Wireless Personal Communications
https://doi.org/10.1007/s11277-020-07702-7

Performance Enhancement in Wireless Body Area Networks with Secure Communication

Syed Jawad Hussain[1] · Muhammad Irfan[1] · N. Z. Jhanjhi[2] · Khalid Hussain[1] · Mamoona Humayun[3]

Abstract
Over the years, the performance of devices used to gather sensitive medical information about individuals has increased substantially. These include implanted devices in the body, placed on or around the body, creating a Wireless body area network. Security and privacy have been a greater concern over a period of time due to the sensitive nature of the data collected and transmitted by the network. It has been noticed that various techniques have been applied to secure the data and provide privacy in WBANs but with a tradeoff of execution overhead. Although the latest available anonymous authentication schemes provide privacy and security but due to the limited computation capacity of WBAN devices, these schemes show greater time cost for authentication and consume more processing time. We review two latest anonymous authentication schemes for the WBAN environment in terms of computation cost. These two schemes provide anonymous authentication and use encryption to secure the data and ensure privacy. Then we analyze a recent lightweight authentication scheme proposed for wearable devices which provides anonymity and privacy along with security with very low computation cost. This scheme uses hash functions in order to obtain authentication and anonymity and doesn't use encryption in the authentication process. This scheme is not proposed for the WBAN environment, but it can be applied on the WBAN environment with necessary variations. The comparison of these available schemes shows clearly that the computation cost is considerably decreased by applying the latest authentication scheme in the WBAN environment. We propose a new authentication scheme for the WBAN environment based on the light-weight scheme proposed for wearable devices. The detailed analysis shows that our proposed scheme minimizes the computation cost and maintains the privacy and security along with anonymous authentication.

Keywords WBAN · Security · Privacy · Authentication · Anonymity · Computation cost

✉ N. Z. Jhanjhi
noorzaman.jhanjhi@taylors.edu.my

[1] University of Lahore Islamabad Campus, Islamabad, Pakistan

[2] School of Computer Science IT, SCE, Lakeside Campus, Taylor's University, Subang Jaya, Selangor, Malaysia

[3] College of Computer and Information Science, Jouf University, Al-Jouf, Saudi Arabia

Published online: 09 August 2020

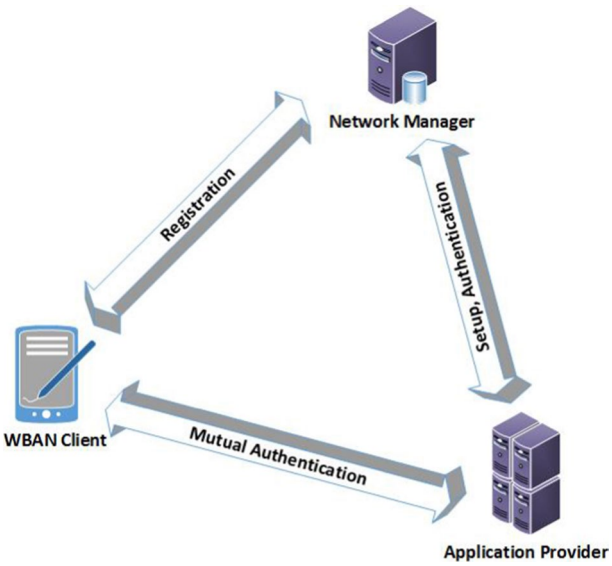
1 Introduction

The health facilities have increased and available to a vast community easily. The availability of cure for various diseases that caused a threat to the life of thousands of people in the past has increased the average age of people in developed countries around the world. This factor also shows that aged people will be abundant in the near future requiring health care facilities. Similarly, various diseases need continuous monitoring so that better treatment could be provided. This will surely require more health care facilities and will also place a burden on the existing available facilities. In order to cope with this situation, very small, intelligent sensing devices capable of recording/collecting data and transmitting it to some distant location can be placed in the near vicinity of the human body i.e. implanted in the human body, placed on or around the human body. These tiny devices including sensors, actuators, form a network called Wireless Body area network (WBAN). The concept of Wireless Body area networks was initially introduced by Zimmerman [1], which consists of many low energy consuming smart sensors, positioned in or around the patient body. This network is capable of sensing real-time data concerning a person (Patient), forwarding it to the concerned health care provider, and even provide medical assistance by injecting the required quantity of medicine to the human body using actuators. This smart network will surely decrease the burden over the health care facilities and help in the timely monitoring of patients. Also, the patients need not to visit the health care facility for the purpose of checkup.

Due to the importance of the functionality of WBANs, IEEE 802.15.6 [2] has been proposed to standardize this new technology all over the world to provide secure and trustworthy communication because of the criticality of the nature of data communicated over the wireless channel. This standard ensures the applicability of devices to transmit safely to human body implanted in, placed at or around the human body. These devices support data rates from 75.9 kbps to 15.6 Mbps depending upon the nature of the application [3].

Figure 1 shows the model of WBAN for the process to setup the system for communication according to our proposed scheme. In this model, the client (C) is responsible to

Fig. 1 Network model of WBAN



send the vital information of the patient/user of WBAN to the application provider. The application provider (AP) is located at a distant location usually in a health facility. The network manager (NM) is a trusted third party Server, which is used to authenticate Client and Application provider for secure communication located over the web. The NM knows both the client and AP and stores important information about both. The client can communicate with the application provider and Network Manager using the internet.

WBANs have the ability to communicate with internet and communicate with a vast range of newly available technologies such as Bluetooth, Zigbee, and Wireless Sensor networks and mobile networks, etc. This shows that the applications of WBANs will no longer be related to personal health but could be expanded to vast fields of life. However, the applicability of WBANs in the real environment poses certain challenges such as delay in communication, the throughput of the system, uptime of system, security, privacy and compatibility with existing technologies etc. [4–6].

The critical authentication data transmitted over the network in WBANs needs to be secure and also provide privacy to the owner of the data. In order to secure this data various anonymous authentication schemes have been proposed in the recent past that provide authentication. These anonymous authentication schemes also focus on privacy. However, the performance of these networks is considerably degraded by applying strict policies and security measures. The purpose of this study is to increase the understanding of WBANs by reviewing the existing research work. Then recent techniques to improve the performance of WBANs are considered and compared in order to get performance advantage by maintaining the security and privacy and propose a new lightweight authentication scheme to improve the performance of WBANs as depicted in Fig. 2.

The rest of the paper follows the following pattern. Related work is presented in Sect. 2. Section 3 shows the motivation, Sect. 4 reveal our contribution and the proposed authentication scheme. Results are shown in Sect. 5, Informal security analysis is discussed in Sect. 6. Finally, Sect. 7 consists of the conclusion and future work.

2 Related Work

Poon et al. [7] proposed a "biometric approach that uses an intrinsic characteristic of the human body as the authentication identity or the means of securing the distribution of a cipher key to secure inter-BASN communications". The timing information of the heartbeat serves the purpose. The scheme assumes that a secure key sharing mechanism is already in place. Their scheme also provides identity authentication of individuals. The requirement of memory and computation is significantly reduced.

Wang et al. [8] proposed an integrated biometric-based security framework [static hidden Markov model (HMM) based verification scheme] which exploits the biometric attributes shared by the sensor nodes present at various locations of a body. The biometric key (ECG signal) of a person is used for encryption. This includes a selective encryption scheme that just encrypts the critical data (subset) instead of encrypting all the biometric data, reducing computational resources. Also the requirement of key sharing is not needed because static features of ECG are applied for encryption.

Mana et al. [9] proposed an efficient and energy-conserving scheme "Trust key management scheme for wireless body area networks" which is capable to generate symmetric cryptographic keys for encryption and decryption along with a secure mechanism for

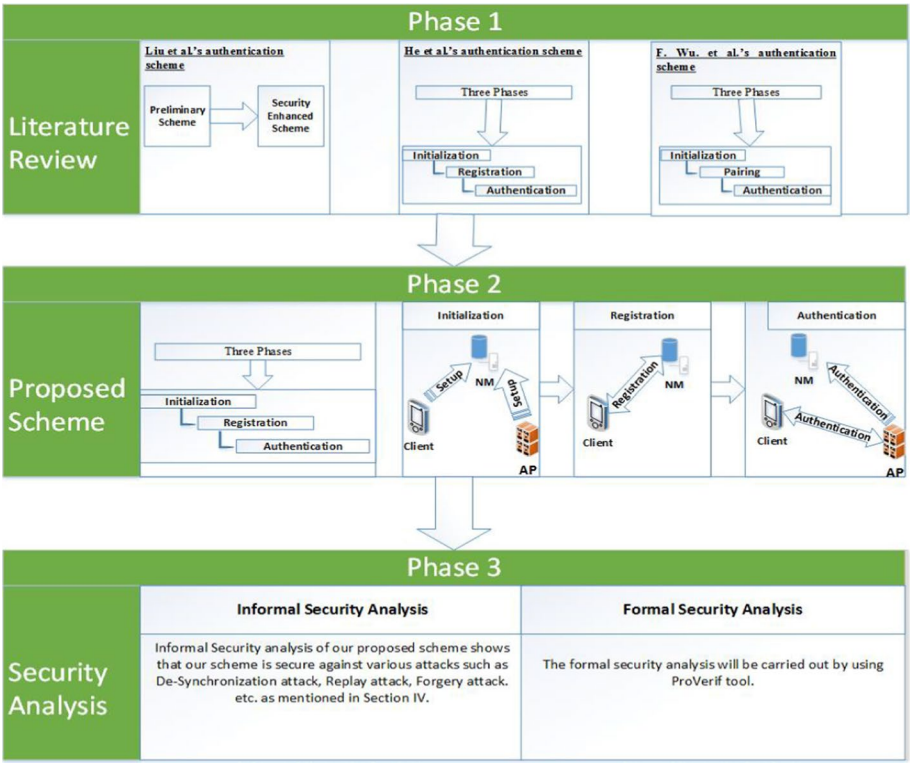


Fig. 2 Flow of research

distribution of keys. The keys are generated by using the ECG signal of a human body, conserving privacy, and energy.

Sarra et al. [10] proposed a multi-hop routing protocol to improve coexistence between WBAN based IEEE 802.15.4 protocol and WIFI. Wireless networks present in the near vicinity of each other loose critical information due to interferences. The proposed multi-hop routing protocol brings reliability to WBAN and ensures connectivity and longer battery life.

Oberoi et al. [11] proposed a scheme of key derivation by collecting sample data using a motion sensor and extracting attributes to derive the cryptographic key. This derived key is used for the pairing of devices. The scheme uses the acceleration of the devices that require interacting with each other. Nodes on one host body tend to have similar acceleration thus similar shared key derived at different sensors. This also ensures that the nodes communicating with each other are part of one physical network because an adversary node could not guess the speed of any node part of a network.

Liu et al. [12] proposed "Certificateless remote anonymous authentication schemes for Wireless Body Area Networks". Their schemes show a preliminary version and an enhanced version of authentication protocols such that remote entities of WBAN could anonymously authenticate themselves to take advantage of health-related services. They presented a certificate-less signature (CLS) Scheme and claimed that their scheme is secure against adaptively chosen message attack in the random oracle model and ensured the

original identity of users were never disclosed by application provider or network manager. They proposed a new CLS scheme as the cryptographic primitive and assumed that the Computational Diffie–Hellman problem (CDHP) is intractable. They used the new CLS scheme to develop two remote anonymous authentication schemes, which used the anonymous account index of users to access WBAN service thus WBAN client's real identity is not revealed.

He et al. [13] proposed "Anonymous Authentication for Wireless Body Area Networks with Provable Security". They reviewed the recent anonymous authentication scheme proposed by Liu et al. and proposed a successful impersonation attack on Liu et al.'s scheme. It was found that Liu et al.'s scheme is vulnerable to impersonation attack because the user's identity used in their scheme remains constant and hence traceable also due to the presence of verification table at the site of Application Provider, the verification table needs to be updated at every joining and removing of client into the system. They show through analysis that their scheme is not only provably secure against various attacks including impersonation attack and also reduces computational burden over the client. They claim that rather than storing data at the Application provider's database for the purpose of verification, it should be stored at Network manager for being a more secure and trusted location.

Wu et al. [14] proposed "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server". A wearable device (WD) collects and provides certain information about a person wearing the device. The wearable device sends this information to a smartphone (SP). The SP is capable of communicating with a cloud server (CS). Their scheme provides mutual authentication and keep the devices anonymous. The proposed scheme consists of three phases: Initialization, Pairing and authentication. They used four channels for communication among entities: Two public channels and two private (Secure) channels. Authentication between the wearable device and the smartphone is done in this scheme. This scheme uses a hash function and concatenation operation and exclusive-OR operation for the purpose of pairing and authentication. This fact makes it a lightweight authentication protocol.

Liu et al. [12] and He et al. [13] focused on anonymous authentication of clients with health-related services such that the computational burden is also reduced on the client. By using Wu et al.'s [14] authentication scheme in the WBAN environment, the computational cost on the client is significantly reduced and the benefit of anonymity is achieved.

Table 1 shows a comparison of the authentication schemes.

3 Motivation and Problem Statement

It is the demand of every authentication scheme that it must be secure to various known threats. It is also demanded that the authentication scheme must be light-weight, so that least resources get consumed during the authentication process. Liu's and He's algorithms are based on WBAN platform to achieve anonymity and security of WBAN clients. Their algorithms provide anonymity and security to the client using encryption. Their algorithms achieve the goal of anonymity and security during authentication on the cost of energy resources. We intend to achieve the same anonymity and security using the hashing scheme used by Wu et al. The WBAN environment is a resource-constrained environment. Therefore, we intend to use a secure light-weight authentication scheme (Table 2).

On comparison, it is found that the computation cost of the three mentioned authentication schemes [12–14] in Sect. 2, vary a lot. Therefore, in order to show the performance

Table 1 Comparison of authentication schemes

Sr. no	Scheme	Description	Drawback/limitation
01	Physiological based	The physiological values such as ECG, IRIS and finger prints are used	Suffer from denial of service attack
02	Channel based	The received signal strength (RSS) of communication channel can be used for authentication schemes	Lack of anonymity
		Zeng et al. [15] used temporal RSS variations	Does not provide anonymity
		Cai et al. [16] proposed device pairing scheme using differential RSS	Not suitable for practical implementation due to requirement of two receiver antennas
03	Proximity based	Using the property of devices that are present in close vicinity of each other. The devices use the radio signal environment signature to identify that the two devices are in close proximity [17]	Devices have to be within half of the wavelength distance of each other
04	Cryptography based	Traditional public cryptography based authentication	Resources (battery capacity, computing power) are limited
	Elliptic curve cryptography	ECC uses smaller key and suitable for resource-limited environments	Trusted certification authority required
		Liu et al. [12] proposed a certificate-less signature scheme by using bilinear pairing defined on ECC	Traceable and vulnerable to impersonation attack
05	ID-based	The identity of the user is used as public key	Suitable for client–server environment Vulnerable to: Impersonation attack, Reflection attack, Denial of Service attack
06	Anonymous authentication scheme	1. Three phase process: Initialization, Registration and authentication 2. Security credentials should be stored at a much secure location: Network Manager [13]	

Table 2 Notations for time cost for the execution of functions

Symbol	Meaning	Time
T_h	Time for one hash function (SHA256)	1.06 µs [14, 18]
TG_e	The execution time of executing a bilinear operation	5.32 s [13]
TG_{mul}	The execution time of a scalar multiplication operation	2.45 s [13]
TG_H	The execution time of a map-to-point hash function operation	0.89 s [13]
TG_{add}	The execution time of a point addition operation	< 0.01 s [13]
T_{exp}	The execution time of a modular exponentiation operation	1.25 s [13]
T_h	The execution time of a general hash function operation	< 0.01 s [13]

Table 3 Computation cost of client of Liu et al.'s scheme

Time cost	Phase Authentication	Total cost
Time cost for client	$4TG_{mul} + 1TG_H + 2TG_{add} + 1$ $T_{exp} + 3T_h \approx 11.95$ s	11.95 s

Table 4 Computation cost of He et al.'s scheme

Time cost	Phase Authentication	Total cost
Time cost for client	$4TG_{mul} + 1TG_H + 1TG_{add} + 4$ $T_h \approx 10.69$ s	10.69 s

Table 5 Computation cost of F. Wu et al.'s scheme

Time cost	Phase		Total cost (pairing + authentication)
	Pairing	Authentication	
Time cost for wearable device (WD)	$5T_h = 5.3$ µs	$5T_h = 5.3$ µs	10.6 µs
Time cost for smart phone (SP)	$6T_h = 6.36$ µs	$6T_h = 6.36$ µs	12.72 µs
Time cost for cloud server (CS)	$9T_h = 9.54$ µs	$7T_h = 7.42$ µs	16.96 µs
Total time cost	21.20 µs	19.08 µs	40.28 µs

of authentication schemes [12–14] in terms of computation time/cost, tables are used. The computation cost of authentication schemes [12–14] are given below in Tables 3, 4, 5 and 6. Table 2 shows symbols used for calculation of computation time of various operations performed during authentication. The time taken for execution by the devices of a certain operation is mentioned for the purpose of comparison between the anonymous authentication techniques.

The comparison of the computation cost is shown in Table 6 and Fig. 3 during the authentication phase at Client shows the obvious difference and F. Wu et al.'s Authentication scheme proves to be lightweight for the client. This later scheme decreases the

Table 6 Comparison of computation costs for the authentication phase of Liu et al., He et al. and F. Wu et al.'s schemes

Time cost	Authentication scheme		
	Liu et al.'s scheme [12]	He et al.'s scheme [13]	F. Wu et al.'s scheme [14]
Time cost for authentication of client	11.95 s	10.69 s	5.3 μs

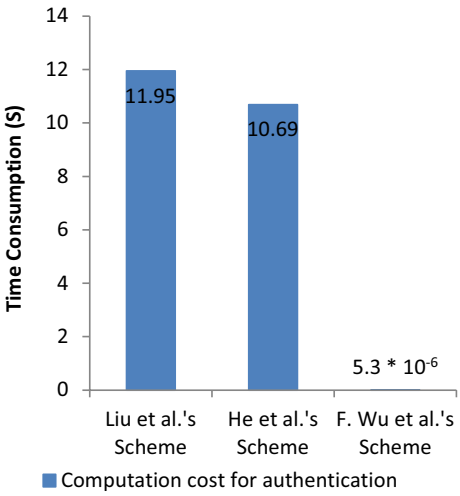


Fig. 3 Comparison of computation costs

computation burden on the client. Moreover, the total computation cost of F. Wu et al.'s authentication scheme tends to be 40.28 μs, which is considerably low with respect to the other two schemes mentioned in Sect. 2.

4 Our Proposed Scheme

Due to the lightweight nature of F. Wu et al.'s authentication scheme, it is applied on the wireless body area network (WBAN) for the purpose of registration and authentication with necessary modifications to suit for WBAN environment.

We propose a mutual authentication scheme for WBANs. It consists of three phases: initialization, Registration, and Authentication. In the initialization phase, the Network manager generates the system parameters and stores the important information about the client and application provider such as the identity of the client and application provider, pseudo-identity of client and application provider, and secret key of client and application provider. The Network Manager acquires this information through a secure channel. The registration phase is responsible for registering of client with the network manager and to come to know the existence of the application provider. In the authentication phase, the client and application provider mutually authenticate each other using the Network manager and a session key is generated for the current session for the purpose of secure communication.

(a) Initialization

The network manager (NM) serves the purpose of a trusted third party and generates the system parameters. NM stores.

Information about client (C) and application provider (AP). The notations used can be referred to from Table 7.

1. The information about Client (C) stored at NM is as follows:

$$\left(\mathrm{ID_C}, \mathrm{X_C}, \mathrm{P_1^{Old}}, \mathrm{P_1^{New}}\right)$$

2. The information about Application Provider (AP) stored at NM is as follows:

$$\left(\mathrm{ID_A}, \mathrm{X_A}, \mathrm{P_2^{Old}}, \mathrm{P_2^{New}}\right)$$

3. "h" is a secure hash function known to C, AP and NM.
4. $\Delta T = 2$ * Computational cost (hash(s) + concatenation operation). The ΔT will be finalized based on statistical data acquired from simulations later on.

Table 7 Notations for the proposed authentication scheme

Notations	Description
C	Client
AP	Application provider
NM	Network manager
$\mathrm{ID_C}$	Identity of client C
$\mathrm{PID_C}$	Pseudo-identity of client C
$\mathrm{X_C}$	Secret key of client C
$\mathrm{ID_A}$	Identity of application provider AP
$\mathrm{PID_A}$	Pseudo-identity of application provider AP
$\mathrm{X_A}$	Secret key of application provider AP
$\mathrm{t_C}$, $\mathrm{t_{C2}}$	Time stamp of C for registration phase
$\mathrm{t_N}$	Time stamp of NM for registration phase
$\mathrm{r_C}$	Random number generated by C for registration phase
$\mathrm{T_C}$, $\mathrm{T_{C2}}$	Time stamp of C for authentication phase
$\mathrm{T_A}$, $\mathrm{T_{A2}}$	Time stamp of AP for authentication phase
$\mathrm{T_N}$	Time stamp of NM for authentication phase
ΔT	Legal delay time interval
$\mathrm{R_C}$	Random Number generated by C for authentication phase
$\mathrm{R_A}$	Random Number generated by AP for authentication phase
$\mathrm{M_1}$, $\mathrm{M_2}$ … $\mathrm{M_6}$	Messages
h(.)	Secure hash function
$\oplus$	Exclusive-OR computation
$\|$	Concatenation operation
$\mathrm{P_1^{New}}$	The new pseudo-identity of client
$\mathrm{P_2^{New}}$	The new pseudo-identity of application provider
$\mathrm{P_1^{Old}}$	The old pseudo-identity of client held by network manager

5. All the network devices are online i.e. connected to internet. The devices can update their time from online servers [19].

(b) Registration

The client (C) needs to register itself at NM to start communicating with AP. Notations used in the registration process can be referred to from Table 7. Following steps are carried out:

(1) The client (C) generates a random number of r_C and picks up its current time stamp t_C.
(2) The client calculates the hash $D\text{-}_1$ using its identity ID_C, its Secret Key X_C, random number r_C and time stamp t_C.
(3) The client creates a message M_1 that includes random number r_C, time stamp t_C, the Pseudo-identity of client PID_C, and the generated hash D_1 and sends it to Network manager (NM).
(4) On receiving message M_1, Network manager picks up its current time stamp t_N and checks to see that if $|t_N - t_C| < \Delta T$, if the delay is not within specific allowed delay time interval, then the message is discarded otherwise further process is carried out.

When the message M1 is validated for time, then the network manager (NM) checks for the validity of client in its database. It finds the tuple (ID_C, X_C) in its database. Calculates the hash function D_1 and checks if the hash D_1 calculated at NM matches hash D_1 received from client (C). If the same hash is calculated at NM, this shows that the client is valid and further process can be continued. Network manager stores two values for client P_1^{New} and P_1^{Old}. Now NM checks two cases:

(a) *Case 1* If $P_1^{New} = PID_C$, this means that the Pseudo-identity of client equals P_1^{New} in the database of NM and it is required that NM now updates the value of P_1^{Old} to P_1^{New}. This case is executed when client registers itself for the first time with NM.
(b) *Case 2* If $P_1^{Old} = PID_C$, this means that the Pseudo-identity of client equal P_1^{Old} in the database of NM. In this case no action is required.

(5) After the validation of Message M_1 and validation of client, NM calculates a new Pseudo-identity P_1^{New} for client C by generating the hash of identity of client ID_C, client's Secret Key X_C, random number r_C generated by client, time stamp t_C generated by client and the time stamp t_N generated by NM. P_1^{New} serves as new Pseudo-identity for Client.
(6) Next, NM generates a hash D_2 using P_1^{New}, secret key of Client X_C and time stamp t_N generated by NM and attaches itself by exclusive OR operation ($\oplus$) with identity ID_A of Application Provider (AP).
(7) NM creates a message M_2, consisting of timestamp t_N generated by NM and the generated hash D_2. NM sends this message to Client.
(8) On receiving message M_2, Client picks up its current time stamp t_{C2} and checks to see that if $|t_{C2} - t_N| < \Delta T$, if the delay is not within specific allowed delay time interval, the message is discarded otherwise further process is carried out.
(9) After the validation of Message M_2, Client calculates its new Pseudo-identity PID_C^{New} by generating the hash of identity of client ID_C, client's Secret Key X_C, random number r_C generated by client, time stamp t_C generated by client and the time stamp t_N

generated by NM, such as PID_C^{New} serves as new Pseudo-identity for Client. It must be noted that the same pseudo-identity for Client was generated at NM.

(10) Client then gets ID_A (the identity of Application Provider) from hash D_2.

(11) Client recalculates D_2 and checks whether it gives the correct D_2 as received from NM, if correct D_2 is calculated then session is valid and Client updates its field of Pseudo-identity. If D_2 is invalid, the message is discarded and registration process is initiated again.

Table 8 shows the process of registration of clients with the Network manager.

(c) Authentication

For the purpose of authentication, all three entities participate in the process. In this process, the Client and Application provider mutually authenticate each other and a session key is generated for further communication between Client and Application Provider. The notations used for authentication refer to Table 7.

The following step are involved in the process of authentication:

(1) The client (C) generates a random number of R_C and picks up its current timestamp T_C.

(2) The client calculates the hash C_1 using its identity ID_C, its Secret Key X_C, random number R_C, time stamp T_C and identity ID_A of application provider (AP).

Table 8 Registration phase of proposed authentication scheme

<table>
<tr><th>Client (C)</th><th>Network Manager (NM)</th></tr>
<tr><td>Generate r_C , t_C
$D_1 \longleftarrow h(ID_C \| X_C \| r_C \| t_C)$
$M_1 = \{ r_C, t_C, PID_C , D_1\}$
M1 is sent to NM</td><td></td></tr>
<tr><td></td><td>Pick t_N and check if $|t_N - t_C| < \Delta T$
Cases
<table>
<tr><td>Case 1</td><td>Case 2</td></tr>
<tr><td>$P_1^{New} = PID_C$</td><td>$P_1^{Old} = PID_C$</td></tr>
<tr><td colspan="2">Common Operations:</td></tr>
<tr><td colspan="2">Find (ID_C , X_C)
Check if $D_1 = h(ID_C \| X_C \| r_C \| t_C)$</td></tr>
<tr><td>$P_1^{Old} \longleftarrow P_1^{New}$</td><td>No Action { Null }</td></tr>
</table>
$P_1^{New} \longleftarrow h(ID_C \| X_C \| r_C \| t_C \| t_N)$
$D_2 \longleftarrow h(P_1^{New} \| X_C \| t_N) \oplus ID_A$
$M_2 = \{ t_N , D_2\}$
M2 is sent to Client (C)</td></tr>
<tr><td>Pick t_{C2} and check if $|t_{C2} - t_N| < \Delta T$
$PID_C^{New} \longleftarrow h(ID_C \| X_C \| r_C \| t_C \| t_N)$
Get $ID_A \longleftarrow D_2 \longleftarrow h(P_1^{New} \| X_C \| t_N)$
Check if D_2 holds
$D_2 = h(P_1^{New} \| X_C \| t_N)$
Set
$PID_C \longleftarrow PID_C^{New}$
Client (C) stores ID_A</td><td></td></tr>
</table>

(3) The client creates a message M_3 that includes random number R_C, time stamp T_C, the Pseudo-identity of client PID_C, and the generated hash C_1 and sends it to Application Provider (AP).
(4) On receiving message M_3, AP picks up its current time stamp T_A and checks to see that if $|T_A - T_C| < \Delta T$, if the delay is not within specific allowed delay time interval, then the message is discarded otherwise further process is carried out.
(5) The application provider (AP) generates a random number R_A.
(6) The AP calculates the hash $C\text{-}_2$ using its identity ID_A, its Secret Key X_A, random number R_A, time stamp T_A, and pseudo-identity PID_A of application provider (AP).
(7) The AP creates a new message M_4 that includes random number R_C, time stamp T_C, the Pseudo-identity of client PID_C, the hash C_1 received from Client, random number R_A generated by AP, time stamp T_A generated by AP, the Pseudo-identity of Application provider PID_A and the generated hash C_2 by AP and sends it to network manager (NM).
8) On receiving message M_4, Network manager picks up its current time stamp T_N and checks to see that if $|T_N - T_A| < \Delta T$, if the delay is not within specific allowed delay time interval, then the message is discarded otherwise further process is carried out.
(9) When the message M_4 is validated for time, then Network manager (NM) checks for the validity of client and application provider in its database. It finds the tuple (ID_C, X_C) for client and tuple (ID_A, X_A) for Application provider in its database. It then recalculates the hash function C_1 and checks if the hash C_1 calculated at NM matches hash C_1 received from client (C). If the same hash is calculated at NM, this shows that the client is valid and further process can be continued. Similarly, it recalculates the hash function C_2 and checks if the hash C_2 calculated at NM matches hash C_2 received from Application Provider (AP). If the same hash is calculated at NM, this shows that the Application Provider is valid and further process can be continued. Network manager stores two values for client P_1^{New} and P_1^{Old}. Now NM selects from three cases:

(a) *Case 1* If $P_1^{New} = PID_C$ and $P_2^{New} = PID_A$, this means that the Pseudo-identity of client equals P_1^{New} in the database of NM and it is required that NM now updates the value of $P_1^{Old} = P_1^{New}$and sets the value of $P_2^{Old} = P_2^{New}$. This case is executed when client and application provider register itself for the first time with NM.
(b) *Case 2* If $P_1^{Old} = PID_C$, and $P_2^{New} = PID_A$ this means that the Pseudo-identity of client equal P_1^{Old} in the database of NM. In this case no action is required for client but sets the value of $P_2^{Old} = P_2^{New.}$
c) *Case 3* If $P_1^{Old} = PID_C$, and $P_2^{old} = PID_A$, then no action is required i.e. no updating of records is required by NM, as the records are already updated.

(10) After the validation of Message M_4, validation of client and validation of Application Provider, NM calculates a new Pseudo-identity P_1^{New} for client C by generating the hash of identity of client ID_C, client's Secret Key X_C, random number R_C generated by client, time stamp T_C generated by client and the time stamp T_N generated by NM. P_1^{New} serves as new Pseudo-identity for Client.
(11) NM calculates a new Pseudo-identity P_2^{New} for Application provider by generating the hash of identity of application provider ID_A, AP's Secret Key X_A, random number R_A generated by AP, time stamp T_A generated by AP and the time stamp T_N generated by NM. P_2^{New} serves as new Pseudo-identity for Application provider.

(12) Next, NM generates a hash C_3 by concatenating ID_C, X_C, ID_A, X_A and $T_{N.}$
(13) NM generates a hash C_4 by concatenating ID_A, X_A and T_A and attaches C_3 to it by exclusive OR operation.
(14) NM generates a hash C_5 by concatenating ID_C, X_C and T_C and attaches C_3 to it by exclusive OR operation.
(15) NM generates a hash C_6 by concatenating C_3 and P_2^{New}.
(16) NM generates a hash C_7 by concatenating C_3 and P_1^{New}.
(17) Finally, NM generates a message M_5 which consists of T_N, C_3, C_4, C_5, C_6 and C_7 and sends it to Application provider.
(18) On receiving M_5, application provider picks up its current time stamp T_{A2} and checks to see that if $|T_{A2} - T_N| < \Delta T$, if the delay is not within specific allowed delay time interval, then the message is discarded otherwise further process is carried out.
(19) After the validation of Message M_5, AP calculates its new Pseudo-identity PID_A^{New} by generating the hash of identity of AP ID_A, AP's Secret Key X_A, random number R_A generated by AP, time stamp T_A generated by AP and the time stamp T_N generated by NM, such as PID_A^{New} serves as new Pseudo-identity for AP. It must be noted that the same pseudo-identity for AP was generated at NM.
(20) AP generates a hash C_8 by concatenating ID_A, X_A and T_A and attaches C_4 to it by exclusive OR operation.
(21) At this point a session key SK_{AC} is generated by AP by hash function and concatenating C_8, PID_C, ID_A, R_C and R_A.
(22) AP then calculates hash C_9 by concatenating SK_{AC} and T_{A2}.
(23) AP sets its Pseudo-identity $PID_A = PID_A^{New.}$
(24) AP creates a message M_6, consisting of T_N, T_{A2}, C_5, C_7 and C_9 and sends it to Client.
(25) On receiving message M_6, Client picks up its current timestamp T_{C2} and checks to see that if $|T_{C2} - T_{A2}| < \Delta T$, if the delay is not within specific allowed delay time interval, the message is discarded otherwise further process is carried out.
(26) After the validation of Message M_6, Client calculates its new Pseudo-identity PID_C^{New2} by generating the hash of identity of client ID_C, client's Secret Key X_C, random number R_C generated by client, time stamp T_C generated by client and the time stamp T_N generated by NM, such as PID_C^{New2} serves as new Pseudo-identity for Client. It must be noted that the same pseudo-identity for Client was generated at NM.
(27) AP generates a hash C_{10} by concatenating ID_C, X_C and T_C and attaches C_5 to it by exclusive OR operation.
(28) It then checks by recalculating the hash function C_7. If the hash function C_7 holds, this verifies the identity of AP.
(29) At this point a session key SK_{CA} is generated by AP by hash function and concatenating C_{10}, PID_C, ID_A, R_C and R_A.
(30) Further, to check the validity of Session key, client recalculates C_9, if it equals the C_9 received from AP, then the session key is valid.
(31) Going through this process successfully, client and AP have mutually authenticated each other.
(32) Now, Client updates it pseudo-identity PID_C to PID_C^{New2}, this new Pseudo-identity will be used to communicate further.

Tables 9, 10, 11 depicts the detailed process of authentication for the proposed authentication scheme.

Table 9 Process of authentication Sect. 4.C: steps 1–7

Client (C)	Application Provider (AP)
Generate R_C , T_C $C_1 \longleftarrow h(ID_C \| X_C \| R_C \| T_C \| ID_A)$ $M_3 = \{ R_C, T_C, PID_C , C_1\}$ M3 is sent to Application Provider	
	Application Provider receives M3 from Client Pick T_A and check if $\|T_A - T_C\| < \Delta T$ Generate R_A $C_2 \longleftarrow h(ID_A \| X_A \| R_A \| T_A \| PID_A)$ $M_4 = \{ R_C, T_C, PID_C , C_1, R_A, T_A, PID_A , C_2 \}$ M4 is sent to Network Manager

Table 10 Process of authentication Sect. 4.C: steps 8–24

Application Provider (AP)	Network Manager (NM)
M4 is sent to Network Manager	**Network Manager receives M4 from Application provider** Pick T_N and check if $\|T_N - T_A\| < \Delta T$ Cases: Case 1: $P_1^{New}=PID_C$, $P_2^{New}=PID_A$ Case 2: $P_1^{Old}= PID_C$, $P_2^{New}=PID_A$ Case 3: $P_1^{Old}= PID_C$, $P_2^{Old}=PID_A$ Common Operations: Find (ID_C , X_C) , (ID_A , X_A) Check if $C_1 = h(ID_C \| X_C \| R_C \| T_C \| ID_A)$ And check if $C_2 = h(ID_A \| X_A \| R_A \| T_A \| P_2^{New})$ Case 1: $P_1^{Old} \leftarrow P_1^{New}$, $P_2^{Old} \leftarrow P_2^{New}$ Case 2: $P_2^{Old} \leftarrow P_2^{New}$ Case 3: { Null } $P_1^{New} \longleftarrow h(ID_C \| X_C \| R_C \| T_C \| T_N)$ $P_2^{New} \longleftarrow h(ID_A \| X_A \| R_A \| T_A \| T_N)$ $C_3 \longleftarrow h(ID_C \| X_C \| ID_A \| X_A \| T_N)$ $C_4 \longleftarrow C_3 \oplus h(ID_A \| X_A \| T_A)$ $C_5 \longleftarrow C_3 \oplus h(ID_C \| X_C \| T_C)$ $C_6 \longleftarrow h(C_3 \| P_2^{New})$ $C_7 \longleftarrow h(C_3 \| P_1^{New})$ $M_5 = \{ T_N, C_3, C_4, C_5, C_6, C_7 \}$ M5 is sent to Application Provider
Application Provider receives M5 from Network Manager Pick T_{A2} and check if $\|T_{A2} - T_N\| < \Delta T$ $PID_A^{New} \longleftarrow h(ID_A \| X_A \| R_A \| T_A \| T_N)$ $C_8 \longleftarrow C_4 \oplus h(ID_A \| X_A \| T_A)$ $SK_{AC} = h(C_8 \| PID_C \| ID_A \| R_C \| R_A)$ $C_9 \longleftarrow h(SK_{AC} \| T_{A2})$ $PID_A \longleftarrow PID_A^{New}$ $M_6 = \{ T_N, T_{A2}, C_5, C_7, C_9 \}$ M6 is sent to Client	

Table 11 Process of authentication Sect. 4.C: steps 25–32

Application Provider	Client
Application provider sends M6 to Client	**Client receives M6 from Application provider** Pick T_{C2} and check if $\lvert T_{C2} - T_{A2}\rvert < \Delta T$ $PID_C^{New2} \longleftarrow h(ID_C \| X_C \| R_C \| T_C \| T_N)$ $C_{10} \longleftarrow C_5 \oplus h(ID_C \| X_C \| T_C)$ Check if $C_7 = h(C_{10} \| PID_C^{New2})$ $SK_{CA} = h(C_{10} \| PID_C \| ID_A \| R_C \| R_A)$ Check if $C_9 = h(SK_{CA} \| T_{A2})$ Set $PID_C \longleftarrow PID_C^{New2}$

5 Results

Based on the factors discussed in our proposed scheme, the following computation costs arise.

1. Computational Cost

Liu et al.'s [12] scheme demonstrates that the client performs four scalar operations of multiplication, one map-to-point hash function operation, two-point addition operations, one modular exponentiation operation, and three general hash function operations. Thus the client consumes computational resource for $4\ TG_{mul} + 1\ TG_H + 2\ TG_{add} + 1\ T_{exp} + 3\ T_h \approx 11.95$ s as shown in Table 3.

He et al.'s [13] scheme demonstrates that the client performs four scalar operations of multiplication, one map-to-point hash function operation, one-point addition operations, and four general hash function operations. Total computation cost at the client side is $4\ TG_{mul} + 1\ TG_H + 1\ TG_{add} + 4\ T_h \approx 10.69$ s as shown in Table 4.

He et al.'s [13] considered the work of Xiong et al. [19] to evaluate the efficiency of their proposed scheme, on the hardware MICAz, that has only 4 KB RAM,128 KB ROM, and a 7.3828-MHz ATmega128L microcontroller and used in wireless sensor network research.

The client in our scheme calculates five hash function operations for registration and five hash function operations for authentication. Then, the computation cost at the client side is $5T_h + 5\ T_h \approx 10.6$ µs.

The total computation cost for the process of registration of a device with the network manager and then authentication takes ≈ 40.28 µs as shown in Table 12.

Table 12 Computational cost of proposed scheme

Time cost	Phase		Total cost
	Registration	Authentication	
C (µs)	$5T_h = 5.3$ µs	$5T_h = 5.3$ µs	10.6 µs
AP (µs)	$6T_h = 6.36$ µs	$6T_h = 6.36$ µs	12.72 µs
NM (µs)	$9T_h = 9.54$ µs	$7T_h = 7.42$ µs	16.96 µs
Total time cost	21.20 µs	19.08 µs	40.28 µs

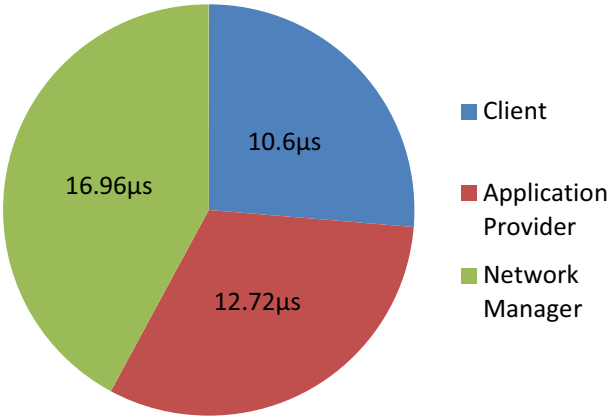


Fig. 4 Time cost taken by devices in our proposed scheme

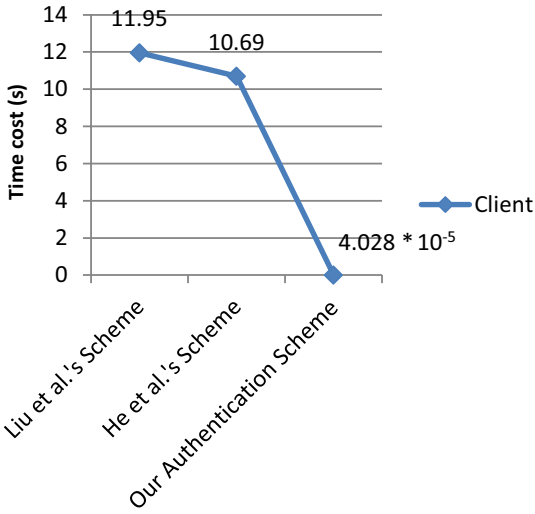


Fig. 5 Gain in computational cost

The results also show that the client is the least active actor in this process of communication as shown in Fig. 4. It is a desirable factor that the computational burden should be decreased over the client, because of client being an energy-constrained node.

Our proposed authentication scheme consumes considerably less time for computation. The former algorithms (Liu et al.'s and He et al.'s) used encryption to provide security and anonymity during authentication. Encryption tends to be a resource-intensive process and consumes more energy of the resource. Our proposed scheme uses hash function to achieve the same (Fig. 5).

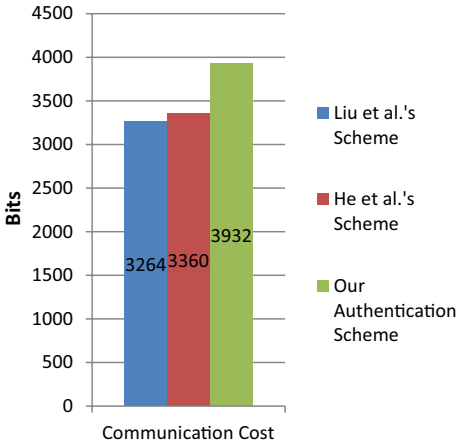
Hashing is a less resource-consuming process as compared to encryption and hence it uses least computational power, which makes it more efficient for this environment as the least the computational resource is used, less energy will be consumed. This fact will increase the battery life of the WBAN device.

F.Wu's et al. used a hash function to anonymously register and authenticate a device in the network.

Table 13 Communication cost

Liu et al.'s scheme	He et al.'s scheme	Our authentication scheme
3264 bits	3360 bits	3932 bits

Fig. 6 Communication cost



2. Communication cost

The communication cost for our proposed authentication scheme is 3932 bits for authentication which tends to be higher than the other two authentication schemes as shown in Table 13.

The communication cost rises to certain bits but the computational cost decreases considerably as shown in Fig. 6. The communication cost is calculated based on the number of bits of a message that travel across network entities.

The rise in communication cost degrades the system but overall performance is achieved by minimizing the computation cost of the system.

6 Security Analysis

A major concern in WBAN is Security due to the sensitive nature of data being transmitted over the network. The breach in security of data or communication could even lead to loss of a life or unrecoverable loss. Being the main concern, we need to maintain security along with improving the performance of WBAN. We prove that our scheme is secure against various attacks through informal security analysis. In order to check the validity of our proposed anonymous authentication scheme, the informal analysis is carried out which shows that our proposed scheme is secure against the following attacks as per Fig. 7.

(a) De-Synchronization Attack

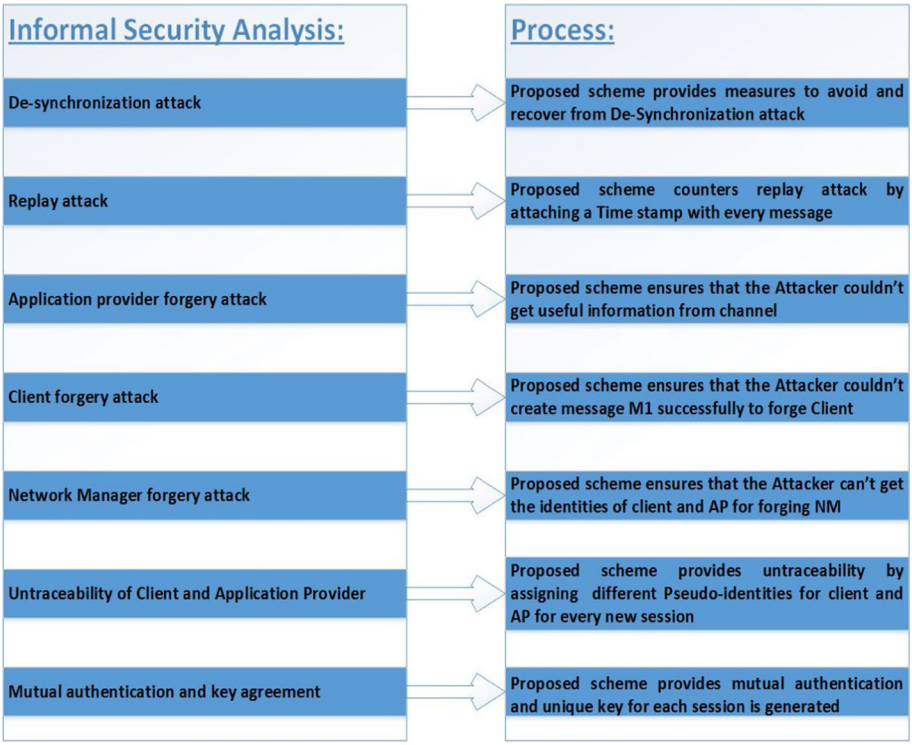


Fig. 7 Informal security analysis

If message M_2 is not received by the client in pairing phase due to network delay or blocked by an attacker, then NM can continue its operations according to last case of step 2 for next pairing.

If message M_5 is not received by the Application Provider in the authentication phase due to network delay or blocked by an attacker, NM can continue its operations according to last case (Case 3) in step 3 of next session. If message $M\text{-}_6$ is not received by the Client in the authentication phase due to network delay or blocked by an attacker, NM can use second case to complete the process.

(b) Replay attack

The time stamp is used in every message to save from replay attack. Therefore, the validity of every message can be checked. If a message is not within the legal time delay, it will be discarded.

(c) Application Provider forgery attack

If the attacker wants to forge message M4, he should make a correct D1 or C2. It is not possible for the attacker to get IDc and XC from communication channels, therefore M4 can't be forged. Similarly, the attacker cannot calculate D1 due to unavailability of IDc and

Xc. C8 requires XA and is used in SKAC, and XA can't be guessed by the attacker. Therefore, M6 cannot be correctly forged.

(d) Client forgery attack

If the attacker wants to forge the client, it needs to reproduce M1 or M3. The attacker requires D1 and C1 for this purpose, but not possible due to unavailability of XC and XA.

(e) Network Manager forgery attack

The attacker requires IDC, XC, IDA and XA to find D2, C3, C4 … etc. in order to forge messages M2 and M5, which is most unlikely.

(f) Untraceability of client and application provider

The client and application provider get a new Pseudo-identity every new session and these pseudo-identities are different from previous ones due to tC and TC. Therefore, the client and application provider are untraceable. The real Identities of client and application provider are never disclosed in the messages.

(g) Mutual authentication and key agreement

Mutual authentication is guaranteed because no entity of any session could be forged. Every session is managed under a unique session key to encrypt information.

7 Conclusion and Future Work

Use of sensors to collect medical information is widely increasing over time. The use of these devices poses certain security and privacy issues for the patient and can be fatal for the life of user. The security of the communication in WBANs has been a great concern but the network is limited due to its low power, computational constrained environment and signal issues. Earlier work in this area has focused on security and privacy issues. They enhance security but on the other hand degrade the performance of WBAN. Our proposed scheme enhances the performance of WBANs considerably maintaining the security and privacy of the whole system. The comparison of our scheme with existing recent anonymous authentication scheme shows that our scheme is improving on performance and hence could increase the life time of the network. The informal security analysis proves the validity of proposed scheme.

In future, we intend to formally analyze this scheme for security using ProVerif tool in future. Also, this scheme can serve as a basis for improving performance issues in WBANs and make the network able to cope with energy issues.

References

1. Zimmerman, T. G. (1996). Personal area networks: Near-field intrabody communication. *IBM Systems Journal, 35*(3.4), 609–617.

2. IEEE standard for local and metropolitan area networks: Part 15.6: Wireless body area networks. *IEEE submission*, Feb. 2012.
3. Smith, D., & Hanlen, L. (2012). Wireless body area networks: Towards a wearable intranet. *ISCIT Tutorial*.
4. Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks, 17*(1), 1–18.
5. Hanson, M. A., Powell, H. C., Jr., Barth, A. T., Ringgenberg, K., Calhoun, B. H., Aylor, J. H., et al. (2009). Body area sensor networks: Challenges and opportunities. *Computer, 42*(1), 58–65.
6. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications Surveys & Tutorials, 16*(3), 1658–1686.
7. Poon, C. C., Zhang, Y. T., & Bao, S. D. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine, 44*(4), 73–81.
8. Wang, H., Fang, H., Xing, L., & Chen, M. (2011une). An integrated biometric-based security framework using wavelet-domain hmm in wireless body area networks (wban). In *2011 IEEE international conference on communications (ICC)* (pp. 1–5). IEEE.
9. Mana, M., Feham, M., & Bensaber, B. A. (2011). Trust key management scheme for wireless body area networks. *IJ Network Security, 12*(2), 75–83.
10. Sarra, E., Moungla, H., Benayoune, S., & Mehaoua, A. (2014). Coexistence improvement of wearable body area network (WBAN) in medical environment. In *2014 IEEE International Conference on Communications (ICC)* (pp. 5694–5699). IEEE.
11. Oberoi, D., Sou, W. Y., Lui, Y. Y., Fisher, R., Dinca, L., & Hancke, G. P. (2016). Wearable security: Key derivation for body area sensor networks based on host movement. In *2016 IEEE 25th international symposium on industrial electronics (ISIE)* (pp. 1116–1121). IEEE.
12. Liu, J., Zhang, Z., Chen, X., & Kwak, K. S. (2014). Certificateless remote anonymous authentication schemes for wireless body area networks. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 332–342.
13. He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2016). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal, 11,* 2590–2601.
14. Wu, F., Li, X., Xu, L., Kumari, S., Karuppiah, M., & Shen, J. (2017). A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. *Computers & Electrical Engineering, 63,* 168–181.
15. Zeng, K., Govindan, K., & Mohapatra, P. (2010). Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. *IEEE Wireless Communications, 17*(5), 56–62.
16. Cai, L., Zeng, K., Chen, H., & Mohapatra, P. Good Neighbor: Ad-Hoc Authentication of Nearby Wireless Devices by Multiple Antenna Diversity.
17. Varshavsky, A., Scannell, A., LaMarca, A., & De Lara, E. (2007). Amigo: Proximity-based authentication of mobile devices. In *UbiComp 2007: Ubiquitous Computing* (pp. 253–270).
18. Moh'd, A., Aslam, N., Phillips, W., Robertson, W., & Marzi, H. (2013). SN-SEC: A secure wireless sensor platform with hardware cryptographic primitives. *Personal and Ubiquitous Computing, 17*(5), 1051–1059.
19. Tirado-Andrés, F., Rozas, A., & Araujo, A. (2019). A methodology for choosing time synchronization strategies for wireless IoT NETWORKS. *Sensors (Basel, Switzerland), 19*(16), 3476. https://doi.org/10.3390/s19163476.

Dr. Syed Jawad Hussain received the Masters in Computer Science degree from International Islamic University Islamabad and the Postgraduate diploma and PhD degree in Multimedia Communication from the Massey University of New Zealand. He is currently an Associate Professor in Computer Science and Information Technology with the CS&IT Department, Islamabad Campus of The University of Lahore. His current research focuses on Computer Networks, Machine Learning and E-Learning.

Muhammad Irfan got his BCS from Allama Iqbal Open University Pakistan in 2003 and received his Masters of Science in Computer Science through research from "The University of Lahore Pakistan" in 2018. His area of interest is optimization of Wireless body area networks. Currently he is seeking admission in Ph.D. with research domain "Security enhancement and optimization of Wireless Body Area Networks.

Prof. Dr. N. Z. Jhanjhi is currently working as Associate Professor with Taylor's University Malaysia. He has great international exposure in academia, research, administration, and academic quality accreditation. He worked with ILMA University, and King Faisal University (KFU) for a decade. He has 20 years of teaching and administrative experience. He has an intensive background of academic quality accreditation in higher education besides scientific research activities, he had worked a decade for academic accreditation and earned ABET accreditation twice for three programs at CCSIT, King Faisal University, Saudi Arabia. He also worked for National Commission for Academic Accreditation and Assessment (NCAAA), Education Evaluation Commission Higher Education Sector (EECHES) formerly NCAAA Saudi Arabia, for institutional level accreditation. He also worked for the National Computing Education Accreditation Council (NCEAC). Dr. Noor Zaman has awarded as top reviewer 1% globally by WoS/ISI (Publons) recently for the year 2019. He has edited/authored more than 13 research books with international reputed publishers, earned several research grants, and a great number of indexed research articles on his credit. He has supervised several postgraduate students, including master's and Ph.D. Dr Noor Zaman Jhanjhi is an Associate Editor of IEEE ACCESS, moderator of IEEE TechRxiv, Keynote speaker for several IEEE international conferences globally, External examiner/evaluator for Ph.D. and masters for several universities, Guest editor of several reputed journals, member of the editorial board of several research journals, and active TPC member of reputed conferences around the globe.

Prof. Dr. Khalid Hussain received his MS IT degree in 1996 from Preston University Islamabad. He did M.S. CS from COMSATS Institute of Information Technology Islamabad in 2007 specializing in Wireless Communication and Networks. He received his Ph.D. from Universiti Tecknolotgi Malaysia specializing Wireless Networks Security.

Dr. Mamoona Humayun has completed her Ph.D. in Computer Sciences from Harbin Institute of Technology, China. She has 13 years of teaching and administrative experience internationally. She has extensive background of teaching, research supervision and administrative work. She has experienced in teaching advanced era technological courses including, Mobile application development (Android), Cyber security and .Net Framework programming besides other undergraduate and postgraduate courses, graduation projects and thesis supervisions. Dr. Mamoona Humayun is the guest Editor and reviewer for several reputable journals and conferences around the globe. She has authored several research papers, supervised a great number of postgraduate students, and external thesis examiner to her credit. She has strong analytical, problem solving, interpersonal and communication skills. Her areas of interest include Cyber Security, Wireless Sensor Network (WSN), Internet of Things (IoT), Requirement Engineering, Global Software Development and Knowledge Management.