Array 27 (2025) 100463

Contents lists available at ScienceDirect

Array

journal homepage: www.sciencedirect.com/journal/array

Anonymous wireless body area networks authentication protocol based on biometrics and asymmetric key cryptography

Keyan Abdul-Aziz Mutlaq [a], Mushtaq A. Hasson [b], Zaid Ameen Abduljabbar [b,c,d,m,*], Vincent Omollo Nyangaresi [e,f], Mustafa A. Al Sibahee [g,h], Junchao Ma [c,**], Samir M. Umran [i,n], Ali Hasan Ali [j,k,o], Abdulla J.Y. Aldarwish [b], Husam A. Neamah [l]

[a] IT and Communications Center, University of Basrah, Basrah, 61004, Iraq
[b] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq
[c] College of Big Data and Internet, Shenzhen Technology University, Shenzhen, 518118, China
[d] Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, 518000, China
[e] Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, 40601, Kenya
[f] Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu, 602105, India
[g] National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen, 518060, China
[h] Department of Management and Marketing, College of Industrial Management for Oil and Gas, Basrah University for Oil and Gas, Basrah, 61001, Iraq
[i] School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, 430074, China
[j] Department of Mathematics, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq
[k] Institute of Mathematics, University of Debrecen, Pf. 400, H-4002, Debrecen, Hungary
[l] Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Otemeto u.4-5, Debrecen, 4028, Hungary
[m] Department of Business Management, Al-Imam University College, Balad, 34011, Iraq
[n] Ministry of Industry and Minerals, Iraqi Cement State Company, Baghdad, 10011, Iraq
[o] Technical Engineering College, Al-Ayen University, Thi-Qar, 64001, Iraq

ARTICLE INFO

Keywords:
Attacks
WBAN
Authentication
Privacy
Security
Anonymity

ABSTRACT

Wireless Body Area Networks (WBANs) have been extensively deployed to offer remote patient monitoring that facilitate timely diagnosis and medication. This has greatly helped reduce costs and stress on the limited healthcare resources. However, the exchange of sensory patient data across wireless public communication media exposes the communication process to a myriad of security threats. To curb these security challenges, past research work has deployed techniques such as identity-based and public key cryptosystems to develop schemes for this environment. Nevertheless, the complex mathematical computations in majority of these schemes render them inefficient for sensors. In this current work, we utilize an amalgamation of asymmetric cryptography and user biometrics to develop a robust authentication protocol for WBANs. The famous Burrows–Abadi–Needham (BAN) logic is then deployed to formally analyze the security posture of the developed scheme, with results indicating that it offers secrecy and reliability of the negotiated session keys. In addition, the informal security analysis shows that it is robust against typical WBAN attacks such as impersonation and privileged insiders. From the performance perspective, our protocol incurs the least communication and computation costs.

1. Introduction

Internet of Things (IoT) has been extensively applied in the medical fields in an effort to minimize healthcare costs and enhance quality [1]. In the IoT-enabled WBANs, real-time tracking and remote monitoring of patients is attained, which greatly enhances communication between hospitals and remote patients [2]. The medical smart devices and software in WBANs can collect, communicate and process a wide range of patient physiological data [3]. To accomplish this, small and low-power sensors are placed on the vicinity of the patient or implanted inside the patient's body to monitor physiological and environmental values such as heart rate, blood oxygen saturation levels, electrocardiogram, blood

* Corresponding author. Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq.
** Corresponding author. College of Big Data and Internet, Shenzhen Technology University, Shenzhen, 518118, China
E-mail addresses: zaid.ameen@uobasrah.edu.iq (Z.A. Abduljabbar), mustafaalsibahee@szu.edu.cn (M.A. Al Sibahee), majunchao@sztu.edu.cn (J. Ma), i201922037@alumni.hust.edu.cn (S.M. Umran).

https://doi.org/10.1016/j.array.2025.100463
Received 24 October 2024; Received in revised form 11 July 2025; Accepted 12 July 2025
Available online 14 July 2025

pressure, respiratory rate, blood sugar and temperature [4]. This enables the healthcare providers to make real-time diagnosis and decisions regarding patient care [5]. In so doing, they help facilitate timely analysis, improve healthcare quality, convenience, reliability and minimize medical costs [6,7]. As explained in Ref. [8], the WBAN devices can communicate with the gateways or other central hubs that can perform data processing and can also forward the collected data to remote locations for further processing. The continued adoption of WBANs has been fueled by the considerable hospital staffing shortages, ageing populations as well as growing healthcare costs.

The collected patient data is forwarded through several resource constraints devices over the public channels [9]. This presents some challenges in maintaining secure communication and preserving data confidentiality. As explained in Ref. [10], the protection of patient information exchanged over the public internet is a major concern. For instance, unauthorized access to the sensor communications or WBAN devices can result in modifications or theft of patient health data [11]. This can potentially lead to misdiagnosis and hence wrong medication which can endanger the patient life. Therefore, the key concerns in WBANs revolve around ensuring that the communication is private and secure, as well as preserving sensor accuracy and reliability [12]. Unfortunately, security challenges such as Denial of Service (DoS), eavesdropping, Man-in-the-Middle (MitM) and impersonations have continued to wreak havoc in WBANs [13,58]. As shown in Fig. 1, an adversary located between the patients and the hospitals is capable of launching all these attacks.

It is therefore important that the sensory data is accessible to legitimate WBAN entities such as clinical staff and doctors [14]. In addition, patient privacy as well as integrity and confidentiality of collected data must be upheld. Without these features being preserved, public confidence in these WBANs diminishes.

In light of these security and privacy challenges, data privacy and remote user verification has become a top priority [15]. Therefore, numerous security techniques have been put forward over the recent past. Most of these security solutions are based on computationally intensive cryptosystems such as blockchain and bilinear pairings. Owing to the resource limitations of WBAN components, these techniques require high communication, processing, and memory overheads. As such, majority of the conventional security methods are unsuitable for the tiny sensors. There is therefore need for the development of strong authentication and the key establishment protocols to secure WBANs at low overheads.

1.1. Contributions

- We leverage on asymmetric cryptography and user biometrics to develop an authentication protocol which is demonstrated to be provably secure against conventional WBAN attacks.
- All the exchanged messages are time-stamped and encapsulated with random numbers to maintain their freshness and hence thwart packet replays.
- To demonstrate the secrecy and reliability of the established session keys, we employ the BAN logic proofs.
- Elaborate informal security analysis is carried out to show that our scheme offers salient security features and resistance against attacks such as offline guessing, forgery, and stolen devices.
- In terms of performance, our protocol is shown to require the lowest energy, communication, and computation costs.

The rest of this work is organized as follows: Related works in this domain are explained in Section 2 while the procedures involved during the development of our scheme are detailed in Section 3. Conversely, the security analyses of the developed scheme are detailed in Section 4 while performance evaluations of our protocol are presented in Section 5. Finally, Section 6 concludes the paper and gives some potential research scopes.

1.2. Attack model

The Dolev–Yao (DY) is very popular in the cryptanalysis of authentication protocols. In this model, a malicious entity is capable of listening, intercepting, eavesdropping, modifying, duplicating and even deleting the messages exchanged between the sensors and the remote healthcare providers. Besides, the assailant is capable of physically capturing the sensors and extracting the secrets stored therein.

1.3. Motivation

A report by *Claroty* noted that a large number of IoHT devices and networks are susceptible to security attacks. For instance, the 99 % of IoHT networks analyzed by *Claroty* were discovered to be having exploitable vulnerabilities. In addition, 20 % of the hospital information systems were found to have vulnerabilities related to ransomware. In the year 2024, the *Change Healthcare Attack* wrecked havoc in IoHT system. It paralyzed a subsidiary of *UnitedHealth Group*, disrupting access to patient information, payments, and claims processing. This was attributed to *ALPHV/Blackcat* ransomware group and it impacted approximately 190 million people. As such, strong defense mechanisms must be put in place to safeguard against these security attacks. As such, numerous security solutions have been developed in order to preserve anonymous communication, integrity, authenticity and confidentiality in WBANs,. Majority of these security solutions are based on computationally extensive techniques such as blockchains, identity-based cryptosystem (IBC), pairing operations, Public-Key Cryptography (PKC), and scalar multiplications. Owing to the sophisticated mathematical calculations in these techniques, the resulting security schemes incur high processing costs. In addition, most of the PKC-based protocols present some challenges in certificate management and revocation. Moreover, these PKC-based schemes deploy Certificate Authority (CA) for binding user identities to the public keys, which results in high management costs. Although IBC-based schemes solve this problem, they have key escrow challenges. Consequently, majority of these security solutions

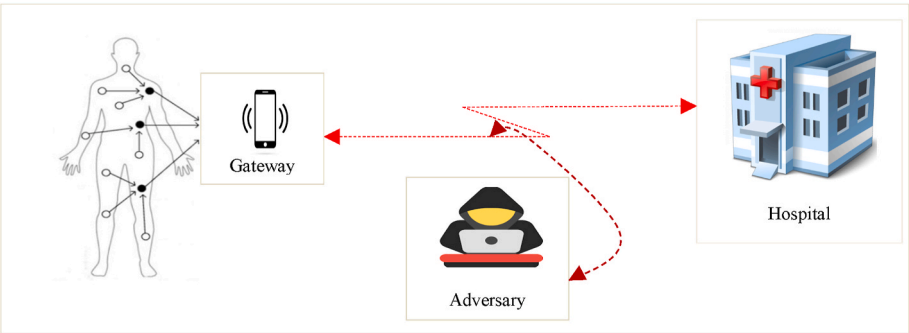

Fig. 1. Adversaries in WBANs.

are not appropriate for WBAN components due to their resource limitations. Therefore, we develop a provably secure but efficient security protocol for deployment in this environment.

2. Related works

A myriad of security solutions have been put forward to protect the communication procedures in WBANs. For instance, and IBC authentication protocol is introduced in Ref. [16] while a protocol based on Elliptic Curve Cryptography (ECC) is presented in Ref. [17]. Nevertheless, the scheme in Ref. [16] requires long processing time and cannot resist attacks such as impersonations and MitM [18]. On the same breadth, the security technique in Ref. [17] is not resistant against impersonate threats [19], and incurs extensive communication and computation overheads [59]. Regarding the protocols in Ref. [20,21], their shortcomings are that they cannot protect against threats such as forgery and impersonations, while the scheme in Ref. [22] fail to protect against attacks such as MitM and replays. Based on the Public Key Infrastructure (PKI), an encryption security solution is presented in Ref. [23]. However, the bilinear pairings render this approach computationally extensive [24]. In addition, certificate management and revocation results in high storage and communication costs. As explained in Ref. [11], this security technique cannot preserve forward secrecy as well as mutual authentication. In addition, it fails to mitigate attacks such as replays.

To offer anonymous communication, certificateless authentication schemes are developed in Ref. [25,26]. However, it cannot offer user anonymity and fails to protect against collusion attacks [27]. Similarly, the protocol in Ref. [28] cannot uphold anonymous communication. Regarding the user authentication technique developed in Ref. [29], the authors in Ref. [20] explain that it is defenseless against insider attacks. In addition, its authentication procedures result in high communication. Due to bilinear pairing operations in Ref. [26], this approach is computationally extensive. Besides, its design does not consider replay attacks and forward secrecy. On the same breadth, the authentication scheme in (X. [30]) cannot preserve ideal forward key secrecy and fails to protect against impersonation, DoS and stolen verifier attacks [31]. To curb some of these threats, a certificate-based encryption technique is introduced in Ref. [32] that is shown to be efficient due to the deployed hyperelliptic curve encryption. Although it offers integrity and protection against replays and privacy leakages, the certificate management becomes problematic with the surging number of devices. To counter this challenge, a verification protocol is developed in Ref. [33]. However, the authors in Ref. [34] demonstrate that this scheme exhibits extensive computation and communication costs and is susceptible to impersonations, MitM, privileged insider and replays. Similarly, the security scheme designed in Ref. [35] cannot withstand attacks such as MitM.

To safely transmit sensitive information over insecure channels, a message verification technique is developed in Ref. [36]. Even though this protocol is lightweight, it is vulnerable to stolen controller device [11]. To ensure anonymous communication, a cipher-based encryption technique is developed in Ref. [37]. Although this technique boosts confidentiality and authenticity, the utilized bilinear pairing operations results in high processing costs [38]. Similarly, the ECC point multiplications in Ref. [39] render this protocol computationally extensive. Using self-certified public keys, a two-party authentication scheme is introduced in Ref. [40]. This scheme is efficient and hence can address the challenges in Ref. [37,39]. However, during the registration phase, the secret parameters are accepted devoid of any validation by the end systems. To offer device authentications, an edge-based IoT verification security technique is introduced in Ref. [41]. Unfortunately, this approach requires high bandwidth and elongated processing time [13]. Similarly, the anonymity-preserving user validation approach developed in Ref. [42] has high bandwidth and processing costs [13]. This is attributed to its lengthy and complicated user authentication procedures. Besides, it cannot provide forward key security [43] and cannot mitigate node capture and privileged insider threats. Regarding the scheme presented in Ref. [44], its shortcomings include vulnerability to Known Session-Specific Temporary Information (KSSTI) as well as forgery threats. To address inefficiencies in Ref. [41,42], an efficient validation scheme is developed in Ref. [45]. However, this scheme is not evaluated against attacks such as hash collusion [6]. Additionally, it cannot mitigate offline password-guessing threats. To curb security vulnerabilities in Ref. [42], a robust user authentication protocol is developed in Ref. [43]. Unfortunately, its sophisticated user authentication procedures are unsuitable for resource-limited WBAN devices [13].

A scheme for secure communication over the public internet is developed in Ref. [46]. Unfortunately, this scheme requires the exchange of massive messages and hence has increased communication overheads [13]. Similarly, the identity-based ring signature protocol in Ref. [47] incurs heavy computation costs [6]. Therefore, a lightweight identity-based verification technique is designed in Ref. [48]. Unfortunately, this approach fails to uphold forward key secrecy [43]. In addition, identity-based schemes have key escrow challenges [49]. Conversely, the scheme in Ref. [50] is not resistant against impersonation, KSSTI, privileged insider and offline password guessing threats [51]. To solve the forward shortfalls in (M. [48]), an IBC scheme is introduced in (C. [52]). Nevertheless, private keys generation is solely accomplished by the trusted key generator [6]. This can potentially present a single point of failure. Therefore, a multi-factor validation protocol is developed in Ref. [53] using the Physically Unclonable Function (PUF). However, its lengthy and complicated verification procedures result in extensive bandwidth and computation overheads [13]. To facilitate secure data sharing, frameworks based on blockchain technology are developed in Ref. [54,55]. However, the deployed blockchain increases the overheads for data management and communication.

Based on the above discussions, it is evident that numerous authentication protocols have been developed for the WBANs. However, numerous security and privacy vulnerabilities in these protocols continue to pose serious challenges as their exploitation results in privacy violations, network disruptions, device corruption or data leakages and losses. Performance constraints in terms of high computation, communication, storage and energy overheads are other serious challenges inherent in most of the conventional authentication schemes. As such, these protocols cannot be deployed in WBANs to offer security protection, owing to the resource-constrained nature of WBAN devices. The developed protocol addresses most of these security threats at the lowest computation, communication and energy overheads.

3. The proposed protocol

In this part, the key design principles of our robust authentication technique are described. This is succeeded by the network model and the stepwise execution of our scheme. These concepts are described in more detail as shown below.

3.1. Fuzzy extractor

In our protocol, we deploy user biometrics as one of the factors during the authentication procedures. During biometric-based authentication, the user biometric data is deployed as input to the fuzzy extraction (*FE*) to yield biometric key. Let us take *HS* as the helper string, *B*i as the user biometrics, and φ as biometrics key. Fundamentally, fuzzy extraction involves the *FE.Gen*(.) and *FE.Rec*(.) functions, in which the former denotes the key generation function, while the latter represents the key reconstruction function. Mathematically, key generation is executed as shown in equation (1).

$$FE.Gen\ (B_i) = (\varphi, H_S) \tag{1}$$

To obtain key φ from the noisy user biometric data B_i*, the *FE.Rec* (.) function is deployed together with the helper string H_S as shown in equation (2).

$$\varphi = FE.Rec\left(H_S, B_i^*\right) \tag{2}$$

To achieve perfect recovery of key φ, the Hamming distance ψ between B_i* and B_i should not exceed maximum value τ. Mathematically, this is expressed as follows:

$$\psi\left(B_i^*, B_i\right) \leq \tau \tag{3}$$

Although it is rare, ideal situation requires that $B_i^* = B_i$, that is, the noisy user biometric data should be equivalent to the initial user biometrics data. This is the basis for the effectual fuzzy extraction carried out in our scheme.

3.2. Key design principles

In order to provide efficient and robust message protection, our protocol should uphold the features below:

Robust authentication: The gateway node, sensor and the user must verify each other's identity before exchanging sensitive patient data over insecure communication channels.

Session key agreement: The communicating entities must negotiate a session key to encipher the sensory data exchanged over the public internet.

Anonymity: It should be impossible for malicious entities to determine the actual identities of the communicating parties based on the captured messages.

Untraceability: The eavesdropping of exchanged messages during the authentication procedures should not assist adversaries in associating any of these messages to a particular communicating party.

Forward and backward key secrecy: It should be mathematically impossible to use the captured current session key to derive keys for the previous and subsequent communication procedures.

Robust against WBAN attacks: For enhanced privacy and security, typical WBAN threats such as forgery, stolen device, privileged insider, KSSTI, impersonation, MitM, replays, and offline guessing should be prevented.

Efficiency: Since the WBAN components are limited in terms of resources, an ideal authentication protocol should be efficient.

3.3. Network architecture

The network architecture of our protocol comprises of sensor node S_j, the medical expert designated as user U_i, and gateway node GW_k. Fig. 2 gives a depiction of this network architecture.

Since S_j has limited communication capabilities, all its data are forwarded to the medical expert via the GW_k, which is well resourced in terms of communication abilities, processing power, and storage. Prior to exchanging the sensory data, both S_j and U_i must register at the GW_k so as to be assigned session-specific parameters for use during the latter phases. The precise particulars of these procedures are detailed in the following sub-sections. The various symbols and notations deployed in this work are presented in Table 1.

3.4. System setup

Prior to registration phase, the GW_k generates its unique identity as GID_k. It also derives its public-private key pair as $\{G_{pk}, G_{sk}\}$. Next, it selects some asymmetric encryption and decryption algorithms E_k (.) and D_k(.) respectively, as shown in Fig. 3.

3.5. User registration

During user U_i registration to the GW_k, the procedures below are carried out over secured communication channels.

Step 1 The U_i generates UID_i and PW_i as his/her unique identity and password respectively. Next, user U_i generates secret key $\varphi = FE.Rec\ (H_S, B_i^*) = B_T \oplus PW_i$. Thereafter, it chooses δ as the shared key between itself and GW_k. Next, biometric data B_i is imprinted onto the appropriate reader in user's smart device SD_i. Next, the reader derives $\varphi = FE.Rec\ (H_S, B_i^*)$ and biometric template as $B_T = \varphi \oplus PW_i$ as shown in Fig. 3.

Step 2 U_i computes $A_1 = h\ (UID_i||PW_i||B_i||\varphi)$ and chooses random number $r_u \in Z_q^*$. Thereafter, values $A_2 = h\ (G_{pk}||\delta)$, $A_3 = h\ (A_1||A_2||(\delta \oplus r_u))$ and $A_4 = E_{G_{pk}}\ (UID_i, A_1, A_3, r_u)$ are calculated. In the end, it sends registration request $Req\text{-}1 = \{A_4\}$ to GW_k.

Step 3 Upon receiving $Req\text{-}1$, the GW_k deploys key G_{sk} to decrypt A_4 as $B_1 = D_{G_{sk}}\ (A_4)$. This decryption yields UID_i, A_1, A_3 and r_u that are used to derive $A_2^* = h\ (G_{pk}||\delta)$, $A_3^* = h\ (A_1||A_2^*||(\delta \oplus r_u))$. It then determines if $A_3^* = A_3$, terminating the registration upon

Table 1
Deployed symbols.

Symbol	Description
GW_k	Gateway k
$\{G_{pk}, G_{sk}\}$	Public-private key pair for GW_k
U_i	User i
$\{K_{puv}, K_{pr}\}$	Public-private key pair for U_i
S_j	Sensor node j
γ	S_j's secret parameter
$\{a_s, a_p\}$	Public-private key pair for S_j
Ψ	Shared symmetric key between GW_k & S_j
δ	Shared symmetric key between GW_k & U_i
UID_i, SID_j, GID_k	Unique user, sensor and gateway node identity
PW_i	User password
B_i, φ	User biometric data and secret key respectively
B_T	Biometric template
H_S	Helper data
E_k (.), D_k(.)	Encryption and decryption using k respectively
h_k (.)	Keyed hash
T_i	Timestamp i
υ	Maximum permissible transmission latency
h (.)	Hashing function
S_{ji}, S_{ij}	Session keys
$\|\|$	Concatenation operation
$\oplus$	Exclusive OR operation

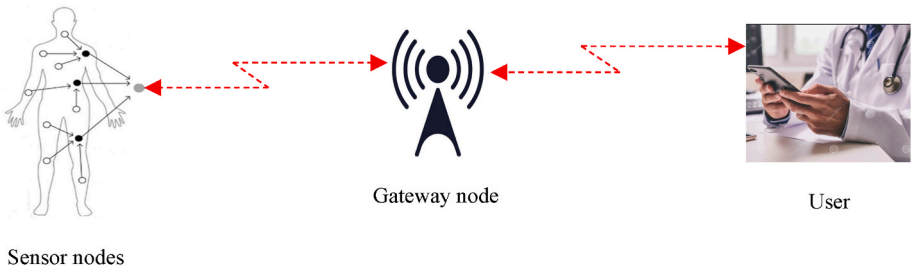

Fig. 2. Network architecture.

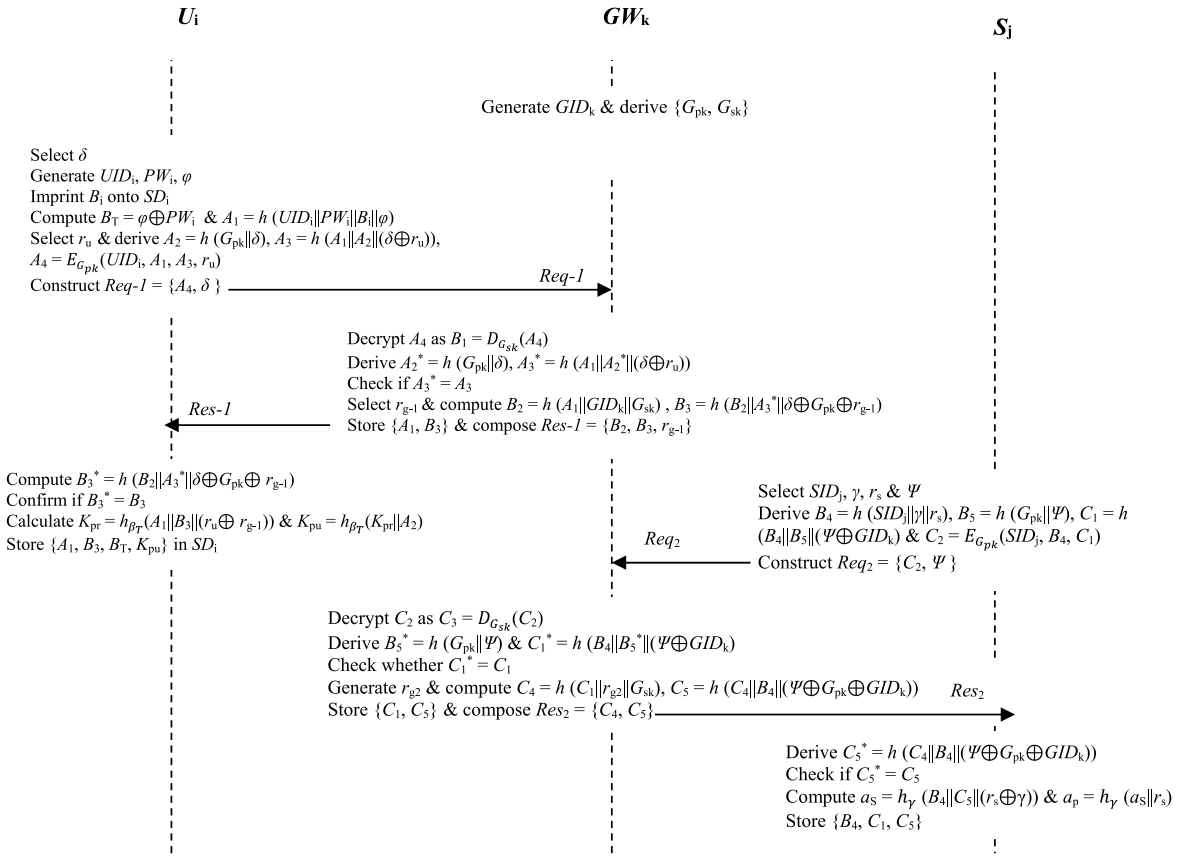

Fig. 3. System setup and registration.

verification failure. Otherwise, it chooses some random number $r_{g\text{-}1} \in Z_q^*$ that is utilized to compute $B_2 = h(A_1||GID_k||G_{sk})$ and $B_3 = h(B_2||A_3^*||\delta \oplus G_{pk} \oplus r_{g\text{-}1})$. Finally, it stores $\{A_1, B_3\}$ in its database indexed by UID_i and forwards response $Res\text{-}1 = \{B_2, B_3, r_{g\text{-}1}\}$ to U_i.

Step 4 After getting *Res-1*, the U_i derives $B_3^* = h(B_2||A_3^*||\delta \oplus G_{pk} \oplus r_{g\text{-}1})$ and confirms if $B_3^* = B_3$. Provided that this condition holds, U_i calculates private key $K_{pr} = h_{\beta_T}(A_1||B_3||(r_u \oplus r_{g\text{-}1}))$ and public key $K_{pu} = h_{\beta_T}(K_{pr}||A_2)$. It then stores $\{A_1, B_3, B_T, K_{pu}\}$ in his/her smart device SD_i. Finally, U_i obtains some list of identities SID_j's for sensor nodes that he/she can access.

3.6. Body sensor registration

Before being deployed at the patient side for physiological data collection, each sensor node S_j must be registered at the GW_k. This is attained by the execution of the following 3 steps across secured communication channels.

Step 1 The sensor node S_j randomly chooses SID_j, γ and $r_s \in Z_q^*$ as its real identity, private key and random number in that order. This is followed by the selection of Ψ as the symmetric key shared between itself and GW_k. In addition, S_j derives $B_4 = h(SID_j||\gamma||r_s)$, $B_5 = h(G_{pk}||\Psi)$, $C_1 = h(B_4||B_5||(\Psi \oplus GID_k)$ and $C_2 = E_{G_{pk}}(SID_j, B_4, C_1)$. Finally, it sends registration request $Req_2 = \{C_2\}$ to GW_k as depicted in Fig. 3.

Step 2 Upon getting Req_2, GW_k employs G_{sk} to decrypt C_2 as $C_3 = D_{G_{sk}}(C_2)$ to obtain values SID_j, B_4, C_1. Afterwards, parameters $B_5^* = h(G_{pk}||\Psi)$ and $C_1^* = h(B_4||B_5^*||(\Psi \oplus GID_k)$ are re-computed. Thereafter, it checks whether $C_1^* = C_1$ and if this is not the case, the S_j registration is halted. If not, it generates arbitrary nonce $r_{g2} \in Z_q^*$ that is used to calculate $C_4 = h(C_1||r_{g2}||G_{sk})$ and $C_5 = h(C_4||B_4||(\Psi \oplus G_{pk} \oplus GID_k))$. It then stores $\{C_1, C_5\}$ in its database indexed by SID_j. Finally, it constructs response $Res_2 = \{C_4, C_5\}$ which is sent to the S_j.

Step 3 On getting Res_2, S_j derives $C_5^* = h(C_4||B_4||(\Psi \oplus G_{pk} \oplus GID_k))$ and checks if $C_5^* = C_5$. Provided that this verification fails, the registration process is halted. Otherwise, it computes secret key $a_S = h_\gamma(B_4||C_5||(r_s \oplus \gamma))$, public key $a_p = h_\gamma(a_S||r_s)$. Finally, it stores $\{B_4, C_1, C_5\}$ in its memory.

3.7. Medical expert login

Upon successful registration, the medical expert can log into his/her smart gadget SD_i and thereafter be able to access the sensory data in WBANs. This is achieved by the execution of the following 2 steps over public channels.

Step 1 The user U_i inputs UID_i and PW_i into SD_i. Afterwards, biometric data B_i is imprinted into SD_i as shown in Fig. 4.

Step 2 The SDi derives $\varphi = B_T \oplus PWi$ and $A_1^* = h(UIDi||PWi||Bi||\varphi)$. Next, it confirms if $A_1^* = A_1$ such that the login request is denied when this validation fails. Otherwise, the medical expert has successfully logged into the SDi.

3.8. Mutual authentication and key setup

The goal of the procedures executed in this phase is to mutually verify the legitimacy of U_i, GWk and Sj. This is accomplished prior to U_i being granted permission to access WBAN resources. After successful authentication procedures, the session key is setup to facilitate secure

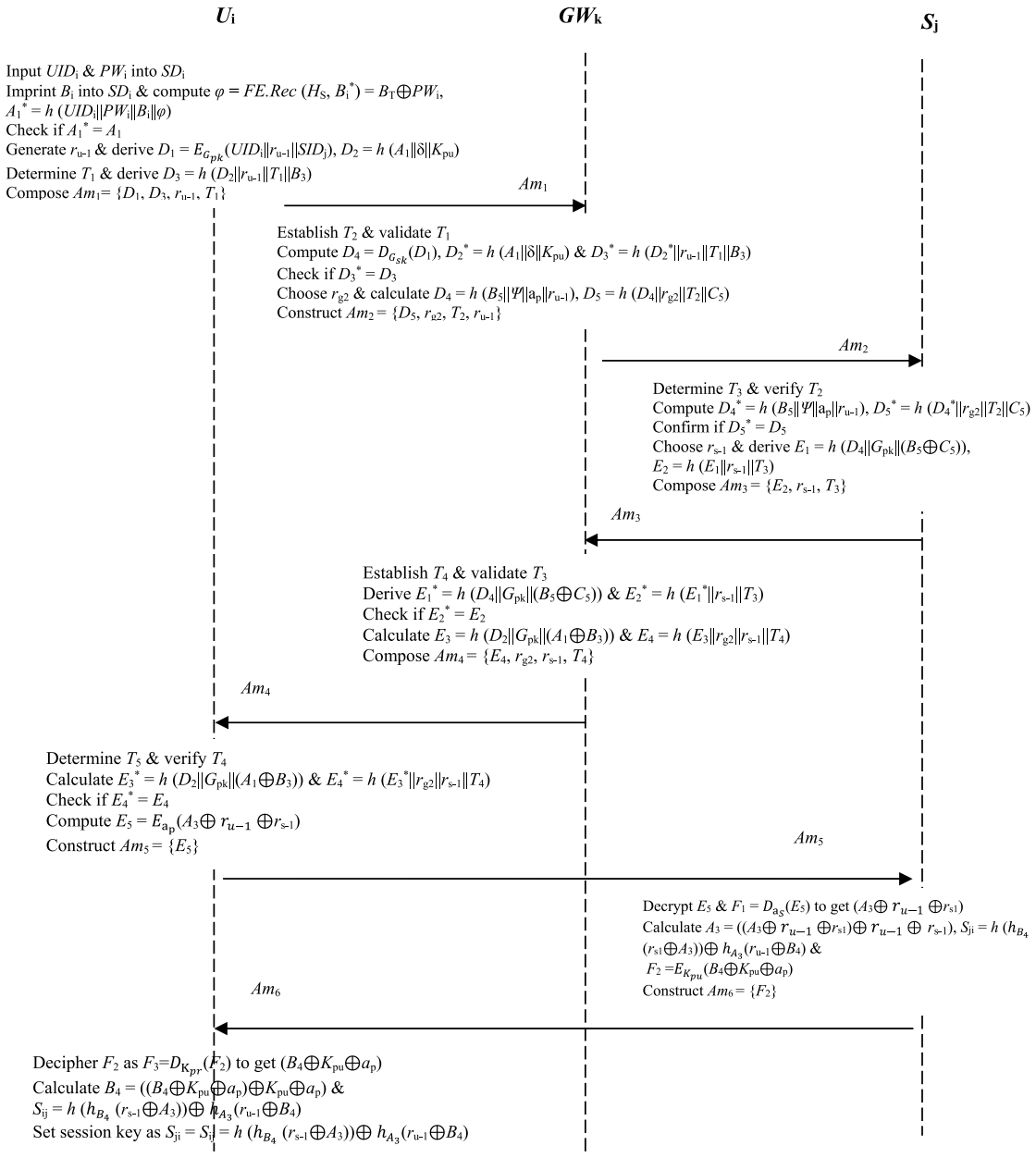

Fig. 4. Login, authentication and key negotiation.

Step 9 Upon getting Am_5, S_j uses key a_S to decipher E_5 and $F_1 = D_{a_S}(E_5)$ to get $(A_3 \oplus r_{u-1} \oplus r_{s-1})$. It then computes $A_3 = ((A_3 \oplus r_{u-1} \oplus r_{s-1}) \oplus r_{u-1} \oplus r_{s-1})$, session key $S_{ji} = h\ (h_{B_4}\ (r_{s-1} \oplus A_3)) \oplus h_{A_3}\ (r_{u-1} \oplus B_4)$ and $F_2 = E_{K_{pu}}\ (B_4 \oplus K_{pu} \oplus a_p)$. At the end, it composes $Am_6 = \{F_2\}$ that is sent to U_i.

Step 10 On receiving Am_6, U_i deploys key K_{pr} to decrypt F_2 as $F_3 = D_{K_{pr}}\ (F_2)$ to obtain $(B_4 \oplus K_{pu} \oplus a_p)$. It then derives $B_4 = ((B_4 \oplus K_{pu} \oplus a_p) \oplus\ K_{pu} \oplus\ a_p)$ and session key $S_{ij} = h\ (h_{B_4}\ (r_{s-1} \oplus A_3)) \oplus h_{A_3}\ (r_{u-1} \oplus B_4)$. Consequently, sensor node S_j and user U_i can now communicate securely over insecure channels through the negotiated session keys $S_{ji} = S_{ij} = h\ (h_{B_4}\ (r_{s-1} \oplus A_3)) \oplus h_{A_3}\ (r_{u-1} \oplus B_4)$.

communication among these entities. This is attained by the 10 steps that follow, across public channels.

Step 1 User *Ui* generates arbitrary number $r_{u-1} \in Z_q^*$ which is used to derive $D_1 = E_{G_{pk}}$ *(*$UID_i||r_{u-1}||SID_j$*)* and $D_2 = h$ *(*$A_1||\delta||Kpu$*)*. Afterwards, it determines the current timestamp T_1 and computes $D_3 = h$ *(*$D_2||r_{u-1}||T_1||B_3$*)*. At the end, it composes authentication message *Am1* = *{*D_1, D_3, r_{u-1}, T_1*}* and sends it to *GWk* as depicted in Fig. 4.

Step 2 Upon getting *Am1*, GW_k gets current timestamp T_2 and validates timestamp T_1 against υ. Basically, the authentication session is halted whenever T_1 fails the freshness check. Otherwise, it derives $D_4 = D_{G_{sk}}$ *(*D_1*)* to obtain *(*$UID_i||r_{u-1}||SID_j$*)*. Thereafter, it uses the resulting UID_i to retrieve the corresponding A_1. Afterwards, GW_k calculates $D_2^* = h\ (A_1||\delta||K_{pu})$ and $D_3^* = h\ (D_2^*||r_{u-1}||T_1||B_3)$. It then confirms whether $D_3^* = D_3$ such that the authentication procedures are halted when the result of this check is negative. Otherwise, U_i is successfully authenticated by the GW_k.

Step 3 The GW_k selects some random number $r_{g2} \in Z_q^*$ that is utilized to compute $D_4 = h\ (B_5||\Psi||a_p||r_{u-1})$ and $D_5 = h\ (D_4||r_{g2}||T_2||C_5)$ in accordance with the received SID_j. Finally, it composes authentication message $Am_2 = \{D_5, r_{g2}, T_2, r_{u-1}\}$ that is transmitted towards S_j.

Step 4 Using υ, S_j obtains T_3 and establishes the freshness of T_2, where T_3 is the current timestamp. Essentially, the verification procedures are halted when this freshness check flops. If not, S_j derives $D_4^* = h(B_5||\Psi||a_p||r_{u-1})$, $D_5^* = h(D_4^*||r_{g2}||T_2||C_5)$ and confirms if $D_5^* = D_5$. Provided that these values are not equivalent, the session is aborted. Otherwise, GW_k is successfully authenticated.

Step 5 The S_j selects some random number $r_{s-1} \in Z_q^*$ which it deploys to compute $E_1 = h(D_4||G_{pk}||(B_5 \oplus C_5))$ and $E_2 = h(E_1||r_{s-1}||T_3)$. At the end, it constructs authentication message $Am_3 = \{E_2, r_{s-1}, T_3\}$ which is forwarded to GW_k.

Step 6 After getting Am_3, the GW_k determines T_4 used to check the freshness of T_3 with the help of threshold υ, where T_4 is the current timestamp. Basically, the mutual validation procedures are abandoned upon validation failure. Otherwise, it calculates $E_1^* = h(D_4||G_{pk}||(B_5 \oplus C_5))$ and $E_2^* = h(E_1^*||r_{s-1}||T_3)$. Afterwards, it checks if $E_2^* = E_2$, halting the session upon verification failure. Otherwise S_j is successfully authenticated.

Step 7 The GW_k derives $E_3 = h(D_2||G_{pk}||(A_1 \oplus B_3))$ as well as $E_4 = h(E_3||r_{g2}||r_{s-1}||T_4)$.This is followed by the construction of $Am_4 = \{E_4, r_{g2}, r_{s-1}, T_4\}$ that is sent to user U_i.

Step 8 After getting Am_4, the U_i establishes the present T_5. Afterwards, it utilizes threshold υ to establish the validity of the received timestamp T_4. Provided that T_4 is invalid, the verification session is terminated. Otherwise, it derives $E_3^* = h(D_2||G_{pk}||(A_1 \oplus B_3))$ and $E_4^* = h(E_3^*||r_{g2}||r_{s-1}||T_4)$. It then confirms if $E_4^* = E_4$ such that GW_k is considered authenticated when this condition holds. Otherwise, the session is terminated. Finally, it derives $E_5 = E_{a_p}(A_3 \oplus r_{u-1} \oplus r_{s-1})$ then constructs message $Am_5 = \{E_5\}$ which is forwarded to S_j via the GW_k.

4. Security analysis

During the formal verification of security schemes, the BAN logic is frequently deployed. As such, we utilize this logic to demonstrate the robustness of the negotiated session key. Thereafter, we state and proof numerous lemmas to show that our scheme is secure under the adversarial capabilities in the Dolev–Yao model.

4.1. Formal security analysis

In this sub-section, we utilize the BAN logic to reveal the secrecy and reliability of the negotiated session keys between sensor node S_j and user U_i. To attain this, we deploy the following notations.

(S): S is fresh.
$R \mid\equiv S$: A trusts S.
$R \lhd S$: R sees S
$R \mid\sim S$: R previously said S.
$\langle S \rangle_M$: S is composed of M
R ⇒ S: R has control over S.
(S, M): S or M is part of (S, M).
S, M_P: S or M is enciphered with key P.
S/M: Provided that numerator P is true, denominator M is also true.
$\langle S \rangle_{P \mapsto R}$: S is enciphered with P, which is a parameter of R
$(S, M)_P$: S or M has been hashed by P.
$R \overset{P}{\leftrightarrow} T$: Y and T utilizes key P to securely exchange data.
During the logic proofs, the following BAN principles are deployed.

Freshness rule (*FR*): $\frac{R \mid\equiv \#(S)}{R \mid\equiv \#(S,M)}$

Nonce Verification Rule (*NVR*): $\frac{R \mid\equiv \#(S), R \mid\equiv T \mid\sim S}{R \mid\equiv T \mid\equiv S}$

Session-key rule (*SKR*): $\frac{R \mid\equiv \#(S), R \mid\equiv T \mid\sim S}{R \mid\equiv R \overset{P}{\leftrightarrow} T}$

Believe Rule (*BR*): $\frac{A \mid\equiv B \mid\equiv (T,M)}{A \mid\equiv B \mid\equiv T}$

Message-Meaning Rule (*MMR*): $\frac{R \mid\equiv R \overset{P}{\leftrightarrow} T, R \lhd \langle S \rangle_M}{R \mid\equiv T \mid\sim S}$

Jurisdiction Rule (*JR*): $\frac{R \mid\equiv T \Rightarrow S, R \mid\equiv T \mid\equiv S}{R \mid\equiv S}$

Further, the messages exchanged between S_j and U_i through the gateway node GW_k are idealized as follows.

$U_i \rightarrow GW_k$: $Am_1 = \{D_1, D_3, r_{u-1}, T_1\}$
Idealized format: $\langle D_1 \rangle_{(UID_i||r_{u-1}||SID_j)}$, D_3: $\langle D_2 \rangle_{(A_1||\delta||K_{pu})}$, T_1, r_{u-1}, B_3
$GW_k \rightarrow S_j$: $Am_2 = \{D_5, r_{g2}, T_2, r_{u-1}\}$
Idealized format: $\langle D_4 \rangle_{(B_5||\Psi||\alpha_p||r_{u-1})}$, T_2, r_{g2}, C_5
$S_j \rightarrow U_i$: $Am_3 = \{E_2, r_{s-1}, T_3\}$
Idealized format: $\langle E_1 \rangle_{(D_4||G_{pk}||(B_5 \oplus C_5))}$, T_3, r_{s-1}
$GW_k \rightarrow U_i$: $Am_4 = \{E_4, r_{g2}, r_{s-1}, T_4\}$
Idealized format: $\langle E_3 \rangle_{(D_2||G_{pk}||(A_1 \oplus B_3))}$, T_4, r_{g2}, r_{s-1}

Finally, we make some initial state assumptions (SA_i) as follows.

SA_f: $U_i \mid\equiv \#(T_1)$.
SA_2: $GW_k \mid\equiv \#(T_2, T_4)$.
SA_3: $S_j \mid\equiv \#(T_3)$.
SA_4: $U_i \mid\equiv \#(r_u, r_{g-1}, r_s, r_{g2}, r_{u-1}, r_{g2}, r_{s-1})$.
SA_5: $GW_k \mid\equiv \#(r_u, r_{g-1}, r_s, r_{g2}, r_{u-1}, r_{g2}, r_{s-1})$.
SA_6: $S_j \mid\equiv \#(r_u, r_{g-1}, r_s, r_{g2}, r_{u-1}, r_{g2}, r_{s-1})$.
SA_7: $U_i \mid\equiv U_i \overset{\delta}{\leftrightarrow} GW_k$
SA_8: $GW_k \mid\equiv GW_k \overset{\delta}{\leftrightarrow} U_i$
SA_9: $GW_k \mid\equiv GW_k \overset{\Psi}{\leftrightarrow} S_j$
SA_{10}: $S_j \mid\equiv S_j \overset{\Psi}{\leftrightarrow} GW_k$
SA_{11}: $S_j \mid\equiv S_j \xleftrightarrow{r_{u1}, r_{s1}} U_i$
SA_{12}: $U_i \mid\equiv U_i \xleftrightarrow{r_{u1}, r_{s1}} S_j$

To proof the secrecy and reliability of the negotiated session keys $S_{ji} = S_{ij} = h(h_{B_4}(r_{s-1} \oplus A_3)) \oplus h_{A_3}(r_{u-1} \oplus B_4)$, the following security goals must be fulfilled.

Goal-1: $U_i \mid\equiv U_i \overset{S_{ji}}{\longleftrightarrow} S_j$
Goal-2: $U_i \mid\equiv S_j \mid\equiv S_j \overset{S_{ji}}{\longleftrightarrow} U_i$
Goal-3: $S_j \mid\equiv S_j \overset{S_{ji}}{\longleftrightarrow} U_i$
Goal-4: $S_j \mid\equiv U_i \mid\equiv U_i \overset{S_{ji}}{\longleftrightarrow} S_j$

Thereafter, the proofs (P_i) proceed as follows.
Based on idealized Am_1, we get the first proof P_1 as follows.
$\boldsymbol{P_1}$: $S_j \lhd r_{u-1}$
Using *MMR* on SA_{11}, and P_1 yields,
$\boldsymbol{P_2}$: $S_j \mid\equiv U_i \mid\sim r_{u-1}$
On the other hand, *NVR* is applied in SA_6 and P_2 to obtain the following,
$\boldsymbol{P_3}$: $S_j \mid\equiv U_i \mid\equiv r_{u-1}$
In addition, the application of *SKR* on SA_6 and P_3 results in P_4.
$\boldsymbol{P_4}$: $S_j \mid\equiv S_j \overset{S_{ji}}{\longleftrightarrow} U_i$, effectively achieving **Goal-3**.
By using NVR on P_4 and SA_6, **Goal-4** is attained as follows.
$\boldsymbol{P_5}$: $S_j \mid\equiv U_i \mid\equiv U_i \overset{S_{ji}}{\longleftrightarrow} S_j$
According to idealized Am_3, we get P_6.
$\boldsymbol{P_6}$: $U_i \lhd r_{s1}$
Using *MMR* in SA_{12} and P_6 results in P_7.
$\boldsymbol{P_7}$: $U_i \mid\equiv S_j \mid\sim r_{s-1}$
On the other hand, *NVR* is applied in SA_4 and P_7 to yield the following.
$\boldsymbol{P_8}$: $U_i \mid\equiv S_j \mid\equiv r_{s-1}$
However, applying *SKR* on both P_8 and SA_4 results in the attainment of **Goal-1**.
$\boldsymbol{P_9}$: $U_i \mid\equiv U_i \overset{S_{ji}}{\longleftrightarrow} S_j$
Finally, *NVR* is applied to SA_4 and P_8 to get P_9 as follows.
$\boldsymbol{P_{10}}$: $U_i \mid\equiv S_j \mid\equiv S_j \overset{S_{ji}}{\longleftrightarrow} U_i$, achieving **Goal-2**.

It is evident that all the four security goals have been attained, confirming that our protocol preserves secrecy and reliability of the negotiated session keys.

4.2. Informal security analyses

In this part, we formulate and proof numerous lemmas concerning the supported security characteristics. The specific details of these procedures are illustrated below.

Lemma 1. *Robust mutual verification is executed.*

Proof. *In our scheme, the three communicating elements jointly validate each other prior to exchanging the sensory data. For instance, upon receiving message* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$ *from* U_i, *the* GW_k *authenticates* U_i *by computing* $D_3^* = h(D_2^*||r_{u\text{-}1}||T_1||B_3)$ *and checking if* $D_3^* = D_3$. *On the other hand, after getting message* $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$ *from* GW_k, *the* S_j *validates it by deriving* $D_5^* = h(D_4^*||r_{g2}||T_2||C_5)$ *and confirming if* $D_5^* = D_5$. *Similarly, after receiving message* $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$ *from* S_j, *it is verified at the* GW_k *by calculating* $E_2^* = h(E_1^*||r_{s\text{-}1}||T_3)$ *and establishing whether* $E_2^* = E_2$. *To authenticate* GW_k, *the user* U_i *receives message* $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, *computes* $E_4^* = h(E_3^*||r_{g2}||r_{s\text{-}1}||T_4)$ *and confirms whether* $E_4^* = E_4$. *On condition that all these verification checks flop, the session is terminated.*

Lemma 2. *Forgery threats are thwarted.*

Proof. *In the proposed scheme, all users are equipped with four parameters, which include* PW_i, UID_i, B_i *and* φ. *All these parameters are needed for effective authentication. Let us assume that attacker* $\bar{E}$ *wants to forge exchanged messages exampled by* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$, *where* $D_1 = E_{G_{pk}}(UID_i||r_{u\text{-}1}||SID_j)$, $D_2 = \mathrm{h}(A_1||\delta||K_{pu})$, $D_3 = \mathrm{h}(D_2||r_{u\text{-}1}||T_1||B_3)$, $A_1 = \mathrm{h}(UID_i||PW_i||B_i||\varphi)$, $B_2 = \mathrm{h}(A_1||GID_k||G_{sk})$ *and* $B_3 = \mathrm{h}(B_2||A_3^*||\delta \oplus G_{pk} \oplus r_{g\text{-}1})$. *Evidently, this requires all the four secrets belonging to user* U_i. *Any attempt at extracting them from* A_1 *will fail since the one-way hashing function is cumbersome to reverse. Similarly, attacker* $\bar{E}$ *is unable to extract* UID_i *from* D_1 *since key* G_{pk} *is unavailable. Even if the attacker manages to obtain* UID_i *and* PW_i, *simultaneously and correctly guessing both* B_i *and* φ *is not possible since they are user-specific. Similarly, due to encryptions and one-way hashing functions, messages* $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$, $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$, $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, $Am_5 = \{E_5\}$ *and* $Am_6 = \{F_2\}$ *cannot be forged.*

Lemma 3. *Key secrecy is preserved.*

Proof. *When executing mutual authentication and setting up the session key, the* S_j *calculates the session key as* $S_{ji} = h(h_{B_4}(r_{s\text{-}1} \oplus A_3)) \oplus h_{A_3}(r_{u\text{-}1} \oplus B_4)$ *while the* U_i *computes it as* $S_{ij} = h(h_{B_4}(r_{s\text{-}1} \oplus A_3)) \oplus h_{A_3}(r_{u\text{-}1} \oplus B_4)$. *Here,* $A_3 = \mathrm{h}(A_1||A_2||(\delta \oplus r_u))$, $A_1 = \mathrm{h}(UID_i||PW_i||B_i||\varphi)$, $A_2 = \mathrm{h}(G_{pk}||\delta)$ *and* $B_4 = \mathrm{h}(SID_j||\gamma||r_s)$. *Evidently, these session keys do not incorporate long-term secret keys such as* G_{pk}, G_{sk}, K_{pu}, K_{pr}, a_s *and* a_p. *Instead, only short-term parameters such as random numbers are utilized. Since these random numbers are refreshed after every session, an attacker is unable to utilize the present session key to compromise past and future session keys.*

Lemma 4. *Our protocol can withstand stolen smart device threats.*

Proof. *Let us assume that malicious entity* $\bar{E}$ *has stolen* U_i*'s smart device* SD_i. *Afterwards, values* $\{A_1, B_3, B_T\}$ *stored in it are extracted by* $\bar{E}$. *Next, an attempt is made to derive user authentication message* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$. *However, Lemma 2 has described the difficulties that* $\bar{E}$ *faces in forging exchanged messages. Similarly, any attempt in using the obtained values to derive the session keys* $S_{ji} = S_{ij} = h(h_{B_4}(r_{s\text{-}1} \oplus A_3)) \oplus h_{A_3}(r_{u\text{-}1} \oplus B_4)$ *will fail. This is because none of the extracted parameters is directly involved in the derivation of these session keys. As such, our scheme is still secure even with the loss of* SD_i.

Lemma 5. *Untraceability is provided.*

Proof. *In our scheme, messages* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$, $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$, $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$, $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, $Am_5 = \{E_5\}$ *and* $Am_6 = \{F_2\}$ *are exchanged over the public channels. Here,* $D_1 = E_{G_{pk}}(UID_i||r_{u\text{-}1}||SID_j)$, $D_3 = \mathrm{h}(D_2||r_{u\text{-}1}||T_1||B_3)$, $D_5 = \mathrm{h}(D_4||r_{g2}||T_2||C_5)$, $E_2 = \mathrm{h}(E_1||r_{s\text{-}1}||T_3)$, $E_4 = \mathrm{h}(E_3||r_{g2}||r_{s\text{-}1}||T_4)$, $E_5 = E_{a_p}(A_3 \oplus r_{u-1} \oplus r_{s\text{-}1})$ *and* $F_2 = E_{K_{pu}}(B_4 \oplus K_{pu} \oplus a_p)$. *Suppose that adversary* $\bar{E}$ *wants to associate these messages to its source or destination. Howver, none of these messages contain plain-text identifieable information such as* UID_i, SID_j, GID_k. *Instead, dynamic parameters such as timestamps and random numbers are incorporated. Since these random numbers and timestamps are different for disparate sessions,* $\bar{E}$ *is unable to associate these messages to a particular* S_j, U_i *or* GW_k.

Lemma 6. *The proposed scheme resists impersonation attacks.*

Proof. *In this analysis, we assume that attacker* $\bar{E}$ *wants to impersonate* S_j, U_i *or* GW_k. *However, the following cases demonstrate how our scheme withstands these impersonations.*

Case 1 User impersonation

In this attack, $\bar{E}$ *attempts to forge message* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$ *sent by* U_i *towards the* GW_k. *Therefore, bogus values* D_1^b, $D_3{}^b$, $r_{u\text{-}1}{}^b$ *and* $T_1{}^b$ *are derived by* $\bar{E}$. *Upon receiving* $Am_1^b = \{D_1^b, D_3^b, r_{u\text{-}1}^b, T_1{}^b\}$, *the* GW_k *re-computes* $D_3^* = h(D_2^*||r_{u\text{-}1}||T_1||B_3)$ *and confirms whether* $D_3^* = D_3^b$. *Since* $\bar{E}$ *lacks valid* D_2^*, $r_{u\text{-}1}$, T_1 *and* B_3, *this verification flops. In addition, since* $T_1{}^b \neq T_1$, *adversarial message* Am_1^b *will fail the freshness check at the* GW_k.

Case 2 *Gateway impersonation*

To impersonate GW_k, *the adversary* $\bar{E}$ *has to forge message* $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$ *that is transmitted from* GW_k *towards* S_j. *As such, bogus message* $Am_2^b = \{D_5^b, r_{g2}^b, T_2^b, r_{u\text{-}1}^b\}$ *is sent over to the* S_j. *Upon receiving this message,* S_j *re-computes* $D_5^* = h(D_4^*||r_{g2}||T_2||C_5)$ *and confirms if* $D_5^* = D_5^b$. *Since* $\bar{E}$ *has no access to valid* D_4^*, r_{g2}, T_2 *and* C_5, *this verification fails. In addition,* $T_2{}^b \neq T_2$ *and hence* Am_2^b *will fail the freshness check at the* S_j. *Any attempt to impersonate* GW_k *using message* $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$ *will flop for the same reasons. That is, the re-computed* $E_4^* = h(E_3^*||r_{g2}||r_{s\text{-}1}||T_4)$ *at the* U_i *will be different from the forged* E_4^b, *and* $T_4{}^b \neq T_4$.

Case 3 *Sensor impersonation*

To carry out this attack, attacker $\bar{E}$ *forges authentication message* $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$ *which is sent from* S_j *towards the* GW_k. *On receiving forged message* $Am_3^b = \{E_2^b, r_{s\text{-}1}^b, T_3^b\}$, *the* GW_k *re-computes* $E_2^* = h(E_1^*||r_{s\text{-}1}||T_3)$ *and checks if* $E_2^* = E_2$. *Since* $E_2^* \neq E_2^b$ *and* $T_3{}^b \neq T_3$, *this forgery is easily detected at the* GW_k.

In all the above impersonation attempts, the sessions are terminated upon freshness or parameter check failures. Consequently, our scheme preserves the integrity of all messages exchanged over the public channels.

Lemma 7. *Anonymous communication is upheld.*

Proof. *In the proposed protocol, messages* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$, $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$, $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$, $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, $Am_5 = \{E_5\}$ *and* $Am_6 = \{F_2\}$ *are exchanged over the public channels. Here,* $D_1 = E_{G_{pk}}(UID_i||r_{u\text{-}1}||SID_j)$, $D_3 = \mathrm{h}(D_2||r_{u\text{-}1}||T_1||B_3)$, $D_5 = \mathrm{h}(D_4||r_{g2}||T_2||C_5)$, $E_2 = \mathrm{h}(E_1||r_{s\text{-}1}||T_3)$, $E_5 = E_{a_p}(A_3 \oplus r_{u-1} \oplus r_{s\text{-}1})$ *and* $F_2 = E_{K_{pu}}(B_4 \oplus K_{pu} \oplus a_p)$. *It is evident that only parameter* D_1 *contains user and sensor node identifiable information. However, these two identities are encapsulated in random number* $r_{u\text{-}1}$ *before being encrypted using the gateway node's public key* G_{pk}. *As such, these unique identities cannot be eavesdropped even if message* Am_1 *is intercepted over the public channels. Consequently, our protocol preserves the secrecy of the communicating entities.*

Lemma 8. *Our protocol protects against KSSTI attacks.*

Proof. *Suppose that session-specific temporary parameters such as* $r_{u\text{-}1}$, $r_{s\text{-}1}$, r_{g2}, δ *and* Ψ *have been leaked to adversary* $\bar{E}$. *Afterwards, an attempt is made to derive session keys* $S_{ji} = S_{ij} = h(h_{B_4}(r_{s\text{-}1} \oplus A_3)) \oplus h_{A_3}(r_{u\text{-}1} \oplus B_4)$. *Although* $\bar{E}$ *has access to* $r_{s\text{-}1}$ *and* $r_{u\text{-}1}$, *parameters* $A_3 = \mathrm{h}(A_1||A_2||(\delta \oplus r_u))$ *and* $B_4 = \mathrm{h}(SID_j||\gamma||r_s)$ *are still unavailable. Therefore, KSSTI attacks against our protocol fails.*

Lemma 9. *The security of the session key is preserved.*

Proof. *In our scheme, session key is calculated as* $S_{ji} = h(h_{B_4}(r_{s\text{-}1} \oplus A_3)) \oplus h_{A_3}(r_{u\text{-}1} \oplus B_4)$ *at the* S_j*. Similarly, the* U_i *calculates the session key as* $S_{ij} = h(h_{B_4}(r_{s\text{-}1} \oplus A_3)) \oplus h_{A_3}(r_{u\text{-}1} \oplus B_4)$*. Here,* $r_{u\text{-}1}$ *is an arbitrary nonce generated at the* U_i *and* $r_{s\text{-}1}$ *is the arbitrary number generated at* S_j*. In our scheme, messages* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$, $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$, $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$, $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, $Am_5 = \{E_5\}$ *and* $Am_6 = \{F_2\}$ *can be intercepted over the public channels. Therefore,* $r_{s\text{-}1}$ *and* $r_{u\text{-}1}$ *can be regarded as public parameters, although they are generated afresh for each session. However, any attempt at compromising these session keys will flop since parameters* A_3 *and* B_4 *are still unknown to* $\bar{E}$ *and are in no way sent in clear text over the communication media.*

Lemma 10. *MiTM attacks are thwarted.*

Proof. *Suppose that adversary* $\bar{E}$ *sits between* U_i *and* GW_k*. Therefore,* $\bar{E}$ *can compose forged message* Am_1^f*. Since* $D_1 = E_{G_{pk}}(UID_i||r_{u\text{-}1}||SID_j)$, $D_3 = \mathrm{h}(D_2||r_{u\text{-}1}||T_1||B_3)$, $D_2 = \mathrm{h}(A_1||\delta||K_{pu})$, $B_3 = \mathrm{h}(B_2||A_3{}^*||\delta \oplus G_{pk} \oplus r_{g\text{-}1})$ *and* $A_1 = \mathrm{h}(UID_i||PW_i||B_i||\varphi)$*, the attacker requires valid identities (*UID_i *and* SID_j*), password* PW_i*, biometric data* B_i*, user secret key* φ*, user public key* K_{pu} *and gateway node public key* G_{pk}*. In accordance with Lemma 2, Lemma 6 and Lemma 7, all these parameters can never be eavesdropped across the public channel. In addition, it is mathematically impossible for them to be concurrently and accurately guessed in polynomial time. Moreover, Lemma 1 describes the various verifications of the exchanged parameters and hence any forged parameters are easily detected in our scheme.*

Lemma 11. *Our scheme withstands offline guessing threats.*

Proof. *The assumption we make here is that malicious entity* $\bar{E}$ *has eavesdropped all the exchanged messages or has stolen user smart device* SD_i*. Upon stealing* SD_i*, the attacker can extract values* $\{A_1, B_3, B_T\}$ *stored in it via side-channeling attack. Here,* $A_1 = \mathrm{h}(UID_i||PW_i||B_i||\varphi)$, $B_3 = \mathrm{h}(B_2||A_3{}^*||\delta \oplus G_{pk} \oplus r_{g\text{-}1})$ *and* $B_T = \varphi \oplus PW_i$*. Due to the one-way hashing in* A_1*,* $\bar{E}$ *is unable to reverse-engineer it to get access to both* UID_i *and* PW_i*. On the other hand, the encapsulation of* PW_i *in* φ *makes it difficult for* $\bar{E}$ *to correctly guess it. On the other hand, the captured messages include* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$, $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$, $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$, $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, $Am_5 = \{E_5\}$ *and* $Am_6 = \{F_2\}$*. Here,* $D_1 = E_{G_{pk}}(UID_i||r_{u\text{-}1}||SID_j)$, $D_3 = \mathrm{h}(D_2||r_{u\text{-}1}||T_1||B_3)$, $D_5 = \mathrm{h}(D_4||r_{g2}||T_2||C_5)$, $E_2 = \mathrm{h}(E_1||r_{s\text{-}1}||T_3)$, $E_5 = E_{a_p}(A_3\, r_{u-1} \oplus r_{s\text{-}1})$ *and* $F_2 = E_{K_{pu}}(B_4 \oplus K_{pu} \oplus a_p)$*. Since none of these messages bears clear text user identity and password* UID_i *and* PW_i *respectively, any effort to recover* UID_i *from* D_1 *will flop since* $\bar{E}$ *does not have* GW_k*'s private key* G_{sk} *needed to decrypt* D_1*.*

Lemma 12. *Our scheme mitigates privileged insider threats.*

Proof. *Suppose that an insider located at the gateway node is attempting to interfere with the security of the proposed scheme. To achieve this,* $\bar{E}$ *retrieves values* $\{A_1, B_3\}$ *and* $\{C_1, C_5\}$ *stored in its database. Here,* $A_1 = \mathrm{h}(UID_i||PW_i||B_i||\varphi)$, $B_3 = \mathrm{h}(B_2||A_3{}^*||\delta \oplus G_{pk} \oplus r_{g\text{-}1})$, $C_1 = \mathrm{h}(B_4||B_5||(\Psi \oplus GID_k))$ *and* $C_2 = E_{G_{pk}}(SID_j, B_4, C_1)$*. Next,* $\bar{E}$ *attempts to recover the secret parameters incorporated in these values. However, the deployed one-way hashing functions and encryptions make this recovery extremely difficult. Additionally,* $\bar{E}$ *may try to use the extracted memory-residents values to derive session keys* $S_{ji} = S_{ij} = h(h_{B_4}(r_{s\text{-}1} \oplus A_3)) \oplus h_{A_3}(r_{u\text{-}1} \oplus B_4)$*. It is clear that none of the retrieved parameters can help* $\bar{E}$ *to compute the session keys.*

Lemma 13. *The proposed scheme resists replay threats.*

Proof. *In these security threats, exchanged data are intercepted across insecure internet, modified before being forwarded to unsuspecting receivers. The messages exchanged over the public internet include* $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$, $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$, $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$, $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, $Am_5 = \{E_5\}$ *and* $Am_6 = \{F_2\}$*. Evidently, messages* Am_1, Am_2, Am_3 *and* Am_4 *incorporate timestamps whose freshness are validated at the receiver end based on the maximum permissible transmission latency* υ*. Although messages* Am_5 *and* Am_6 *do not incorporate direct timestamps,* $E_5 = E_{a_p}(A_3 \oplus ru - 1 \oplus r_{s\text{-}1})$, $F_2 = E_{K_{pu}}(B_4 \oplus K_{pu} \oplus a_p)$ *and* $B_4 = \mathrm{h}(SID_j||\gamma||r_s)$ *incorporate random nonces. As such, forwarding messages with previous random numbers will fail various checks at the receiver end, such as* $D_3{}^* \stackrel{?}{=} D_3$, $D_5{}^* \stackrel{?}{=} D_5$, $E_2{}^* \stackrel{?}{=} E_2$*, and* $E_4{}^* \stackrel{?}{=} E_4$*.*

5. Performance evaluation

Communication costs, storage requirements, computation overheads and energy requirements are the most popular performance measures in most security protocols. The obtained values are then compared with the ones attained by other peer protocols as discussed below.

5.1. Computation complexity

To derive the computation complexity of the authentication and session key setup requests, we utilize the time it takes to execute the various cryptographic primitives. The proposed protocol is implemented in a machine running Ubuntu 23.10 operating system, 4 GB of RAM, and installed with a 2.8 GHz i5-7600T Quad-Core CPU. The programming language deployed is Python and the cryptographic library used is PyCryto. Table 2 presents the durations it takes to carry out various cryptographic primitives in this environment.

In the process of mutually verifying all the communicating elements and setting up session key, the U_i carries out $3T_p + 6T_h + 2T_k$ while the GW_k executes $T_p + 8T_h$ computations. Regarding S_j, it executes $2T_p + 5T_h + 2T_k$ operations. Using the values in Table 2 above, Table 3 details the derivation of the computation complexities for the other peer schemes.

As evidenced in Fig. 5, the protocol in Ref. [20] exhibits the longest processing time of 37.7036 ms, owing to extensive exponential operations carried out in this scheme. This is followed by the protocols in Ref. [21,28] with 33.6990 ms and 25.1256 ms. These two schemes also execute computationally extensive fuzzy extractions and ECC point multiplications respectively. Next are the schemes in Ref. [22,35,44] with computation overheads of 6.3 ms, 1.2176 ms and 1.0658 ms in that order.

In contrast, our scheme takes only 0.9196 ms to execute mutual authentication and setup the session key. Therefore, it is the most efficient among its peers. This is due to the execution of mainly relatively efficient operations such as hashing functions.

5.2. Communication complexity

To derive the communication complexity of our scheme, consideration is given to the sizes of the messages exchanged while carrying out mutual validations and setting up session keys. When carrying out these procedures, messages $Am_1 = \{D_1, D_3, r_{u\text{-}1}, T_1\}$, $Am_2 = \{D_5, r_{g2}, T_2, r_{u\text{-}1}\}$, $Am_3 = \{E_2, r_{s\text{-}1}, T_3\}$, $Am_4 = \{E_4, r_{g2}, r_{s\text{-}1}, T_4\}$, $Am_5 = \{E_5\}$ and $Am_6 = \{F_2\}$ are exchanged among the U_i, GW_k and S_j. Here, $D_1 = E_{G_{pk}}(UID_i||r_{u\text{-}1}||SID_j)$, $D_3 = h(D_2||r_{u\text{-}1}||T_1||B_3)$, $D_5 = h(D_4||r_{g2}||T_2||C_5)$, $E_2 = h(E_1||r_{s\text{-}1}||T_3)$, $E_4 = h(E_3||r_{g2}||r_{s\text{-}1}||T_4)$, $E_5 = E_{a_p}(A_3\, r_{u-1} \oplus r_{s\text{-}1})$ and $F_2 = E_{K_{pu}}(B_4 \oplus K_{pu} \oplus a_p)$. Using the values in Ref. [56], the sizes of hashing, real identities, timestamp, exponential, random numbers, encrypted messages and passwords are 160 bits, 32 bits, 32 bits, 512 bits, 32 bits, 128 bits and 32 bits correspondingly. This means that As such, $Am_1 = \{128 + 160 + 32 + 32\} = 352$ bits; $Am_2 = \{160 + 32 + 32 + 32\} = 256$ bits;

Table 2
Cryptographic durations.

Operation	Time (ms)
Exponential operation, T_e	1.9258
Hashing, T_h	0.0008
Scalar multiplication, T_m	6.2752
Public key encryption/decryption, T_p	0.1502
Fuzzy extraction, T_{FE}	6.2752
Keyed hash, T_k	0.0008
PUF operation, T_{puf}	0.0097

Table 3
Computation costs.

Protocol	User	Gateway	Sensor	Total (ms)
Subramani et al., [20]	$6T_H + 2T_{FE}$ $+ 2T_{PUF}$	$5T_H +$ $2T_{FE}$	$6T_H +$ $2T_{FE} +$ $2T_{PUF}$	$17T_H + 6T_{FE} +$ $4T_{PUF} \approx 37.7036$
Yuanbing et al., [21]	$14T_H + 2T_m$	$11\ T_H$	$6T_H + 2T_m$	$31T_H + 4T_{PM} \approx$ 25.1256
Wu et al., [22]	$2T_p + 10T_h$	$5T_p +$ $6T_h$	$T_p + 4T_h$	$8T_p + 20T_h \approx$ 1.2176
Dodangeh & Jahangir, [28]	$3T_p + 9T_h$ $+ T_{FE} + 4T_e$	$6T_e + 2T_h$	$4T_e + 4T_h$	$3T_p + 15T_h + T_{FE}$ $+ 14T_e \approx 33.6990$
Srinivas et al., [35]	$3T_p + 8T_h$	$2T_p +$ $5T_h$	$2T_p + 5T_h$	$7T_p + 18T_h \approx$ 1.0658
Wazid et al., [44]	$14\ T_H + T_{FE}$	$9T_H$	$10\ T_H$	$33T_H + T_{FE} \approx$ 6.3000
Proposed	$3T_p + 6T_h$ $+ 2T_k$	$T_p + 8T_h$	$2T_p + 5T_h$ $+ 2T_k$	$6T_p + 19T_h + 4T_k$ ≈ 0.9196

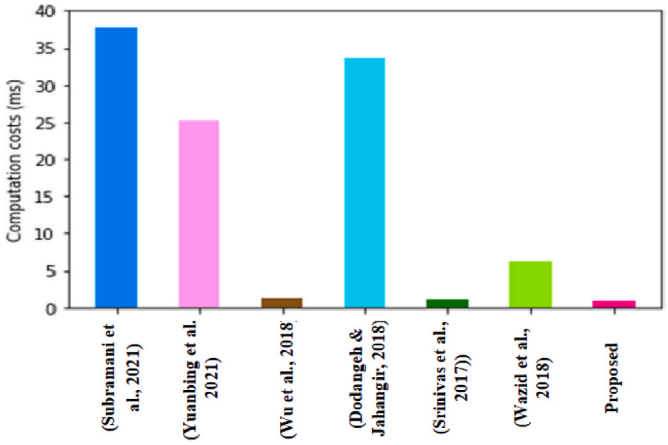

Fig. 5. Computation complexities.

$Am_3 = \{160 + 32 + 32\} = 224$ bits; $Am_4 = \{160 + 32 + 32 + 32\} = 256$ bits; $Am_5 = 128$ bits; and $Am_6 = 128$ bits. This means that the overall communication cost of our scheme is 1344 bits. The communication complexities of other related techniques are detailed in Table 4.

As demonstrated in Fig. 6, the scheme in Ref. [21] exhibits the highest communication complexity of 8192 bits. This is followed by the security approaches in Ref. [20,22,28,35,44] with communication complexities of 5311 bits, 2880 bits, 2816 bits, 2496 bits and 1696 bits respectively.

On the other hand, our scheme incurs the lowest communication cost of 1344 bits. Therefore, our protocol is the most bandwidth-friendly while the protocol in Ref. [21] is the most inefficient in terms of bandwidth usage.

5.3. Storage costs

To derive the storage complexity of our protocol, we deploy the size of the security tokens stored in the database of GW_k as well as memories

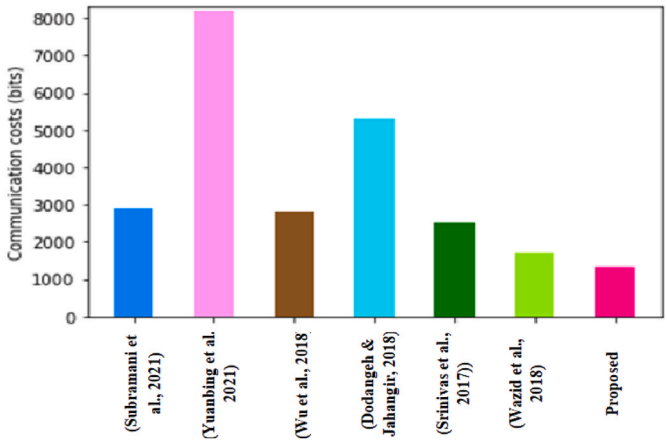

Fig. 6. Communication costs.

of S_j and SD_i. During the registration phase, the GW_k stores $\{A_1, B_3\}$ and $\{C_1, C_5\}$ in its database while SD_i stores $\{A_1, B_3, B_T\}$ in its memory. Similarly, the S_j stores $\{C_1, C_5\}$. Here, $A_1 = h\ (UID_i||PW_i||B_i||\varphi)$, $B_3 = h\ (B_2||A_3^*||\delta \oplus G_{pk} \oplus r_{g\text{-}1})$, $C_1 = h\ (B_4||B_5||(\Psi \oplus GID_k)$ and $C_5 = h\ (C_4||B_4||(\Psi \oplus G_{pk} \oplus GID_k))$. This means that the storage costs at the GW_k, S_j and SD_i are 640 bits, 352 bits and 320 bits respective. SAs such, the cumulative storage overhead of our scheme is 1312 bits. The storage requirements of other related approaches are detailed in Table 5.

Based on Fig. 7, the technique developed in Ref. [44] requires the largest storage space of 4008 bits. This is closely followed by the protocol in Ref. [35] with 1344 bits. On the other hand, the proposed protocol requires the third largest storage costs of 1312 bits. The schemes in Ref. [20–22,28] follow our scheme with storage overheads of 992 bits, 960 bits, 960 bits and 384 bits in that order.

It is evident that the protocol in Ref. [28] requires the least storage space. However, it cannot resist numerous attacks as shown in Table 7 below. On their part, the protocols in Ref. [20,21] cannot withstand threats such as impersonations and forgery. Concerning the scheme in Ref. [22], it fails to mitigate against attacks such as MitM, replays and KSSTI.

5.4. Energy consumption

To derive the energy requirement of our scheme, we deploy the energy model in Ref. [57] in which the transmission of one bit consumes 4.602 mJ (4.602×10^{-3} J) of energy. Therefore, the energy consumption of our protocol and other related protocols is obtained as:

$$Energy\ consumption = communication\ cost\ (in\ bits) \times 4.602 \times 10^{-3}\ J.$$

Using the above formula, Table 6 details the energy consumptions for other related protocols.

According to Fig. 8, the schemes in Ref. [20–22,28,35,44] require 24.441 J, 11.487 J, 12.959 J, 7.805 J, 13.254 J and 37.670 J in that order. Regarding our proposed scheme, it consumes only 6.185 J.

As such, the scheme in Ref. [21] is the most inefficient since it drains the battery power of WBAN devices. Conversely, our protocol is

Table 4
Communication costs.

Protocol	Total (bits)
Subramani et al., [20]	2880
Yuanbing et al., [21]	8192
Wu et al., [22]	2816
Dodangeh & Jahangir, [28]	5311
Srinivas et al., [35]	2496
Wazid et al., [44]	1696
Proposed	1344

Table 5
Storage costs.

Protocol	Total (bits)
Subramani et al., [20]	960
Yuanbing et al., [21]	960
Wu et al., [22]	992
Dodangeh & Jahangir, [28]	384
Srinivas et al., [35]	1344
Wazid et al., [44]	4008
Proposed	1312

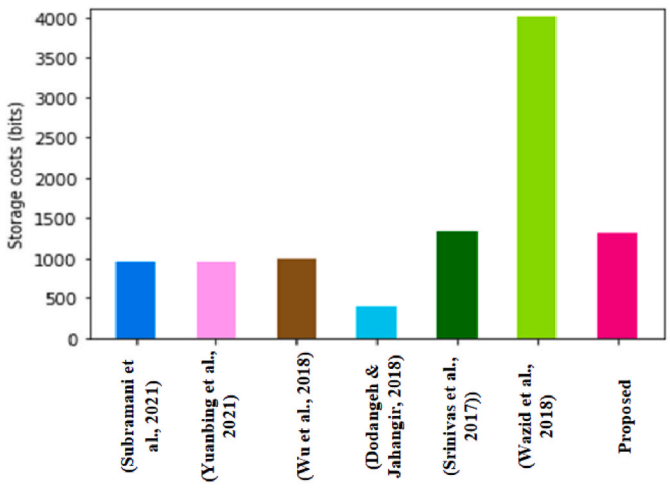

Fig. 7. Storage costs.

Table 6
Energy consumptions.

Scheme	Total (J)
Subramani et al., [20]	13.254
Yuanbing et al., [21]	37.670
Wu et al., [22]	12.959
Dodangeh & Jahangir, [28]	24.441
Srinivas et al., [35]	11.487
Wazid et al., [44]	7.805
Proposed	6.185

battery-friendly and hence is the most suitable for authenticating WBAN devices.

5.5. Supported security characteristics

The proposed protocol has been shown to offer numerous salient security features such as anonymity, mutual verification, key setup, untraceability, perfect key secrecy, and formal verification. Besides, it can withstand offline guessing, privileged insider, impersonation, forgery, stolen device, KSSTI, MitM and replays. Table 7 details the comparisons of our protocol against its peers in terms of the supported functionality.

Based on Table 7, the schemes in Ref. [20–22,28,35,44] and the proposed scheme support 8, 13, 10, 10, 7, 13 and 15 functionalities respectively. Therefore, the scheme in Ref. [22] is the most insecure and hence extremely vulnerable. Conversely, our scheme is the most secure and hence the best suited for deployment in insecure WBANs.

The comparative evaluations above have shown that the our scheme takes the shortest time to authenticate and setup the session keys. In addition, it has been shown to incur the minimum communication costs. Moreover, it consumes the least amount of energy. Although our scheme has relatively high storage costs, it supports the highest number of security functionalities, and hence is the most secure. This endears it as the best choice for deployed in resource limited WBAN environment.

6. Conclusion

IoT-based remote monitoring of patients has helped improve quality of healthcare and reductions in medical costs. By facilitating remote and instantaneous monitoring of patient vital physiological data, WBANs have enabled doctors to perform early detection of health problems and provision of well-timed intervention. Nevertheless, the exchange of these vital patient data over the public internet has been shown to expose it to several security threats. For example, attackers can intercept

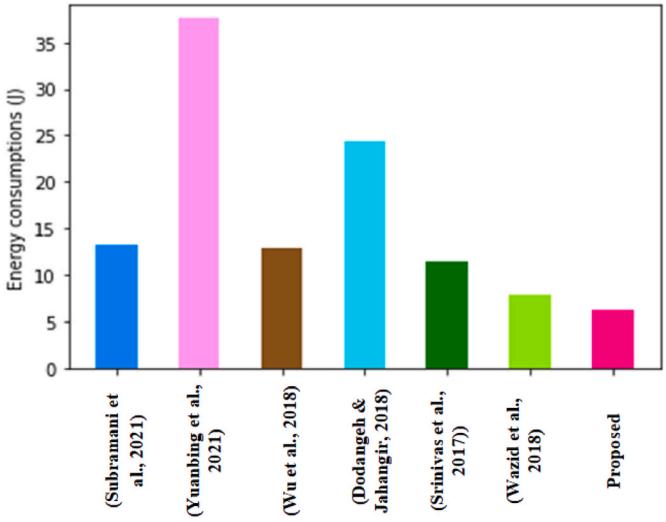

Fig. 8. Energy consumptions.

Table 7
Supported security features.

	Subramani et al., [20]	Wazid et al., [44]	Dodangeh & Jahangir, [28]	Srinivas et al., [35]	Wu et al., [22]	Yuanbing et al., [21]	Proposed
Security features							
F_1	✓	✓	✓	✓	✓	✓	✓
F_2	✓	✓	✓	✓	✓	✓	✓
F_3	✓	✓	×	✓	✓	✓	✓
F_4	✓	✓	×	×	×	✓	✓
F_5	✓	✓	✓	✓	×	✓	✓
F_6	×	✓	×	×	×	✓	✓
F_7	✓	✓	✓	✓	✓	✓	✓
Attacks resilience							
F_8	×	✓	✓	×	✓	✓	✓
F_9	×	✓	×	✓	✓	✓	✓
F_{10}	×	✓	✓	✓	✓	×	✓
F_{11}	×	×	✓	×	×	×	✓
F_{12}	✓	✓	✓	✓	✓	✓	✓
F_{13}	×	×	×	✓	×	✓	✓
F_{14}	×	✓	✓	×	×	✓	✓
F_{15}	✓	✓	✓	✓	×	✓	✓

√ Supported; × Not supported or not considered; F_1 - Mutual verification; F_2- Session key setup; F3– Anonymity; F_4 - Untraceability; F_5 - Forward key secrecy; F_6- Backward key secrecy; F_7- Formal verification; F_8 - Offline guessing; F_9- Privileged insider; F_{10}- Impersonation; F_{11}- Forgery; F_{12}- Stolen device; F_{13}- KSSTI; F_{14}- MitM; F_{15}- Replays.

and modify sensory data which can lead to misdiagnosis, wrong medications and hence endangering patient life. Although many security solutions have been developed over the recent past, they either fail to provide perfect security protection or they require large storage, computation, energy and bandwidth overheads. To address this issue, we have presented a verifiably secure and relatively efficient security protocol. It has been demonstrated to mitigate numerous security attacks such as forgery, stolen device, KSSTI, MitM and replays. To add to this, it requires the least energy, communication and computation resources. Future work will focuses on further reductions of the yielded storage complexities.

CRediT authorship contribution statement

Keyan Abdul-Aziz Mutlaq: Writing – original draft, Validation, Resources. **Mushtaq A. Hasson:** Investigation, Funding acquisition, Formal analysis. **Zaid Ameen Abduljabbar:** Supervision, Resources, Conceptualization. **Vincent Omollo Nyangaresi:** Validation, Methodology, Investigation. **Mustafa A. Al Sibahee:** Methodology, Formal analysis, Resources, Funding acquisition, Data curation. **Junchao Ma:** Supervision, Methodology, Data curation. **Samir M. Umran:** Funding acquisition, Formal analysis. **Ali Hasan Ali:** Methodology, Data curation. **Abdulla J.Y. Aldarwish:** Formal analysis, Data curation, Conceptualization. **Husam A. Neamah:** Formal analysis, Data curation, Conceptualization.

Funding

This work is supported by the Scientific Research Capacity Enhancement Program for Key Construction Disciplines in Guangdong Province under Grant 2024ZDJS063.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] Mohindru V, Vashishth S, Bathija D. Internet of things (IoT) for healthcare systems: a comprehensive survey. Recent Innovat Comput: Proceed ICRIC 2021 2022;1:213–29.
[2] Sharma A, Kumar R. A constrained framework for context-aware remote E-healthcare (CARE) services. Transact Emerg Telecommun Technol 2022;33(8):e3649.
[3] Comert C, Kulhandjian M, Gul OM, Touazi A, Ellement C, Kantarci B, D'Amours C. Analysis of augmentation methods for RF fingerprinting under impaired channels. In: Proceedings of the 2022 ACM workshop on wireless security and machine learning; 2022. p. 3–8.
[4] Singla R, Kaur N, Koundal D, Bharadwaj A. Challenges and developments in secure routing protocols for healthcare in WBAN: a comparative analysis. Wirel Pers Commun 2022:1–40.
[5] Ahad A, Ali Z, Mateen A, Tahir M, Hannan A, Garcia NM, Pires IM. A comprehensive review on 5G-based smart healthcare network security: taxonomy, issues, solutions and future research directions. Array 2023;18:100290.
[6] Mandal S. Provably secure certificateless protocol for wireless body area network. Wirel Netw 2023;29(3):1421–38.
[7] Zhang L, Zhu Y, Ren W, Zhang Y, Choo KKR. Privacy-preserving fast authentication and key agreement for e-health systems in iot, based on three-factor authentication. IEEE Transact Service Comput 2022;1(1).
[8] Arif MS, Mukheimer A, Asif D. Enhancing the early detection of chronic kidney disease: a robust machine learning model. Big Data Cognit Comput 2023;7(3):144.
[9] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJY. Elliptic curve cryptography-based scheme for secure signaling and data exchanges in precision agriculture. Sustainability 2023;15(13):10264.
[10] Chen C-M, Li Z, Chaudhry SA, Li L. Attacks and solutions for a two-factor authentication protocol for wireless body area networks. Secur Commun Network 2021;2021(1):3116593.
[11] Nagasundharamoorthi I, Venkatesan P, Velusamy P. Hash message authentication codes for securing data in wireless body area networks. Concurrency Comput Pract Ex 2024;36(5):e7934.
[12] Cornet B, Fang H, Ngo H, Boyer EW, Wang H. An overview of wireless body area networks for Mobile health applications. IEEE Network 2022;36(1):76–82.
[13] Ashraf Z, Mahmood Z, Iqbal M. Lightweight privacy-preserving remote user authentication and key agreement protocol for next-generation IoT-Based smart healthcare. Future Internet 2023;15(12):386.
[14] Peng K, Li M, Huang H, Wang C, Wan S, Choo K-KR. Security challenges and opportunities for smart contracts in internet of things: a survey. IEEE Internet Things J 2021;8(15):12004–20.
[15] Annane B, Alti A, Lakehal A. Blockchain based context-aware CP-ABE schema for internet of medical things security. Array 2022;14:100150.
[16] Hassan A, Omala AA, Ali M, Jin C, Li F. Identity-based user authenticated key agreement protocol for multi-server environment with anonymity. Mobile Network Appl 2019;24:890–902.
[17] Challa S, Wazid M, Das AK, Kumar N, Reddy AG, Yoon E-J, Yoo K-Y. Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access 2017;5:3028–43.
[18] Kumar P, Liyanage M. Efficient and anonymous mutual authentication protocol in multi-access edge computing (MEC) environments. IoT Secur: Advan Authenticat 2020:119–31.
[19] Jia X, He D, Li L, Choo K-KR. Signature-based three-factor authenticated key exchange for internet of things applications. Multimed Tool Appl 2018;77:18355–82.
[20] Subramani J, Maria A, Rajasekaran AS, Al-Turjman F. Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs. IEEE Trans Ind Inf 2021;18(5):3484–91.
[21] Yuanbing W, Wanrong L, Bin L. An improved authentication protocol for smart healthcare system using wireless medical sensor network. IEEE Access 2021;9:105101–17.
[22] Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Gener Comput Syst 2018;82:727–37.
[23] Saeed MES, Liu Q, Tian G, Gao B, Li F. HOOSC: heterogeneous online/offline signcryption for the internet of things. Wirel Netw 2018;24:3141–60.
[24] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic security ephemeral generation protocol for 5G enabled internet of things. In: International conference on internet of things as a service. Springer; 2021. p. 3–18.
[25] Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J Netw Comput Appl 2018;106:117–23.
[26] Prameela P. Enhanced certificateless security improved anonymous access control with obfuscated QualityAware confidential data discovery and dissemination protocol in WBAN. Int J Pure Appl Math 2018;118:2627–35.
[27] Tao H, Bhuiyan MZA, Abdalla AN, Hassan MM, Zain JM, Hayajneh T. Secured data collection with hardware-based ciphers for IoT-based healthcare. IEEE Internet Things J 2018;6(1):410–20.
[28] Dodangeh P, Jahangir AH. A biometric security scheme for wireless body area networks. J Inf Secur Appl 2018;41:62–74.
[29] Sharma G, Kalra S. A lightweight user authentication scheme for cloud-IoT based healthcare services. Iran J Sci Technol Transact Electr Eng 2019;43:619–36.
[30] Li X, Peng J, Kumari S, Wu F, Karuppiah M, Choo K-KR. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Comput Electr Eng 2017;61:238–49.
[31] Sowjanya K, Dasgupta M, Ray S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int J Inf Secur 2020;19(1):129–46.
[32] Ullah I, Alomari A, Ul Amin N, Khan MA, Khattak H. An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things. Electronics 2019;8(10):1171.
[33] Zhou L, Li X, Yeh K-H, Su C, Chiu W. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Gener Comput Syst 2019;91:244–51.
[34] Masud M, Gaba GS, Alqahtani S, Muhammad G, Gupta BB, Kumar P, Ghoneim A. A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care. IEEE Internet Things J 2020;8(21):15694–703.
[35] Srinivas J, Mishra D, Mukhopadhyay S. A mutual authentication framework for wireless medical sensor networks. J Med Syst 2017;41:1–19.
[36] Rehman ZU, Altaf S, Ahmad S, Huda S, Al-Shayea AM, Iqbal S. An efficient, hybrid authentication using ECG and lightweight cryptographic scheme for WBAN. IEEE Access 2021;9:133809–19.
[37] Azees M, Vijayakumar P, Karuppiah M, Nayyar A. An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks. Wirel Netw 2021;27(3):2119–30.
[38] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems. Appl Sci 2023;13(2):691.
[39] Wan T, Wang L, Liao W, Yue S. A lightweight continuous authentication scheme for medical wireless body area networks. Peer- -Peer Network Appl 2021;14(6):3473–87.
[40] Lara E, Aguilar L, Garcia JA. Lightweight authentication protocol using self-certified public keys for wireless body area networks in health-care applications. IEEE Access 2021;9:79196–213.

[41] Wazid M, Das AK, Shetty S, Jpc Rodrigues J, Park Y. LDAKM-EIoT: lightweight device authentication and key management mechanism for edge-based IoT deployment. Sensors 2019;19(24):5539.
[42] Masud M, Gaba GS, Choudhary K, Hossain MS, Alhamid MF, Muhammad G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet Things J 2021;9(4):2649–56.
[43] Chen C-M, Liu S, Chaudhry SA, Chen Y-C, Khan MA. A lightweight and robust user authentication protocol with user anonymity for IoT-based healthcare. Comput Model Eng Sci 2022.
[44] Wazid M, Das AK, Vasilakos AV. Authenticated key management protocol for cloud-assisted body area sensor networks. J Netw Comput Appl 2018;123:112–26.
[45] Soni M, Singh DK. LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network. Wirel Pers Commun 2022; 127(2):1067–84.
[46] Rana M, Shafiq A, Altaf I, Alazab M, Mahmood K, Chaudhry SA, Zikria Y Bin. A secure and lightweight authentication scheme for next generation IoT infrastructure. Comput Commun 2021;165:85–96.
[47] Liu S, Chen L, Wang H, Fu S, Shi L. O^3HSC: outsourced online/offline hybrid signcryption for wireless body area networks. IEEE Transact Network Serv Manag 2022;19(3):2421–33.
[48] Kumar M, Chand S. A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. IEEE Syst J 2020;15(2):2779–86.
[49] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJJ, Ma J, Qays Abduljaleel I, Aldarwish AJY. Session-dependent token-based payload enciphering scheme for integrity enhancements in wireless networks. J Sens Actuator Netw 2022;11(3):55.
[50] Rajaram S, Maitra T, Vollala S, Ramasubramanian N, Amin R. eUASBP: enhanced user authentication scheme based on bilinear pairing. J Ambient Intell Hum Comput 2020;11:2827–40.
[51] Son S, Park Y, Park Y. A secure, lightweight, and anonymous user authentication protocol for IoT environments. Sustainability 2021;13(16):9241.
[52] Li C, Xu C. Efficient anonymous authentication for wireless body area networks. IEEE Access 2022;10:80015–26.
[53] Kumar Chaudhary RR, Chatterjee K. A lightweight puf based multi-factor authentication technique for intelligent smart healthcare system. Peer- -Peer Network Appl 2023;16(4):1975–92.
[54] Hasan K, Chowdhury MJM, Biswas K, Ahmed K, Islam MS, Usman M. A blockchain-based secure data-sharing framework for software defined wireless body area networks. Comput Netw 2022;211:109004.
[55] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet Things 2023;24:100969.
[56] Cheng Q, Li Y, Shi W, Li X. A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network. Mobile Network Appl 2022;27(1):346–56.
[57] Das AK, Sutrala AK, Kumari S, Odelu V, Wazid M, Li X. An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks. Secur Commun Network 2016;9(13):2070–92.
[58] Al-Fayoumi M, Al-Haija QA. Capturing low-rate DDoS attack based on MQTT protocol in software Defined-IoT environment. Array 2023;19:100316.
[59] Ashraf Z, Sohail A, Yousaf M. Robust and lightweight symmetric key exchange algorithm for next-generation IoE. Internet Things 2023;22:100703.