), $E_u = X_u \oplus hf(\mathrm{ID}_u \parallel RN^*_u \parallel SK_{gu}$), UM_1= hf($ID_u \| X_u \parallel RN_1 \| T_1$) and $UM_2 = RN_1 \oplus hf(\mathrm{RN}^*_u \parallel T_1)$. Then, it forwards the information $< CID_U, UM_1, UM_2, T_1 >$ to GTW.

Step 2: After receiving the information, GTW compares the validity of timestamp T_1 by $|T_1 - T| < \Delta T$. If the time to receive the message is fewer than the time break for the communication delay ΔT, the message has not been captured by the invader. GTW then computes $RN^*_u = D_u \oplus hf(\mathrm{ID}_{GTW} \| S\_K$), $ID_u = CID_U \oplus hf(\mathrm{RN}^*_u \parallel T_1$), $RN_1 = UM_2 \oplus hf(\mathrm{RN}^*_u \parallel T_1$),$X_u = E_u \oplus hf(\mathrm{ID}_u \parallel RN^*_u \parallel SK_{gu}$), UM^*_1= hf($ID_u \| X_u \parallel RN_1 \| T_1$). Then, GTW verifies whether $UM^*_1 ?= UM_1$ holds. If it holds, then GTW come to the conclusion that U_i sent UM_1 authentic message; else, it terminates the session. If the condition holds, GTW generates RN_2 and computes UM_3= hf($RN_2 \| T_2 \parallel SK_{gsn}$),

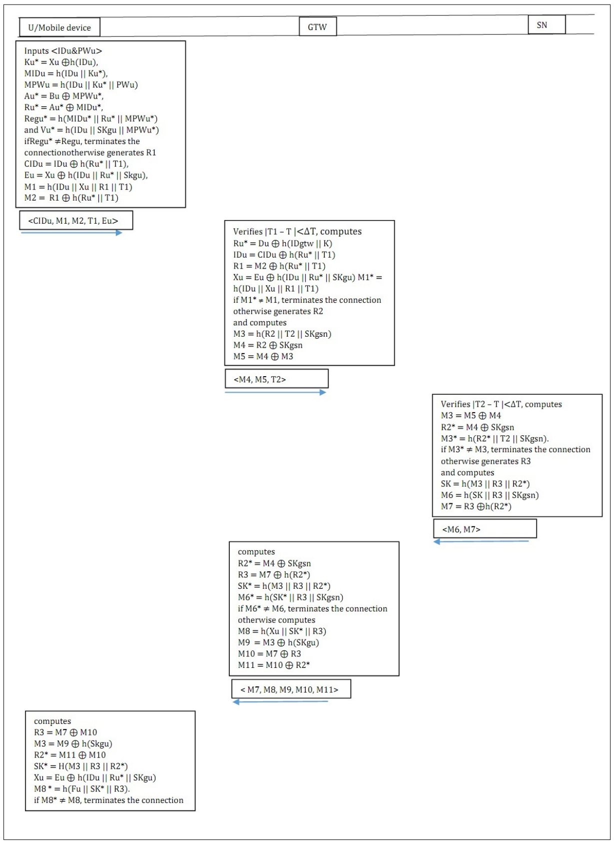

Figure 3. Login and authentication phase

UM_4= RN_2 $\oplus SK_{gsn}$ and UM_5= UM_4 $\oplus UM_3$. Then, sends the information < UM_4, UM_5, T_2 > to SN sensor.

Step 3: Upon getting < UM_4, UM_5, T_2 > SN authenticates $|T_2 - T| < \Delta T$. If it holds, then the message has not been intercepted by the intruder. Now SN calculates $UM3$= $UM_5 \oplus UM_4$, RN_2^*= $UM_4 \oplus SK_{gsn}$, UM_3^* = hf($RN_2^* \|$ T_2 $\| SK_{gsn}$). Then, SN proves the equivalence of UM_3^* with UM_3. If both are the same, SN produces an arbitrary number RN_3 and calculates SK= hf($UM_3 \|$ $RN_3 \|$ RN_2^*), UM_6 = hf($SK \|$ $RN_3 \|$ SK_{gsn}) and UM_7= $RN_3 \oplus hf(RN_2^*)$. Now SN forwards < UM_6, UM_7 > to GTW.

Step 4: After receiving the information, SN computes RN_2^*= UM_4 $\oplus SK_{gsn}$, RN_3= UM_7 $\oplus hf(RN_2^*)$, SK^* = hf($UM_3 \|$ $RN_3 \|$ RN_2^*), UM_6^*= hf(SK^* $\|$ $RN_3 \|$ SK_{gsn}). Now, SN checks whether UM_6^* equals UM_6. If both are equal, then it computes UM_8 = hf($X_u \|$ $SK^* \|$ RN_3), UM_9= UM_3 $\oplus hf(SK_{gu})$, UM_{10}= UM_7 $\oplus RN_3$ and UM_{11}= $UM_{10} \oplus RN_2^*$. Finally, it sends < UM_7, UM_8, UM_9, UM_{10}, UM_{11} > to U.S.

Step 5: After obtaining the information, GTW calculates RN_3= UM_7 $\oplus UM_{10}$, UM_3= $UM_3(SK_{gu}$), RN_2^*= $UM_{11} \oplus UM_{10}$, SK^* = H($UM_3 \|$ $RN_3 \|$ RN_2^*), X_u = $E_u(ID_u$ $\|$ RN_u^* $\|$ SK_{gu}) and UM_8^*= hf($X_u \|$ SK^* $\|$ RN_3). Then, GTW checks UM_8^* ?= UM_8. If it matches, then UM_8 is sent by GTW.

Figure 3 shows the explanation of this segment.

E. *Password change stage*

In this stage allows users to change the old password with updated password. The steps are described below:

Step 1: U_i enters ID_u and password PW_u into the smart device.

Step 2: It computes K_u^* =X_u $\oplus hf(ID_u)$, MID_u = hf(ID_u $\|$ K_u^*), MPW_u = hf(ID_u $\|$ K_u^* $\|$ PW_u). It also calculates A_u^* =B_u $\oplus MPW_u^*$, RN_u^* =A_u^* $\oplus MID_u^*$, Reg_u^* = hf(MID_u^* $\|$ RN_u^* $\| MPW_u^*$). If Reg_u^* matches Reg_u and V_u^* matches V_u, then U_i enters accurate ID and password. Then, it requests for a latest password.

Step 3: user U_i inputs the latest password PW_u^{new}.

Step 4: The mobile device calculates K_u^{new} =X_u $\oplus hf(ID_u$

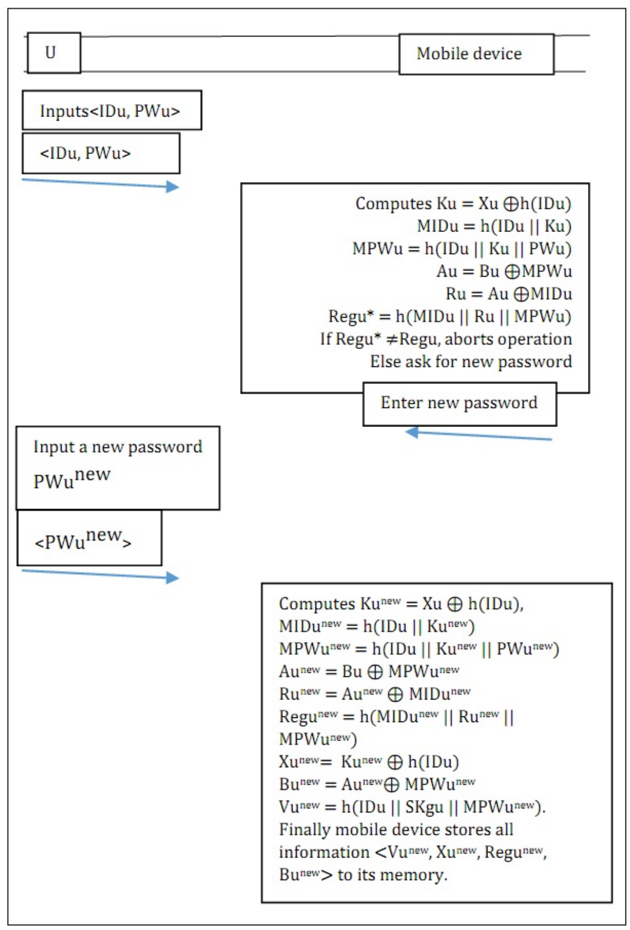

Figure 4. Password change phase

), MID_u^{new}=hf(ID_u ∥ K_u^{new}), MPW_u^{new} = hf(ID_u ∥ K_u^{new}∥ PW_u^{new}). It also calculates A_u^{new} = B_u ⊕MPW$_u^{new}$, RN_u^{new}= A_u^{new} ⊕MID$_u^{new}$, Reg_u^{new} = hf(MID_u^{new}∥ RN_u^{new}∥ MPW_u^{new}), X_u^{new}= K_u^{new} ⊕hf(ID$_u$), B_u^{new}= A_u^{new} ⊕MPW$_u^{new}$ and V_u^{new}= hf(ID_u ∥ SK_{gu} ∥ MPW_u^{new}). Finally, the mobile device stores all information < V_u^{new}, X_u^{new}, Reg_u^{new}, B_u^{new} > to its memory. This phase is explained in Figure 4.

6. Security analysis and performance of the proposed protocol

In this segment, we have performed an informal security investigation of this procedure. This protocol protects privileged insider attacks and stolen smart device attacks. It preserves user anonymity and achieves mutual authentication. It also presents a strong password change phase. It reduces the communication cost between the sensor and medical professional. The detailed description is as follows:

A. *Privileged insider attack*

This protocol is resistant to privileged insider attacks. ID_u and PW_u are never sent clear text in this protocol. Therefore, the attacker cannot guess the password. Assume that the attacker knows MID_u and MPW_u. To presumption the password invader needs to know ID_u and K_u. K_u is a arbitrary number created by the user and only known to him. K_u is also hidden inside X_u, and ID_u is never sent clear text in the communication channel. Therefore, even privileged insiders are not able to know the password.

B. *Stolen mobile device attack*

User U_i stores < V_u, X_u, C_u^*, Reg_u, B_u, hf(.) > to mobile devices. With this information, attacker cannot extract other information to launch another attack using a power analysis attack [44], [45], such as password change or denial of service attack.

C. *Strong password change stage*

The password change stage is well protected in this procedure. As an attacker, even a privileged insider does not know the password, so he cannot initiate the password change phase.

D. *Denial of service attack*

As the attacker cannot initiate the password change phase, there is no option of denial-of-service attack by the invader.

E. *Achievement of mutual authentication*

This protocol achieves mutual authentication in the sign in and validation stage. Each participant verifies the source of the message so that U_i, GTW and SN authenticate each other before exchanging information.

F. *Replay attack*

This protocol involves a timestamp in the sign in and authentication stage and verifies the freshness of each message on every communication. It also authenticates each other before establishing any session. Therefore, this protocol is resistant to replay attacks.

G. *Anonymity preservation*

This protocol preserves user anonymity because it uses masked identity MID_u and masked password MPW_u. Identity ID_u is never sent clear text throughout the communication. Therefore, it protects the disclosure of user identity.

H. *Increase in sensor lifetime*

The proposed protocol architecture increases the lifetime of the sensor node by introducing a gateway between the communication of the sensor node and the medical profession. Direct communication incurs higher communication costs [1], [14], [15]. Therefore, we have modified our architecture and introduced a gateway between the sensor node and medical professional so that information is exchanged through the gateway.

7. Correctness of authentication using the BAN logic model

Burrows–Abadi–Needham logic (also known as BAN logic) has some set of guidelines to verify the source of message, genuineness of origin, and freshness of the authentication protocol. The model is described in [46]. We have used this BAN rule to verify our authentication protocol. Here are some basic points of the BAN model for better perception.

- **Keys**: Keys are used for encryption and decryption Principals: The person assigned to the protocol or the agent as the program is called the principal.
- **Public keys**: It is similar to keys but has a pair of keys for encryption and decryption.
- **Nonce's**: It is part of message and not to be repeated.
- **Timestamp**: It is similar to nonce but less likely to happen again.

A. *Notation of BAN logic:*

The symbolization's for BAN rules are described below:

- $A_i \mid\equiv S_i$: A_i believes S_i as true.
- $A_i \triangleleft S_i$: A_i can see message S_i and read or repeat it.
- $A_i \sim S_i$: A_i once said the message S_i.
- $A_i \Rightarrow S_i$: A_i has authority over message S_i
- #(S_i): Message S_i is fresh
- (S_i, T_i): Rule S_i or T_i is one part of (S_i, T_i).
- < S_i > T_i: Rule S_i combined with rule T_i.
- $\{S_i\}$ K_i : Rule S_i is encrypted under the key K_i .
- (S_i) K_i : Rule S_i is hashed with the key K_i .
- $A_i \xleftrightarrow{K_i} D_i$: A_i communicate with D_i using shared key K_i .

- $A_i \overset{S_i}{\rightleftharpoons} D_i$: Only A_i and D_i know the secret S_i.

B. BAN logic rules

The subsequent rules are used in BAN logic.

- **Message-meaning rule:** $\frac{A_i|\equiv A_i \overset{S_i}{\rightleftharpoons} D_i, A_i \triangleleft < S_i >_{K_i}}{A_i|\equiv D_i|\sim S_i}$
- **Freshness-conjuncatenation rule:** $\frac{A_i|\equiv \#(S_i)}{A_i|\equiv \#(S_i, Y)}$
- **Belief rule:** $\frac{A_i|\equiv (S_i), A_i|\equiv Y}{A_i|\equiv (S_i, Y)}$
- **Nonce-verification rule:** $\frac{A_i|\equiv \#(S_i), A_i|\equiv D_i|\sim S_i}{A_i|\equiv D_i|\equiv S_i}$
- **Jurisdiction rule:** $\frac{A_i|\equiv D_i \Rightarrow S_i, A_i|\equiv D_i|\equiv S_i}{A_i|\equiv S_i}$
- **Session key rule:** $\frac{A_i|\equiv (S_i), A_i|\equiv D_i|\equiv S_i}{A_i|\equiv A_i \overset{K_i}{\longleftrightarrow} D_i}$

Our proposed procedure should gratify the subsequent goals to prove its safety.

- **Goal 1:** $GL_i| \equiv GL_i \overset{Ki}{\longleftrightarrow} U\_i$
- **Goal 2:** $GL_i| \equiv GL_i \overset{Ki}{\longleftrightarrow} SN$
- **Goal 3:** $SN| \equiv SN \overset{Ki}{\longleftrightarrow} GL_i$
- **Goal 4:** $U\_i| \equiv U\_i \overset{Ki}{\longleftrightarrow} GL_i$

Perfect form: The standard version of the proposed procedure is given below.

- **UM1:** $U\_i \rightarrow GL_i : CID_{U\_i}, UM_1, UM_2, T_1, E_{U\_i}, ID_{SN} :< RN_1 >_{SKgu}$
- **UM2:** $GL_i \rightarrow SN : UM_4, UM_5, T_2, :< RN_2 >_{SKgsn}$
- **UM3:** $SN \rightarrow GL_i : UM_6, UM_7 :< RN_3 >_{SKgsn}$
- **UM4:** $GL_i \rightarrow U\_i : UM_7, UM_8, UM_9, UM_{10}, UM_{11}: < RN_1, RN_2 >_{SKgu}$

C. Initial assumption

The subsequent are primary conventions of the proposed procedure.

- **A1:** $U\_i| \equiv \#(RN_1, RN_2, RN_3)$
- **A2:** $GL_i| \equiv \#(RN_2, RN_1, RN_3)$
- **A3:** $SN| \equiv \#(RN_2, RN_3)$
- **B1:** $SN| \equiv GL_i \Rightarrow RN_2$
- **B2:** $GL_i| \equiv SN \Rightarrow RN_3$
- **B3:** $GL_i| \equiv U\_i \Rightarrow RN_1$
- **B4:** $U\_i| \equiv GL_i \Rightarrow (RN_2, RN_3)$
- **C1:** $U\_i| \equiv U\_i \overset{SK_{gu}}{\longleftrightarrow} GL_i$
- **C2:** $GL_i| \equiv GL_i \overset{SK_{gsn}}{\longleftrightarrow} SN$

Below is the proof of our protocol by achieving the above-mentioned goals

- UM_1: $U\_i \rightarrow GL_i : CID_U, UM_1, UM_2, T_1, E_u, ID_{SN}: < RN_1 > SK_{gu}$
- **Using the seeing formula**:
  S1: $GL_i \rightarrow CID_U, UM_1, UM_2, T_1, E_u, ID_{SN}: < RN_1 > SK_{gu}$
- **Using C1, S1 message-meaning formula**:
  S2: $GL_i| \equiv U\_i| \sim RN_1$
- **Using A2, S2 freshness conjuncatenation name verification formula**:
  S3: $GL_i| \equiv U\_i| \equiv RN_1$, where RN_1 is essential information to compute the session key.
- **Using the B3, S3 jurisdiction formula**:
  S4: $GL_i| \equiv RN_1$
- **Using A2, S3 session-key formula**:
  S5: $GL_i| \equiv GL_i \overset{SK\_i}{\longleftrightarrow} U\_i$ (*Goal* 1)
- UM_3: $SN \rightarrow GL_i : UM_6, UM_7 :< RN_3 >_{SKgsn}$
- **Using the seeing formula**:
  Q1: $SN \rightarrow GL_i : UM_6, UM_7 :< RN_3 >_{SKgsn}$
- **Using C2, Q1 and message-meaning formula**:
  Q2:$GL_i| \equiv GL_i| \sim RN_3$
- **Using A2, Q2 freshness conjuncatenation nonce authentication formula**:
  Q3:$GL_i| \equiv SN| \equiv RN_3$
- **Using B2, Q3 jurisdiction formula**:
  Q4:$GL_i| \equiv RN_3$
- **Using A2, Q3 session-key formula**:
  Q5:$GL_i| \equiv GL_i \overset{SK\_i}{\longleftrightarrow} SN$ (*Goal* 2)
- UM_2:$GL_i \rightarrow SN : UM_4, UM_5, T_2 :< RN_2 >_{SKgsn}$
- **Using the seeing formula**:
  V1: $SN \triangleleft UM_4, UM_5, T_2 :< RN_2 >_{SKgsn}$
- **Using C2, the V1 message-meaning formula**:
  V2: $SN| \equiv GL_i| \sim RN_2$
- **Using A3, V2 freshness conjuncatenation nonce verification formula**:
  V3: $SN| \equiv GL_i| \equiv RN_2$
- **Using B1, V3 jurisdiction formula**:
  V4: $SN| \equiv SN \overset{SK\_i}{\longleftrightarrow} GL_i$ (*Goal* 3)

- **Using A3, V3 session-key formula**:
  V5: $SN| \equiv SN \overset{SK\_i}{\longleftrightarrow} GL_i$ (*Goal* 3)
- UM_4: $U\_i \triangleleft UM_7, UM_8, UM_9, UM_{10}, UM_{11} :< RN_1, RN_2 >_{SKgu}$
- **Using the seeing formula**:
  W1: $U\_i \triangleleft UM_7, UM_8, UM_9, UM_{10}, UM_{11} :< RN_1, RN_2 >_{SKgu}$
- **Accordingly, C1, W1 message-meaning formula**:
  W2: $U\_i| \equiv GL_i| \sim (RN_2, RN_3)$
- **Using A1, W2 freshness conjuncatenation nonce verification formula**:
  W3: $U\_i| \equiv GL_i| \equiv (RN_2, RN_3)$
- **Using B4, W3 jurisdiction formula**:
  W4: $U\_i| \equiv (RN_2, RN_3)$
- **Using A1, W3 session-key formula**:
  W5: $U\_i| \equiv U\_i \overset{SK\_i}{\longleftrightarrow} GL_i$ (*Goal* 4)

Hence, we have achieved our goals, and it is proven that our procedure satisfies mutual authentication and session key agreement.

8. Conclusion

In this article, we rigorously studied the procedure described in [40] and found that their protocol is prone to different attacks, such as privileged insider attacks and stolen smart device attacks. It does not protect against denial-of-service attacks and does not disclose usernames. It also has flaws in the password change phase. Our endeavor is to remove the limitations of the protocol presented in [40]. We have proposed a masked identity and hash function-based protocol that fixes the referenced security issues. we have proven that our proposed security model contributes better results than the existing security model. An informal security investigation was performed, which express that our proposed security protocol is safe and appropriate for patient monitoring systems using WMSNs. In the future, we will implement it in a cloud environment.

References

[1] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, Feb. 2015. [Online]. Available: http://dx.doi.org/10.1007/s00530-013-0346-9

[2] Y. K. Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks," *IEEE Systems Journal*, pp. 1–12, 2018.

[3] L. X. Hung, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," *JNW*, vol. 6, pp. 355–364, 2011.

[4] F. Wu and L. Xu, "Security analysis and improvement of a privacy authentication scheme for telecare medical information systems," *J. Medical Systems*, vol. 37, no. 4, p. 9958, 2012.

[5] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 1, pp. 316–326, Jan 2014.

[6] P. Gope and T. Hwang, "Bsn-care: A secure iot-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, March 2016.

[7] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Security and Communication Networks*, vol. 9, no. 15, pp. 2643–2655, 2016. [Online]. Available: https://doi.org/10.1002/sec.1214

[8] M. J. Hossain, M. A. H. Wadud, and M. Alamin, "Hdm-chain: A secure blockchain-based healthcare data management framework to ensure privacy and security in the health unit," in *2021 5th International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, 2021.

[9] M. J. Hossain, M. A. H. Wadud, A. Rahman, J. Ferdous, M. S. Alam, T. M. Amir Ul Haque Bhuiyan, and M. F. Mridha, "A secured patient's online data monitoring through blockchain: An intelligent way to store lifetime medical records," in *2021 International Conference on Science Contemporary Technologies (ICSCT)*, 2021, pp. 1–6.

[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *Trans. Info. For. Sec.*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016. [Online]. Available: https://doi.org/10.1109/TIFS.2016.2590944

[11] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016. [Online]. Available: https://doi.org/10.1109/TPDS.2015.2506573

[12] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing." *IEICE Transactions*, vol. 98-B, no. 1, pp. 190–200, 2015. [Online]. Available: http://dblp.uni-trier.de/db/journals/ieicet/ieicet98b.htmlFuSLZS15

[13] K. Romer and F. Mattern, "The design space of wireless sensor networks," *Wireless Commun.*, vol. 11, no. 6, pp. 54–61, Dec. 2004. [Online]. Available: https://doi.org/10.1109/MWC.2004.1368897

[14] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-sap: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012. [Online]. Available: http://www.mdpi.com/1424-8220/12/2/1625

[15] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multimedia Syst.*, vol. 23, no. 2, pp. 195–205, 2017. [Online]. Available: https://doi.org/10.1007/s00530-015-0476-3

[16] M. A. H. Wadud, T. M. Amir-Ul-Haque Bhuiyan, M. A. Uddin, and M. M. Rahman, "A patient centric agent assisted private blockchain on hyperledger fabric for managing remote patient monitoring," in *2020 11th International Conference on Electrical and Computer Engineering (ICECE)*, 2020, pp. 194–197.

[17] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks," *Ad Hoc Netw.*, vol. 27, no. C, pp. 159–194, Apr. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2014.11.018

[18] T. Maitra, R. Amin, D. Giri, and P. D. Srivastava, "An efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card," *I. J. Network Security*, vol. 18, no. 3, pp. 553–564, 2016. [Online]. Available: http://ijns.femto.com.tw/contents/ijns-v18-n3/ijns-2016-v18-n3-p553-564.pdf

[19] C. Li, "A secure chaotic maps-based privacy-protection scheme for multi-server environments," *Security and Communication Networks*, vol. 9, no. 14, pp. 2276–2290, 2016.

[20] M.-L. Messai, H. Seba, and M. Aliouat, "A lightweight key management scheme for wireless sensor networks," *J. Supercomput.*, vol. 71, no. 12, pp. 4400–4422, Dec. 2015. [Online]. Available: https://doi.org/10.1007/s11227-015-1534-5

[21] P. Rawat, K. D. Singh, J.-M. BONNIN, and H. Chaouchi, "Wireless sensor networks: a survey on recent developments and potential synergies," *Journal of Supercomputing*, p. ., Oct. 2013. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00955283

[22] P. Rawat, K. Deep Singh, H. Chaouchi, and J.-M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *The Journal of Supercomputing*, vol. 68, 04 2013.

[23] M. L. Das, "Two-factor user authentication in wireless sensor networks," *Trans. Wireless. Comm.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009. [Online]. Available: http://dx.doi.org/10.1109/TWC.2008.080128

[24] H. Huang, Y. Chang, and C. Liu, "Enhancement of two-factor user authentication in wireless sensor networks," in *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Oct 2010, pp. 27–30.

[25] S. G. Yoo, K. Y. Park, and J. Kim, "A security-performance-balanced user authentication scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 8, no. 3, p. 382810, 2012. [Online]. Available: https://doi.org/10.1155/2012/382810

[26] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, Jan. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2012.05.010

[27] C.-T. Li, C.-Y. Weng, and C.-C. Lee, "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks," in *Sensors*, 2013.

[28] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography," *J. Medical Systems*, vol. 39, no. 11, p. 180, 2015. [Online]. Available: https://doi.org/10.1007/s10916-015-0351-y

[29] S. H. Islam, R. Amin, G. Biswas, M. S. Farash, X. Li, and S. Kumari, "An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments," *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 3, pp. 311 – 324, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1319157815000828

[30] R. Amin and G. P. Biswas, "An improved RSA based user authentication and session key agreement protocol usable in TMIS," *J. Medical Systems*, vol. 39, no. 8, p. 79, 2015. [Online]. Available: https://doi.org/10.1007/s10916-015-0262-y

[31] R. Amin and G. Biswas, "Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment," *Wireless Personal Communications*, vol. 84, no. 1, pp. 439–462, 2015. [Online]. Available: https://doi.org/10.1007/s11277-015-2616-7

[32] S. H. Islam, "Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps," *Inf. Sci.*, vol. 312, no. C, pp. 104–130, Aug. 2015. [Online]. Available: https://doi.org/10.1016/j.ins.2015.03.050

[33] S. Kumari, M. K. Khan, X. Li, and F. Wu, "Design of a user anonymous password authentication scheme without smart card," *Int. J. Communication Systems*, vol. 29, no. 3, pp. 441–458, 2016. [Online]. Available: https://doi.org/10.1002/dac.2853

[34] S. Kumari, M. K. Khan, and X. Li, "An improved remote user authentication scheme with key agreement," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1997–2012, 2014. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2014.05.007

[35] S. Kumari and M. K. Khan, "More secure smart card-based remote user password authentication scheme with user anonymity," *Security and Communication Networks*, vol. 7, no. 11, pp. 2039–2053, 2014. [Online]. Available: https://doi.org/10.1002/sec.916

[36] S. Kumari, M. K. Gupta, M. K. Khan, and X. Li, "An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement," *Security and Communication Networks*, vol. 7, no. 11, pp. 1921–1932, 2014. [Online]. Available: https://doi.org/10.1002/sec.906

[37] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and X. Li, "Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems," *J. Medical Systems*, vol. 39, no. 11, pp. 140:1–140:21, 2015. [Online]. Available: https://doi.org/10.1007/s10916-015-0318-z

[38] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, no. C, pp. 263–277, Nov. 2015. [Online]. Available: https://doi.org/10.1016/j.ins.2015.02.010

[39] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1899–1933, 2017. [Online]. Available: https://doi.org/10.1007/s11277-016-3718-6

[40] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Comp. Syst.*, vol. 80, pp. 483–495, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2016.05.032

[41] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed

security model and threat taxonomy for the internet of things (iot)," in *Recent Trends in Network Security and Applications Communications in Computer and Information Science*, vol. 89. Germany: Springer, 2010, pp. 420–429.

[42] P. Kaur Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for iot services," *Journal of Information Security and Applications*, vol. 34, 01 2017.

[43] J. Lee and H. Kim, "Security and privacy challenges in the internet of things [security and privacy matters]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 134–136, July 2017.

[44] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '99. Berlin, Heidelberg: Springer-Verlag, 1999, pp. 388–397.

[45] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002. [Online]. Available: https://doi.org/10.1109/TC.2002.1004593

[46] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990. [Online]. Available: http://doi.acm.org/10.1145/77648.77649

M. F. Mridha (Senior Member, IEEE) received the Ph.D. degree in AI/ML from Jahangirnagar University, in 2017. He joined the Department of Computer Science and Engineering, Stamford University Bangladesh, in June 2007, as a Lecturer, where he was promoted a Senior Lecturer and an Assistant Professor, in October 2010 and October 2011, respectively. Then, he joined UAP, in May 2012, as an Assistant Professor. He is currently working as an associate professor with the Department of Computer Science and Engineering, Bangladesh University of Business and Technology. He also worked as a faculty member of the CSE Department, University of Asia Pacific, and as a graduate coordinator, from 2012 to 2019. His research experience, within both academia and industry, has resulted in over 80 journal and conference publications. His research interests include artificial intelligence (AI), machine learning, deep learning, big data analysis, and natural language processing (NLP). For more than ten years, he has been with the master's and undergraduate students, as a supervisor of their thesis work. He has served as a program committee member of several international conferences and workshops. He also served as an associate editor in several journals.

Md. Al Imran was born on 13th December 1987 in a city of Bangladesh named Khulna. He obtained his B.Sc. in Computer Science Engineering in 2010 from Khulna University of Engineering Technology, Khulna, Bangladesh and M.Sc. in Information Systems Security in 2017 from Bangladesh University of Professionals. He has published more than three research papers including international journal. Among them, one journal was published in Journal of Communication in 2011 and another is yet to publish in Journal of Telecommunication, Electronic and Computer Engineering. Two conference papers were published in 12th International Conference on Computer Information Technology, Dec. 2009 and 13th International Conference on Computer Information Technology, Dec. 2010, Dhaka, Bangladesh.

Md. Anwar Hussen Wadud is a lecturer in the Department of Computer Sciecne and Engineering, Bangladesh University of Business and Technology, Dhaka, Bangladesh. He received his B.Sc. and M.Sc. Engineering degree in CSE from Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. He participated in several ACM ICPC programming contests during his university life. He worked on several programming platforms such as Java Spring Hibernate, Android apps developments, Python NumPy, Keras etc. for big data and deep learning analysis in several software companies. His area of interest is Big Data Analysis, Deep Learning, Natural Language Processing, Internet of Things and Machine Learning.

MD. ABDUL HAMID has been working as a Professor with the Department of Information Technology, King Abdul Aziz University, Jeddah, Kingdom of Saudi Arabia Since 2019. His research interests include network/cyber-security, natural language processing, machine learning, wireless communications, and networking protocols. He was born in the village Sonatola, Pabna, Bangladesh. His education life spans over different countries wordwide. He received his B.E. degree in Computer and Information Engineering from International Islamic University Malaysia, from 1996 to 2001, and the combined master's-Ph.D. degree majoring in information communication from the Computer Engineering Department, Kyung Hee University, South Korea, in August 2009. He has been in the teaching profession throughout his life, which also spans over different parts of the globe. He was a lecturer with the Computer Science and Engineering Department, Asian University of Bangladesh, Dhaka, Bangladesh, from 2002 to 2004. He was an assistant professor with the Department of Information and Communications Engineering, Hankuk University of Foreign Studies, South Korea, from 2009 to 2012. He was an Assistant Professor with the Department of Computer Science and Engineering, Green University of Bangladesh, from 2012 to 2013. He was an Assistant Professor with the Department of Computer Engineering, Taibah University, Madinah, Saudi Arabia, from 2013 to 2016. He was an associate professor with the department of Computer Science, Faculty of Science and Information Technology, American International University Bangladesh, Dhaka, from 2016 to 2017. He was an associate professor and a professor with the department of Computer Science and Engineering, University of Asia Pacific, Dhaka, from 2017 to 2019.