IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 26, 2020, accepted October 12, 2020, date of publication October 15, 2020, date of current version October 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3031484

An Improved Lightweight Authentication Protocol for Wireless Body Area Networks

BANDER A. ALZAHRANI[1], (Member, IEEE), AZEEM IRSHAD[2], AIIAD ALBESHRI[1], KHALID ALSUBHI[1], (Member, IEEE), AND MUHAMMAD SHAFIQ[3]

[1]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2]Department of Computer Science and Software Engineering, International Islamic University Islamabad, Islamabad 44000, Pakistan
[3]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea

Corresponding authors: Bander A. Alzahrani (baalzahrani@kau.edu.sa), Azeem Irshad (irshadazeem2@gmail.com), and Muhammad Shafiq (shafiq@ynu.ac.kr)

ABSTRACT The wireless body area networks (WBANs) play a vital role in the state-of-the-art medical systems for remote monitoring and maintaining the health of patients. These WBANs collect the real-time health status of patients using intelligent sensors and submit to servers through internet for being utilized by the medical experts. This communication must be anonymous as well as secure from attackers for reliable dispensation of medical services. In recent years, many authentication protocols for WBAN could be witnessed. In this study, we demonstrate that one of the most recently presented WBAN-based authentication protocol is found to be prone to session-specific temporary information attack, key compromise impersonation as well as session key recovery attacks. Thereafter, we propose an efficient, secure and anonymous WBAN authenticated key agreement scheme addressing the identified concerns in previous scheme. In due course, we assess the performance of contributed scheme informally as well as formally with the use of ProVerif automated tool and random oracle model. The performance findings also indicate that our scheme not only achieves efficiency but offers robust and implementable security features.

INDEX TERMS Authentication, wireless body area networks, patient healthcare, cryptography, medical sensors.

I. INTRODUCTION

The increasing pace of development in the wireless communication, implantable medical sensors, and low-cost technology of cloud computing facilitated the successful deployment of WBANs [1], [2]. The WBAN network comprises a mobile device (such as smart phone or PDA) and several medical sensors that continuously capture the real-time status for biological parameters of patient such as heart beat, blood sugar, blood pressure etc. The captured data is then submitted to medical servers over wireless communication channel for further processing and possible action if the medical professional suggests. The medical sensors could be implanted over and under the body skin, or even in clothes, and could accommodate the whole body. Owing to WBAN, the patient can freely move, leave bed and go out of hospital for a short period of time, which improves the life style of patient and also reduces treatment cost. Besides, collecting data in a comfortable zone of the patient would produce more reliable and accurate diagnostic results.

The WBAN system comprises first level nodes, second level nodes, and server acting as a hub node [3]–[5], [9], [10]. The second level nodes comprising body sensors and wearable devices of the patient, submit the captured data to hub node through first level nodes which act as the intermediary nodes having more computational, communication and storage capacity than second level nodes. This model is composed of three tiers, i.e., the first-tier (intra BAN) enables the interaction between second and first level nodes, the second-tier (inter BAN) helps to establish contact between first level nodes and server nodes, while the third-tier being beyond the WBAN deals with communication between hub node server and medical experts as shown in Fig. 1. The WBAN system is meant for exchanging critical health status and information of patients with the corresponding server or medical professionals. The privacy of the patient needs to be maintained through ensuring confidentiality, and the exchanged data must not be forged or tampered on the way to warrant a reliable health-monitoring system. The inherent nature of WBAN is based on

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

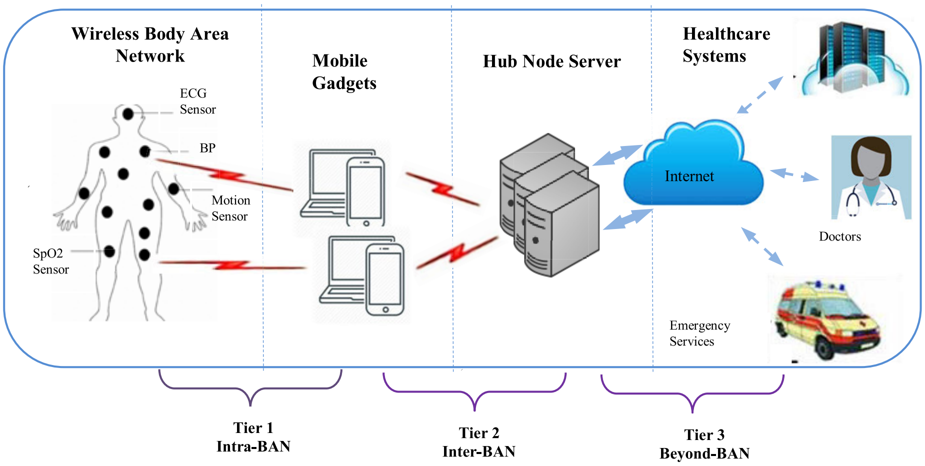


FIGURE 1. A generic architecture of WBAN.

wireless communication as the patient could walk and roam in the hospital or home which further underscores the need for underlying communication protocol to be computationally efficient as well as secure from various attacks. The wireless channel is more prone to attack, and an adversary can attempt eavesdropping and misusing the public channel by modifying the message contents [11], [12]. Hence, due to the power and computational constraints in second level nodes or mobile devices, the solutions presented for other applications cannot be directly applied in WBAN systems. Many researchers have presented several authentication protocols for WBAN systems however with limitations in terms of security or efficiency. Moreover, these schemes along with other security loopholes were unable to comply with anonymity properties.

A. THREAT MODEL

In this scheme, we assume an attacker $\overset{\frown}{A}$ having control over public channels in the first two tiers, i.e. Intra-BAN and Inter-BAN. Owing to this, $\overset{\frown}{A}$ may eavesdrop, alter, delete, and replay contents eavesdropped from the public channel. In this scenario, the constructed protocol must ensure that the attacker cannot attempt modifying, deleting, and replaying contents, or initiate any forgery or de-synchronization attacks. As per the Canetti and Krawczyk [49] model, an adversary may access either session specific temporary information, or sensor node's private key, or hub node's master secret key, but not all simultaneously. Further, the adversary may attempt guessing the identity or intruding into the privacy of the sensor node.

B. MOTIVATION AND CONTRIBUTION

In order to aid remote-patient monitoring for hospitals and physicians outside of the conventional clinic-setting, a secure and efficient authenticated key agreement (AKA) for WBAN is crucial. For this purpose, an effective WBAN-based AKA must hold the following properties. i.e. 1) Anonymity as well as un-traceability for the user, 2) Session key security, i.e. the attacker may not be able to compute or extract the session key from eavesdropped contents, 3) Replay and impersonation attacks, i.e. the attacker may not be able to initiate forgery attacks, 4) Backward and forward secrecy, i.e. the attacker should not be able to compute earlier sessions keys in case the long term secret or current session key is revealed to the former. Nonetheless, many AKA schemes for WBAN network including few recent schemes [4], [31], [35]–[37], [44] do not comply with the stipulated objectives, since these are prone to many issues such as lacking anonymity, susceptible to impersonation, replay and forgery attacks [50].

This paper makes the understated key contributions:

1) We proposed a novel lightweight patient-health monitoring authentication protocol in the wake of critical evaluation based on a recent state-of-the-art research study.
2) Our security solution not only withstands well known attacks, but also confers anonymity to the user by permitting the authenticated key agreement through hiding its identity.
3) The security features of proposed scheme are verified with the help of automated protocol analyzer i.e., ProVerif tool, and validated under random oracle model.
4) The comparative analysis of the contributed scheme is performed with other related models that positively warrant the practical implications the scheme.

The rest of the scheme is organized as follows: Section II illustrates the related work in authentication protocols for WBAN. Section III presents the review for Ostad-Sharif *et al.* and limitations. Section IV demonstrates the proposed model. Section V analyzes the contributed scheme on informal basis as well as presents formal security analysis using ProVerif tool and BAN logic analysis. The section VI evaluates the performance results, while the last section depicts the concluded findings.

II. RELATED WORK

In 2011, Al Rassan and Khan [8] presented an efficient key agreement scheme for WBAN. Later, Kumbhare *et al.* [9] demonstrated another message authentication code (HMAC)-based WBAN authenticated key agreement protocol. Afterwards, in 2012 Liu *et al.* [10] introduced an anonymous authenticated key agreement WBAN protocol with other sound security features, including the inability of application servers to guess the subscriber's identity. Then, Zhang *et al.* [11] presented a new authentication protocol for body area networks by employing a shared key based on electrocardiogram (ECG) signals with the implementation of Improved Jules Sudan (IJS) algorithm to authenticate the message. Thereafter, in 2013, He *et al.* [12] came forward with another efficient transmission protocol for WBAN by employing the symmetric encryption algorithm, i.e., advanced encryption standard (AES) for low communication and computational cost. Then, Ma *et al.* [13] suggested another lightweight authenticated key agreement protocol with the use of zero-knowledge proof (ZKP). Later, Ramli *et al.* [14] applied ECG signals to secure the communication in WBAN network. Then, Igbal *et al.* [15] presented a cost-efficient smart-crypto protocol with the introduction of cluster heads for securing wireless body area networks. Next, Chen *et al.* [16] demonstrated another lightweight protocol for wearable body sensors, however, Li *et al.* found weaknesses in Chen *et al.* regarding inability to detect wrong password in login phase, and non-compliance to forward secrecy. Then, Li *et al.* presented an improved WBAN authentication protocol [17]. Again Liu *et al.* [18] demonstrated an anonymous and cost-efficient authentication scheme for WBANs. Thereafter, Zhao [19] indicated that [18] protocol is vulnerable to stolen-verifier attack, and then introduced an improved scheme. Also, Xiong [20] found that [18] protocol does not comply with scalability and forward secrecy, and later on suggested an anonymous, scalable and certificateless authentication protocol which supports forward secrecy as well. Next, Sangari and Manickam [43] presented an enhanced diagnostic healthcare system in WBAN with a focus on privacy. In 2015, Chhajed *et al.* [21] demonstrated two certificate-less WBAN protocols supporting anonymity to the user while the latter accesses the medical services. Then, Xiong and Qin [22] introduced a scalable and revocable certificate-less WBAN authentication key agreement protocol. Next, Wang and Zhang [23] employed bilinear pairing operations to design an authentication protocol for WBAN ensuring anonymity after putting forward the privacy-based drawbacks in Zhao scheme [19]. Ali and Khan [24] took a critical and comparative analysis of various WBAN authentication protocols in terms of efficiency and security. Then, He and Zeadally [25] exhibit another healthcare monitoring protocol for Ambient Assisted Living (AAL) system. In 2016, Ibrahim *et al.* [26] introduced exhibited a novel protocol for authentication in WBAN system using two tier topology with claim that it could resistant forgery attacks, spoofing attacks and replay attacks. Onwards, Andrew Omala *et al.* [27] pointed that any malicious application provider may forge the user in Wang and Zhang scheme, while presenting an improved scheme for WBANs. Next, Li *et al.* [28] came with a cloud-oriented health monitoring protocol for body area networks. Later, He *et al.* [29] introduced an improved WBAN scheme after discovering impersonation attack in Liu *et al.* scheme [18]. Wu *et al.* [30] depicts that Wang and Zhang [23] do not provide immunity of impersonation attacks. Also Wu *et al.* presented a new authentication protocol for body area networks and is supported with random oracle model-based security validation. Then, Shen *et al.* [31] put forward an elliptic curve cryptography (ECC)-based certificate less authentication protocol for body sensors. Later, Jiang *et al.* [32] proposed a bilinear pairing authentication for WBANs with a focus on patient health as well as anonymity. The Liu *et al.* [33] protocol was designed by an efficient one-round anonymous authenticated key agreement in WBAS. In 2017, Yessad *et al.* [34] presented a reliable body-motion based authenticated key agreement scheme for body area networks. Later on, Priya and Visalakshi [35] exhibited a lightweight encryption protocol for securing the communication among sensors and users. In 2018, Li *et al.* [36] presented another anonymous and efficient authenticated key agreement for 3-tier WBAN systems, and employed BAN logic analysis for validation. The reviewed schemes above although claim to be lightweight, however these are not suitable for perfect WBAN environment due to limited power constraints, and were also bearing many security loopholes. Recently, we came across another efficient WBAN-based authentication protocol [37], nonetheless, we examine that the scheme is susceptible to session-specific ephemeral information attack, key compromise impersonation attack, and master secret compromise leading to session key recovery attack. In this study, we propose an efficient, secure and anonymous WBAN authenticated key agreement scheme which overcomes the pointed limitations in [37]. We validate the security findings of proposed model using ProVerif automated tool and analyze the security features using BAN logic, and compared the results with contemporary schemes.

III. REVIEW OF OSTAD-SHARIF ET AL. SCHEME

This section presents the working and cryptanalysis of Ostad-Sharif *et al.*'s scheme [37].

A. WORKING OF OSTAD-SHARIF ET AL

This sub-section illustrates the working of Ostad-Sharif *et al.*'s protocol.

1) INITIALIZATION PROCEDURE

In this stage, some basic parameters are initialized by the system administrator among the hub node and sensor nodes in a wireless body area network as shown below.

1. The system administrator constructs a master private secret key K_H for hub node.
2. Next, it selects a unique identity *IDs* along with temporary identity *TIDs* for every sensor node.

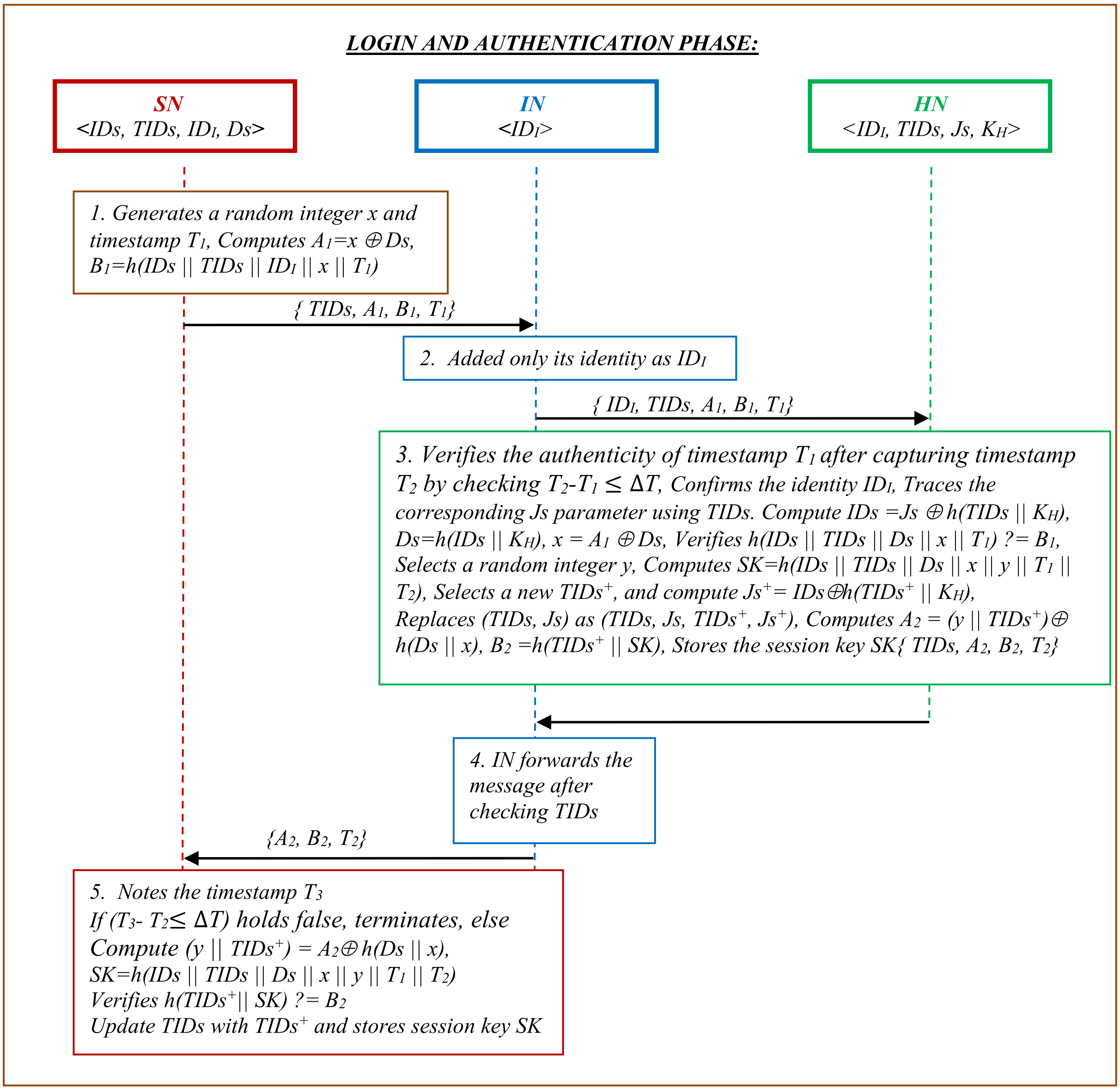

LOGIN AND AUTHENTICATION PHASE:
SN
<IDs, TIDs, ID_I, Ds>
IN
<ID_I>
HN
<ID_I, TIDs, Js, K_H>
1. Generates a random integer x and timestamp T_1, Computes A_1=x ⊕Ds, B_1=h(IDs || TIDs || ID_I || x || T_1)
{ TIDs, A_1, B_1, T_1}
2. Added only its identity as ID_I
{ ID_I, TIDs, A_1, B_1, T_1}
3. Verifies the authenticity of timestamp T_1 after capturing timestamp T_2 by checking T_2-T_1 ≤ ΔT, Confirms the identity ID_I, Traces the corresponding Js parameter using TIDs. Compute IDs =Js ⊕h(TIDs || K_H), Ds=h(IDs || K_H), x = A_1 ⊕Ds, Verifies h(IDs || TIDs || Ds || x || T_1) ?= B_1, Selects a random integer y, Computes SK=h(IDs || TIDs || Ds || x || y || T_1 || T_2), Selects a new TIDs^+, and compute Js^+= IDs⊕h(TIDs^+ || K_H), Replaces (TIDs, Js) as (TIDs, Js, TIDs^+, Js^+), Computes A_2 = (y || TIDs^+)⊕ h(Ds || x), B_2 =h(TIDs^+ || SK), Stores the session key SK{ TIDs, A_2, B_2, T_2}
4. IN forwards the message after checking TIDs
{A_2, B_2, T_2}
5. Notes the timestamp T_3
If (T_3- T_2≤ ΔT) holds false, terminates, else
Compute (y || TIDs^+) = A_2⊕h(Ds || x),
SK=h(IDs || TIDs || Ds || x || y || T_1 || T_2)
Verifies h(TIDs^+|| SK) ?= B_2
Update TIDs with TIDs^+ and stores session key SK

FIGURE 2. Ostad-Sharif *et al.* login & authentication steps.

3. Then, it computes private key as $Ds = h(IDs \,||\, K_H)$ and $J_S = IDs\oplus h(TIDs \,||\, K_H)$ for sensor node (SN).
4. In the end, it stores the parameters $\{IDs, TIDs, ID_I, Ds\}$ and $\{IDI, TIDs, J_S, K_H\}$ in the memory of sensor node and hub node, respectively.

2) MUTUAL AUTHENTICATION PHASE

For accessing the hub node, the SN submits the request for authentication towards hub node in the WBAN network. Then, SN in the network chooses a random integer and shares it with hub node. It would be used in the communicating sessions for the purpose of encryption. The procedure is as follows:

1. First, the SN selects a random integer x, and also generates time stamp T_1. Later, it calculates $A_1 = x\oplus Ds$, $B_1 = h(IDs \,||TIDs \,||\, ID_I \,||\, x \,||\, T_1)$. The SN, then, submits $\{TIDs,\, A_1,\, B_1,\, T_1\}$ towards the intermediate first-level SN using a public channel as depicted in Fig. 2.
2. The intermediate first level node (IN) receives the message from SN, and adds its identity ID_I and forwards again the message $\{ID_I,\, TIDs,\, A_1,\, B_1,\, T_1\}$ towards hub node using a public channel. Upon receiving the message, the hub node generates time stamp T_2 and verifies the received time stamp T_1 by comparing the difference against the threshold ΔT as $|T_2 - T_1| \leq \Delta T$. It aborts the message if it is not fresh, otherwise, confirms the identity ID_I in its repository. If it proves to be valid, it finds $<TIDs, J_S>$ and the corresponding private key K_H and the hub node computes $IDs = J_S\oplus h(TIDs \,||\, K_H)$, $Ds = h(IDs \,||\, K_H)$, $x = A_1\oplus Ds$. Next, it verifies the

equation as $h(IDs \,||\, TIDs \,||\, Ds \,||\, x \,||\, T_1)? = B_1$. If it does not hold true, it aborts. Otherwise, the hub node selects *a* random integer y and computes $SK = h(IDs \,||\, TIDs \,||\, Ds \,||\, x \,||\, y \,||\, T_1 \,||\, T_2)$. Next, the hub node chooses novel temporary identity for *SN* as $TIDs^+$ and computes $J_S^+ = IDs \oplus h(TIDs^+ \,||\, K_H)$. Afterwards, it replaces $(TIDs, J_S)$ with $(TIDs, J_S, TIDs^+, J_S^+)$ and constructs the message as $A_2 = (y \,||\, TIDs^+) \oplus h(Ds \,||\, x)$, $B_2 = h(TIDs^+ \,||\, SK)$. Finally, it stores the session key *SK* safely and submits $\{TIDs, A_2, B_2, T_2\}$ towards IN using a public channel. The IN, in return, further forwards $\{A_2, B_2, T_2\}$ to the SN on public channel after confirming its identity.

3. After receiving the message, the SN verifies the validity of T_3 time stamp by checking $|T_3 - T_2| \leq \Delta T$. Next, the SN computes $(y \,||\, TIDs^+) = A_2 \oplus h(Ds \,||\, x)$, session key as $SK = h(IDs \,||\, TIDs \,||\, Ds \,||\, x \,||\, y \,||\, T_1 \,||\, T_2)$, and verifies the equality for $h(TIDs^+ || \, SK)\ ? = B_2$. If it does not hold true, the SN terminates the session. Otherwise, the SN replaces *TIDs* with $TIDs^+$ upon successful verification of the authenticity.

B. CRYPTANALYSIS OF OSTAD-SHARIF ET AL

The Ostad-Sharif *et al.* scheme is found to be prone to several attacks, i.e. it cannot resist session-specific ephemeral information attack, HN's master secret attack, and key compromise impersonation attack. This sub-section presents the cryptanalysis and description of drawbacks in Ostad-Sharif *et al.* scheme.

1) SESSION SPECIFIC TEMPORARY INFORMATION ATTACK

The author assumes that the ephemeral secrets are kept secret in their scheme. Almost all of the authentication schemes attempt to ensure the security of ephemeral secrets, smart card parameters, and long term secrets by storing at safe place. However, the risk is always associated with the protected entities or parameters, which leads to many attacks based on assumptions related to stolen ephemeral secrets, stolen smart card parameters, stolen verifiers or long term secrets. That is why every authentication scheme is benchmarked on account of the resistance from these discussed threats. The Ostad-Sharif *et al.*'s scheme does not comply with forward secrecy in case a single ephemeral secret is exposed to the adversary. This attack can be described by illustrating the following steps.

1. Assume, the ephemeral secret x is exposed to the adversary, and then the latter may compute *Ds* from the intercepted A_1 parameter on public channel.
2. Next, it further computes $(y \,||\, TIDs^+) = A_2 \oplus h(Ds \,||\, x)$ from the intercepted A_2 parameter.
3. After recovering x and y parameters, it may guess the identity of user *IDs* by checking all the possible strings from dictionary. For this, it picks the IDs^* from the dictionary and computes $B_1{}^* = h(IDs^* \,||\, TIDs || \, ID_I \,||\, x \,||\, T_1)$. Next, it compares $B_1{}^*$ against the intercepted B_1, i.e. $B_1{}^*\ ? = B_1$. In this manner, it may attempt by repeatedly checking the selected identities to match the equality. Once the identity is recovered it proceeds to next step in the calculation of current session key.
4. Now, it computes the session key as $SK = h(IDs \,||\, TIDs \,||\, Ds \,||\, x \,||\, y \,||\, T_1 \,||\, T_2)$, where *TIDs*, T_1 and T_2 are intercepted parameters. In this manner, the adversary could recover all the previous session keys on the compromise of ephemeral secrets used in the past.

2) HN'S MASTER SECRET COMPROMISE ATTACK

The author claims that if the long term secret K_H is exposed to the adversary, it may not harm the legal participants. However, we observe that if the secret K_H is revealed accidentally then the attacker may not only recover the identity but also compute all previous session keys. It is assumed that the adversary intercept the messages A_1 and B_1 on public channel, while *Ds* is a user's long term secret parameter and is computed by the server as $D_S = h(IDs \,||\, K_H)$. By envisioning the weak construction of *Ds*, the adversary may recover the identity *IDs* by choosing the possible words from password dictionary $\mathcal{D}$ and launching a brute force guessing attack by taking the following steps.

1. First the adversary picks a string IDs^* from $\mathcal{D}$ and computes $Ds^* = h(IDs^* \,||\, K_H)$.
2. Next it computes $x^* = Ds^* \oplus A_1$ and $B_1^* = h(IDs^* || \, TIDs || \, ID_I \,||\, x^* \,||\, T_1)$, where ID_I is the identity of intermediate node will be generally known to participants, and T_1 is also available on public channel.
3. Next it compares the intercepted parameter B_1 against $B_1{}^*$. If the match is true, there comes the legitimate identity *IDs*. Otherwise, it will keep on matching the equality B_1 and B_1^* by computing the Ds^*, IDs^* and x^* parameters until the identity is guessed.

After initiating the above attack, the adversary may further compute all previous session keys by taking the following steps.

1. Let us suppose, the attacker seizes the parameter A_2 on public channel.
2. The attacker having K_H may compute $(y \,||\, TIDs) = A_2 \oplus h(TIDs || \, K_H)$
3. Once, y is recovered, it may further compute the session key from the guessed parameters, i.e. *IDs,*, *x, y,* as well as from the intercepted parameters *TIDs*, T_1, T_2 by computing *SK*, i.e. $SK = h(IDs || \, TIDs || \, x || \, y || \, T_1 || \, T_2)$

3) KEY COMPROMISE IMPERSONATION ATTACK (KCI)

In case, the user's private secret key *Ds* is compromised, the adversary may initiate an HN impersonation attack towards the same user. After intercepting the authentication request $\{TIDs, A_1, B_1, T_1\}$ from SN on public channel, the adversary may construct the response message (A_2, B_2, T_2) by taking the following steps.

1. Assuming that adversary intercepts the parameters $\{TIDs, A_1, B_1, T_1\}$.
2. Next, the adversary computes $x = A_1 \oplus Ds$ from the intercepted A_1.

TABLE 1. Notations description.

Notations	Description
SN/IN/HN:	Sensor node, Intermediate node, Hub node
ID_S, ID_I :	Identity of SN/Identity of Intermediate node
Ds:	SN's secret key created during system initialization
K_H	Master secret key of HN
x, y:	Temporary secrets created by SN and HN
T_1, T_2, T_3:	Timestamps
a.b	Multiplication operation
$a^{k\text{-}1}$	Multiplication inverse operation using key k
TIDs:	Temporary pseudonym used in place of identity
SK:	Session key
h(.):	A secure one-way hash digest function
||,	Concatenation, XOR

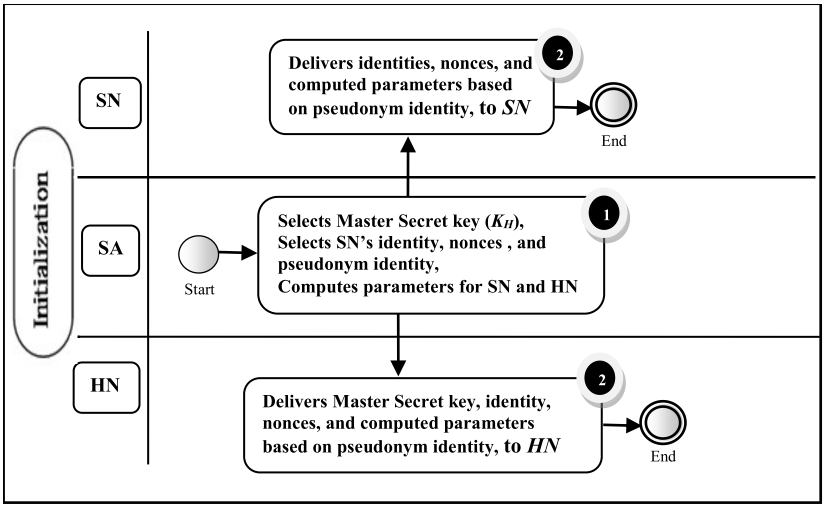

Initialization
SN
SA
HN
Start
Selects Master Secret key (K_H), Selects SN's identity, nonces , and pseudonym identity, Computes parameters for SN and HN
1
Delivers identities, nonces, and computed parameters based on pseudonym identity, to *SN*
2
End
Delivers Master Secret key, identity, nonces, and computed parameters based on pseudonym identity, to *HN*
2
End

FIGURE 3. A high-level illustrative figure describing Initialization procedure of the proposed model.

3. Then it attempts to guess the identity by using brute force method and picking strings for locating possible *IDs* from dictionary *D*. Next it computes $H_1^* = h(IDs^*$ $|| \ TIDs \ || \ ID_I \ || \ x \ || \ T_1)$ and compares B_1^* against the intercepted B_1. If it is matched there comes the valid identity. Otherwise, it keeps on checking other words of identities from D sequentially, until the true identity is traced.
4. Once, the identity *IDs* is successfully guessed by employing the *Ds* parameter, it may generate a random number *y* and temporary identity *TIDs*. Next, it computes $A_2 = (y \ || \ TIDs) \oplus h(Ds \ || \ x)$, $SK = h(IDs \ || \ TIDs \ || \ Ds \ || \ x \ || \ y, T_1$ and $T_2)$ and ultimately $B_2' = h(TIDs \ || \ SK)$.
5. Next, the computed parameter B_2' is matched against H_2, and if it is successful, the adversary becomes successful in initiating a KCI attack.

IV. PROPOSED MODEL

In this section, we present an improved and enhanced lightweight authentication protocol for WBAN. The symbols related to this scheme are described in Table 1. This section comprises initialization procedure bearing registration details, and mutual authentication procedure. In this setup, the sensor node SN gets mutually authenticated from the HN via intermediate node IN. After this the SN may securely communicate with HN by establishing an agreed session key. The details of these steps are illustrated below.

A. INITIALIZATION PROCEDURE

The high level description of initialization phase is depicted in Fig. 3 and Fig. 4. In the initialization phase, the administrator initializes the participants' systems with appropriate

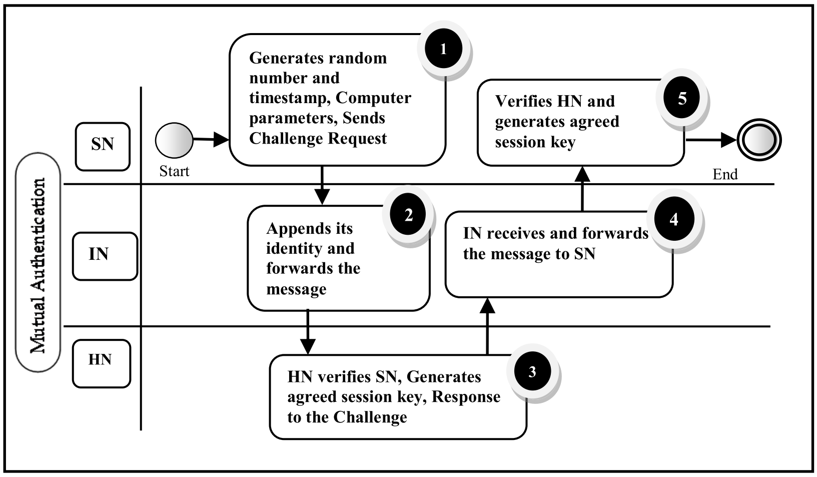

Generates random number and timestamp, Computer parameters, Sends Challenge Request
1
Verifies HN and generates agreed session key
5
SN
Start
End
Mutual Authentication
IN
Appends its identity and forwards the message
2
IN receives and forwards the message to SN
4
HN
HN verifies SN, Generates agreed session key, Response to the Challenge
3

FIGURE 4. A high-level illustrative figure depicting mutual authentication procedure.

parameters and stores safely in the memories of respective entities. In wireless body area network-based proposed solution, the system administrator computes the related factors and stores in the memory of sensor node and hub node as shown below.

1. The system administrator constructs a master private secret key K_H for hub node.
2. Next, it selects a unique identity *IDs*, a temporary session key variable SK_T, and a temporary identity *TIDs* for every sensor node.
3. Then, it computes private key as $Ds = h(IDs \,||\, K_H)$, and other parameters as $a_{SN} = (TIDs)^{KH-1}$ and $J_S = IDs \oplus h(TIDs \,||\, K_H)$ for sensor node (SN).
4. In the end, it stores the parameters $\{IDs, a_{SN}, ID_I, Ds, SK_T\}$ and $\{ID_I, J_S, K_H, SK_T\}$ in the memory of sensor node and hub node, respectively.

B. MUTUAL AUTHENTICATION PHASE

To ensure the safe communication with hub node, the SN forwards the request of authentication to HN in the WBAN network. The SN's memory is initialized with $\{IDs, a_{SN}, ID_I, Ds, SK_T\}$ parameters, while the HN's memory is initialized with $\{ID_I, J_S, K_H, SK_T\}$ factors. The procedure of constructing an agreed session key between SN and HN is illustrated as follows.

Step 1. Initially, the SN chooses a random integer x, and generates a time stamp T_1. Then, it computes $A_1 = x \oplus h(Ds||SK_T)$, $b_{SN} = h(SK_T)$, $B_1 = h(IDs \,||\, a_{SN} \,||\, b_{SN} \,||\, ID_I \,||\, x \,||\, T_1)$. Next it sends the message $\{a_{SN}, A_1, B_1, T_1\}$ to the intermediate first-level node IN employing a confidential channel as depicted in Fig. 5.

Step 2. The IN receives the message from SN, and adds its identity $\mathrm{ID_I}$ and forwards again the message $\{ID_I, a_{SN}, A_1, B_1, T_1\}$ towards hub node over a public channel. After receiving the message, the hub node generates time stamp $\mathrm{T_2}$ and checks the authenticity of received time stamp T_1 by monitoring the difference with threshold ΔT as $|T_2 - T_1| \leq \Delta T$. It abandons the message in case it is expired, otherwise, further confirms the identity $\mathrm{ID_I}$ in its repository. If it proves to be valid, it computes $TIDs = a_{SN}. K_H$ using its private key K_H. Next, the hub node computes $IDs = J_S \oplus h(TIDs \,||\, K_H)$, $Ds = h(IDs||K_H)$, $x = A_1 \oplus h(Ds||SK_T)$. Next, it checks the equality for $h(IDs \,||\, TIDs \,||\, Ds \,||\, x \,||\, T_1)? = B_1$. If it is not true, it will terminate the session. On the other hand, the hub node selects a random integer y and computes $SK = h(IDs \,||\, TIDs \,||\, Ds \,||\, x \,||\, y \,||\, T_1 \,||\, T_2)$. Next, the hub node chooses novel temporary identity for *SN* as $TIDs^+$ and computes $a^+_{SN} = (TIDs^+)^{KH-1}$, $J^+_S = IDs \oplus h(TIDs^+||K_H)$. Thereafter, it replaces J_S with J^+_S and constructs the message as $A_2 = (y \,||\, TIDs^+) \oplus h(Ds||SK_T \,||\, x)$, $B_2 = h(a^+_{SN} \,||\, SK)$. Then it stores the session key *SK* safely and replaces SK_T with the current session key *SK*. Finally, it submits $\{a_{SN}, A_2, B_2, T_2\}$ towards IN using a public channel. The IN, in return, further forwards $\{A_2, B_2, T_2\}$ to the SN on public channel after confirming its identity.

Step 3. After getting the message from HN, the SN verifies the validity of T_3 time stamp by checking $|\mathrm{T_3} - \mathrm{T_2}| \leq T$. Then, the SN computes $(y \,||\, a^+_{SN}) = A_2 \oplus h(Ds \,||\, SK_T \,||\, x)$, session key as $SK = h(IDs \,||\, TIDs \,||\, Ds \,||\, x \,||\, y \,||\, T_1 \,||\, T_2)$, and verifies the equality for $h(a^+_{SN} || SK)\ ? = B_2$. If it does not hold true, the SN terminates the session. Otherwise, the SN replaces a_{SN} with a^+_{SN} and stores session key *SK* upon successful verification of the authenticity. Finally, it replaces SK_T with the current session key *SK*.

V. SECURITY ANALYSIS

This section describes informal security discussion, verification and validation of proposed protocol using formal analysis based on Real-or-Random (ROR) model, BAN logic and ProVerif automated tool.

A. INFORMAL SECURITY ANALYSIS

This sub-section illustrates few salient features for informal analysis on security.

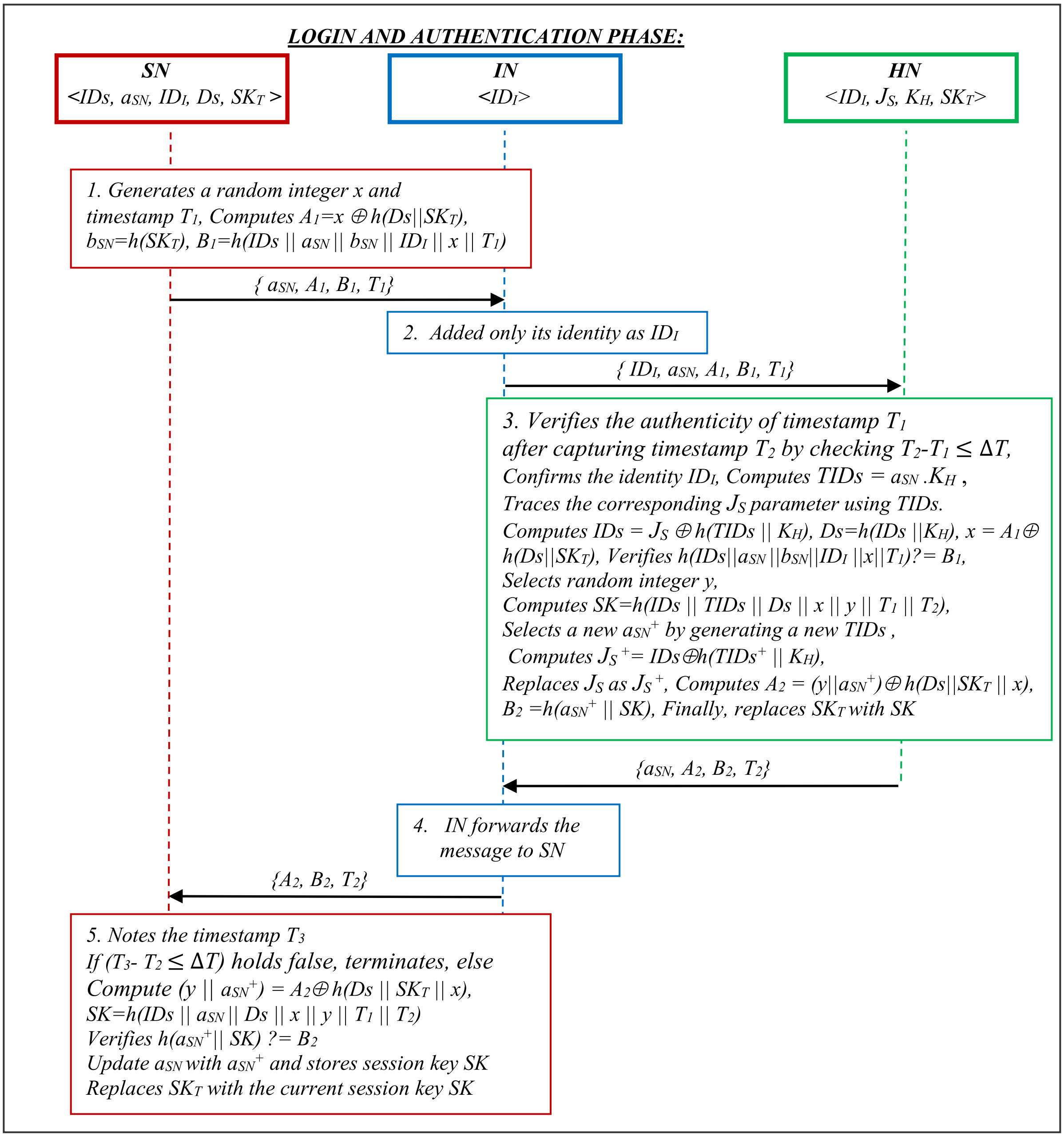

LOGIN AND AUTHENTICATION PHASE:
SN
<IDs, a_{SN}, ID_I, Ds, SK_T >
IN
<ID_I>
HN
<ID_I, J_S, K_H, SK_T>
1. Generates a random integer x and timestamp T_1, Computes A_1=x ⊕ h(Ds||SK_T), b_{SN}=h(SK_T), B_1=h(IDs || a_{SN} || b_{SN} || ID_I || x || T_1)
{ a_{SN}, A_1, B_1, T_1}
2. Added only its identity as ID_I
{ ID_I, a_{SN}, A_1, B_1, T_1}
3. Verifies the authenticity of timestamp T_1 after capturing timestamp T_2 by checking T_2-T_1 ≤ ΔT, Confirms the identity ID_I, Computes TIDs = a_{SN} .K_H , Traces the corresponding J_S parameter using TIDs. Computes IDs = J_S ⊕ h(TIDs || K_H), Ds=h(IDs ||K_H), x = A_1⊕ h(Ds||SK_T), Verifies h(IDs||a_{SN}||b_{SN}||ID_I ||x||T_1)?= B_1, Selects random integer y, Computes SK=h(IDs || TIDs || Ds || x || y || T_1 || T_2), Selects a new a_{SN}^+ by generating a new TIDs , Computes $J_S$$^+$= IDs⊕h(TIDs$^+$ || K_H), Replaces J_S as $J_S$$^+$, Computes A_2 = (y||a_{SN}^+)⊕ h(Ds||SK_T || x), B_2 =h(a_{SN}^+ || SK), Finally, replaces SK_T with SK
{a_{SN}, A_2, B_2, T_2}
4. IN forwards the message to SN
{A_2, B_2, T_2}
5. Notes the timestamp T_3 If (T_3- T_2 ≤ ΔT) holds false, terminates, else Compute (y || a_{SN}^+) = A_2⊕ h(Ds || SK_T || x), SK=h(IDs || a_{SN} || Ds || x || y || T_1 || T_2) Verifies h(a_{SN}^+|| SK) ?= B_2 Update a_{SN} with a_{SN}^+ and stores session key SK Replaces SK_T with the current session key SK

FIGURE 5. Proposed scheme.

1) RESISTANT OF SESSION SPECIFIC TEMPORARY INFORMATION ATTACK

Our scheme is resistant of session specific temporary information attack. In case, the ephemeral secret x is exposed to the attacker, the latter cannot recover either *IDs*, or *Ds* or session key SK_T from the intercepted A_1 parameter on public channel. For recovering *IDs* from $B_1 = h(IDs \,||\, a_{SN} \,||\, b_{SN} \,||\, ID_I \,||\, x \,||\, T_1)$, the adversary needs the b_{SN} which may not be computed until the previous session key SK_T is recovered. Similarly, to extract *Ds* from A_1, one requires accessing SK_T which is safely protected on both ends, and assumption of $\mathrm{SK_T}$ parameter's revelation along with x parameter constitutes a strong supposition. Further, the attacker might not recover y from A_2 which is required to construct the mutually agreed session key SK. To recover y from $A_2 = (y||a_{SN}^{+}) \oplus h(Ds||SK_T \,||\, x)$, the attacker must compromise *Ds*, SK_T and x parameters, which again constitutes a strong assumption and improbable. Hence, our scheme is immune to attacks if session specific temporary information is exposed to the adversary.

2) RESISTANT OF HN'S LONG TERM SECRET COMPROMISE ATTACK

As we observed in Ostad Sharif *et al.* [37] if the secret K_H is revealed accidentally then the attacker could not only recover the identity *IDs* but may also compute all previous session keys with the help of intercepted contents on public channel, i.e., A_1 and B_1. Using the A_1 and B_1 parameters, the attacker may guess the identity *IDs*, x, *Ds*, and y parameter, and ultimately the session key $SK = h(IDs|| TIDs|| x|| y|| T_1|| T_2)$. Whereas, in proposed scheme the leakage of secret K_H may not reveal the user's identity *IDs* or previous session keys to the attacker using the same intercepted contents. Since, the attacker may not guess the identity *IDs* from B_1 due to lacking x and b_{SN} parameters. Neither it may compute x from A_1 due to lacking knowledge of *Ds* as well as SK_T. Thus, our scheme is resistant of hub node's long term secret compromise attack.

3) RESISTANT TO KEY COMPROMISE IMPERSONATION ATTACK

In [37], the adversary could initiate an HN impersonation attack towards user, in case the user's private key *Ds* is exposed to that adversary. However, in proposed scheme the adversary may not construct a valid response message upon acquiring the private key *Ds*. This is because, to construct a valid response message (A_2, B_2, T_2), the adversary needs to compute $A_2 = (y||a^+_{SN})\oplus h(Ds||SK_T \; || \; x)$ and $B_2 = h(a^+_{SN} \; || \; SK)$, nonetheless, the adversary does not bear x and SK_T parameters for building a valid A_2 parameter, neither it may construct a legitimate B_2 parameter as it may not compute a valid session key *SK* of the current session. Hence our scheme is immune to key compromise impersonation attack.

4) RESISTANT OF REPLAY ATTACK

If the adversary replays the messages $\{a_{SN}, A_1, B_1, T_1\}$ and $\{a_{SN}, A_2, B_2, T_2\}$ on either of the side, the use of timestamps T_1 and T_2 may prevent any kind of replay attack [41]–[43]. The HN upon receiving the authentication request checks the timestamp $T_1's$ validity, confirms the identity ID_I, and verifying the equality for $h(IDs||TIDs||Ds||x \; ||T_1)? = B_1$. After the verification of B_1, the server validates the legitimacy of SN. Similarly, if the message $\{a_{SN}, A_2, B_2, T_2\}$ is replayed towards SN, the latter may foil this attack by comparing the timestamp as well as computing the session key $SK = h(IDs \; || \; a_{SN} || \; Ds \; || \; x \; || \; y \; || \; T_1 \; || \; T_2)$ and verifying the equation $h(a^+_{SN} || \; SK) \; ? = B_2$. If this equation holds true, the SN may comfortably dispel any probability of replay attack. Thus our proposed scheme is immune to replay attacks.

5) RESISTANT OF IMPERSONATION ATTACK

The proposed scheme is resistant to impersonation attacks by the adversary that could be initiated either by replaying or modification of the messages [44]. We have demonstrated above that our scheme is protected from any sort of replay attacks. However, if an adversary attempts to initiate an impersonation attack by modifying the messages in our scheme, it could be thwarted by the recipient, since the (A_1, B_1) and (A_2, B_2) parameters used in the communication messages cannot be constructed without employing either the private key of user *Ds* and SK_T on user's end, or the long term master key K_H and SK_T on the hub node's end, respectively. Hence, our scheme is resistant of impersonation or forgery attack.

6) SUPPORTS BACKWARD AND FORWARD SECRECY

The proposed scheme complies with the backward and forward secrecy, as the leakage of previous session key does not reveal future session key, neither the leakage of current session key reveals any previous session key. This is because; the construction of any session key requires some essential parameters such as *Ds*, x and y. The non-availability of those parameters would hamper the adversary to establish a valid session key. Hence, merely the knowledge of any session key does not help the adversary in any manner to ascertain the essential parameters or any previous or future session key. Likewise, the contributed scheme fully supports perfect forward secrecy, that is, even if the long term secret key K_H is leaked to the adversary, the latter may not be able to compute previous session keys, since the adversary has no access to the random integer y as generated by the HN.

7) SUPPORTS ANONYMITY AND UNTRACEABILITY

The Ostad Sharif *et al.*'s scheme exposes the real identity of user or SN if the temporary session variables pertaining to a particular user are stolen by the adversary [45]–[47]. The proposed scheme employs pseudonym identity *TIDs*, a temporary identity, to communicate instead of real identity *IDs* which ensures the user's anonymity. It does not reveal the identity of SN to the adversary even if the temporary session variables are leaked, or any private key of the participants is leaked. The pseudonym identity *TIDs* gets changed with each session that ensures untraceability to the user since no attacker can differentiate or link different sessions of the same user. Hence, our scheme ensures compliance to anonymity as well as untraceability for a particular SN or user.

B. FORMAL SECURITY ANALYSIS

In this section, we perform the formal analysis on the security of the demonstrated model, and employ a widely recognized Real-or-Random (ROR) model [40] for validating the session key properties as regards to the proposed model. As per ROR model, the attacker should be capable of differentiating the actual session key of instance from randomly generated key. In the login and authentication phase of the protocol, the three participating entities SN, IN and HN interact one another. We demonstrate the security validation using ROR model as shown below.

C. SECURITY MODEL

Participants: Let $\prod_{HN}^{x}$ be the *x-th* instance of server *HN*, $\prod_{SN}^{y}$ be the *y-th* instance of user *SN*, and $\prod_{IN}^{z}$ be the *z-th* instance of user *IN*, termed as oracles.

Collaborating instances: The collaborating instance $\prod_{SN}^{y}$ for *SN* is regarded as the corresponding instance $\prod_{HN}^{x}$ of *HN* and vice-versa. We assume pid_{SN}^{y} as the collaborator identity of $\prod_{HN}^{x}$ regarding the instance,while the partial transcript in relation to the communication session between SN and HN is unique, making the session identity sid_{SN}^{y} between the same SN and HN.

Novelty: The instances such as $\prod_{HN}^{x}$ or $\prod_{SN}^{y}$ are regarded as novel or fresh in case the associated session key SK is never disclosed to the malicious intruder $\mathcal{J}$.

Malicious Intruder: Considering ROR model, the intruder $\mathcal{J}$ may not only scans the communicated messages on public channel, but also can block, modify or delete the messages in transit. On the other hand, $\mathcal{J}$ bears absolute control over the public channel and is in better jurisdiction to initiate the following queries.

- *Execute* ($\prod^{x}$, $\prod^{y}$): With the application of this query, the significant parameters exchanged among entities SN and HN can be eavesdropped by $\mathcal{J}$, to model other attacks.
- *Send*($\prod^{x}$, m_s): This query assists the participating instances in forwarding or getting the message m_s which is simulated to be an attack.
- *Corrupt_SN*($\prod_{SN}^{y}$) : This query models the stolen parameters on the SN. After initiating this query by $\mathcal{J}$, the later may get access to critical factors.
- *Reveal*($\prod^{x}$): This query may expose the existing session key to $\mathcal{J}$ as created between the instance $\prod^{x}$ and the other collaborator.
- *Test*($\prod^{x}$) : The Test query is utilized to test the consistency of game output as well settling indistinguishability in the ROR model, to estimate the session key *SK* as established between *SN* and *HN* [27], [28]. Prior to the game initiation, any unbiased coin c gets flipped whereas the attacker would be keeping its output secret so that it can decide onwards regarding this. Alternatively, the result will be utilized later on to check the consistency of the output for Test query. After executing this query if the session key is ascertained to be fresh, the instance would be delivering SK in case the coin's output equates '1', or it shall be returning any random number, if the coin's output is '0'. On the other hand, it returns null ($\perp$).

D. SEMANTIC SECURITY OF SK

Considering ROR security model, the attacker $\mathcal{J}$ requires to differentiate a random secret against the legal session key *SK*. In this regard, multiple Test queries may be issued by $\mathcal{J}$ to these instances, i.e. $\prod_{HN}^{x}$ or $\prod_{SN}^{y}$. The outcome for the Test query must be in correspondence with the randomly defined bit c. At the end of simulated experiment, $\mathcal{J}$ attempts to win by making a guess of the bit c'. If the bits such as c' and c are matched, $\mathcal{J}$ wins the challenge game. We can express the benefit of $\mathcal{J}$ in damaging the semantic security of the proposed model $\prod$ in t amount of time as $Adv_{\prod}^{Ak}(t) = |\ 2.$ *Pr* [*Sucx*]-1, where *Sucx* shows the winning chances of the game by $\mathcal{J}$. The contributed scheme $\prod$ shall be secure in ROR-based model if and only if the benefit $Adv_{\prod}^{Ak} \leq \omega$ for any negligibly small ω greater than 0.

Random Oracle: As per the modeling with Random Oracles ($\mathcal{RO}$), the interacting participants as well as the attacker $\mathcal{J}$ may access the collision-free hash function.

Definition 1: The lightweight and deterministic cryptographic primitive–hash function $h{:}\{0,\ 1\}^{*} \rightarrow \{0,\ 1\}^{n}$, generates an n-bit output string with predetermined span after inputting a binary string of variable length. The $Adv_{\mathcal{J}}^{h\_f}\ (\tau)$ function embodies the benefit of $\mathcal{J}$ in locating the hash-based collision, and can be shown as:

$$Adv_{\mathcal{J}}^{h\_f}(t) = Pr[(\mathcal{L}_1, L_2) \Leftarrow_R \mathcal{J} : \mathcal{L}_1 \neq \mathcal{L}_2 \text{ and } h\,(\mathcal{L}_1) = h\,(L_2)]$$

An $(\varkappa, t)$-adversary having compromised the $h\_f(\cdot)$ hash function signifies that $Adv_{\mathcal{J}}^{h\_f}\ (t) \leq \varkappa$ with the maximum running time t.

E. SECURITY PROOF

The theorem 1 adequately establishes the fact that the proposed model strengthens security of session key.

Theorem 1: Assuming a probabilistic polynomial time malicious intruder $\mathcal{J}$ executing the contributed model $\prod$ in time t, ℓ being the number of bits in biometric string of impression B_s, while $\mathcal{D}$ be a password repository with uniform distribution, then the benefit of the malicious intruder to bust the semantic security for scheme $\prod$ and building a legitimate SK may be computed as:

$$Adv_{\prod}^{AKS}\ (\mathcal{J}) \leq \frac{q_{hs}^{2}}{|hash|} + \frac{q_s}{2^{\ell-1}.|\mathcal{D}|} \tag{1}$$

where q_{hs}, q_s, $|\mathcal{D}|$ and $|hash|$ shows the respective number of $\mathcal{RO}$ queries, the number of Send queries, the size of dictionary, and range span for $h(\cdot)$, respectively.

Proof 1: To support the proof, a sequence of four games is defined as G_{gk}, $(0 \geq k \leq 3)$. We characterize an event $Scss_i$ as the probability to win for $\mathcal{J}$ in game G_k, where the adversary might guess correctly the random bit c. The gain for $\mathcal{J}$ in the game G_{gk} may be depicted as $Adv_{\prod}^{AKS} = Pr[Scss_i]$.

We provide a detailed demonstration of these games in the following:

$\boldsymbol{G_{g0}}$: The game G_{g0} is simulated as a genuine attack in which the random bit c needs to be selected by the attacker $\mathcal{J}$. Then it is followed as:

$$Adv_{\prod}^{AKS}\ (\mathcal{J}) = |2.Adv_{Gg0} - 1 \tag{2}$$

$\boldsymbol{G_{g1}}$: Using the game G_{g1}, an eavesdropping attack is simulated. In the beginning, $\mathcal{J}$ initiates with the Execute oracle query which is then followed by Test oracle query. Now, $\mathcal{J}$ needs to prove the fidelity of session key SK as created between SN and HN, and whether it is real one or some random number. The SK is calculated in the demonstrated scheme as $SK = h(IDs\ ||\ a_{SN}\ ||\ Ds\ ||\ x\ ||\ y\ ||\ T_1\ ||\ T_2)$. This comprises $SK = IDs$, a_{SN}, Ds, x, y, T_1 and T_2 parameters. Nonetheless, the revelation and seizure of $\{ID_I, TIDs, A_1, B_1, T_1, A_2, B_2, T_2\}$ factors on publicly insecure channel cannot aid $\mathcal{J}$ to calculate the factors of session key SK. The access to those critical factors making the session key requires further access to short as well as long-term keys to compute session key. This warrants that the chance of winning G_{g1} for $\mathcal{J}$ with message eavesdrop is not boosted, and consequently we deduce that the games G_{g0} and G_{g1} be the same.

$$Adv_{Gg0} = Adv_{Gg1} \tag{3}$$

$\boldsymbol{G_{g2}}$: In this game, $\mathcal{J}$ may query $\mathcal{RO}$ as well as *Send* queries. The intruder could alter the intercepted parameters to reproduce the legal messages, i.e m_1, m_2 and m_3. Nevertheless, the corresponding long term secrets such as D_s and K_H are not known to the $\mathcal{J}$. In addition, these factors are shielded with the use of cryptographic hash digest function $h(\cdot)$. The use of temporary low-entropy integers such as x, y and fresh timestamps such as T_1 and T_2 contribute in constructing unique m_1, m_2 and m_3 messages. Hence, there exists no occurrence of collisions in hash function if the attacker happens to submit the *Send* queries. It merits mentioning here that both the games G_{g1} and G_{g2} are similar with the exception of $\mathcal{RO}$ and *Send* queries as modeled in G_{g2}. We get to the understated outcome on the application of the principle of birthday paradox, i.e.

$$|Adv_{Gg1} - Adv_{Gg2}| \leq \frac{q_{hs}^2}{2.|hash|} \tag{4}$$

$\boldsymbol{G_{g3}}$: In game G_{g3}, the attacker $\mathcal{J}$ may employ the *Corrupt_SN* query to reveal the parameters, say K_H the long term secret. Using this secret, $\mathcal{J}$ may attempt to guess the identity *IDs* of SN or earlier session keys. Nonetheless, $\mathcal{J}$ may not be able to guess the same even from the B_1 factor since it can never approach x and b_{SN} factors. The probability to guess the user's identity is given as $\frac{1}{2^l}$, where l be the length of the identity string. At the same time, $\mathcal{J}$ can never recover x from the approached A_1 since it does not have access to SK_T and *Ds* parameters. Hence, in the absence of long term secrets, it would not be viable to compute the session key in polynomial amount of time. Thus, it follows as

$$|Adv_{Gg2} - Adv_{Gg3}| \leq \frac{q_{hs}}{2^l.|\mathcal{D}|} \tag{5}$$

Alternatively, given that $\mathcal{J}$ has no knowledge regarding the bit c, since the SK is computed in independent and random manner between SN and HN. Thus

$$Adv_{Gg3} = \frac{1}{2} \tag{6}$$

Using (2), (3) and (6) we deduce:

$$\frac{1}{2}.Adv_{\prod}^{AKs}(\mathcal{J}) = |Adv_{Gg0} - \frac{1}{2}| = |Adv_{Gg1} - Adv_{Gg3}| \tag{7}$$

Using triangular inequality, we solve the equations (4), (5) and (6) as:

$$\begin{aligned} |Adv_{Gg1} - Adv_{Gg3}| &\leq |Adv_{Gg1} - Adv_{Gg2}| \\ &\quad + |Adv_{Gg2} - Adv_{Gg3}| \\ &\leq \frac{q_{hs}^2}{2.|hash|} + \frac{q_{hs}}{2^l.|\mathcal{D}|} \end{aligned} \tag{8}$$

Using (7) and (8), we can deduce the following equation:

$$|Adv_{Gg1} - \frac{1}{2}| \leq \frac{q_{hs}^2}{2.|hash|} + \frac{q_{hs}}{2^l.|\mathcal{D}|} \tag{9}$$

Using (8) and (9), we have

$$\frac{1}{2}.Adv_{\prod}^{AKs}(\mathcal{J}) \leq \frac{q_{hs}^2}{2.|hash|} + \frac{q_{hs}}{2^l.|\mathcal{D}|} \tag{10}$$

The above equation can be further simplified as

$Adv_{\prod}^{AKs}(\mathcal{J}) \leq \frac{q_{hs}^2}{|hash|} + \frac{q_{hs}}{2^{l-1}.|\mathcal{D}|}$ ■

F. BAN LOGIC ANALYSIS

In this section we focus on few significant security properties by using Burrows-Abadi-Needham logic (BAN) logic [38] which is utilized for verifying those security properties, i.e., key agreement, key protection, mutual authentication, and session key disclosure etc.

We employed few symbols to prove this logical analysis as given below:

$\mathcal{Y}, \mathcal{Y}'$: Two principals;

$\flat, \flat'$: Two statements;

$\mathcal{Y}| \equiv \flat$: $\mathcal{Y}$ believes $\flat$;

$\mathcal{Y} \triangleleft \flat$: $\mathcal{Y}$ sees $\flat$;

$\mathcal{Y}| \sim \flat$: $\mathcal{Y}$ said $\flat$;

$\mathcal{Y} \Rightarrow \flat$: $\mathcal{Y}$ has jurisdiction over $\flat$;

$\sharp\,(\flat)$: The content $\flat$ is fresh;

$(\flat, \flat')$: $\flat$ or $\flat'$ are parts of content $(\flat, \flat')$;

$\langle\flat\rangle_{\flat'}$: The formulae $\flat$ is implemented with combining another formulae $\flat'$;

$\{\flat, \flat'\}_K$: $\flat$ or $\flat'$ is encrypted with key K;

$(\flat, \flat')_K$: $\flat$ or $\flat'$ is hashed with key K;

$\mathcal{Y} \overset{K}{\longleftrightarrow} \mathcal{Y}'$: $\mathcal{Y}$ and $\mathcal{Y}'$ interact using mutually agreed key K;

Some rules are used to prove the features and are defined as under:

$$Rule-1.(\text{Message meaning}): \frac{\mathcal{Y}| \equiv \mathcal{Y} \overset{K}{\longleftrightarrow} \mathcal{Y}', \triangleleft \langle\flat\rangle_{\flat'}}{\mathcal{Y} |\equiv \mathcal{Y}'| \sim \flat}$$

$$Rule-2.(\text{Nonce verification}): \frac{\mathcal{Y}| \equiv \sharp\left(\flat\right), \mathcal{Y} |\equiv \mathcal{Y}'| \sim \flat}{\mathcal{Y} |\equiv \mathcal{Y}'| \equiv \flat}$$

$$Rule-3.(\text{Jurisdiction}): \frac{\mathcal{Y}| \equiv \mathcal{Y}' \Rightarrow \flat, \mathcal{Y} |\equiv \mathcal{Y}'| \equiv \flat}{\mathcal{Y}| \equiv \flat}$$

$$Rule-4.(\text{Freshness conjuncatenation}): \frac{\mathcal{Y}| \equiv \sharp(\flat)}{\mathcal{Y}| \equiv \sharp(\flat, \flat')}$$

$$Rule-5.(\text{Belief}): \frac{\mathcal{Y}| \equiv \left(\flat\right), \mathcal{Y}| \equiv \left(\flat'\right)}{\mathcal{Y}| \equiv \left(\flat, \flat'\right)}$$

$$Rule-6.(\text{Session keys}): \frac{\mathcal{Y}| \equiv \sharp\left(\flat\right), \mathcal{Y} |\equiv \mathcal{Y}'| \equiv \flat}{\mathcal{Y}| \equiv \mathcal{Y} \overset{K}{\longleftrightarrow} \mathcal{Y}'}$$

This scheme is contributed to target the understated goals while the BAN logic is used as a benchmark for the attainment of these goals. The stipulated goals are defined as under:

Goal-1 : $N_H| \equiv N_S \overset{SK}{\longleftrightarrow} N_H$
Goal-2 : $N_H| \equiv S_N \mid \equiv S_N \overset{SK}{\longleftrightarrow} N_H$
Goal-3 : $S_N| \equiv S_N \overset{SK}{\longleftrightarrow} N_H$
Goal-4 : $S_N| \equiv N_H \mid \equiv S_N \overset{SK}{\longleftrightarrow} N_H$

The protocol can be described in generic terms as following:

m$_1$: $S_N \rightarrow N_H$: a_{SN}, A_1, B_1, T_1:
m$_2$: $N_H \rightarrow S_N$: A_2, B_2, T_2

The protocol messages could be adapted in the following idealized forms.

m$_1$: $S_N \rightarrow N_H$: a_{SN}, A_1, B_1, T_1: $\{\langle TIDs\rangle_{\boldsymbol{Kh}}, \langle x\rangle_{\boldsymbol{h(Ds||SKT)}}, (\ IDs, a_{SN}, ID_I, T_1\ )_{\boldsymbol{bSN}}, T_1\}$
m$_2$: $N_H \rightarrow S_N$: A_2, B_2, T_2 : $\{\langle y||a_{SN}^{+}\rangle_{\boldsymbol{h(Ds||SKT||x)}}, (\ aSN^{+})_{\boldsymbol{SK}}, T_2\ \}$

Onwards, we take few premises to prove the supported features in this analysis.

L1 : $S_N| \equiv \sharp x$
L2 : $N_H| \equiv \sharp y$
L3 : $S_N| \equiv N_H \overset{Ds,SK_T}{\longleftrightarrow} S_N$
L4 : $N_H| \equiv N_H \overset{Ds,SK_T}{\longleftrightarrow} S_N$
L5 : $S_N| \equiv N_H \Rightarrow T_2$
L6 : $N_H| \equiv S_N \Rightarrow T_1$

The contributed protocol employs the above laid assumptions to verify the strength of session key and achieve the designed goals. We lay down some premises to prove the security strength of contributed protocol.

After utilizing the defined symbols, rules, premises and idealizations, we proceed to the following derivations and proofs.

1) MUTUAL AUTHENTICATION ACCURACY

To testify the accomplishment of mutual authentication between the entities such as S_N and N_H, we adapt the message strings m$_1$ and m$_2$ into idealized forms as given below:

m$_1$: $S_N \rightarrow N_H$: a_{SN}, A_1, B_1, T_1: $\{\langle TIDs\rangle_{\boldsymbol{Kh}}, \langle x\rangle_{\boldsymbol{h(Ds||SKT)}}, (IDs, a_{SN}, ID_I, T_1)_{\boldsymbol{bSN}}, T_1\}$

m$_2$: $N_H \rightarrow S_N$: A_2, B_2, T_2 : $\{\langle y||a_{SN}^{+}\rangle_{\boldsymbol{h(Ds||SKT||x)}}, (aSN^{+})_{\boldsymbol{SK}}, T_2\ \}$

Lemma 1: N_H may verify the authenticity of login request coming from S_N.

Proof: The S_N constructs the message (a_{SN}, A_1, B_1, T_1) and submits to N_H for login and getting its services. The N_H gets the timestamp including other session-related factors and authenticates the accuracy of the source of the received message as follows.

We use the seeing rule, and the following derivation results:

$$D1 : N_H \triangleleft a_{SN}, A_1, B_1, T_1 : \{\langle TIDs\rangle_{\boldsymbol{Kh}}, \langle x\rangle_{\boldsymbol{h(Ds||SKT)}}, (IDs, a_{SN}, ID_I, T_1)_{\boldsymbol{bSN}}, T_1\}$$

In view of D1, L4 and *Rule*-1,

$$D2 : N_H| \equiv S_N \sim \{\langle TIDs\rangle_{\boldsymbol{Kh}}, \langle x\rangle_{\boldsymbol{h(Ds||SKT)}}, (IDs, a_{SN}, ID_I, T_1)_{\boldsymbol{bSN}}, T_1\}$$

In view of L1, L6, and *Rule*-4

$$D3 : N_H| \equiv \sharp\{\langle TIDs\rangle_{\boldsymbol{Kh}}, \langle x\rangle_{\boldsymbol{h(Ds||SKT)}}, (IDs, a_{SN}, ID_I, T_1)_{\boldsymbol{bSN}}, T_1\}$$

In consideration of D2, D3 and *Rule*-2, we have

$$D4 : N_H| \equiv S_N| \equiv \{\langle TIDs\rangle_{\boldsymbol{Kh}}, \langle x\rangle_{\boldsymbol{h(Ds||SKT)}}, (IDs, a_{SN}, ID_I, T_1)_{\boldsymbol{bSN}}, T_1\}$$

After applying L4, D4 and *Rule*-3, we can say

$$D5 : N_H| \equiv \{\langle TIDs\rangle_{\boldsymbol{Kh}}, \langle x\rangle_{\boldsymbol{h(Ds||SKT)}}, (IDs, a_{SN}, ID_I, T_1)_{\boldsymbol{bSN}}, T_1\}$$

Thus, after verifying the freshness of timestamp, the N_H proves the accuracy of source of the message.

Lemma 2: S_N may aptly verify the authenticity of response received of N_H.

Proof: In contributed scheme, the N_H constructs the response (A_2, B_2, T_2) and submits to S_N to respond S_N's login request message. The S_N verifies the N_H's authenticity by verifying the freshness of parameters as given below.

After using seeing rule, the following derivation results:

$$D6 : S_N \triangleleft A_2, B_2, T_2 : \{\langle y||a_{SN}^{+}\rangle_{\boldsymbol{h(Ds||SKT||x)}}, (aSN^{+})_{\boldsymbol{SK}}, T_2\}$$

In consideration of D6, L3 and *Rule*-1,

$$D7 : S_N| \equiv N_H \sim \{\langle y||a_{SN}^{+}\rangle_{\boldsymbol{h(Ds||SKT||x)}}, (aSN^{+})_{\boldsymbol{SK}}, T_2\}$$

In view of L2, L5, and *Rule*-4

$$D8 : S_N| \equiv \sharp\{\langle y||a_{SN}^{+}\rangle_{\boldsymbol{h(Ds||SKT||x)}}, (aSN^{+})_{\boldsymbol{SK}}, T_2\}$$

In view of D7, D8 and *Rule*-2, we have

$$D9 : S_N| \equiv N_H| \equiv \{\langle y||a_{SN}^{+}\rangle_{\boldsymbol{h(Ds||SKT||x)}}, (aSN^{+})_{\boldsymbol{SK}}, T_2\}$$

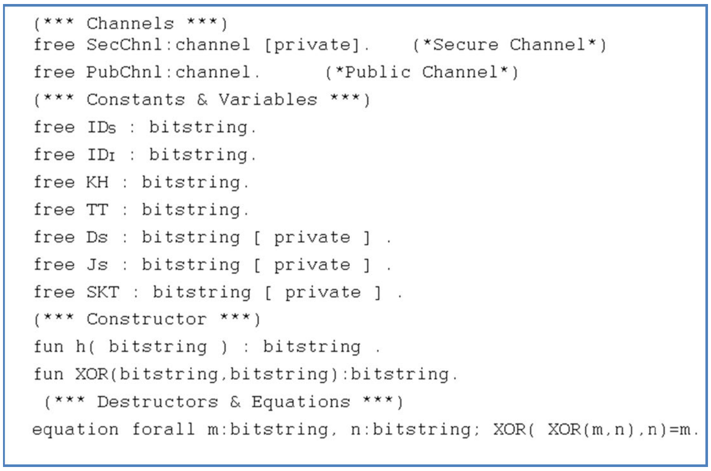
On applying L3, D9 and *Rule*-3, we can say

$$D10 : S_N| \equiv \{\langle y||a_{SN}^{+}\rangle_{\boldsymbol{h(Ds||SKT||x)}}, (aSN^{+})_{\boldsymbol{SK}}, T_2\}$$

Therefore, after checking the freshness of timestamp, Ui authenticates the accuracy of source of the message.

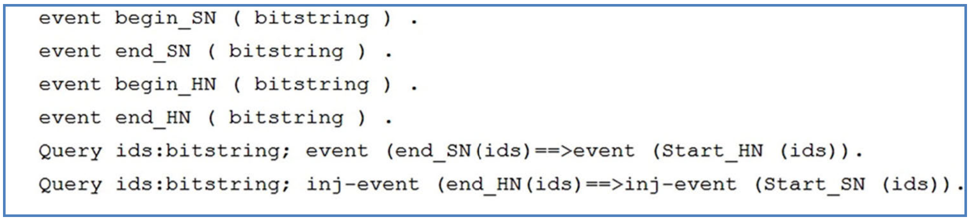
Theorem 1:

Proof: Referring to Lemma 1, the N_H may correctly verify the legitimacy of a received login request from S_N. Referring to Lemma 2, the S_N may accurately verify authenticity of response content from N_H. Thus, we might infer that S_N and N_H mutually authenticate each other.



```
(*** Channels ***)
free SecChnl:channel [private].    (*Secure Channel*)
free PubChnl:channel.      (*Public Channel*)
(*** Constants & Variables ***)
free IDs : bitstring.
free IDI : bitstring.
free KH : bitstring.
free TT : bitstring.
free Ds : bitstring [ private ] .
free Js : bitstring [ private ] .
free SKT : bitstring [ private ] .
(*** Constructor ***)
fun h( bitstring ) : bitstring .
fun XOR(bitstring,bitstring):bitstring.
 (*** Destructors & Equations ***)
equation forall m:bitstring, n:bitstring; XOR( XOR(m,n),n)=m.
```

FIGURE 6. Channels and variables.



```
event begin_SN ( bitstring ) .
event end_SN ( bitstring ) .
event begin_HN ( bitstring ) .
event end_HN ( bitstring ) .
Query ids:bitstring; event (end_SN(ids)==>event (Start_HN (ids)).
Query ids:bitstring; inj-event (end_HN(ids)==>inj-event (Start_SN (ids)).
```

FIGURE 7. Events and queries.

2) SESSION KEY AGREEMENT

A session key, i.e. $SK = h(IDs||a_{SN}||Ds||x\,||y\,||T_1\,||T_2)$ could be constructed by mutual agreement among the interacting participants in contributed scheme. Here, the factors such as *IDs, aSN, Ds, x* and *y* are crucial for creating a legitimate session key. This session key agreement among the entities could be achieved as follows.

In view of L2, D4, and *Rule*-2, we get

$$\mathrm{D11}: \mathrm{N_H}| \equiv \mathrm{S_N}| \equiv \mathrm{N_H} \overset{SK}{\longleftrightarrow} \mathrm{S_N} \quad (\mathbf{Goal-2})$$

In view of L2, D11, and *Rule*-6

$$\mathrm{D12}: \mathrm{N_H}| \equiv \mathrm{N_H} \overset{SK}{\longleftrightarrow} \mathrm{S_N} \quad (\mathbf{Goal-1})$$

In connection with L1, D9, and *Rule*-2, we get

$$\mathrm{D13}: \mathrm{S_N}| \equiv \mathrm{N_H}| \equiv \mathrm{N_H} \overset{SK}{\longleftrightarrow} \mathrm{S_N} \quad (\mathbf{Goal-4})$$

In connection with L1, D13, and *Rule*-6

$$\mathrm{D6}: \mathrm{S_N}| \equiv \mathrm{N_H} \overset{SK}{\longleftrightarrow} \mathrm{S_N} \quad (\mathbf{Goal-3})$$

Therefore, the above analysis (BAN) suitably verifies that our scheme could mutually authenticate the involved participants by establishing the mutually shared session key between $\mathrm{S_N}$ and $\mathrm{N_H}$.

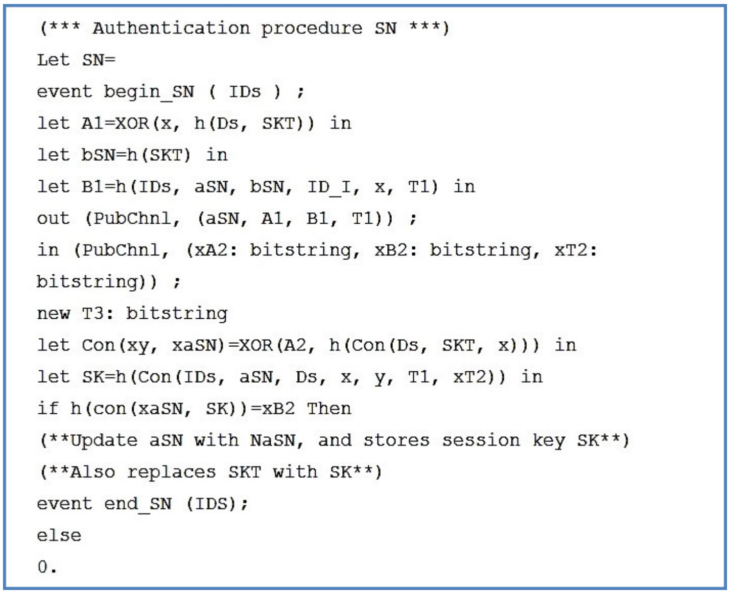
The discussed cases in relation to the BAN logic sufficiently prove that our proposed scheme achieves mutual authentication in absolute terms, while the constructed session key *(SK)* is mutually negotiated and agreed between $\mathrm{S_N}$ and $\mathrm{N_H}$.

TABLE 2. Operations equivalency with T_h operation.

Operation	*Equivalent in T_h*
T_h	T_h
T_s	$2T_h$
T_i	$4T_h$
T_{ec}	$69.5\ T_h$
T_b	$1468\ T_h$
T_e	$527\ T_h$
T_{pa}	$15\ T_h$

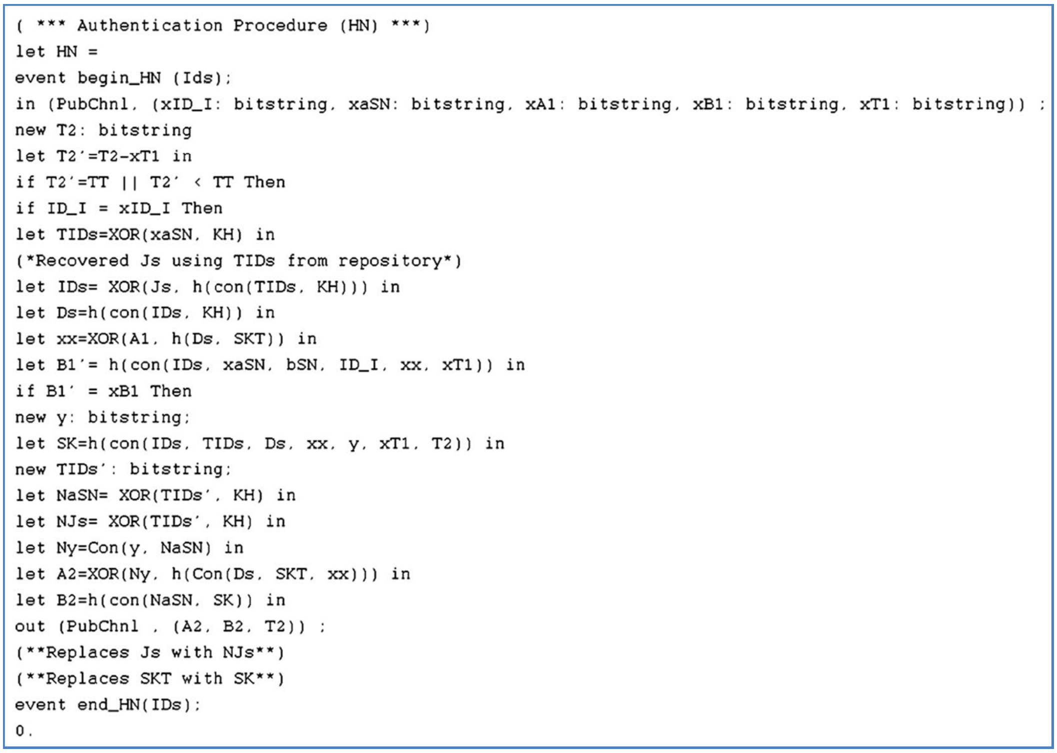
G. PROVERIF TOOL-BASED VALIDATION

We validated our results with the help of a widely adopted ProVerif automated analysis tool [39]. This tool aids in formally verifying the robust cryptographic security features including the session key strength, mutual authenticity, and the equivalence for various processes. This tool takes advantage of strong π calculus features to support many state-of-the-art crypto-primitives including digital signatures, hash function, encryption-decryption etc. The protocol is tested with the initiation of two channels_ one is defined as a secure channel with the characterization of *SecChnl*, while the other as public channel with the characterization of *PubChnl* between sensor node (SN) and hub node (HN).



```
(*** Authentication procedure SN ***)
Let SN=
event begin_SN ( IDs ) ;
let A1=XOR(x, h(Ds, SKT)) in
let bSN=h(SKT) in
let B1=h(IDs, aSN, bSN, ID_I, x, T1) in
out (PubChnl, (aSN, A1, B1, T1)) ;
in (PubChnl, (xA2: bitstring, xB2: bitstring, xT2:
bitstring)) ;
new T3: bitstring
let Con(xy, xaSN)=XOR(A2, h(Con(Ds, SKT, x))) in
let SK=h(Con(IDs, aSN, Ds, x, y, T1, xT2)) in
if h(con(xaSN, SK))=xB2 Then
(**Update aSN with NaSN, and stores session key SK**)
(**Also replaces SKT with SK**)
event end_SN (IDS);
else
0.
```

FIGURE 8. Authentication procedure for SN.



```
( *** Authentication Procedure (HN) ***)
let HN =
event begin_HN (Ids);
in (PubChnl, (xID_I: bitstring, xaSN: bitstring, xA1: bitstring, xB1: bitstring, xT1: bitstring)) ;
new T2: bitstring
let T2'=T2-xT1 in
if T2'=TT || T2' < TT Then
if ID_I = xID_I Then
let TIDs=XOR(xaSN, KH) in
(*Recovered Js using TIDs from repository*)
let IDs= XOR(Js, h(con(TIDs, KH))) in
let Ds=h(con(IDs, KH)) in
let xx=XOR(A1, h(Ds, SKT)) in
let B1'= h(con(IDs, xaSN, bSN, ID_I, xx, xT1)) in
if B1' = xB1 Then
new y: bitstring;
let SK=h(con(IDs, TIDs, Ds, xx, y, xT1, T2)) in
new TIDs': bitstring;
let NaSN= XOR(TIDs', KH) in
let NJs= XOR(TIDs', KH) in
let Ny=Con(y, NaSN) in
let A2=XOR(Ny, h(Con(Ds, SKT, xx))) in
let B2=h(con(NaSN, SK)) in
out (PubChnl , (A2, B2, T2)) ;
(**Replaces Js with NJs**)
(**Replaces SKT with SK**)
event end_HN(IDs);
0.
```

FIGURE 9. Authentication procedure for HN.

For protocol execution, we employ the understated procedure. First the processes related to both entities, SN and HN, are initiated and then both are authenticated on mutual basis. Thereafter, both of the processes are abolished with success. The related codes for the channels, queries, events and variables are depicted in Fig. 6 and Fig. 7. Next, we modeled the two events for both participants, i.e. HN and SN. The two events such as begin_SN (bitstring) and event end_SN (bitstring) are utilized by the sensor node for authenticating hub node. Likewise, the events begin_HN (bitstring) and event end_HN (bitstring) are utilized by the hub node for authenticating the corresponding SN.

TABLE 3. Computational cost of comparative schemes.

	Hub Node (ms)	*User/Sensor (ms)*
Li et al. [4]	$5\ T_h \approx 0.28ms$	$3\ T_h \approx 0.17ms$
Li et al. [16]	$4\ T_h + 4T_e = 2112T_h \approx 120ms$	$3T_h + 3T_e = 1584T_h \approx 90ms$
Liu et al. [18]	$3\ T_h + 1T_e + 1T_{ec} + 1T_b = 2067T_h \approx 117ms$	$3\ T_h + 4T_{ec} + 1T_e + 1T_{pa} = 823T_h \approx 47ms$
Zhao [19]	$5\ T_h + 1T_s + 6T_{ec} = 424T_h \approx 24ms$	$4\ T_h + 1T_s + 3T_{ec} = 214T_h = 13ms$
He and Zeadally [25]	$1\ T_h + 2T_s + 2T_{ec} = 144T_h \approx 8ms$	$2\ T_h + 2T_s + 3T_{ec} = 214T_h \approx 13ms$
Li et al. [36]	$2T_{ec} + 1T_p + 1T_s = 155T_h \approx 8.8ms$	$2T_{ec} + 1T_p + 1T_s = 155T_h \approx 8.8ms$
Ostad-Sharif et al. [37]	$7\ T_h \approx 0.406ms$	$4\ T_h \approx 0.228ms$
Proposed	$8T_h + 1T_i \approx 0.627\ ms$	$6T_h \approx 0.342\ ms$

The contributed scheme must protect few significant factors including the master secret key of HN (KH) as well as the identity (ids) of SN.

```
Query attacker (KH).
Query attacker (ids).
```

The Fig. 6 and Fig. 7 describe channels, variables, events and queries. The Fig. 8 and Fig. 9 show the procedures for HN and SN. For the sake of ease, the entity AP is purged given that it does merely the role of forwarding agent upon receiving the message from one entity to another. The corresponding AP appends merely its identity id_A in the forwarded message forgoing the complex computations.

```
Process
Let aSN = XOR(TIDs, KH) in
Let Js = XOR(IDs, h(TIDs, KH)) in
((!SN(ids, aSN, bSN, Ds))|
  (!HN(SK, Js, KH)
```

The constructors such as XOR() and h() are delineated as exclusive-OR and one-way hash functions [48], [49], respectively. We may describe an equation for exclusive-OR employing the XOR function, such that, XOR(XOR (p, q), q) = p. The corresponding constructors/destructors, and the utilized equations in the scheme are modeled in ProVerif simulation as shown in Fig. 4.

We design the queries in this simulation in order to test the security strength of the contributed model as given below:

```
RESULT inj-event(end_HN(ids))==>
 inj-event(begin_HN(ids)) is true.   (1)
RESULT inj-event(end_SN(id_1681))
 ==>inj-event(begin_SN(id_1681))
 is true.                            (2)
RESULT not attacker(KH) is true.
RESULT not attacker(ids) is true.    (3)
```

The results in Eq. (1) and Eq. (2) manifest that the above designed procedures are started as well as terminated with success, while the results in Eq. (3) depict that the attacker query may not either divulge or extract the agreed session key among the participants.

VI. PERFORMANCE EVALUATION

In this section we analyze and evaluate the performance of contributed scheme against other protocols in terms of computation delay, communication cost and consumed energy. We employed a lightweight exclusive-OR and one-way hash digest operations to design the authenticated key agreement in WBAN. By employing the 32-bit Cortex-M4 microcontroller having 72 Mhz frequency, we get the timing for hash digest operation (SHA-1) as 0.057 ms, while the equivalency of operations in Table 2 is based on the same calculation. In ambient temperature and non-active mode it consumes 36mA of power with 3.3V. It takes 118.8 mW power in active mode. This power consumption is related to the estimation of the energy consumption during the computations. According to this estimate, the hub node consumes 0.39ms and sensor node takes 0.228ms, while the energy consumption according the described scenario amounts to (0.228*118.8)/1000 = 0.027mJ. Similarly, for sensor node it is calculated as 0.399*118.8/1000 = 0.047mJ.

The schemes [16] and [18] bear high computational cost due to utilizing cost intensive crypto-primitives, i.e. 120ms and 117ms for hub node and 90ms and 47ms for sensor node, respectively. Similarly, the schemes [19], [25], [36] bear high computational cost as compared to Ostad-Sharif *et al.* [37] and proposed scheme. Although, our scheme bears a little higher cost than [37], yet it is immune to many attacks that [37] could not resist at all, as depicted in Table 4 and is lightweight than most of the compared schemes.

The scheme [16] is vulnerable to password guessing attack and impersonation attack. The Liu *et al.* [18] does not provide resistance to denial of service attack and neither it provide anonymity to the user. Besides, it fails to mutually authenticate the intended participants. The Zhao [19] does not comply with perfect forward secrecy and could reveal future session keys in case the current session is revealed. Moreover, this scheme [19] employs costly computational operations.

The scheme He and Zeadally [25] is prone to key compromise impersonation attack, and it suffers backward secrecy incompliance, in case the user's private key is revealed. The scheme [19] does not support backward secrecy, mutual authentication, and the password may also be guessed. The Li *et al.* [36] is vulnerable to password guessing attack in case the temporary session secrets are revealed, and also it fails to provide mutual authentication to participants, and forward secrecy. The scheme [4] is susceptible to de-synchronization attack and session-specific temporary information attacks. For WBAN systems, the scheme [37] also suffers from master

TABLE 4. Comparison of security features.

	IPGA	*HCC*	*IA*	*DoSA*	*UA*	*DA*	*BS/PFS*	*MA*	*SSTIA*	*MSCA*	*KCI*
[4]	√	√	√	√	√	×	√	√	×	√	√
[16]	×	√	×	√	√	√	√	√	√	√	√
[18]	√	√	√	×	×	√	√	×	√	√	√
[19]	√	×	×	√	√	√	×	√	√	√	√
[25]	√	√	√	√	√	√	×	√	√	√	×
[36]	×	√	√	√	√	√	×	×	√	√	√
[37]	√	√	√	√	√	√	√	√	×	×	×
Ours	√	√	√	√	√	√	√	√	√	√	√

√: Resistant to Attack or supports the feature,
×: Not resistant to Attack, or does not support the security feature
IPGA: Identity or Password Guessing Attack, **HCC**: High Computational Cost, **IA**: Impersonation Attack, **DoSA**: Denial of Service Attack, **UA**: supports User's Anonymity, **DA**: De-synchronization Attack, **BS/PFS**: supports Backward Secrecy/Perfect Forward Secrecy, **MA**: supports Mutual Authentication, **SSTIA**: Session Specific Temporary Information Attack, **MSCA**: Master's Secret Compromise Attack, **KCI**: Key Compromise Impersonation Attack

TABLE 5. Communication cost (bits).

Communication among nodes	**[4]**	**[16]**	**[18]**	**[19]**	**[26]**	**[36]**	**[37]**	**Ours**
SN => IN	896	2352	2184	2880	1120	1232	672	672
IN => HN	952	-	-	-	728	2164	704	704
HN => IN	896	-	-	-	728	1986	672	672
IN =>SN	840	2352	448	1008	728	1568	544	544
Total	3584	4704	2632	3888	3284	6950	2602	2602

Abbreviations: SN: Sensor Node, HN: Hub node, IN: Intermediate node

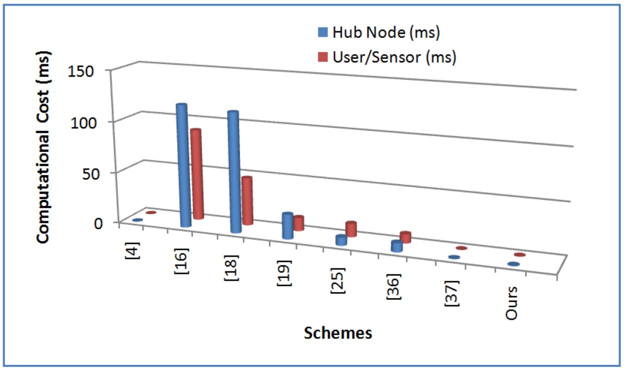


FIGURE 10. Graphical comparative analysis of computational costs.

TABLE 6. Operations costs (Communication).

Primitive operations	**Number of bits**
Timestamp	32 bits
Hash function	256 bits
Random number	128 bits
Identity	32 bits

secret compromise attack, temporary information attack if the session secrets are revealed. In addition, [37] is prone to key compromise impersonation attack. It is evident from Table 3 and 4 that our scheme is resistant to all known attacks and also fulfills many significant security requirements including anonymity and backward/forward secrecy. The schemes [16] and [36] have comparatively higher communication cost as shown in Fig. 10. Similarly the protocols [4], [18], [19], [25] bear more communication cost as compared to [37] and our scheme as evident from Table 5 and Table 6. Although, [37] and our scheme bear the same amount of communication cost, however the former is vulnerable to many attacks in terms of security. Hence, our scheme not only bears the least communication cost but also immune to most of the known attacks.

VII. CONCLUSION

In order to safeguard the life-critical data, only a few researchers have demonstrated or designed strong security system for wireless body area networks. In this paper we present the review of Ostad-Sharif *et al.*, a remote authentication protocol for monitoring the patient's health status in wireless body area networks. Even though, being an efficient protocol in terms of computation, that scheme is found to be having serious security concerns. We revealed in the crypt-analysis section that the Ostad-Sharif *et al.* is defenseless against few attacks notably session-specific ephemeral information threat, key-compromise impersonation threat, and hub node's master secret compromise attack. In the light of these shortcomings, we brought about a new authentication protocol for remote monitoring of patient's health in WBAN. We proved the security features formally under ROR model as well as the logical BAN logic analysis. We also validated the session key strength using automated ProVerif tool analysis. In the near future, we would be exploring more efficiencies and cost optimizations in the authentication protocol for wireless body area networks in cloud-oriented framework.

ACKNOWLEDGEMENT

This Project was funded by the Deanship of Scientific Research (DSR), at King Abdulaziz University, Jeddah, under grant no. (RG-13-611-38). The authors, therefore, acknowledge with thanks DSR technical and financial support.

REFERENCES

[1] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Netw.*, vol. 17, no. 1, pp. 1–18, Jan. 2011.

[2] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks," *J. Med. Syst.*, vol. 36, no. 3, pp. 1065–1094, 2012.

[3] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *Int. J. Commun. Syst.*, vol. 32, no. 16, p. e4139, Nov. 2019.

[4] 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. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[5] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102502.

[6] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," *Comput. Netw.*, vol. 73, pp. 41–57, Nov. 2014.

[7] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 20, pp. 1–15, Sep. 2014.

[8] I. A. Al-Rassan and N. Khan, "Secure & energy efficient key management scheme for WBAN—A hybrid approach," *Int. J. Comput. Sci. Netw. Secur.*, vol. 11, no. 6, p. 169, 2011.

[9] Y. L. Kumbhare, P. H. Rangaree, and G. M. Asutkar, "Wireless body area sensor network authentication using HMAC function," in *Proc. 2nd Nat. Conf. Inf. Commun. Technol. (NCICT)*, 2011, pp. 22–27.

[10] J. Liu, Z. Zhang, R. Sun, and K. S. Kwak, "An efficient certificateless remote anonymous authentication scheme for wireless body area networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 3404–3408.

[11] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.

[12] D. He, C. Chen, S. Chan, J. Bu, and P. Zhang, "Secure and lightweight network admission and transmission protocol for body sensor networks," *IEEE J. Biomed. Health Informat.*, vol. 17, no. 3, pp. 664–674, May 2013.

[13] L. Ma, Y. Ge, and Y. Zhu, "TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 1077–1090, Jul. 2014.

[14] S. N. Ramli, R. Ahmad, and M. F. Abdollah, "Electrocardiogram (ECG) signals as biometrics in securing wireless body area network," in *Proc. IEEE 3rd Int. Conf. Inf. Sci. Technol. (ICIST)*, London, U.K., Dec. 2013, pp. 536–541.

[15] J. Iqbal, Nizamuddin, N. U. Amin, and A. I. Umar, "Authenticated key agreement and cluster head selection for wireless body area networks," in *Proc. 2nd Nat. Conf. Inf. Assurance (NCIA)*, Rawalpindi, Pakistan, Dec. 2013, pp. 113–117.

[16] B.-L. Chen, W.-C. Kuo, and L.-C. Wuu, "Robust smart-card-based remote user password authentication scheme," *Int. J. Commun. Syst.*, vol. 27, no. 2, pp. 377–389, 2014.

[17] X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *J. Netw. Comput. Appl.*, vol. 36, no. 5, pp. 1365–1371, Sep. 2013.

[18] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.

[19] Z. Zhao, "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 38, no. 2, p. 13, Feb. 2014.

[20] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2327–2339, Dec. 2014.

[21] P. Chhajed, D. Baviskar, R. Ahire, A. Bumb, and M. V. Korade, "Certificateless remote anonymous authentication technique for wireless body area networks," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Noida, India, Oct. 2015, pp. 1035–1041.

[22] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1442–1455, Jul. 2015.

[23] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *J. Med. Syst.*, vol. 39, no. 11, p. 136, Nov. 2015.

[24] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *J. Med. Syst.*, vol. 39, no. 10, p.115, Oct. 2015.

[25] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 71–77, Jan. 2015.

[26] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Comput. Methods Programs Biomed.*, vol. 135, pp. 37–50, Oct. 2016.

[27] A. A. Omala, K. P. Kibiwott, and F. Li, "An efficient remote authentication scheme for wireless body area network," *J. Med. Syst.*, vol. 41, no. 2, p. 25, Feb. 2017.

[28] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *J. Med. Syst.*, vol. 40, no. 5, p. 117, May 2016.

[29] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.

[30] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *J. Med. Syst.*, vol. 40, no. 6, p. 134, Jun. 2016.

[31] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.

[32] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth," *J. Med. Syst.*, vol. 40, no. 11, p. 231, Nov. 2016.

[33] J. Liu, L. Zhang, and R. Sun, "1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors*, vol. 16, no. 5, p. 728, May 2016.

[34] N. Yessad, S. Bouchelaghem, F.-S. Ouada, and M. Omar, "Secure and reliable patient body motion based authentication approach for medical body area networks," *Pervas. Mobile Comput.*, vol. 42, pp. 351–370, Dec. 2017.

[35] C. L. Priya and U. S. Visalakshi, "Secure and efficient communication using ECC algorithm in wireless body area network," *Int. J. Eng. Sci.*, vol. 7, no. 4, p. 10073, 2017.

[36] X. Li, M. H. Ibrahim, S. Kumari, and R. Kumar, "Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors," *Telecommun. Syst.*, vol. 67, no. 2, pp. 323–348, Feb. 2018.

[37] A. Ostad-Sharif, M. Nikooghadam, and D. Abbasinezhad-Mood, "Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks," *Int. J. Commun. Syst.*, vol. 32, no. 12, p. e3974, Aug. 2019.

[38] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[39] B. Blanchet, "ProVerif automatic cryptographic protocol verifier user manual," Dept. dInformatique, Ecole Normale Superieure, CNRS, Paris, France, Tech. Rep., 2005.

[40] M. Abdalla, P.-A. Fouque, and D. Pointcheval "Password-based authenticated key exchange in the three-party setting," in *Proc. PKC*, in Lecture Notes in Computer Science, vol. 3386. Berlin, Germany: Springer, 2005, pp. 65–84.

[41] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2603–2611, Apr. 2020.

[42] P. Soni, A. K. Pal, and S. H. Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote healthcare system," *Comput. Methods Programs Biomed.*, vol. 182, Dec. 2019, Art. no. 105054.

[43] A. S. Sangari and J. M. L. Manickam, "Light weight security and authentication in wireless body area network," *Indian J. Comput. Sci. Eng.*, vol. 4, no. 6, pp. 438–446, 2013.

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

[45] S. H. Islam, M. S. Obaidat, and R. Amin, "An anonymous and provably secure authentication scheme for mobile user," *Int. J. Commun. Syst.*, vol. 29, no. 9, pp. 1529–1544, Jun. 2016.

[46] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4081–4092, Sep. 2018.

[47] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.

[48] S. H. Islam, "Design and analysis of an improved smartcard-based remote user password authentication scheme," *Int. J. Commun. Syst.*, vol. 29, no. 11, pp. 1708–1719, Jul. 2016.

[49] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Innsbruck, Austria: Springer, 2001, pp. 453–474.

[50] B. Narwal and A. K. Mohapatra, "SEEMAKA: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks," *Wireless Pers. Commun.*, vol. 113, pp. 1–24, Apr. 2020.

[51] X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart card," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 73–79, 2011.

BANDER A. ALZAHRANI (Member, IEEE) received the M.Sc. degree in computer security and the Ph.D. degree in computer science from Essex University, U.K., in 2010 and 2015, respectively. He is currently an Assistant Professor with King Abdulaziz University, Saudi Arabia. His research interests include wireless sensor networks, information centric networks, bloom filter data structure and its applications, secure content routing, and authentication protocols in the IoT. He has published more than 50 research papers in international journals and conferences.

AZEEM IRSHAD received the master's degree from Arid Agriculture University, Rawalpindi, Pakistan, and the Ph.D. degree from International Islamic University, Islamabad, Pakistan. He has authored more than 64 international journal and conference publications, including 33 SCI-E journal publications. His research work has been cited over 646 times with 12 H-index and 14 i-10-index. He received Top Peer-Reviewer Award from Publons in 2018 with 126 verified reviews. He has served as a reviewer for more than 40 reputed journals including the IEEE Systems Journal, *IEEE Communications Magazine, IEEE TII, IEEE Consumer Electronics Magazine*, IEEE Sensors Journal, IEEE Transactions on Vehicular Technology, IEEE IAS, *Computer Networks, Information Sciences, CAEE, Cluster Computing, AIHC, JNCA and FGCS*, notably. His research interests include strengthening of authenticated key agreements in cloud-IoT, smart grid, pervasive edge computing, CPS, 5G networks, WSN, Ad hoc Networks, e-health clouds, SIP, and multi-server architectures.

AIIAD ALBESHRI received the M.S. and Ph.D. degrees in information technology from the Queensland University of Technology, Brisbane, Australia, in 2007 and 2013, respectively. He has been an Associate Professor with the Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia, since 2018. His current research focuses on security and trust in cloud computing and big data.

KHALID ALSUBHI (Member, IEEE) received the M.S. and Ph.D. degrees in computer science from Waterloo University, Waterloo, Canada, in 2009 and 2016, respectively. His research interests include intrusion detection systems, privacy of healthcare systems, big data, resource management in distributed systems.

MUHAMMAD SHAFIQ received the M.S. degree in computer science from the University Institute of Information Technology, Arid Agriculture University, Rawalpindi, Pakistan, the master's degree in information technology from the University of the Punjab, Gujranwala, Pakistan, and the Ph.D. degree in information and communication engineering from Yeungnam University, South Korea, in 2018. He was a Postdoc Fellow with Yeungnam University, South Korea. He is currently working as a Research Professor with the Department of Information and Communication Engineering, Yeungmnma University, South Korea. His research interests include the design of spectrum management, routing, and medium access control protocols for mobile ad hoc networks, the IoT, and cognitive radio networks.