Design a sturdy and secure authentication scheme capable of early detection of COVID-19 patients using WBANs

Abdulla J. Y. Aldarwish[1], Ali A. Yassin[1], Abdullah Mohammed Rashid[1], Hamid Ali Abed Alasadi[1], Aqeel Adel Yaseen[2], Eman Thabet Khalid[1]
[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[2]Basrah Education Directorate, Ministry of Education, Basrah, Iraq

Article Info

Article history:

Received Apr 27, 2021
Revised Jun 3, 2022
Accepted Jun 10, 2022

Keywords:

Authentication
AVISPA
COVID-19
Health care
Wireless body area networks

ABSTRACT

COVID-19 was first reported in China Wuhan and rapidly grown up to more than 58 countries based on the World Health Organization (WHO). Well ahead of any health emergency, the health care server has the ability to access these data via authorization and then s/he performs necessary actions. In order to protect medical data from malicious activities, authentication is the starting point for this. Authentication systems represent a network support factor to reduce ineffective users and radically eliminate phishing because authentication determines the identity of the real user. Many schemes and technologies have been suggested for authentication in wireless body area networks (WBANs). In this paper, we suggest a strong dynamic password authentication system for WBANs. We adopt a (different/new) way to calculate a password and make it coherent and dynamic for each login session. Our work also provides additional security properties to get rid of hub node impersonation attacks and resolve key escrow issues. Our scheme resist fishing attach which keep patient from any illegal change of drugs. By comparison, the proposed scheme is considered active and has strong security based on formal security analysis tools such as AVISPA.

Corresponding Author:

Abdulla J. Y. Aldarwish
Department of Computer Science, College of Education for Pure Sciences, University of Basrah
Basrah, Iraq
Email: abdullajas@uobasrah.edu.iq

1. INTRODUCTION

The World Health Organization (WHO) caught the first COVID-19 case in China Wuhan on the morning of 30 January 2020 [1]. From this date right the moment writing this paper the pandemic has spread to more than 75 countries (World Health Organization). The number of cases confirmed by corona virus was around 93000 offered the entire world by the end of February. This kind of disease is one of the most dangerous infectious due to the rapid spread and transmission of infection and because it not usually expected in a particular community geographical region, or time period. Therefore the world requires immediate action to prevent the pandemic at the community level [2], [3]. Information technology works hard to tackle this COVID-19 by developing several apps analyzing the patient data for pre prediction. The development in wireless communication technologies and information technology has affected all aspects of our daily life: scientific, social, health and industrial. In the era of innovative technology, cloud computing, internet of things (IoTs), and big data are available to people to benefit from their services and applications, for example, the need to go to the hospital and other medical care centers for regular medical examinations has diminished. Based on the medical care side, we note that there is advanced technology development in the health sector; as patients who suffer from such chronic diseases as cardiac arrest, but at the same time are physically capable to move, do not need to lie in hospitals for continuous monitoring [4], [5]. As a result, there has been a noticeable decrease in hospitalization due to this tremendous development in the health sector. Moreover, e-health services have become mobile and hence called mobile health (mHealth). A wireless body area network (WBAN) is a network of small biometric sensors which can wearable or implanted inside the human body, these sensors are suitable for collect vital signals from the body and connect with the personal device (smart mobile/PC) that responsible for interpreting the sensors' signals and transferring them to the authenticated server.

In order to take advantage of wireless sensor networks to monitor and improve people's health conditions, WBAN has emerged. It is also useful for monitoring elderly people who have chronic conditions. WBAN has the ability to monitor and check vital signs (such as high body temperatures) of healthy people in order to get rid of symptoms of diseases and avoid them in the future. Currently, the rapid technological development of WBAN makes it possible for people to benefit from e-health services anywhere in the world at any time [6], [7]. This type of network consists of a number of small and economical medical sensors, which can be implanted into, worn on the human's body such as accessories, or installed inside clothes. The medical sensors are characterized by being devices that have limited capabilities in terms of storage space, computability and battery usage. The medical sensors are connected through such short-range wireless communication equipment as Bluetooth and ZigBee. These networks need accessory devices that work as a gate-way such as a mobile phone or personal digital assistant (PDA), which collect data from medical sensors and redirect this information to an authenticated server via the Internet remotely, where data processing and analysis occur with the help of applications' software. Figure 1 explains the main architecture of WBAN. Additionally, WBAN works in an efficient and comfortable way for users with a 24-hour monitoring and follow-up system. Moreover, it can have several other uses such as the remote monitoring of critical conditions in the hospital as well as monitoring the health conditions of athletes [8], [9].

Researchers and those interested in the WBAN network expect a big revolution in the field of health care because of the huge potential of these networks, but at the same time they point to the need to pay attention to the security of WBAN that sends large amounts of personal data. Therefore, it is necessary to fortify and secure sensitive biomedical data transferred between parts of the network and data previously referred to. Any security breaches, such as an unauthorized change in the dose of the drug, can have a negative effect or lead to the patient's death. Patients do not wish their personal data to be disclosed or misused. Therefore, the WBAN must prevent the eavesdropping on and leak of patient's private information to neighboring networks. Authentication is an essential part of any network's security, and it also helps the network to reduce unwanted users and avoid many malicious security attacks on WBANs. The authentication in WBAN is necessary to prevent unauthorized users from access the system. It depends on two-factor used multi- layer authentication; the first layer is related with sensors side and personal device while the second one goes inside personal device and authenticated server. As well as, there are many scheme based on mutual authentication between personal device and authenticated server. So, our proposed scheme depends on multi-layer and mutual authentication between main components.

An attacker can eavesdrop on connections between network components. This eavesdropping can lead to a severe damage to the patient because the attacker can use the acquired data for various illegal purposes. Any hack of the health care system data will immediately affect the hosted patient life such us change the duration of drugs. Our main contributions to this paper are listed in the following points:

- The proposed scheme is protected against malicious impersonation such as insider, replay, hub node spoofing, key escrow, the tracing, and meet-in-the-middle (MITM) attacks. Our work provides by strong mutual authentication among users, medicalsensors , and the authenticated server.
- Our work has been validated by automated verification tool which is AVISP. These tools are used to ensure whether the exchanged information is honest, secure against well-known attacks such as eavesdropping.
- Practical experience results show that our solution to our proposal is easy to use, has fast response times and works well for wireless IoT devices.
- The current relevant approaches are compared with our proposed work and we have noticed that the proposed scheme has an advantage over theme in terms of computing cost, communication expenses, and numerous security tasks.
- Our scheme supports dynamic password authentication, which is more secure than fixed password. Our authentication solution ensures the privacy of user identity and provides long-term private keys distributed by a trusted third party.
- Providing multilayer authentication, first layer is providing mutual authentication between user and server, while the second layer providing a lightweight authentication scheme between sensor and user.

- In the field of health care, the method is designed to take care of patients with chronic diseases by observing them remotely without the need for hospitalization, and this results in reducing costs and improving the patient's health condition more quickly.
- Within the COVID-19 pandemic, the proposed work contributes to the expectation of patients with chronic disease patients by measuring their temperature, which is within the scope of the COVID-19 disease. Where the medical sensors send a signal to the personal device that interprets to expect this disease, and then it sends it to each of the patient's relatives and the medical care center to take the necessary measures.
- In the practicalure side, the proposed work can apply in the several healthcare institutes such ICU room, recovery room, and chronic disease room.

The paper is organized as follows: In section 2, we focus on relevant works. Section 3 explains the primitive tools used in the proposed scheme and briefly discusses the mathematical definitions required. In section 4, we afford an exhaustive description of the proposed work. In section 5, we analyses the security of the proposed scheme and evaluate the efficiency and security of our proposed scheme based on simulation tools and practical experience. In section 6, we conclude the paper.

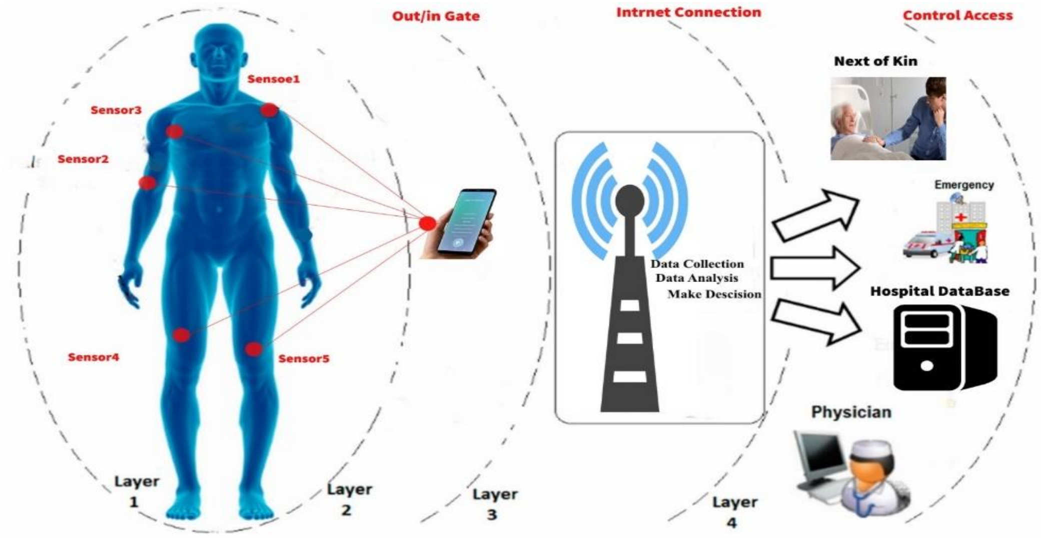


Figure 1. Organization of WBAN

2. RELATED WORKS

In the past few years, many researchers have suggested methods that contribute to improving the security behavior of authentication schemes with a high level of implementing time. There are several major exchange schemes using hard cryptography issues are distinguished by high computation requirements and identity loss [10], [11]. Furthermore, some schemes suffer from resisting familiar malicious attacks such as insider and replay.

Chatterjee *et al.* [12], presented an authentication scheme based on the ECC cryptography, which supports mutual authentication between the user, the base station, and the sensor. The scheme also allows adding a new node after the first design of the network. Lee *et al.* [13], suggested an efficient scheme for key management based on ECC cryptography to protect the patient’s health information. The researchers used the SIM card number of the patient as an identification number next to the private key. Eldefrawy *et al.* [14], suggested designing a protocol that supports adding new nodes and canceling nodes within the network. The proposed protocol based on RSA and diffie hellman ECC (DHECC) cryptosystems, and it provides security requirements.

Toorani [15] concluded that IEEE 802.15.6 has serious security problems based on security analysis performed on these protocols. Mohit *et al.* [16] offer a mutual authentication protocol that maintains anonymity for mobile users, which achieves anonymity with a smaller balance. Although their work can withstand many attacks, but it is susceptible to personal information disclosure attacks. Wazid *et al.* [17] propose authentication scheme using smart card in WBAN, which depends on symmetric encryption of information transmission via communication channel. Their works fails to resist tracing attack, insider user attack, and jamming attack. Ibrahim *et al.* [18] offer anonymous mutual authentication and a key agreement protocol based on simple cryptography alternatives like hash function and XOR process. However, it is suffered to resist malicious attacks such as jamming attack, hub node impersonation attack, and key escrow problem. Li *et al.* [19] presented mutual authentication protocol depending on low-entropy password. Their scheme can be applied to WBAN because it relies on an easy-to-remember password. Kompara *et al.* [20] suggested a mutual authentication scheme for a two-hop WBAN and an untraceable key establishing, with an emphasis on anonymity and a non-tracking feature. Liu *et al.* [21] proposed research paper for robust authentication scheme that depends on dynamic password and uses computation method to produce once password per login request.

In this paper, the proposed scheme distinguishes in many good metrics such as the immune against malicious attacks and uses a homomorphic encryption (Damgård, Geisler and Krøigaard method (DGK)) [22] and crypto hash function. This scheme includes low computational and communication costs and paid more attention in patient's healthcare compared to other related schemes. All of the previous researchers run their works but never consider the WBANs. We proposed new approach to tracking the patients any where any time no need to hosted them of special location (hospital). Our work pays more attention to keep the privacy of data transfer through the WBAN in duration of pandemic COVID-19. Our proposed work focuses on healthcare side and immunity against malicious attacks because the hackers can play bad role to change/ delay the transferred information of patients and then may be caused to death case.

3. CRYPTOGRAPHIC PRELIMINARIES AND SECURITY ISSUES

3.1. Damgård, geisler and krøigaard

DGK considers is type of homomorphic encryption Yassin *et al.* [23] and Damgård *et al.* [22] and was suited to work with the small plaintexts spaces and generate shorter ciphertext size compared with associated probabilistic encryption methods. For more detail, the public key consists of main parameters $(\mathrm{N}, \mathrm{g}, \mathrm{h}, \mathrm{u})$ and while the parameters $(\mathrm{p}, \mathrm{q}, \mathrm{v_p}, \mathrm{v_q})$ are connected with the private key. So, $N = p \times q$ refers to the ciphertext modulus of k-bits, p and q are two large primes, $\mathrm{u} \in \mathbb{Z}_u$ denotes to the plaintext, it is a small prime divisor of both $\mathrm{p} - 1$ and $\mathrm{q} - 1$. The contents of u are very small values, usually it is selected as the minimal prime greater than ℓ +2; where ℓ is number of bits in associated integers. The supplementary factors $\mathrm{v_p}$and $\mathrm{v_q}$ contain t-bit prime and $\mathrm{uv_p}|(\mathrm{p} - 1)$ and $\mathrm{uv_q}|(\mathrm{q} - 1)$. Factors k, t, and ℓ must accept $\mathrm{k} > \mathrm{t} > \ell$. Usually these values may be k=1024, t=160, and the range of ℓ from 8 to 32 bits. The items g, h $\in \mathbb{Z}_\mathrm{N}^*$ where g has command of $\mathrm{uv_p v_q}$ and h has mater of $\mathrm{v_p v_q}$. Looking at the message x $\in\mathbb{Z}_\mathrm{u}$, the result of encryption message [x] by DGK and it is computed as $[\mathrm{x}] = \mathrm{g}^\mathrm{x}.\mathrm{h}^\mathrm{r} \bmod \mathrm{N}$, so the value of r is selected integer number in 2.5t-bits. DGK considers as additively homomorphic where$[\mathrm{x}].[\mathrm{y}] = [\mathrm{x} + \mathrm{y}] \bmod \mathrm{N}$. The Impressive feature of DGK is that to detect whether x is zero and it is answer for verifying $\mathrm{x}^{\mathrm{v_p v_q}} \bmod \mathrm{N} = 1$. Moreover, since $\mathrm{u} < \mathrm{p}$ it is even adequate to verify $\mathrm{x}^{\mathrm{v_p v_q}} \bmod \mathrm{p} = 1$.

3.2. Crypto hash function

A cryptographic hash function takes an input such as text, numbers, file or a password and then produces a fixed-size string of bytes based on type of hash function (MD5, SHA-1). There are many names of string like message digest, checksum. The major utilize of this function is to validate the legitimacy of data. A hash function is a basic word that covers cryptographic hash functions along with other sorts of algorithms like cyclic redundancy checks Yassin *et al.* [23].

4. THE PROPOSED SCHEME

The main four phases of our scheme are setup and registration phase, login phase, mutual authentication phase, and healthcare phase. As well as, the entities of WBAN are legal user/ patient (P_i), an authenticated server (AS), the personal device (PD_i), and medical sensors ($MS_1, \dots\dots, MS_n$); where n is the number of sensors. Finally, a new patient needs to add the major containing the details of the patient, his relatives, and his doctors, which should be registered on the AS. Table 1 defines the symbols and their meanings used in this paper.

4.1. Setup and registration phase

The generating main parameters related by healthcare center as follows (see Subsection (3.1)). The public key is known as $(N_{P_i}, g_{P_i}, h_{P_i}, m_{P_i})$ while the parameters $(p_{P_i}, q_{P_i}, v_{p_{P_i}}, v_{q_{P_i}})$ are connected with the private key. These keys are linked with each user (P_i). Then, the healthcare center (HC) sends public and private keys to personal device (PD_i) and trust server (AS), respectively.

Table 1. Common symbols used

Symbol	Description
N_{P_i}	Homorphic modulus.
ℓ	Number of bits in compared integers.
K	The bit-length of N.
$N_{P_i}, g_{P_i}, h_{P_i}, m_{P_i}$	Public key.
$(p_{P_i}, q_{P_i}, v_{p_{P_i}}, v_{q_{P_i}})$	Private Key.
IDp_i, PWp	The identity of user (patient (P_i)).
$AIDp_i$, $APWp_i$	User’s anonymity.
HCR_i	Health Care Record of P_i.
AS	Authenticated Server.
HC	Healthcare center is responsible for generating and distributing public and private keys to patients and authenticated server.
MS	Medical Sensor.
ID_{MS_j}, PW_{MS_j}	The anonymity of MS.
$[m_{P_{i1}}]$, $[m_{P_{i2}}]$, $\mathrm{C}_{\mathrm{p_i}}$, $C_{p_i}{}'$	Encryption messages by DGK homorphic.

4.1.1. User registration

User (P_i) registers his main information in AS by performing the following steps:

a) P_i chooses his identity (IDp_i) and password (PWp_i) by using application attached on his personal device (PD_i). Also, P_i records information about his doctor and relatives (health care record (HCR_i)). HCR_i includes phone numbers of doctors and relatives, Name of patient, Pathological case, and others.

b) PD_i chooses a random number, $r_i \in \mathbb{Z}_{N_{P_i}}$, and computes the following anonymous parameters:

$$AIDp_i = h(IDp_i || r_i) \tag{1}$$

$$APWp_i = h(PWp_i || r_i) \tag{2}$$

c) PD_i submits $(AIDp_i, APWp_i)$ to AS.

d) AS verifies its database to check if P_i is previously registered. If so, AS terminates this phase. Otherwise, the AS adds a new patient’s record $(AIDp_i, APWp_i)$ in the main secure database.

4.1.2. MS_j registration

Based on the serial number (Se_{num_j}) related to each medical sensor and each user (P_i) has many medical sensors ($MS1$ ... MSm), the HC registers the MS_j as follows:

a) Calculate the identity of medical sensor $\left(ID_{MSj}\right)$:

$$ID_{MS_j} = Se_{num_j} \oplus g_{P_i} \oplus h_{P_i} \tag{3}$$

b) Choose a password (PW_{MS_j}) for medical sensors and then save and submit ($ID_{MS_j}, PW_{MS_j}, N_{P_i}, g_{P_i}$) to MS_j and PD_i, respectivally. Finally, the parameters (ID_{MS_j}, PW_{MS_j}) saves inside health record of P_i.

4.2. The login, mutual authentication, health care phases

4.2.1. Login and authentication, health care of medical sensor

The medical sensor (MS_j) is responsible for sending the examination signals to the personal device that determines the healthcare decision. Therefore, it is necessary to confirm the reliability of the sensor and according to the following:

a) MS_j generates integer random $r_i \in \mathbb{Z}_{N_{P_i}}$ and computes $PW_{MS_j}{}' = PW_{MS_j} \oplus r_i \oplus g_{P_i}$.

b) MS_j sends message *M1*($ID_{MS_j}, r_i, PW_{MS_j}{}'$) to PD_i.

c) After receiving the message *M1* from MS_j. The PD_i performs the following processes to verify the identity of the sensor.
   - Retrieves the main information of MS_j based on $ID_{MS_j}$and healthcare record of user (P_i).
   - Compare $PW_{MS_j}{}' - PW_{MS_j} \oplus r_i \oplus g_{P_i} == 0$; If the result is false then MS_j is not authenticated and terminates this phase. Otherwise; PD_i allows MS_j to sends its measurements and starts in the health care phase.

d) In health care phase MS_j.

The MS_j will send signals (Sg) to PD_i at periodic intervals that depend on the measured health condition of the patient. The personal device will perform the following operations:

a) Sending alert messages to the patient in the event that the received signal (Sg) exceeded the critical cases as shown in Figure 2.

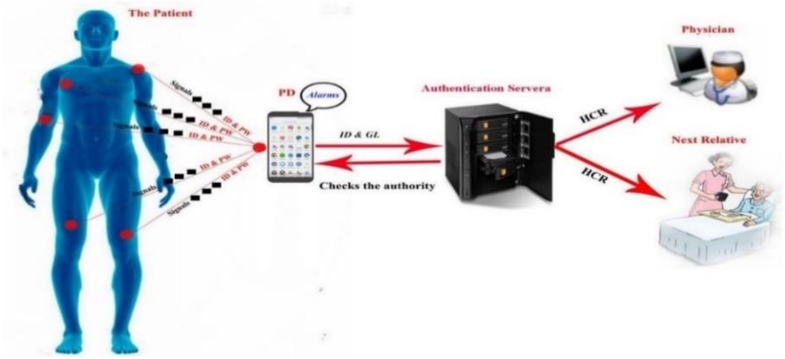


Figure 2. Health care phase in our proposed work

b) After a period of patient unresponsiveness and the persistence of critical cases, the personal device will send the patient's identity (IDp_i) and geographical location (GL_i) to AS. The authenticated server checks the authority of PD_i at first time in the next phases and then AS sends health care record HCR_i and GL_i to make the appropriate health decision for the patient. Critical cases are determined by relying on the type of the sensor, for example temperatures when it exceeds 38 are dangerous and must be treated.

c) Within the COVID-19 pandemic, PD_i pays more attention for dealing with the signals (Sg) received from MS_j, if Sg belongs to the critical cases of COVID-19 then PD_i sends very urgent warning messages to the patient's relatives and the medical care canter as shown in Figure 3.

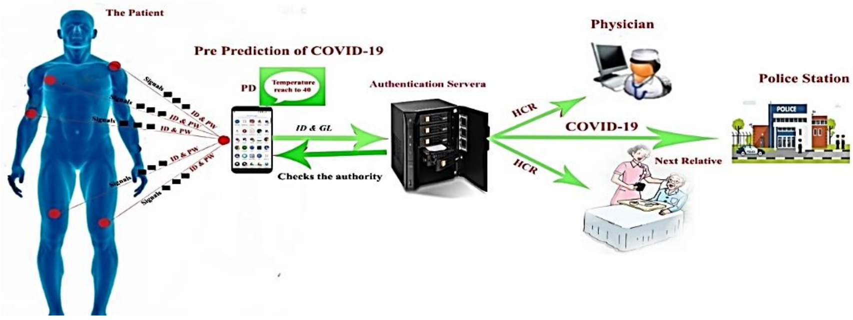


Figure 3. COVID-19 process in our proposed work

4.3. Login and authentication of personal device

At the moment when the patient does not respond to the notifications of the personal device (PD_i) that addresses the patient's relatives. Here you must achieve the following steps:

a) PD_i encrypts ($AIDp_i, APWp_i$) using DGK method; PD_i selects an integer random $r_i \in \mathbb{Z}_{N_{P_i}}$ and separates $APWp_i$ into two equal portions ($APWp_{i1}, APWp_{i2}$). Then, computes $[m_{P_{i1}}] = g^{APWp_{i1}} . h_{P_i}{}^{r_i} \; mod \; N_{P_i}$, $[m_{P_{i2}}] = g_{P_i}{}^{\mathrm{APWp_{i2}}} . h_{P_i}{}^{\mathrm{r_i}}$ mod N_{P_i}, and $\mathrm{C_{p_i}} = [\mathrm{m_{P_{i1}}}].[\mathrm{m_{P_{i2}}}]$.

b) PD_i sends $M2(AIDp_i, C_{p_i}, \; r_i)$ to AS.

c) After receiving the message ($M2$) from the patient's personal device (PD_i), AS performs the following operations:

- Check authority of PD_i by restoring its identity $AIDp_i{}'$ from server's database and then compare $AIDp_i$ with $AIDp_i{}'$. If the result is false, AS terminates phase. Otherwise, he applies an additively homomorphic property by computing $C_{p_i}{}' = [m_{P_{i1}} + m_{P_{i2}}] mod \; N_{P_i} = [APWp_i] mod N_{P_i} = (g_{P_i}{}^{APWp_i} . h_{P_i}{}^{r_i} \; mod \; N_{P_i}) mod \; N_{P_i}$.

- Compare $C_{p_i}{}'$ with C_{p_i}; if the values are not equal then AS finishes this process. Otherwise, AS computes $Ch = C_{p_i}{}' \oplus g_{P_i}$ and then sends Ch to PD_i.

d) PD_i ensures from authority of AS by comparing Ch with $C_{p_i} \oplus g_{P_i}$ and then sends (GL_i, Sg) to AS.

e) AS submits GL_i and warring message to doctor and relatives of patient to take the appropriate health aid.

5. SECURITY ANALYSIS AND EXPERIMENTAL RESULTS

5.1. Informal analysis

As mentioned in the creatine kinase (KC) threat model. Earlier publications over the last decade have shown in the related work section that a security proof suffers from an insufficient security model that fails to identify all of an attacker's true capabilities. Using the CK threat model, we show that the proposed system is safe in the following ways.

5.1.1. Providing agreement and freshness of session key

We notice the key agreement based on two folds. The first one is going in the side dialog between MS_i and the PD_i, the XOR operation plays a prominent role by creating the session key based on $(PW_{MS_j}, g_{P_i}, r_i)$. On the side of PD_i and AS, the transactions (g_{P_i}, h_{P_i}, r_i) mainly manage the public key based on the basic criteria of the DGK encryption method. Furthermore, including the random number r_i in the key management session in the login and authentication phases resulted in a key freshness feature.

5.1.2. Providing anonymous and untraceable features

Assume an attacker (Ā) has the ability to access messages exchanged among the basic components (MS_i, PD_i, AS). These messages (*M1*($ID_{MS_j}, r_i, PW_{MS_j}{}'$), *M2*($AIDp_i, C_{p_i}, \ r_i$), *Ch*) are verified in a highly confidential and anomaly manner and without being disclosed. The anonymous identification parameters are generated once due to the use of the random number r_i. As a result, hiding the tracking of these messages causes the attacker to fail to achieve his goals by clearing and following the messages exchanged between the main components.

5.1.3. Correctness

- The fast authentication of MS_i refers to correctness where $ID_{MS_j}, r_i, PW_{MS_j}{}'$ are calculated using r_i, g_{P_i}. Finally, the process of check the anonymous identity of the biometric sensor MS_i is correct: $PW_{MS_j}{}' - PW_{MS_j} \oplus r_i \oplus \ g_{P_i} = PW_{MS_j} \oplus r_i \oplus \ g_{P_i} - PW_{MS_j} \oplus r_i \oplus \ g_{P_i} = 0$
- The correctness of fast authentication of PD_i is proved as follows:

$$\begin{aligned} C_{p_i} &= [m_{P_{i1}}].[m_{P_{i2}}] \\ &= [m_{P_{i1}} + m_{P_{i2}}] mod\ N_{P_i} \\ &= [APWp_i] mod N_{P_i} = (g_{P_i}{}^{APWp_i}.h_{P_i}{}^{r_i}\ mod\ N_{P_i}) mod\ N_{P_i} = \ C_{p_i}{}' \end{aligned}$$

- In the another side, also the fast mutual authentication from AS to PD_i is correctness:

$$Ch = C_{p_i}{}' \oplus g_{P_i} = Ch'$$

Finally, we notice the fast mutual authentication has verified between PD_i and AS.

5.1.4. Resistant to eavesdropping, MITM, traffic attacks, and intruder detection

In this type of malicious attack, the attacker's function (Ā) is to monitor the messages exchanged between the main components (BS_i, PD_i, AS) of the communication environment and then extract information to carry out the attack. The messages exchanged between the main parties in the proposed work are immune from these attacks. The messages are as follows:

a) MS_j submits message *M1*($ID_{MS_j}, r_i, PW_{MS_j}{}'$) to PD_i.

b) PD_i replies message *M2*($AIDp_i, C_{p_i}, \ r_i$) to *AS*.

c) AS sends challenge Ch to PD_i.

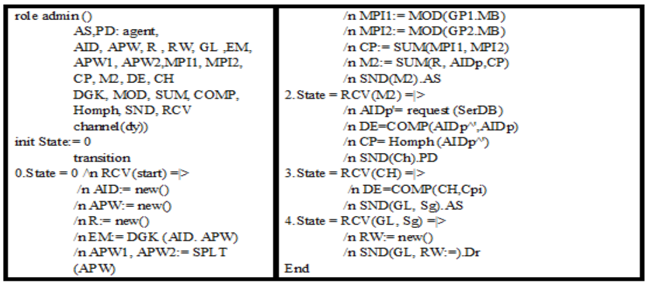
The manipulation of the attacker will not work, as the messages above are used only once. Any modification of messages will help the system to identify the source of the manipulation and thus detect the identity of the intruder.

5.1.5. Protected from a Forged MS_i & PD_i

The attacker (Ā) fails to impersonate the medical sensor MS_i and the personal device PD_i. Because it does not have the security factors and keys ($Se_{num_j}, g_{P_i}, h_{P_i}, PW_{MS_j}, AIDp_i, APWp_i, HCR_i$). That help him to build reliable and secure messages to the rest of the network.

5.2. Simulation

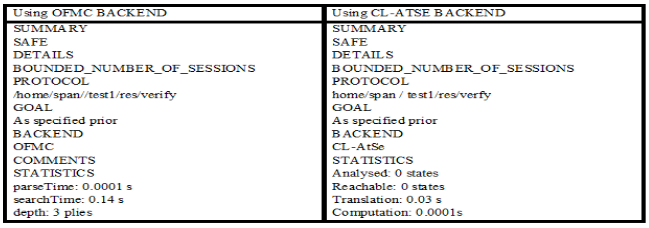
AVISPA explained as push-button tool which is the most recent techniques employed for examine the proposed schemes, protocols, and frameworks security by applied different kinds of attacks and find the final security weaknesses report. AVISPA protocol was implemented in the high-level protocol specification language (HLPSL). The selection criterion for mutants' authentication is the positive correlation with common errors at the implementation level. HLPSL specification consist of basic role, working environment, and security goal and the details shows in Figures 4-6.



```
role admin ()
            AS,PD: agent,
            AID, APW, R , RW, GL ,EM,
            APW1, APW2,MPI1, MPI2,
            CP, M2, DE, CH
            DGK, MOD, SUM, COMP,
            Homph, SND, RCV
            channel(dy))
init State:= 0
            transition
0.State = 0 /\n RCV(start) =|>
             /n AID:= new()
            /n APW:= new()
            /n R:= new()
            /n EM:= DGK (AID. APW)
            /n APW1, APW2:= SPLT
            (APW)
```

```
            /n MPI1:= MOD(GP1.MB)
            /n MPI2:= MOD(GP2.MB)
            /n CP:= SUM(MPI1, MPI2)
            /n M2:= SUM(R, AIDp,CP)
            /n SND(M2).AS
2.State = RCV(M2) =|>
            /n AIDp'= request (SerDB)
            /n DE=COMP(AIDp^',AIDp)
            /n CP= Homph (AIDp^')
            /n SND(Ch).PD
3.State = RCV(CH) =|>
             /n DE=COMP(CH,Cpi)
            /n SND(GL, Sg).AS
4.State = RCV(GL, Sg) =|>
            /n RW:= new()
            /n SND(GL, RW:=).Dr
End
```

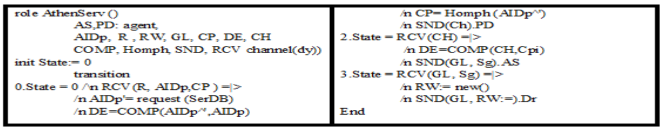
Figure 4. Specification of personal device (admin) role in HLPSL



```
Using OFMC BACKEND
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span//test1/res/verify
GOAL
As specified prior
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.0001 s
searchTime: 0.14 s
depth: 3 plies
```

```
Using CL-ATSE BACKEND
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
home/span / test1/res/verfy
GOAL
As specified prior
BACKEND
CL-AtSe
STATISTICS
Analysed: 0 states
Reachable: 0 states
Translation: 0.03 s
Computation: 0.0001s
```

Figure 5. Security verification result obtained using the AVISPA tool



```
role AthenServ ()
            AS,PD: agent,
            AIDp, R , RW, GL, CP, DE, CH
            COMP, Homph, SND, RCV  channel(dy))
init State:= 0
            transition
0.State = 0 /\n RCV (R, AIDp,CP ) =|>
            /n AIDp'= request (SerDB)
            /n DE=COMP(AIDp^',AIDp)
```

```
            /n CP= Homph (AIDp^')
            /n SND(Ch).PD
2.State = RCV(CH) =|>
             /n DE=COMP(CH,Cpi)
            /n SND(GL, Sg).AS
3.State = RCV(GL, Sg) =|>
            /n RW:= new()
            /n SND(GL, RW:=).Dr
End
```

Figure 6. Specification of authentication server (AS) role in HLPSL

6. COMPARISON WITH PREVIOUS WORKS

Table 2 explains main comparison between the proposed scheme and related works based on security metrics. Additionally, Table 3 shows a comparison of the computational cost between the most important previous methods and the current work, based on the scales in the following:

- T_h : The time allotted to the crypto hash function.
- T_F : The processing time for the fuzzy extractor operation.
- T_{Dec} : The processing time for a symmetric decryption function.
- T_{Enc} : The processing time for a symmetric encryption function.
- $T_{\oplus}$: The processing time for the XOR operation.

Depending on Kilinc *et al.* [24], the processing times for the basic functions are approximately as follows. T_h is 0.0023 ms, T_{Enc} is 0.0046 ms, T_{Dec} is 0.0046 ms, T_F is 0.442 ms, and $T_{\oplus}$ and $T_{||}$ are unnoticed due to its insignificant time Ibrahim *et al.* [18]. In terms of the communication cost of the login and authentication phases, we assume the value (128 bits) is related with each of the identity, password, and crypto hash function. The value of random number is one byte (8 bits). Both Table 3 and Table 4 are used to compare our scheme with others in computation and communication costs respectively. The computation time is computed based on a 32-bit

Cortex-M3 micro-controller at 72 MHz Wazid *et al.* (see Table). A 32-bit Cortex-M3 micro-controller Kompara *et al.* [20] running at 72 MHz executes a main process such as encryption, hash in 0.06 ms.

Table 2. Security metrics comparison

Security features	Ibrahim *et al.* [18]	He and Wang [11]	Kompara *et al.* [20]	Ryu and Kim [25]	Alzahrani *et al.* [26]	Current
Mutual Authentication	√	√	√	√	√	√
Anonymous & Untraceable	√	√	√	√	√	√
Forward Secrecy	√	√	√	√	√	√
Key Agreement	√	×	×	√	√	√
Key Freshness	×	×	×	√	√	√
MITM Attack	√	√	√	√	√	√
Replay Attack	√	√	√	√	√	√
Eavesdropping Attack	√	√	√	√	×	√
Stolen Personal Device	√	√	√	√	√	√
Forged Biometric Sensor	√	√	√	×	×	√
Healthcare Phase	×	×	×	√	×	√
COVID-19	×	×	×	×	×	√
Health Care	×	×	×	×	×	√

Table 3. Computation cost in (ms)

Scheme	Registration phase	Login & authentication phases	Total cost
Ibrahim *et al.* [18].	$2\,T_h + 1\,T_\oplus$	$12\,T_h + 6\,T_\oplus$	$14\,T_h + 7\,T_\oplus \approx 0.0322$
He and Wang [11]	$9\,T_h + 4T_\parallel + 2\,T_F + T_\oplus$	$12\,T_h + 5\,T_F + 9\,T_\oplus + 18\,T_\parallel$	$21\,T_h + 7\,T_F + 10\,T_\oplus + 22\,T_\parallel \approx 3.0023$
Kompara *et al.* [20].	$1\,T_h + 2\,T_\oplus + 1\,T_\parallel$	$8\,T_h + 13\,T_\oplus + 16\,T_\parallel$	$9\,T_h + 15\,T_\oplus + 17\,T_\parallel \approx 0.0207$
Ryu and Kim [25]	$2\,T_h + 3\,T_\oplus + 2\,T_\parallel$	$12\,T_h + 16\,T_\oplus + 38\,T_\parallel$	$14\,T_h + 19\,T_\oplus + 40\,T_\parallel \approx 0.0322$
Alzahrani *et al.* [26]	$1\,T_h + 2\,T_\oplus$	$10\,T_h + 14\,T_\oplus$	$11\,T_h + 16\,T_\oplus \approx 0.0253$
Our Scheme	$2\,T_h + 2\,T_\parallel$	$2\,T_\oplus + 4\,T_{Enc}$	$2\,T_h + 2\,T_\oplus + 4\,T_{Enc} + 2\,T_\parallel \approx 0.0184$

Table 4. The communication cost in bit

Communication link	Damgård *et al.* [22]	Somasundaram and Sivakumar [27]	He & Wang [11]	Our Scheme
$MS_i \longrightarrow PD_i$	480	384	512	264
$PD_i \longrightarrow AS$	640	384	528	264
$AS \longrightarrow PD_i$	640	1,280	496	128
$PD_i \longrightarrow MS_i$	480	384	480	-
Total	2,240	2,432	2,016	563

7. CONCLUSION

In this paper, we present a strong authentication scheme with anonymous password to prevent any adversaries from attempting to eavesdrop on the data exchanged at the login or authentication stage for WBANs. Our work pays more attention to make user's password dynamic, anonymous, and trusted for each login request among components. The strong passwords are established to fight the personal information revelation attack excellently and much more securely compared with the static passwords. The proposed work also implements continuously restructured pseudo identities and needs the undisclosed key of WBAN, which is related with the secret key of user for withstanding tracing, replaying, MITM, insider, and Impersonate attacks. Based on performance and security analysis, we detect that our presented scheme can negotiate the resist numerous malicious attacks, support numerous applied supplementary phases, dynamic anonymous password, and strong secret key. The proposed scheme distinguishes low computation cost, communication cost compared to those for the relating scheme. A great effort is being made to deal with the signals received from the patient through the medical sensors, if they are within illness or critical cases, it will send very urgent warning messages to the patient's relatives and the medical care centre. For taking the initial checks before the case gets out of control.

REFERENCES

[1] A. Arshad, Z. M. Hanapi, S. Subramaniam, R. Latip "A survey of Sybil attack countermeasures in IoT-based wireless sensor networks," *PeerJ Computer Science*, no. 7, p. e673, 2021, doi: 10.7717/peerj-cs.673.

[2] D. Toppenberg-Pejcic, J. Noyes, T. Allen, N. Alexander, M. Vanderford, and G. J. H. C. Gamhewage, "Emergency risk communication: lessons learned from a rapid review of recent gray literature on Ebola, Zika, and yellow fever," *Health Communication Journal*, vol. 34, no. 4, pp. 437-455, 2019.

[3] B. Gilmore *et al.*, “Community engagement for COVID-19 prevention and control: a rapid evidence synthesis,” *BMJ Global Health*, vol. 5, no. 10, p. e003188, 2020.

[4] D. P. Isravel and S. Silas, “A comprehensive review on the emerging IoT-cloud based technologies for smart healthcare,” in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2020, pp. 606-611, doi: 10.1109/ICACCS48705.2020.9074457.

[5] M. Kumar and S. Chand, “MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: regulation in COVID-19 pandemic,” *Journal of Network and Computer Applications*, vol. 179, p. 102975, 2021.

[6] K. Hasan, X.-W. Wu, K. Biswas, and K. Ahmed, “A novel framework for software defined wireless body area network,” in *2018 8th International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*, 2018, pp. 114-119, doi: 10.1109/ISMS.2018.00031.

[7] V. Patil, S. S. Thakur, and V. Kshirsagar, “Health monitoring system using internet of things,” in *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2018. doi: 10.1109/ICCONS.2018.8662915.

[8] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, and M. S. Islam, “A comprehensive review of wireless body area network,” *Journal of Network and Computer Applications*, vol. 143, pp. 178-198, 2019, doi: 10.1016/j.jnca.2019.06.016.

[9] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, “A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599-3609, 2017, doi: 10.1109/TII.2017.2773666

[10] L. K. Ramasamy, F. K. KP, A. L. Imoize, J. O. Ogbebor, S. Kadry, and S. Rho, “Blockchain-based wireless sensor networks for malicious node detection: a survey,” *IEEE Access*, vol. 9, pp. 128765-128785, 2021, doi: 10.1109/ACCESS.2021.3111923.

[11] D. He and D. Wang, “Robust biometrics-based authentication scheme for multiserver environment,” *IEEE Systems Journal*, vol. 9, no. 3, pp. 816-823, Sep. 2015, doi: 10.1109/JSYST.2014.2301517.

[12] S. Chatterjee, A. K. Das, and J. K. Sing, “A novel and efficient user access control scheme for wireless body area sensor networks,” *Journal of King Saud University-Computer and Information Sciences*,vol. 26, no. 2, pp. 181-201, 2014.

[13] Y. S. Lee, E. Alasaarela, and H. Lee, “Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system,” in *The International Conference on Information Networking 2014 (ICOIN2014)*, 2014, pp. 453-457doi: 10.1109/ICOIN.2014.6799723.

[14] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, A. S. Tolba, and K. J. Kim, “Authenticated key agreement with rekeying for secured body sensor networks,” *Sensors*, vol. 11, no. 6, pp. 5835-5849, 2011, doi: 10.3390/s110605835.

[15] M. Toorani, “Security analysis of the IEEE 802.15. 6 standard,” *International Journal of Communication Systems*, vol. 29, no. 17, pp. 2471-2489, 2016.

[16] P. Mohit, R. Amin, A. Karati, G. P. Biswas, and M. K. Khan, “A standard mutual authentication protocol for cloud computing based health care system,”. *Journal of medical systems*, vol. 41, no. 4, pp. 1-13, doi: 10.1007/s10916-017-0699-2.

[17] M. Wazid, A. K. Das, and A. V. Vasilakos, “Authenticated key management protocol for cloud-assisted body area sensor networks,”.*Journal of Network and Computer Applications*, vol. 123, pp. 112-126, doi: 10.1016/j.jnca.2018.09.008.

[18] H. M. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, “Secure anonymous mutual authentication for star two-tier wireless body area networks,” *Computer methods and programs in biomedicine*, vol. 135, 2016, doi: 10.1016/j.cmpb.2016.07.022.

[19] X. Li *et al.*, “An enhanced 1-round authentication protocol for wireless body area networks with user anonymity,” *Computers & Electrical Engineering*, vol. 61, pp. 238-249, 2017, doi: 10.1016/j.compeleceng.2017.02.011.

[20] M. Kompara, S. H. Islam, and M. Hölbl, “A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs,” *Computer networks*, vol. 148, pp. 196-213, 2019, doi: 10.1016/j.comnet.2018.11.016.

[21] X. Liu, R. Zhang, and M. J. C. N. Zhao, “A robust authentication scheme with dynamic password for wireless body area networks,” *Computer Networks*, vol. 161, pp. 220-234, 2019, doi: 10.1016/j.comnet.2019.07.003.

[22] I. Damgård, M. Geisler, and M. Krøigaard, “Efficient and secure comparison for on-line auctions,” in *Australasian conference on information security and privacy*, 2007, pp. 416-430, doi: 10.1007/978-3-540-73458-1_30.

[23] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, “A practical privacy-preserving password authentication scheme for cloud computing,” in *2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum*, 2012, pp. 1210-1217, doi: 10.1109/IPDPSW.2012.148.

[24] H. H. Kilinc and T. Yanik, “A survey of SIP authentication and key agreement schemes,” *IEEE communications surveys & tutorials*, vol. 16, no. 2, pp. 1005-1023, 2013, doi: 10.1109/SURV.2013.091513.00050.

[25] H. Ryu and H. Kim, “Privacy-preserving authentication protocol for wireless body area networks in healthcare applications,” In *Healthcare. MDPI*, 2021, vol. 9, no. 9, p. 1114, doi: 10.3390/healthcare9091114.

[26] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, “A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks,” *Wireless Personal Communications*, vol. 117, 2021, doi: 10.1007/s11277-020-07237-x.

[27] M. Somasundaram and R. Sivakumar, “Security in wireless body area networks: a survey,” In *2011 the International Conference on Advancements in Information Technology*, 2011.

BIOGRAPHIES OF AUTHORS

Abdulla J. Y. Aldarwish is Lecturer with the computer science Departments, College of Education for Pure Science, University of Basrah. He received the bachelor’s from the University of Basrah, Iraq, and the M.Sc. from Near East University, Cyprus Nicosia, the main focusing research area much related to Cloud Computing, QR code, Mobile application, IOT authentication, and Security He can be contacted at email: abdullajas@uobasrah.edu.iq.

Prof. Dr. Ali A. Yassin is a Professor with the Department of Computer Science, College of Education for Pure Science, University of Basrah. He received the bachelor's and master's degrees from the University of Basrah, Basrah, Iraq, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China. His research interests include the security of cloud computing, image processing, pattern recognition, biometrics, data integrity, DNA cryptography, steganography, sharing data, graphical password, QR code, and soft computing, He can be contacted at email: ali.Yassin@uobasrah.edu.iq.

Abdullah Mohammed Rashid is Lecturer with the computer science departments, college of education for pure science, University of Basrah. He received the bachelor's from the University of Basrah, Iraq, and the M.Sc. from Tenaga Nassional University, Kuala Lumpur, Malaysia. The main focusing research area much related to image processing, artificial Intelligence, and security. He can be contacted at email: abdullah.rashid @uobasrah.edu.iq.

Hamid Ali Abed Alasadi was born in Iraq. He received the B.Sc and M.S. degrees in electrical engineering and communication engineering from Basra University, Basra, Iraq, in 1987 and 1994, respectively, and the Ph.D. degree from the University Putra Malaysia in Computer and Communication Network Engineering in 2011. From 1995-2018, he was a faculty member in the Department of Computer science, Basra University. In 2014, he joined the Basra University as a Full Professor. He is member of scientific and reviewing committees of many journals and international conferences in the domains of Computer and communications engineering. He can be contacted at email: hamid.abed@uobasrah.edu.iq.

Aqeel Adel Yaseen is Lecturer with Ministry of Education. He received his bachelor's (2004) from Basra University, Basra, Iraq and master's degrees from Islamic University of Lebanon, Lebanon, 2011. His research interest includes security using data hiding, image processing. His research is focused on data hiding through image and voice in mobile environment. Aqeel is also broadly interested in other research areas such as data integrity and image retrieval, network and HER. He can be contacted at email: aay.ali80@gmail.com.

Eman Thabet Khalid is an assistant lecturer at University of Basrah. She received her BSc in computer science form from Basra University, College of Education for Pure Sciences, Department of Computer Science, Iraq in 2007, and the MSc in Computer Vision from University of Putra Malaysia, Malaysia in 2017. Her research interests include computer vision, machine learning, and deep learning. She can be contacted at email: eman.alasadi@uobasrah,edu.iq.