IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

An Efficient, Hybrid Authentication using ECG and Lightweight Cryptographic Scheme for WBAN

Zia ur Rehman[1], Saud Altaf[1], Shafiq Ahmed[2], Shamsul Huda[3], Abdel M. Al-Shayea[2], and Sofia Iqbal[4]

[1]University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi 46000, Pakistan
[2]Industrial Engineering Department, College of Engineering, King Saud University, P.O. Box 800, Riyadh 11421, Saudi Arabia
[3]School of Information Technology, Deakin University, Burwood VIC 3128, Australia
[4]Pakistan Space & Upper Atmosphere Research Commission, Islamabad, Pakistan.

Corresponding author: Saud Altaf (e-mail: saud@uaar.edu.pk).

This work is funded by King Saud University, Riyadh, Saudi Arabia through Researchers Supporting Project Number (RSP-2021/387).

ABSTRACT The Wireless Body Area Network (WBAN) plays a pivotal role in providing ubiquitous computing and has applications in different fields, especially in health monitoring. The advancement in wearable devices has revolutionized the concept of medical services and brought ease to our daily lives. However, the latent threat imposed by attackers has increased concerns related to the security and privacy of patient's data due to the open nature of the wireless network. The authentication schemes are used to secure patient's critical data from different types of cyber-attacks. In this paper, we extend our previous work by presenting an anonymous, hybrid authentication scheme that utilized physiological signals in combination with a lightweight cryptographic method to provide robust security against well-known attacks especially key escrow, base station compromise, and untraceability of sessions. The broadly accepted BAN logic is utilized to offer formal proof of mutual authentication and key agreement. The informal verification is performed by the Automated Validation of Internet Security Protocol and Applications (AVISPA) tool. Furthermore, the comparative analysis of the proposed scheme with peer work highlighted that it accomplished better security at low computational, communicational, energy consumption, and storage overheads.

INDEX TERMS Authentication, Cryptography, Cyber-Attacks, Key Agreement, Sensors, Security.

I. INTRODUCTION

The recent developments in technology have opened new avenues in the field of research. The Wireless Body Area Network (WBAN) is one of the promising research directions that has received extensive attention. The medical services have been enhancing due to emerging trends in this technology that has added more convenience to our daily lives. However, the reliance on wireless technology is accompanied by the potential threat of an attacker breaching the privacy and confidentiality of the medical data by passively slipping into the network. The physiological data is usually collected through sensors that are attached to the human body and with the mediation of smartphones it is reached ultimately to the medical practitioner [1]. The architecture of WBAN is depicted in Fig. 1.

The authentication schemes provide a remedy to secure the most critical data of oneself carrying records like Electrocardiogram (ECG), Blood Pressure (BP), sugar level, etc. There are different classifications found in literature, every author has diversely categorized them [2]–[4]. The authentication schemes that utilized the physiological features of patients are considered adequate for the resource constraint devices like in WBAN [5]–[7]. However, they are considered vulnerable to Denial of Service (DoS) attacks, and capturing similar signals from different devices on various parts of the human body is also a challenging issue [8].

The anonymous authentication schemes are another promising category where a lot of research work is going on. It offers lightweight cryptographic solutions suitable for the WBAN environment. Kompara *et al.* [9] presented lightweight anonymous authentication and key agreement scheme using a hash function and XOR operations. Their work protected against various known attacks like

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access

eavesdropping, unlinkable session, hub, and sensor node impersonation attacks. However, the performance results showed that the scheme holds equivalent ground in terms of computation time, energy consumptions, computational cost, and storage overheads. Moreover, on scrutinizing further, we unleashed few vulnerabilities in Kompara *et al.* [9] like sensor node impersonation, base-station, and Intermediate Node (IN) compromise attacks and offered solutions to these vulnerabilities in one of our earlier works, Rehman *et al.* [10]. In the work of Rehman *et al.*, we offered an enhanced scheme by providing not only the solution of identified vulnerabilities but also made architectural level vital changes in the original scheme. Thus reduced the overall communicational cost up to remarkably lower than not only with the original scheme but with peer schemes as well. Similarly, the authentication schemes [11]–[13] are also anonymous, lightweight based on the hash function and XOR operations. These schemes enhanced the earlier work of Li *et al.*'s work [11].

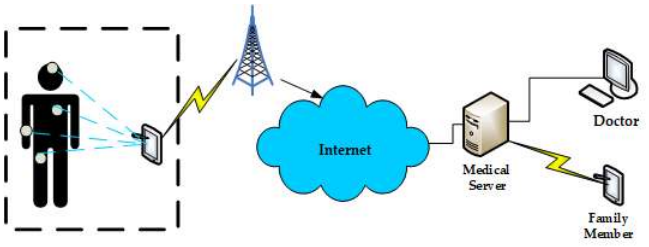


FIGURE 1. The Architecture of WBAN [10]

The hybrid authentication schemes have caught much attention in the research communities because of the promising results achieved by combining physiological signals like ECG, Electroencephalogram (EEG), Photoplethysmogram (PPG), etc with cryptographic solutions. The resultant schemes are more flexible and robust, in providing mutual authentication. Koya et al.[14] presented a hybrid scheme by combining the authentication protocol of Li et al. [11] with ECG signals. The authors devised a 128bit biokey from the ECG signal to enhance the authentication process and thus providing better security. In another recent study, Tao et al. [15] proposed a continuous authentication protocol by utilizing the biokey generation procedure of Koya et al. [14] and mixing it with their authentication algorithm to come up with energy and time-efficient solution. Similarly, the authentication schemes [16]–[18] also utilized biometric signals joint with cryptographic solutions to produce cost-effective solutions. This research work also belongs to the same category.

The major contribution of our paper is to extend our earlier work [10] to further enhance security via the utilization of ECG signals. Our work is summarized as:

- We have extended our earlier work [10] by utilizing physiological signal i.e. ECG and extracted features from the ECG signal to generate a bio-key of variable length. It adds up key entropy and robustness to the authentication process. Moreover, it enhances resilience against key escrow, anonymous unlinkable sessions, and eavesdropping attacks besides the security features already offered in the original work.
- We have proved the correctness of our scheme by well-adopted BAN logic and informally verified by using the Automated Validation of Internet Security Protocol and Applications (AVISPA) tool.
- We have further tuned up the computational cost and energy consumption of the proposed work compared to our earlier work [10]. The performance analysis of our scheme showed that our scheme outperforms based on computational and energy consumption overheads and security characteristics.

The remaining part of the paper is arranged as; section II details the system model of our proposed scheme, section III depicts the details of the proposed authentication scheme containing all its phases, section IV contributed as by providing the details of formal verification using BAN logic, security features analysis and simulation results, section V discusses performance evaluation of proposed scheme with other peer work, section VI provides discussion and finally conclusion as section VII.

II. SYSTEM MODEL

The system model utilized in the proposed scheme consists of network and rival models which are detailed as under:

A. NETWORK MODEL

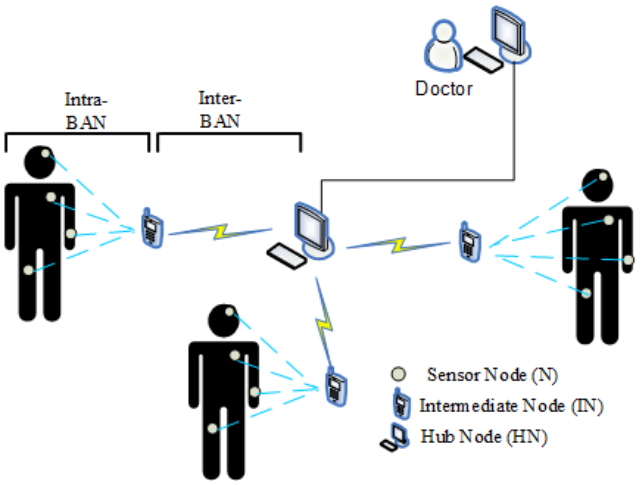
We have retained the network model of our earlier work [10] in this extended scheme which consists of three tiers. Tier 1 consists of sensor nodes denoted by N, tier 2 contains Intermediate Node (IN) normally smartphone or PDA, and tier 3 comprises of Hub Node (HN) normally the server computer. We have modified the communication between N – HN as IN plays the relaying role in the whole model. It does not store any information or identity in itself but passes on any data received from either N or HN to the destination. Thus the role of IN is rather supportive than authoritarian. The network model is depicted in Fig. 2.

B. RIVAL MODEL

We have furnished the following suppositions for our scheme.

- An adversary may not be able to recover the master key K_{UN} because HN is considered secured.
- The data can be falsely injected, altered, or replayed by intercepting the communication.
- An attacker can maliciously disturb the communication by compromising the sensor nodes N and hence disturbing the authentication process. Additionally, N cannot be physically made secured due to cost constraints.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access



- The renowned Dolev-Yao [19] rival model is followed in our scheme which undertakes the parties communicate over insecure channels.

FIGURE 2. The Proposed Scheme's Network Model is based on [10]

III. THE PROPOSED SCHEME

We propose a hybrid authentication scheme that utilizes physiological signals especially ECG and pre-deployed keys for security enhancement of WBAN. The proposed authentication scheme is an extension of our earlier work [10]. Our scheme comprises four phases namely: Bio-key Extraction, registration, authentication, and key update phase. The Intermediate Node (IN) or Hub Node (HN) is referred to as Upstream Node (UN). The notations used are listed in Table I.

A. BIO-KEY EXTRACTION PHASE

We have taken the raw ECG signal and then pre-processed it using Symlet4 (Sym4) Wavelet Transform. The Sym4 wavelet is considered a better choice for QRS detection due to its resemblance with the QRS complex. As we are using Sym4 so the No. of vanishing moments or length of the filter is 8. Here our main objective is to preserve R-waves and eliminate all other frequencies components. Therefore, bandpass action is required which can be achieved using wavelet transform by segregating signal components into different frequency bands. The bandpass filtering can be implemented by removing some unwanted frequency bands (high and low frequencies) and keeping the important ones. This process is shown in Fig. 3. We have taken the following three considerations into account for bio-key extraction:

- The selected method should be less computational suitable for a key update in real-time.
- The extracted key should be random to confirm its robustness.
- The key should be capable of identifying Intra and Interpersonal variations

The bio-key is excerpted from the Inter-Pulse-Interval (IPI) of the filtered ECG signal. We estimate variable-length key size for our proposed authentication scheme. The sync signal from UN will initiate the sampling process of ECG signal for extraction of variable length bio-key. The process of extracting bio-key starts firstly by calculating IPI then the gray coding is applied and lastly, the output bits of gray coding are concatenated to get the result.

TABLE I
THE LIST OF REPRESENTATIONS

Symbol	Description
SA	System Administrator
UN	Upstream Node
N	Sensor Node
id_N	Identity of sensor node N
tid_N	Interim ID
K_{UN}	Master key for UN
K_N	The provisional key for N
r_N, r_{SN},	Bio-Keys extracted from ECG signal.
a_N, x_N, b_N, Z_N	Parameters for authentication.
α, μ, η	Parameters authenticate N.
β	Parameter for Integrity
k_S	Session key
t_N	Timestamp
h(.)	Cryptographic one-way hash operation
$\|$	Concatenate operation
$\oplus$	Exclusive OR operation
x^*	Calculated value lacking an integrity check
x^+	Value for the next authentication round.

The experiments are conducted using multiple channels of ECG data available at PTB Diagnostic ECG database (PTBDB), on PhysioBank ATM resource to check the performance of extracted bio-keys. We have taken data from 8 channel leads i.e., "I, II, V1" to "V6" and calculated the entropy of bio-keys extracted from 4 different subjects as depicted in Table II. It is noticeable that bio-keys exhibit higher randomness as entropy values are closer to 1. The hamming distance between extracted bio-keys is shown in Table III. It is also evident that the technique used for bio-key extraction reveals satisfactory entropy with intra-inter personal variations.

B. REGISTRATION PHASE

This phase is initiated when a new sensor node (N) registers with UN through a secure channel. We have retained the registration phase of our earlier work [10].

1. A distinct identity id_N is assigned.
2. Key K_N is picked for N.
3. $x_N = \mathrm{h}(K_{UN} \| K_N)$
4. $a_N = K_{UN} \oplus K_N \oplus id_N$
5. $Z_N = h(K_{UN} \| id_N)$

The tuple x_N, a_N, Z_N and id_N are stored on N while other parameters $K_{UN}, id_N, and\ K_N$ are stored on UN. The new parameter Z_N holds secret values regarding the key and identity of UN.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access

C. AUTHENTICATION PHASE

The details of this phase (Fig. 4) is as follows:

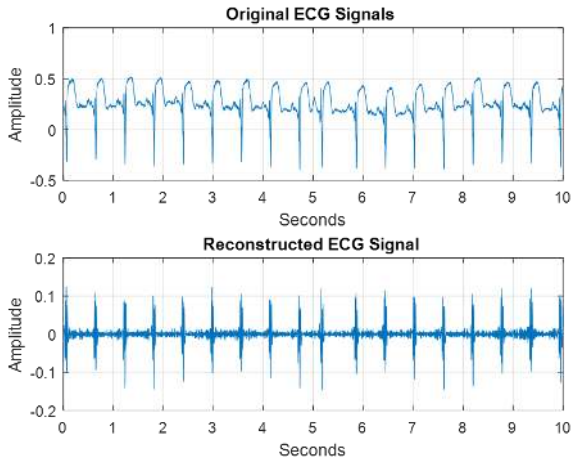


FIGURE 3. The Raw ECG Signal is Reconstructed using Sym4.

1. The upstream node (UN) initiates the process and sends a synchronization signal to sensor node (N) that acquires ECG signals and then bio-key r_N is extracted from it. N generates timestamp t_N and takes another ECG signal to extract another bio-key r_{SN}
   a) $b_N = x_N \oplus r_N$,
   b) $tid_N = \mathrm{h}(id_N \oplus t_N \| r_N \| Z_N)$
   c) Sends (tid_N, a_N, b_N, t_N) to UN

2. The UN ensures the validity of timestamp on receiving (tid_N, a_N, b_N, t_N) and then computes:
   d) $K_N \oplus id_N = K_{UN} \oplus a_N$
   e) Find and confirm valid id_N from the stored values.
   f) $x_N^* = h(K_{UN} \| K_N), r_N^* = x_N^* \oplus b_N$
   g) $Z_N^* = h(K_{UN} \oplus id_N)$
   h) $tid_N^* = \mathrm{h}(id_N \oplus t_N \| r_N^* \| Z_N^*)$
   i) Check $tid_N^* ?= tid_N$ Aborts if the condition fails
   j) Calculates the Hamming distance between two bio-keys r_N and r_{SN}. If it is under the threshold level then both N and UN can be authenticated.
   k) Pick New K_N^+
   l) $x_N^+ = h(K_{UN} \| K_N^+)$
   m) $\alpha = (Z_N^* \oplus r_N) \oplus (x_N^+ \| x_N)$
   n) $\eta = x_N^+ \oplus Z_N^*$
   o) $\mu = K_{UN} \oplus K_N^+ \oplus \alpha$
   p) $\beta = h(r_N \| x_N^+ \| \eta \| \mu)$
   q) Finally the session key
   r) $k_S = \alpha \oplus x_N^+$
   s) Now the UN sends the tuple (β, μ, η) to N.

3. On reception of (β, μ, η), N will compute the following:
   t) $x_N^{+*} = \eta \oplus Z_N$
   u) $\beta^* = h(r_N \| x_N^{+*} \| \eta \| \mu)$
   v) Confirm if $\beta^* = \beta$
   w) $\alpha = (Z_N^* \oplus r_N) \oplus (x_N^{+*} \oplus x_N)$
   x) $a_N^+ = \mu \oplus \alpha \oplus id_N$
   y) $k_S = \alpha \oplus x_N^{+*}$
   z) Now N replaces parameters (x_N, a_N) with (x_N^{+*}, a_N^+)

TABLE II.
THE ENTROPY WORK OUT OF BIO-KEYS

Datasets	I	II	V1	V2	V3	V4	V5	V6	Average
s0020arem	0.982	0.989	0.975	0.982	0.975	0.982	0.982	0.989	0.982
s0022lrem	0.984	0.986	0.99	0.982	0.979	0.989	0.982	0.982	0.98425
s0046lrem	0.986	0.989	0.976	0.986	0.982	0.986	0.996	0.986	0.985875
s00409lrem	0.978	0.982	0.989	0.982	0.978	0.982	0.975	0.982	0.981

TABLE III.
THE HAMMING DISTANCE (HD) AMONG BIO-KEYS

	Datasets	I	II	V1	V2	V3	V4	V5	V6	Average
HD taken at same time between bio-key of Lead I and j	s0020arem	0	6	13	7	5	5	1	4	5.125
	s0022lrem	0	7	6	5	5	5	3	4	4.375
	s0046lrem	0	5	3	5	7	8	5	7	5
	s00409lrem	0	9	3	6	7	10	9	9	6.625
HD taken at different time between bio-key of Lead I and j	s0020arem	62	65	62	61	57	57	61	60	60.63
	s0022lrem	75	74	76	70	73	70	75	77	73.75
	s0046lrem	68	64	62	67	61	64	64	64	64.25
	s00409lrem	58	62	61	60	62	59	62	60	60.5

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access

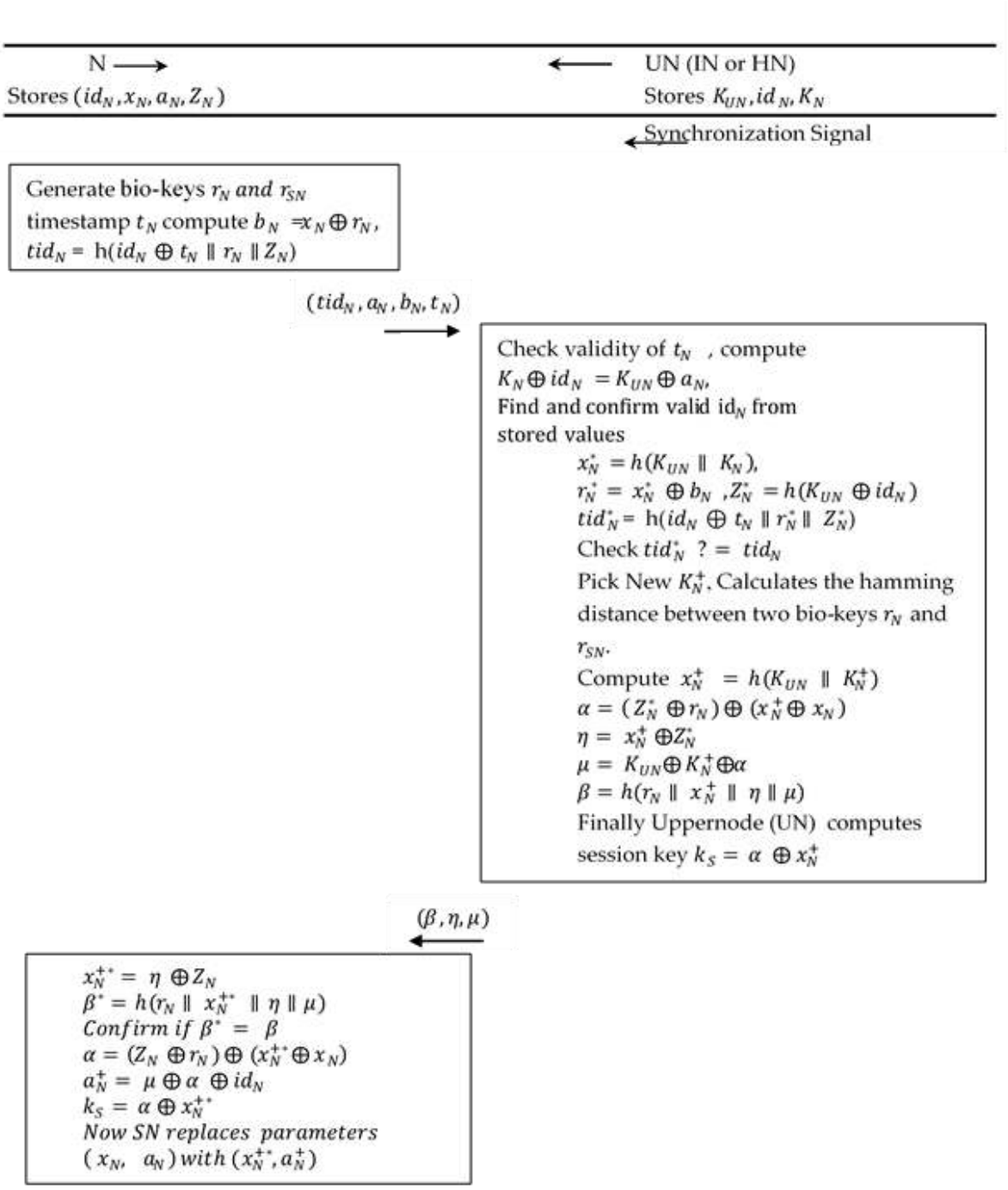


FIGURE 4. **The Proposed Authentication Phase of Hybrid Scheme.**

D. UPDATE PHASE OF MASTER KEY

The key for the UN can be updated in either of two ways, firstly, it can be pre-deployed during installation of nodes at the beginning, or secondly, the nodes can be added dynamically later on. In the first case, the single master key can be pre-deployed while installation of all nodes. In the second case, the UN can have two master keys one is fixed, and the other is a dynamic one. The dynamic bio-key will be used to update all related parameters after the first round of the authentication phase. The procedure of the updated master key begins by following steps.

- The bio-key r_{SN} generated at the registration phase can be utilized to update the master key as:-
- $K_{UN}^+ = K_{UN} \oplus r_{SN}$ This updated master can be utilized to update all the relevant parameter links (x_N^{+*}, a_N^+).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access

IV. SECURITY ANALYSIS OF PROPOSED SCHEME

Here, we analyze our scheme based on formal proof using mathematical modeling commonly based on BAN logic [20] to verify the correctness proposed scheme's correctness. We present security features analysis, and lastly, simulation results depicting informal analysis.

A. FORMAL EVIDENCE USING BAN LOGIC

The BAN logic [20] is widely used to present formal proof of authentication schemes, we have utilized the same to verify that our scheme provides mutual authentication between the nodes N and UN. The following four goals ensure that the proposed scheme is secure.

1) GOALS

G1: $UN \mid \equiv N \mid \equiv (N \overset{x_N^+}{\leftrightarrow} UN)$

G2: $UN \mid \equiv (N \overset{x_N^+}{\leftrightarrow} UN)$

G3: $N \mid \equiv UN \mid \equiv (N \overset{k_S}{\leftrightarrow} UN)$

G4: $N \mid \equiv (N \overset{k_S}{\leftrightarrow} UN)$

2) IDEALIZED FORM

The communicated messages are idealized as:

If1: $N \rightarrow UN : (N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N)_{N \overset{id_N}{\longleftrightarrow} UN}$

If2: $UN \rightarrow N: (N \overset{x_N^+}{\leftrightarrow} UN, r_N, N \overset{k_S}{\leftrightarrow} UN)_{N \overset{id_N}{\longleftrightarrow} UN}$

3) ASSUMPTIONS

To achieve goals we have made few assumptions as:

A1: $UN \mid \equiv (N \overset{id_N}{\longleftrightarrow} UN)$

A2: $UN \mid \equiv \#(t_N)$

A3: $UN \mid \equiv N \mid \Longrightarrow (N \overset{x_N}{\leftrightarrow} UN)$

A4: $N \mid \equiv (N \overset{id_N}{\longleftrightarrow} UN)$

A5: $N \mid \equiv \#(r_N)$

A6: $N \mid \equiv UN \mid \Longrightarrow (N \overset{k_S}{\leftrightarrow} UN)$

4) ANALYSIS

We prove mutual authentication of the proposed scheme based on assumptions, idealized form, and interference rules.

V1: From If1, message-meaning rule, and A1, we get

$$\frac{UN \mid \equiv (N \overset{id_N}{\longleftrightarrow} UN),\ UN \triangle \left(N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N\right)_{N \overset{id_N}{\longleftrightarrow} UN}}{UN \mid \equiv N \mid \sim \left(N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N\right)} \quad (1)$$

V2: By applying the freshness rule and A2, we infer:

$$\frac{UN \mid \equiv \#(t_N)}{UN \mid \equiv \#\left(N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N\right)} \quad (2)$$

V3: From nonce verification rule, (1) and (2), we obtain:

$$\frac{UN \mid \equiv \#\left(N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N\right), UN \mid \equiv N \mid \sim \left(N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N\right)}{UN \mid \equiv N \mid \equiv \left(N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N\right)} \quad (3)$$

V4: From Belie rule, and (3), we achieve the goal G1 as:

$$\frac{UN \mid \equiv\ N \mid \equiv \left(N \overset{x_N^+}{\leftrightarrow} UN, r_N, t_N\right)}{UN \mid \equiv N \mid \equiv \left(N \overset{x_N^+}{\leftrightarrow} UN\right)} \quad (4)$$

Hence we achieve **Goal G1.**

V5: By jurisdiction rule, A3 and (4).

$$\frac{UN \mid \equiv N \mid \Rightarrow (N \overset{x_N^+}{\leftrightarrow} UN),\ UN \mid \equiv\ N \mid \equiv \left(N \overset{x_N^+}{\leftrightarrow} UN\right)}{UN \mid \equiv \left(N \overset{x_N^+}{\leftrightarrow} UN\right)} \quad (5)$$

Hence we achieve **Goal G2.**

V6: By If2, A4, the message meaning rule, we get

$$\frac{N \mid \equiv \left(N \overset{id_N}{\longleftrightarrow} UN\right), N \triangle (x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN)_{N \overset{id_N}{\longleftrightarrow} UN}}{N \mid \equiv UN \mid \sim \left(x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN\right)} \quad (6)$$

V7: By the freshness rule, and A5, we obtain

$$\frac{N \mid \equiv \#(r_N)}{N \mid \equiv\ \#\left(x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN\right)} \quad (7)$$

V8: By nonce verification rule, (6), and (7), we acquire

$$\frac{N \mid \equiv \#\left(x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN, N \overset{id_N}{\longleftrightarrow} UN\right), N \mid \equiv UN \mid \sim \left(x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN\right)}{N \mid \equiv UN \mid \equiv \left(x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN\right)} \quad (8)$$

V9: By the belief rule and (8)

$$\frac{N \mid \equiv UN \mid \equiv \left(x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN\right)}{N \mid \equiv UN \mid \equiv \left(N \overset{k_S}{\leftrightarrow} UN\right)} \quad (9)$$

Hence the **goal G3** is achieved.

V10: By the jurisdiction rule, A6 and (9), we have

$$\frac{N \mid \equiv UN \mid \Rightarrow (N \overset{k_S}{\leftrightarrow} UN), N \mid \equiv UN \mid \equiv \left(x_N, x_N^+, r_N, N \overset{k_S}{\leftrightarrow} UN\right)}{N \mid \equiv \left(N \overset{k_S}{\leftrightarrow} UN\right)} \quad (10)$$

Therefore, we obtained **goal G4**.

B. SECURITY FEATURES ANALYSIS

The following are the security features provided by the proposed scheme that extends our earlier work [10].

1) RESILIENCE AGAINST KEY ESCROW

It becomes a problem when a security threat is imposed by an insider like system admin, physician, etc., Therefore, fixed master key K_{UN} would be a potential threat. Our scheme has provided a dynamic update of the master key by extracting a new bio-key and generating the new master key. This feature eliminates the potential threat of impersonation of nodes N and UN. Hence we resolved Key escrow problem.

2) EAVESDROPPING ATTACK

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access

An eavesdropper can collect the parameters sent over a public network like (tid_N, a_N, b_N, t_N) and the same holds for (β, μ, η). Even if an adversary can collect it but it cannot forge secret values like bio-key r_N, x_N^+, K_{UN}^+, K_N^+, x_N, and K_N. Some of these values are XOR-ed with other secrets parameters in such a blend that it is impossible to eliminate all. Therefore, an eavesdropper cannot uncover or even construct the secret key k_S.

3) ANONYMOUS AND UNLINKABLE SESSIONS

Anonymity is a feature that allows us to keep the identity hidden from an adversary. This feature is well preserved in our scheme by utilizing the temporary identity tid_N, that is secured by a non-reversible hash function and it also contains the bio-key r_N forged randomly by N. An adversary cannot guess the valid set of tuples used for tid_N and hence it cannot link the two sessions. Another reason is that all parameters transmitted over the public network are formalized using fresh and secret values. Some parameters keep on changing in each session like b_N that is constructed on random bio-key and K_N^+. Therefore, unlinkability and anonymity of sessions are achieved in our proposed scheme.

4) SENSOR NODE IMPERSONATION AND CAPTURE ATTACK

To implement a sensor node impersonation attack, an adversary has to generate the valid tuple (tid_N, a_N, b_N, t_N) which would be impossible because they are protected by hash functions, the randomness of bio-key and Z_N. An attacker would have to know the master key K_{UN} for capturing sensor node, which would not be possible because the key is updated afterward and it would also require another bio-key r_{SN}. Therefore, the proposed scheme provides resilience against both types of attacks.

5) BACKWARD AND FORWARD SECRECY

An adversary would have to know the parameters α and x_N^+ before forging the session key k_S which would be impossible and even if somehow he has constructed it, the session keys for past and future will not be revealed. The parameters are calculated dynamically during every session and the values would be changed. Therefore, this feature is added to the list.

6) BASE STATION CAPTURE ATTACK

If the base station (UN in our case) is compromised somehow, and the master key K_{UN} is captured. An adversary would also require some other valid parameters like $x_N^+, \alpha, \beta, \eta, k_S$ and the master key is also updated with random bio-key r_{SN} which is constructed through a random ECG sample of the patient. Therefore, this attack would not be possible.

7) IN COMPROMISE ATTACK

The Intermediate Node (IN) does not store any identity, it is utilized only as relaying node, therefore, compromising it would not make much of the difference. Therefore, launching successive impersonation attack would be difficult. To forge identity parameters like bio-key r_N and Z_N would also be required which are not communicated publically.

8) DESYNCHRONIZATION / JAMMING ATTACK

This type of attack prevents the communicating entities (N and UN in our case) to synchronously update their mutual parameters by jamming the link. In such a case the sensor node N would not able to calculate new values for (x_N^{+*}, a_N^+). Nevertheless, the proposed scheme can continue with a new authentication phase along with older values (x_N, a_N).

C. SIMULATION USING AVISPA TOOL

Here, we accomplish informal verification using a widely utilized tool for cryptographic protocols' verification called AVISPA [21] which testifies the safety of the proposed scheme. The High-Level Protocol Specification Language (HLPSL) is utilized to code the scheme which is translated into Intermediate Format (IF). The IF is run through backends verification models i.e., On-the-Fly Model Check (OFMC) and Constraint Logic-based Attack Searcher (CL-AtSe). The output of these models assures that the proposed scheme is safe and provides resilience against attacks whether active or passive. The summary report of OFMC and CL-AtSe are shown in Fig. 5 (a) and (b) respectively.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/keyAthn1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.20s
```

(a) OFMC Implementation Results

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/keyAthn1.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed  : 1 states
  Reachable  : 1 states
  Translation: 2.15 seconds
  Computation: 0.00 seconds
```

(b) CL-AtSe Implementation Results

Figure 5. **The Simulation Results depicted in (a) and (b)**

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access

V. PERFORMANCE EVALUATION

The performance of the proposed scheme is evaluated based on storage, energy communicational, and computational overheads with related work i.e., Koya *et al.*[14], Tao *et al.* [15], Xu *et al.* [22], Wazid e*t al.* [16]., Rehman *et al.*[10] We present a comparison with state-of-the-art authentication schemes of a similar category. The performance of our proposed scheme can easily be judged throughout this section. The security features comparison is detailed in Table IV.

TABLE IV
SECURITY FEATURES COMPARISON

	[14]	[15]	[16]	[22]	[10]	Ours
Z1	Y	Y	Y	N	N	Y
Z2	Y	N	Y	Y	Y	Y
Z3	Y	Y	Y	Y	Y	Y
Z4	Y	Y	Y	Y	Y	Y
Z5	Y	Y	Y	Y	Y	Y
Z6	Y	N	N	N	Y	Y
Z7	N	N	N	N	Y	Y
Z8	Y	N	N	Y	N	Y

Z1: Key escrow, Z2: Eavesdropping attack, Z3: Anonymous and unlinkable sessions, Z4: Sensor node impersonation & capture attack, Z5: Backward & forward secrecy, Z6: Base-station capture attack, Z7: IN compromise attack, Z8: Desynchronization/jamming attack

A. STORAGE COST

As per [10], the sensor node (N) stores parameters like (id_N, x_N, a_N, Z_N) along with session key k_S requires 160bits each, while Intermediate Node (IN) performs as relaying node without storing anything. The Upstream Node (UN) saves the tuple like K_{UN}, id_N, K_N besides session key k_S, each requires 160 bits. The storage cost and comparison with peers is depicted in Table V.

TABLE V
THE STORAGE COST COMPARISON

Peers	N	IN	UN (HN)
[14]	640 b	640 b	(320+160n) b
[15]	800 b	480 b	(480n+480m+160) b
[16]	1600 b	800 b	(800n+800m+160) b
[22]	1280 b	32 b	(768n+32m+512) b
[10]	800 b	0 b	(480n+160)b
Ours	800 b	0 b	(480n+160)b

n: No. of sensor nodes, m: No. of the intermediate nodes, b: bits

B. COMMUNICATION COST

The communication cost or proposed scheme is calculated by the number of messages exchanged between N and UN. The first message transmitted to UN from N is (tid_N, a_N, b_N, t_N) and the timestamp $|t_N|$ = 32 b. Therefore, the cost of sending a message from N ⟶ UN is 512 b whereas, the cost of receiving the message is 480 b. The communication cost is detailed in Table VI.

TABLE VI
THE COMMUNICATION COST COMPARISON

Peers	N→ IN	IN→HN	HN→IN	IN→N
[14]	672	1344	960	480
[15]	672	864	496	496
[16]	512	672	672	512
[22]	832	864	1120	1088
[10]	512	512	480	480
Ours	512	512	480	480

C. COMPUTATION COST AND TIME

The time it takes to perform the hash function be denoted as t_h while the time it takes for XOR operation to perform is denoted as t_{xor}. The N-side of the authentication phase of our scheme used 2 hash functions and 8 XOR operations while UN-side has 5 hash functions and 10 XOR. So, the equation on N-side as well as on UN-side is formalized as $2t_h + 8t_{xor} \approx 2t_h$ and $5t_h + 10t_{xor} \approx 5t_h$ respectively as XOR operations require negligible time therefore it is ignored.

As per an experiment performed by [22] t_h = 0.0023ms, t_r = 0.65 ms, t_{ecm}= 0.123 ms. Therefore, our scheme consumes 0.0069 ms on N-side and 0.0138ms on UN-side. The comparison on the basis of same parameters are detailed in Table VII.

TABLE VII
THE COMPUTATIONAL COST AND TIME COMPARISON

Peers	Node	Cost	Time
[14]	N	$5t_h + 5t_{xor} \approx 5t_h$	0.0115ms
	UN	$8t_h + 11t_{xor} \approx 8t_h$	0.0184ms
[15]	N	$13t_h + 4t_{xor} + 2t_r \approx 13t_h + 2t_r$	0.160ms
	HN	$11t_h + 4t_{xor} + 3t_r \approx 11t_h + 3t_r$	0.220ms
[16]	N	$14t_h + t_{ecm}$	0.1552ms
	HN	$19t_h$	0.0437ms
[22]	N	$5t_h + 5t_{xor} \approx 5t_h$	0.0115ms
	HN	$7t_h + 9t_{xor} \approx 7t_h$	0.0161ms
[10]	N	$3t_h + 6t_{xor} \approx 3t_h$	0.0069ms
	UN	$6t_h + 10t_{xor} \approx 6t_h$	0.0138ms
Ours	N	$2t_h + 8t_{xor} \approx 2t_h$	0.0046ms
	UN	$5t_h + 10t_{xor} \approx 5t_h$	0.0115ms

D. ENERGY CONSUMPTION

The consumption of power during active mode is calculated as 118.8mW, this implies our scheme consumes 0.0046 * 118.8 / 1000 ≈ 0.547μJ on N-side and 0.0115*118.8/1000≈1.366 μJ. The comparison with peer work is depicted in Table VIII.

TABLE VIII
THE COMPARISON OF ENERGY CONSUMPTION

Peers	N (μJ)	HN (μJ)
[14]	1.366	2.186
[15]	9.0	6.14
[16]	8.44	5.19
[22]	1.366	1.913
[10]	0.819	1.639
Ours	0.547	1.366

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3115706, IEEE Access

C. THE PERFORMANCE RESULTS COMPARISON

While comparing the results of storage cost in Table V, it is noticeable that the proposed scheme does not store any data on IN therefore it can be concluded that the overall storage requirement is less than other schemes except our earlier work [10]. Moreover, while comparing communicational cost, it is revealed from Table VI, the reflection of no storage on IN impacted positively in terms of no extra communication cost added to the scheme but it is the same as [10]. Therefore, our proposed scheme has incurred the lowest communicational cost than the peer work. It is also highlighted through Fig. 6 that the communication process between IN – UN and vice-versa has been improved significantly. It is also worth stating here that the communication cost depicted, is the cost of the whole process starting from N – UN and reverse.

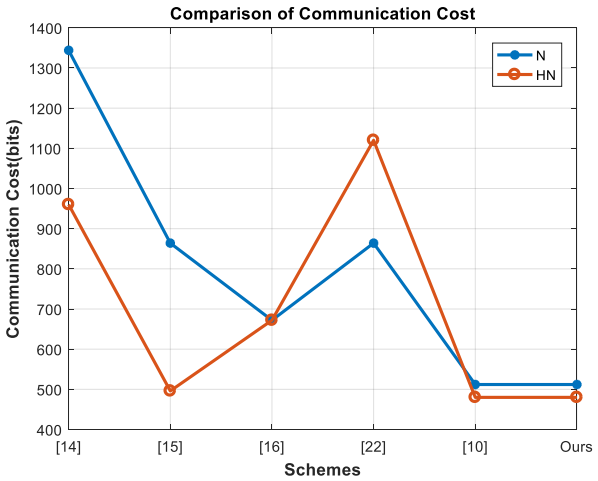


Figure 6. **The Comparison of Communicational Cost**

The computational cost and time are depicted in Table 7 where it is evident that the proposed scheme has achieved the lowest computation on N and UN (in our case) as compared to peer work including our earlier work [10]. Therefore, our scheme is efficient in terms of computational cost as well. This fact is made evident from Fig. 7 as well

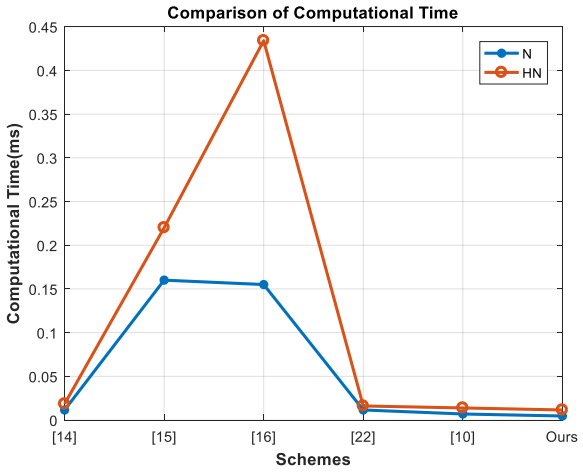


Figure 7. **The Comparison of Computational Cost**

Furthermore, the energy consumption is shown in Table 8. It is calculated in micro Joules (µJ) and by comparing it with peer work, we claim that the proposed scheme is efficient in terms of energy consumption as well. As shown in Fig. 8.

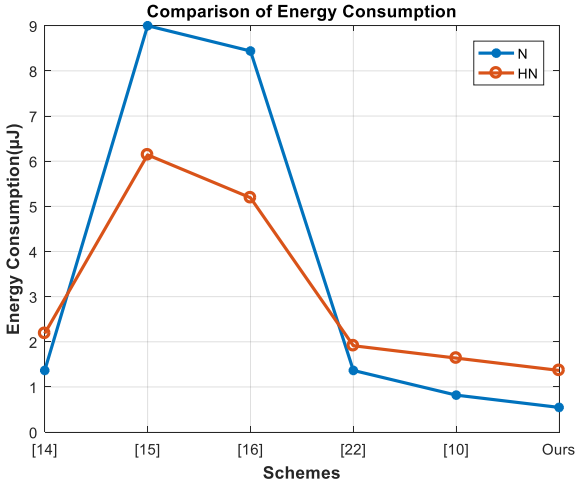


Figure 8. **The Comparison of Energy Cost**

VI. DISCUSSION

We have extracted variable-length bio-key from ECG signal with high randomness and key entropy. The variable-length keys are usually difficult to judge, therefore, the chances of applying a guessing attack are eliminated. We have adopted a bio-key extraction procedure that requires less computation time thus resulting in increased efficiency. The proposed scheme offered a dynamic key update feature that added up resilience against attacks like key escrow, eavesdropping, base-station compromise, and untrackability, etc. Moreover, the performance evaluation discussed in the previous section highlighted the concept that the proposed scheme behaved better than other hybrid schemes as shown in Figures 6 – 8. It is also worth mentioning here, although we have enhanced our work successfully in terms of computational cost and energy consumption, however, the storage requirements and communicational cost remains the same as previously [10] because storage and communicational requirements are already optimized enough that cannot be further reduced. Therefore, we claim that the proposed scheme further tune-up the authentication algorithm. Hence the proposed scheme accomplished efficiency, to provide anonymous and lightweight authentication and key agreement scheme.

VII. CONCLUSION

We have presented a hybrid authentication scheme that utilized physiological features extracted from ECG signal to generate a variable length bio-key and mixed it with a cryptographic solution of our earlier work [10] by further optimizing it. The formal proof of concept is provided using BAN logic and it is shown that the proposed scheme achieved security goals and mutual authentication. The simulation

results informally proved that the schemes withstand the various known security attacks using the AVISPA tool. We have evaluated the performance in terms of storage, computation, communication, and energy consumption overheads. We have also compared the results with renowned related schemes and proved that our scheme is efficient in terms of storage, computation, communication, and energy consumption costs.

ACKNOWLEDGMENT

The authors extend their appreciation to King Saud University for funding this work through Researchers Supporting Project number (RSP-2021/387), King Saud University, Riyadh, Saudi Arabia.

REFERENCES

[1] C. K. Yeh, H. M. Chen, and J. W. Lo, "An authentication protocol for ubiquitous health monitoring systems," *J. Med. Biol. Eng.*, vol. 33, no. 4, pp. 415–419, 2013.

[2] Z. U. Rehman, S. Altaf, and S. Iqbal, "Survey of Authentication Schemes for Health Monitoring: A Subset of Cyber Physical System," in *Proceedings of 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019*, 2019, pp. 653–660.

[3] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, no. June, p. 101660, 2019.

[4] M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, "Authentication Techniques and Methodologies used in Wireless Body Area Networks," *J. Syst. Archit.*, vol. 101, p. 101655, 2019.

[5] A. Farajidavar, G. Weiss, A. Alhayajneh, T. Hayajneh, and A. Baccarini, "Biometric Authentication and Verification for Medical Cyber Physical Systems," *Electronics*, vol. 7, no. 12, p. 436, 2018.

[6] H. Tan and I. Chung, "Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019.

[7] P. Dodangeh and A. H. Jahangir, "A biometric security scheme for wireless body area networks," *J. Inf. Secur. Appl.*, vol. 41, pp. 62–74, 2018.

[8] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks.," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–8, 2010.

[9] M. Kompara, S. H. Islam, and M. Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," *Comput. Networks*, vol. 148, pp. 196–213, 2019.

[10] Z. Rehman, S. Altaf, and S. Iqbal, "An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN," *IEEE Access*, vol. 8, pp. 175385–175397, 2020.

[11] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Networks*, vol. 129, pp. 429–443, 2017.

[12] C. Chen, B. Xiang, T. Wu, and K. Wang, "An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks," *MDPI*, vol. 8, no. 1074, pp. 1–15, 2018.

[13] C. Chen, B. Xiang, T. Wu, and K. Wang, "An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks," MDPI, vol. 8, no. 1074, pp. 1– 15, 2018

[14] A. M. Koya and D. P. P., "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Networks*, vol. 140, pp. 138–151, 2018.

[15] T. Wan, L. Wang, W. Liao, and S. Yue, "A lightweight continuous authentication scheme for medical wireless body area networks," 2021.

[16] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *J. Netw. Comput. Appl.*, vol. 123, no. September, pp. 112–126, 2018.

[17] S. Challa *et al.*, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, 2018.

[18] H. Chen, D. Ding, S. Su, and J. Yin, "Biometrics-based cryptography scheme for E-Health systems," *J. Phys. Conf. Ser.*, vol. 1550, no. 2, 2020.

[19] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[20] S. J. Mullender, "BAN Logic A Logic of Authentication," pp. 1–23.

[21] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, and L. Compagna, "The AVISPA Tool for the Automated Validation," *Comput. Aided Verif.*, vol. 3576, pp. 281–285, 2005.

[22] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical internet of things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019.

[23] G. C. C. F. Pereira, R. C. A. Alves, F. L. da Silva, R. M. Azevedo, B. C. Albertini, and C. B. Margi, "Performance evaluation of cryptographic algorithms over IoT platforms and operating systems," *Secur. Commun. Networks*, vol. 2017, 2017.

ZIA UR REHMAN is currently Ph.D. Scholar at the University Institute of Information Technology (UIIT) of Pir Mehr Ali Shah Arid Agriculture University (PMAS - AAR), Rawalpindi, Pakistan. He received his master's degree in Computer Science in 2008 from Muhammad Ali Jinnah University, Islamabad, Pakistan. His major research interests involve security issues in health monitoring aspects of Cyber-Physical System (CPS), Internet of Things (IoT), and wireless sensor networks.

SAUD ALTAF is an Assistant Professor at UIIT of PMAS - AAR University, Rawalpindi, Pakistan. He received his Ph.D degree in Computer Science from Auckland University of Technology (AUT), New Zealand in 2015 and master degree in Computer Science from Iqra University, Islamabad, Pakistan in 2007. He is author of number of research publications in international journals or conferences proceedings. His research interests span over several fields of Wireless Sensor Networks, Biomedical signal and image processing, security of Cyber Physical System (CPS), Gesture Recognition, Through-the-wall Radar Imaging and sensing, visible light communication, Internet of Things (IoT), Artificial Intelligence and Data Mining.

SHAFIQ AHMAD received the PhD degree from RMIT University, Melbourne, Australia. He is currently working as an Associate Professor at Industrial Engineering Department, College of Engineering King Saud University Riyadh Saudi Arabia. He has more than two decades working experience both in industry and academia in Australia, Europe and Asia. He has published a research book and several research articles in

international journals and refereed conferences. His research interests are related to smart manufacturing, IIOT and data analytics, multivariate statistical quality control; process monitoring and performance analysis; operations research models and bibliometric network analysis. He is also a certified practitioner in Six Sigma business improvement model.

ADEL AL-SHAYEA is a consultant industrial engineer (CE-SCE). He is a member of the Saudi Council of Engineers (SCE) Saudi Arabia as well as a member of several national committees. He is currently consultant in the office of Deputy Minister of Education and associate professor at Industrial Engineering Department, College of Engineering. Previously, Dr. Al-Shayea was the assistant vice rector for educational and academic affairs at King Saud University, and a consultant for Shaqra University Rector, as well as consultant at King Saud University Rector's Office. Dr. Al-Shayea worked for SABIC Marketing Ltd. in Riyadh and at the Institute of Public Administration (IPA). In addition, Dr. Al-Shayea is a consultant in King Abdullah Institute of Research and Consulting Studies. He participated and conducted several researches and consultative works for governmental and private organizations

SHAMSUL HUDA received his PhD degree in computer science at the Centre for informatics and applied optimization (CIAO) at Federation University Australia. Currently he is a Lecturer in School of Information Technology, Deakin University, Australia. Prior to join Deakin, he worked as an academic in Federation University and as an Assistant Professor in Khulna University of Engineering and Technology (KUET), Bangladesh. Dr Huda is a Certified Information System Security Professional (CISSP) by The International Information System Security Certification Consortium, (ISC)² . He is also a member of Cyber Security Research and Innovation Centre (CSRI) at Deakin University. Dr Huda is involved in many international cyber security projects including Cybersecurity capacity maturity for nations at Oceania Cyber Security Centre (OCSC), Melbourne with partnership of the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. His main research areas are Communication and network security, strategies for secure operations for Industrial Control systems (SCADA) and Critical infrastructure, Intelligent counter measure for threats against Mobile system, detection of data breaches through the darknet, IoT security, Malware analysis and detection, reverse engineering for endpoint security, malware analysis and detection for SCADA systems. He has published more than 60 journal and conference papers in well reputed journals including IEEE Transactions.

SOFIA IQBAL received the MPhil. degree in Applied Statistics from Quaid-e-Azam University, Islamabad, Pakistan, in 2012. She has had more than twelve years of practical experience in the public sector in the area of data analysis. She is a member of different professional societies around the world. Currently, she is working as data analyst manager in Pakistan Space and Upper Atmosphere Research Commission (SUPARCO), Islamabad, Pakistan; Email; sofiaiqbal.suparco@gmail.com.