Wireless Personal Communications
https://doi.org/10.1007/s11277-021-08565-2

LAKA: Lightweight Authentication and Key Agreement Protocol for Internet of Things Based Wireless Body Area Network

Mukesh Soni[1] · **Dileep Kumar Singh**[1]

Accepted: 4 May 2021

Abstract
The concept of wireless body area network (WBAN) is conquered the medical field while considering hospitals, patients, doctors to exchange crucial health data for efficient medical services. Health data includes personal medical information of patients, quality of life, reproductive outcomes, and behavioral information. While transferring health data for medical treatment/review, it is essential to provide proper security during device-to-device communication among WBAN players. Researchers have suggested different health data transmission mechanisms to achieve security, but these schemes are weak against various security attacks, such as modification, session key disclosure, impersonation, replay, man-in-the-middle, and stolen smart card, making crucial information in a susceptible situation specifically for patients. Further, they require high computational resources during WBAN communications. In this paper, we propose a secure and lightweight health authentication and key agreement protocol using low-cost operations. To confirm the robustness of the proposed mechanism, we do security analysis against various security attacks. Based on the computational analysis, the proposed protocol comparatively takes less execution cost, computation time, and power consumption. Moreover, LAKA requires around 57% less communication overhead and 15% less storage cost.

Keywords Attack · Health data · Key agreement · Lightweight · Security · WBAN

1 Introduction

Wireless Body Area Network (WBAN) is a distinctive type of sensor network to connect patients with the medical service providers to exchange critical health data remotely [1]. WBAN is a crucial wearable and implant network while sensing various vital data from different wireless sensors (deployed in/over body) for health diagnosis, monitoring, and

✉ Mukesh Soni
soni.mukesh15@gmail.com

Dileep Kumar Singh
dileep.singh@jlu.edu.in

[1] Jagran Lakecity University, Bhopal, India

Published online: 27 May 2021

controlling actuators. It has various benefits, such as location independent monitoring facility, no impact of patients' mobility, early disease detection and early prevention, patient assistance remotely, etc. Thus, it is very useful and effective for continuous monitoring, allowing correct diagnostics and real-time feedback to medical professionals [2].

WBAN is an application of Internet of Things (IoT) to improve the quality of the services for the patients [3]. In next few years, the market of IoT is expected to make over USD 19 trillion [4]. It is projected that by 2025, around 100 billion IoT devices will be practiced around the world, expecting its economic value more than USD 11000 Billion [5]. WBAN is one of the proficient wireless sensor technologies for health care, as it offers real-time data transmission for health care system users for crucial applications, such as remote health monitoring, sports, home/patient care, emergency response, and early intrusion detection [6–9]. However, the absence of a strong protection for data exchange in such a networking model creates an opportunity for malicious users to perform illegal activities on crucial medical data. Thus, it makes a huge lose of sensitive data and user privacy, impacting patients extensively. For example, a patient is suffering from a heart attack, and it is detected by a wearable device or wireless sensors (deployed over/in his/her body). Thus, user and data protection is required in a public network, allowing a doctor to start the immediate treatment [10, 11].

Figure 1 shows the data exchange system between patients and the medical server. Since data is sent over a public channel, an adversary can capture transferred messages to launch different malicious activities, such as modification of data, delay in data delivery, impersonation in information, and interruption in data exchange [12]. Any one of these problems can disrupt real-time data transmission in the medical field. Besides, it is also vital to satisfy user anonymity during the data communication phase to protect user privacy, as medical data is transferred from a patient to the medical server in a public network. Furthermore, wireless sensors are enabled with the fixed computing power to perform different operations for data exchanges and thus, it is necessary to design a low-cost protocol for WBAN [13]. Therefore, a secure and lightweight authentication mechanism is essential for data exchange while protecting from illegal activities in the WBAN system. There are various authentication methods based on different approaches (smart card, biometric, and text password, and combination of these approaches), but it is also required to assure that the authentication process should be executed quickly to transfer crucial medical data immediately [14].

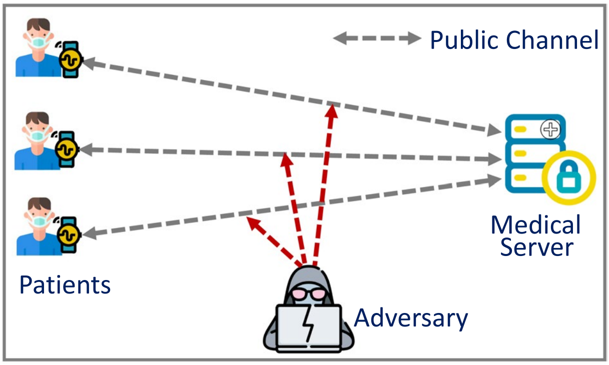

Fig. 1 A general overview of patient health data exchange system

Motivation Researchers suggested various authentication mechanisms to transfer crucial data between a patient and the medical server. However, the existing schemes are insecure to various security attacks, i.e., impersonation, modification, replay, smart card lost, and other relevant threats [15]. Moreover, it is required to save user variables in a Tamper Resistance Memory (TRM) to protect from an adversary, increasing the initial cost for its installation and protected storage memory cost. Furthermore, the existing authentication mechanisms for WBAN need high computational resources, as they are designed using high-cost cryptographic operations. Thus, it increases the transmission delay whenever data is transmitted between a patient and the server [2, 16]. Hence, it is essential to satisfy better security, performance, and privacy in the protocol design for WBAN.

Considering the above discussed challenges, we come up with a reliable authentication and key agreement protocol for WBAN to transfer critical data quickly between the server and a patient via a common channel. Our contributions are as follows.

- Propose an authentication and key agreement mechanism using low-cost functions (one-way hash, bit-wise XOR, and concatenation) for data exchanges in WBAN.
- Do security analysis to assure the robustness of the proposed scheme against vital security attacks, such as modification, impersonation, replay, stolen smart card, man-in-the-middle, plain-text, and session key disclosure.
- Do performance analysis of the proposed protocol to measure the execution cost, communication cost, power consumption, and storage cost. We compare performance results of the suggested mechanism with relevant schemes to understand its efficiency.

Paper Structure Section 2 presents a literature survey for related WBAN schemes. Section 3 gives an outline of the proposed scheme by describing the system model and threat model. In Sect. 4, we propose an authentication and key agreement protocol for WBAN. Section 5 discusses security analysis of the proposed protocol, and performance analysis is given in Sect. 6. We conclude this paper in Sect. 7.

2 Literature Survey

We discuss various strengths and drawbacks of the existing authentication schemes for WBAN.

In 2012, Zhang et al. [17] suggested an authentication scheme using electrocardiogram signals to reduce the computation and storage costs, but this protocol is weak against Sybil, sink, and wormhole attacks, as messages include vital information (helpful to an adversary to launch possible attacks). Liu et al. [18] came up with a certificate-less signature protocol using elliptic curve cryptography (ECC) and bi-linear pairing to protect against forgery attacks and offer user anonymity. However, the suggested approach in [18] is susceptible to an impersonation and insider attacks.

Das et al. [19] proposed a user authentication mechanism using user biometric identity to improve security in WBAN, and it also offers legitimate users to extract information from any cluster head. Further, the computation cost is reasonable due to the usage of symmetric key cryptography, and it resists to stolen verifier, smart card lost, replay, man-in-the-middle, and replay attacks, but it does not satisfy user anonymity. Jiang et al. [20] presented a bi-linear pairing based anonymous authentication protocol using public key cryptography for WBANs to overcome various relevant attacks. However, it is designed using high-cost operations (i.e., bi-linear paring and public key cryptography), leading to high computation resources requirements in WBAN. Thus, it is a challenging task to exchange vital information quickly through [20]. Wu et al. [21] suggested an anonymous two-factor authentication mechanism to improve security in medical application based user verification system. However, it is vulnerable to stolen smart card, impersonation, password guessing, and replay attacks. Further, it requires high computation and communication costs. Therefore, the protocol design in [21] is not adequate for data exchange in WBAN.

In 2017, Li et al. [22] proposed an anonymous authentication key agreement protocol for WBANs. Since this scheme is constructed using bi-linear paring, ECC, and symmetric key cryptography, it requires high communication and computation costs. Besides, it is insecure replay, impersonation, and modification attacks. Arya et al. [23] came up with an enhanced user authentication mechanism for WBAN to resist insider, plain-text, replay, stolen verifier, and fake sensor attacks. However, it is designed using asymmetric key cryptography, taking more computational resources and thereby, it is not appropriate for WBAN to rapidly transmit medical information. He et al. [24] came up with an anonymous authentication mechanism to deal with user anonymity and medical data protection issues in WBAN. It can withstand against replay, modification, impersonation, stolen verifier, and man-in-the-middle attacks. However, the communication overhead and computation cost are high in [24], as they have used multiple ECC operations in the computations and in messages during the authentication phase.

Koya and Deepthi [25] suggested a mutual authentication and key agreement approach for WBAN to resist impersonation and forgery attacks. Further, they claimed that their scheme is secure against impersonation and man-in-the-middle attacks, but it is insecure to sensor node capture and replay attacks. Kompara et al. [26] came up with a mutual authentication and key agreement mechanism to improve performance while providing untraceability in WBANs. They claimed that their approach can resist to impersonation, man-in-the-middle, replay, modification, and forward secrecy, but it is insecure to stolen smart card and replay attacks, and the communication cost is high in [26].

Recently, Xu et al. [27] designed an authentication and key agreement protocol to reduce the resource requirement, but it comparatively needs high communication cost. Furthermore, it is susceptible to impersonation and stolen smart attacks. Moreover, it does not satisfy user privacy. Fotouhi et al. [28] proposed an authentication mechanism for WBAN to minimize the requirement of computational resources and improve security while authenticating users. However, the scheme in [28] is vulnerable to impersonation, replay, and stolen smart card attacks. Besides, it requires very high execution cost and communication overhead. Kasyoka et al. [29] suggested a certificate-less access control mechanism to improve performance results in WBAN data exchange system. However, it cannot withstand an impersonation attack, leading to a crucial interpretation while exchanging health data. Furthermore, the computation time is more in [29] due to the usage of multiple number of ECC operations, and it also requires more power consumption. In 2021, Hussain et al. [30] proposed an authentication protocol using one-way hash function to enhance computational results, but the communication overhead requirement is very high because the scheme [30] needs to transfer multiple variables before establishing a connection. Moreover, it is vulernable to impersonation and replay attacks.

3 Preliminaries

This section gives a general overview of the system model and the threat model, making it easier to understand the proposed scheme's working.

3.1 System Model

We explain the system model for the proposed scheme in which three different players involved during data exchanges in WBAN. The description of each player is illustrated as follows, and different phases are displayed in Fig. 2 to understand registration, authentication and key agreement procedures of the proposed mechanism.

1. *The registration center authority (RCA)* It is the central trusted entity to register patient and deploy the medical server so that registered patients can avail relevant services from the medical server. The RCA saves details of registered patients in its secure database and regularly shares its database information with the deployed medical server through the secure infrastructure (i.e., the transport layer security (TLS) protocol) [28, 31].
2. *The medical server* It is an entity to provide medical services to legitimate patients by exchanging relevant information over a common channel, but the medical server firstly confirms the legality of patients and the received request by checking the patient credentials and time-stamp based on the obtained request. Besides, the medical server has access to the RCS database, which is also used during the authentication phase.
3. *Patient* This entity is an end-user in the system, who has a smart wearable device to collect real-time health information from a patient body, and this information is sent to the medical server to understand the health status of a patient. However, it is not adequate to simply send this sensitive information via a common channel. Thus, on behalf of a patient, a smart wearable device performs different cryptographic operations for mutual authentication between a patient and the medical server before exchanging messages.

3.2 Threat Model

We consider different relevant assumptions for data exchange mechanisms [12, 32], and they are as follows.

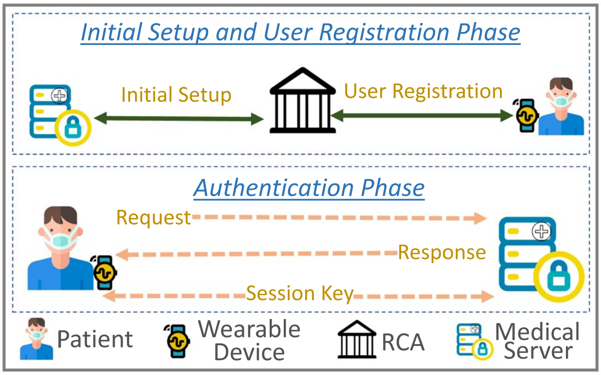

Fig. 2 A system model for the proposed mechanism

1. The patient registration phase is executed over a secure channel (i.e, TLS protocol), whereas the authentication and key agreement phase is performed via a public channel. Thus, an attacker can capture public channel messages, but not secure channel messages [28, 31].
2. An attacker ($\boldsymbol{A}$) has knowledge of the authentication and key agreement mechanism design.
3. One-way function is an irreversible operation, and thus, it is not possible to extract any information from the hash computed parameter.
4. If $\boldsymbol{A}$ has gets a smart wearable device of any legitimate patient, then s/he can extract saved parameters in a smart card of a smart wearable device.
5. If a registered patient (say P_i) can compute all necessary parameters on behalf of another legal user (say P_j) to satisfy mutual authentication in the system, then s/he is an attacker for P_j, playing two roles (legal user and attacker) in the system.
6. It is feasible to guess only one unknown parameter as a guessable credential in the computation to know the correctness of a guessed variable. However, it is not feasible consider two or more variables as guessable parameters to know the exactness of them in polynomial time.
7. We assume one equation as $\mathcal{P} = \mathcal{Q} \oplus \mathcal{R}$ in which $\boldsymbol{A}$ can get $\mathcal{P}$ if s/he has both values ($\mathcal{Q}$ and $\mathcal{R}$). However, it is not feasible to know $\mathcal{P}$ while having only one known value ($\mathcal{Q}$ or $\mathcal{R}$).

4 The Proposed Scheme

We propose an authentication and key agreement protocol (named LAKA) for WBAN based health care system to transfer crucial information over a common communication channel between a patient and the medical server. The proposed protocol is designed using a one-way hash function (i.e. SHA-256), and its security is well established by National Institute of Standards and Technology (NIST), which is secure against the polynomial time algorithm [33]. LAKA mainly includes four phases as (i) initial setup (ii) patient registration (iii) authentication and key agreement (iv) patient password change. We have used different notations in the proposed mechanism, and they are explained in Table 1.

4.1 Initial Setup Phase

The registration center authority (RCA) generates a unique hospital identity (ID_H) of 128 bits to compute a private key for the medical server (SER) as $K_{SER} = h(RN_{SER}||IT_{SER}||ID_H)$, where IT_{SER} = the initial time-stamp SER, RN_{SER} = random nonce, and . RCA keeps K_{SER} in its database and in the SER's database securely. To have the updated database of newly registered patients, SER regularly connects with RCA over a secure channel [28, 31].

4.2 Patient Registration Phase

A patient (P_i) enrolls with RCA to get services in the future from SER legitimately. Thus, P_i executes the following steps over a secure channel (i.e., TLS protocol) [28, 31]. It is also displayed in Fig. 3.

Table 1 Notations used in the schemes

Notation	Explanation
PU_i	A patient
ID_{P_i}	Identity of P_i
$UNID_{P_i}$	Unidentified identity of P_i
PW_{P_i}	Password of P_i
SC_i	Smart card of P_i
SWD_i	Smart wearable device of P_i
$x_i/y_i/b_i/c_i$	Generated random nonce
a_i	A large prime number
RCA	The registration center authority
DB_{RCA}	The secure database of RCA
SER	The server
K_{SER}	The privet key for SER
$\boldsymbol{A}$	An attacker
T_1/T_3	Current time-stamp at P_i end
T_2	Current time-stamp at SER side
ΔT	Threshold time period
$\|\|$	Concatenation operation
$\oplus$	Bit-wise XOR operation
$h(\cdot)$	One-way hash function

1. P_i chooses ID_{P_i}, PW_{P_i}, x_i, and y_i to compute $Z_i = h((x_i \oplus y_i)||ID_i)$, $A_i = h(ID_{P_i} \oplus Z_i \oplus PW_{P_i})$, and $Q_i = h(ID_{P_i} \oplus Z_i \oplus A_i)$. After that, P_i transfers $\{ID_{P_i}, A_i, Q_i, Z_i\}$ to RCA.
2. RCA confirms availability of ID_{P_i} and computes $Q'_i = h(ID_{P_i} \oplus Z_i \oplus A_i)$ to check $Q'_i \overset{?}{=} Q_i$. If it is valid, then RCA generates a large prime number a_i to calculate $R_i = h(ID_{P_i}||A_i||Z_i)$, $S_i = h(K_{SER} \oplus h(a_i) \oplus R_i)$, $W_i = A_i \oplus h(a_i) \oplus R_i$, and $UNID_{P_i} = h(ID_{P_i}||R_i||S_i)$. After that, RCA stores $UNID_{P_i}$, R_i, W_i, and A_i in its secure database. Further, RCA saves R_i, S_i, W_i, Z_i in SC_i and installs it in a smart portable device (SWD_i).

4.3 Authentication and Key Agreement Phase

When a patient (P_i) wants to exchange health data or require medical services from the medical server (SER), s/he should firstly prove his/her legality based on own credentials (PW_{P_i} and ID_{P_i}). Further, a smart wearable device (SWD_i) computes a message request to send it to SER for user authentication. If the received request is valid, then SER also sends a computes response message to P_i t confirm the legitimacy of SER at P_i end, providing mutual authentication in the proposed scheme. If it holds, then P_i and SER calculates a temporary session key to exchange crucial health data over a common channel. The detailed steps are as follows, and it is also shown in Fig. 4.

1. P_i inserts ID_{P_i} and PW_{P_i} into SWD_i to compute $A_i = h(ID_{P_i} \oplus PW_{P_i} \oplus Z_i)$, $R'_i = h(ID_{P_i}||A_i||Z_i)$ and verifies $R'_i \overset{?}{=} R_i$. If both are equal, SWD_i takes a ran-

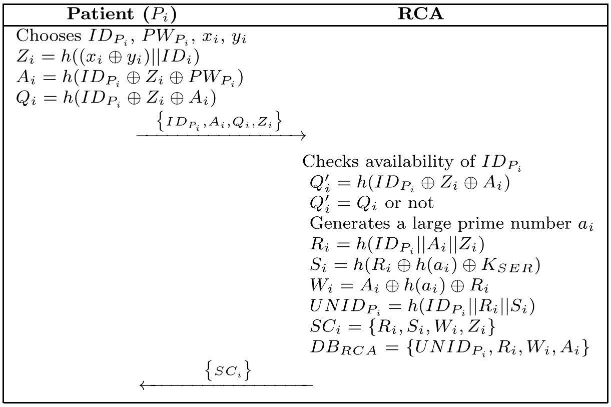

Fig. 3 The proposed user registration phase

Patient (P_i) | **RCA**

Chooses ID_{P_i}, PW_{P_i}, x_i, y_i
$Z_i = h((x_i \oplus y_i)||ID_i)$
$A_i = h(ID_{P_i} \oplus Z_i \oplus PW_{P_i})$
$Q_i = h(ID_{P_i} \oplus Z_i \oplus A_i)$

$\xrightarrow{\{ID_{P_i}, A_i, Q_i, Z_i\}}$

Checks availability of ID_{P_i}
$Q_i' = h(ID_{P_i} \oplus Z_i \oplus A_i)$
$Q_i' = Q_i$ or not
Generates a large prime number a_i
$R_i = h(ID_{P_i}||A_i||Z_i)$
$S_i = h(R_i \oplus h(a_i) \oplus K_{SER})$
$W_i = A_i \oplus h(a_i) \oplus R_i$
$UNID_{P_i} = h(ID_{P_i}||R_i||S_i)$
$SC_i = \{R_i, S_i, W_i, Z_i\}$
$DB_{RCA} = \{UNID_{P_i}, R_i, W_i, A_i\}$

$\xleftarrow{\{SC_i\}}$

dom nonce (b_i) to enumerate $h(a_i) = W_i \oplus A_i \oplus R_i'$, $UNID_{P_i} = h(ID_{P_i}||R_i'||S_i)$, $M_i = h(a_i) \oplus T_1 \oplus h(A_i||UNID_{P_i}) \oplus b_i$, and $N_i = h(UNID_{P_i}||b_i||T_1||A_i)$. SWD_i sends $\{UNID_{P_i}, M_i, N_i, T_1\}$ to SER to prove the legality of P_i.

2. SER does $\Delta T \leq T_2 - T_1$ to check the validity of $\{UNID_{P_i}, M_i, N_i, T_1\}$. If valid, then SER calculates $h(a_i) = W_i \oplus R_i \oplus A_i$, $b_i = h(A_i||UNID_{P_i}) \oplus h(a_i) \oplus M_i \oplus T_1$, $N_i' = h(UNID_{P_i}||b_i||T_1||A_i)$ to confirm $N_i' \overset{?}{=} N_i$. If both are equal, then SER enumerates $O_i = h(c_i||T_2) \oplus h(N_i'||h(a_i)||b_i)$, $X_i = h(b_i||h(c_i||T_2)||h(a_i)||T_1)$ and transfers $\{O_i, X_i, T_2\}$ to SWD_i for mutual verification.
3. SWD_i verifies the validity of $\{O_i, X_i, T_2\}$ through $\Delta T \leq T_3 - T_2$. If it is within ΔT, then SWD_i computes $h(c_i||T_2) = h(N_i||h(a_i)||b_i) \oplus O_i$, $X_i = h(b_i||h(c_i||T_2)||h(a_i)||T_1)$ for $X_i' \overset{?}{=} X_i$. If equal, then both (SWD_i and SER) calculates the session key, $SK_{P_i} = h(UNID_{P_i} \oplus h(a_i) \oplus h(c_i||T_2) \oplus b_i)$. SK_{P_i} is used to exchange sensitive information between SWD_i and SER, and it is valid for a temporary period. If SK_{P_i} is expired, then both should perform the authentication phase again.

4.4 Patient Password Change Phase

If P_i is interested to update his/her password (PW_{P_i}) due to some reasons (e.g., improve password robustness), then s/he should perform the following steps to confirm his/her legality to proceed to the password change procedure. After that, RCA allows P_i to change PW_{P_i}. Accordingly, RCA also updates its database. This procedure is shown in Fig. 5.

1. P_i inserts ID_{P_i} and PW_{P_i} into SWD_i to calculate $A_i = h(ID_{P_i} \oplus PW_{P_i} \oplus Z_i)$, $R_i' = h(ID_{P_i}||A_i||Z_i)$. If $R_i' = R_i$, then only SWD_i enumerates $h(a_i) = W_i \oplus A_i \oplus R_i'$, $Y_i = h(A_i||R_i'||h(a_i)||T_1)$, $UNID_{P_i} = h(ID_{P_i}||R_i'||S_i)$ to send $\{UNID_{P_i}, Y_i, T_1\}$ to RCA.
2. RCA confirms the validity of a received request. If valid, RCA computes $h(a_i) = W_i \oplus R_i \oplus A_i$, $Y_i' = h(A_i||R_i||h(a_i)||T_1)$ and checks $Y_i' \overset{?}{=} Y_i$. If equal, then RCA asks P_i for a new password ($PW_{P_i}^N$).
3. P_i computes $A_i^N = h(ID_{P_i} \oplus Z_i \oplus PW_{P_i}^N)$, $R_i^N = h(ID_{P_i}||A_i^N||Z_i)$, $\alpha_i = h(T_1||T_3||h(a_i)||R_i') \oplus A_i^N$, $\beta_i = (R_i^N||||ID_{P_i}) \oplus h(T_1||A_i||h(a_i)||A_i^N)$, and $\gamma_i = h(A_i^N||R_i^N||h(a_i)||T_1||T_3)$. Moreover, P_i sends $\{\alpha_i, \beta_i, T_3\}$ to RCA.
4. Next, RCA calculates $A_i^N = \alpha_i \oplus h(T_1||T_3||h(a_i)||R_i')$, $(R_i^N||ID_{P_i}) = \beta_i \oplus h(T_1||A_i||h(a_i)||A_i^N)$, and $\gamma_i' = h(A_i^N||R_i^N||h(a_i)||T_1||T_3)$ to con-

User (U_{P_i})		Server (SER)
Inserts ID_{P_i} & PW_{P_i} $A_i = h(ID_{P_i} \oplus PW_{P_i} \oplus Z_i)$ $R'_i = h(ID_{P_i} \| A_i \| Z_i)$ $R'_i \overset{?}{=} R_i$ Generates a random nonce b_i $h(a_i) = W_i \oplus A_i \oplus R'_i$ $UNID_{P_i} = h(ID_{P_i} \| R'_i \| S_i)$ $M_i = h(a_i) \oplus T_1 \oplus h(A_i \| UNID_{P_i}) \oplus b_i$ $N_i = h(UNID_{P_i} \| b_i \| T_1 \| A_i)$		
	$\xrightarrow{\{UNID_{P_i}, M_i, N_i, T_1\}}$	
		$\Delta T \leq T_2 - T_1$ $h(a_i) = W_i \oplus R_i \oplus A_i$ $b_i = h(A_i \| UNID_{P_i}) \oplus h(a_i) \oplus M_i \oplus T_1$ $N'_i = h(UNID_{P_i} \| b_i \| T_1 \| A_i)$ $N'_i \overset{?}{=} N_i$ Generates a random nonce c_i $O_i = h(c_i \| T_2) \oplus h(N'_i \| h(a_i) \| b_i)$ $X_i = h(b_i \| h(c_i \| T_2) \| h(a_i) \| T_1)$
	$\xleftarrow{\{O_i, X_i, T_2\}}$	
$\Delta T \leq T_3 - T_2$ $h(c_i \| T_2) = h(N_i \| h(a_i) \| b_i) \oplus O_i$ $X_i = h(b_i \| h(c_i \| T_2) \| h(a_i) \| T_1)$ $X'_i \overset{?}{=} X_i$		
$SK_{P_i} = h(UNID_{P_i} \oplus h(a_i) \oplus h(c_i \| T_2) \oplus b_i)$		

Fig. 4 The proposed authentication phase

firm $\gamma'_i \overset{?}{=} \gamma_i$. If they are equal, then RCA calculates $S_i^N = h(R_i^N \oplus h(a_i) \oplus K_{SER})$, $W_i^N = A_i^N \oplus R_i^N \oplus h(a_i)$, and $UNID_{P_i} = h(ID_{P_i} || R_i^N || S_i^N)$. Finally, RCA updates SC_i and its secure database with newly computed relevant parameters.

5 Security Analysis

We evaluate the security robustness of the proposed mechanism against vital security attacks. The proposed protocol is designed using a one-way hash function (i.e. SHA-256), and its security is well established by National Institute of Standards and Technology (NIST), which is secure against the polynomial time algorithm [33]. We analyze security strengths of the proposed system based on the adversary model (as discussed in Sect. 3.2).

Proposition 1 *The proposed scheme, LAKA is robust against an impersonation attack.*

Proof If an attacker ($\boldsymbol{A}$) can compute login parameters (M_i, $UNID_{P_i}$, and N_i) on behalf of a legitimate patient (P_i) and s/he receives (O_i, X_i, T_2) from SER to establish a connection for health data exchange, then an impersonation attack is possible in the proposed scheme. However, $\boldsymbol{A}$ cannot execute this attack due to unavailability of essential values, explained as follows.

If $\boldsymbol{A}$ only changes time-stamp and sends $\{UNID_{U_i}, M_i, N_i, T'_1\}$ to SER, then s/he can clear ΔT test. However, $\boldsymbol{A}$ fails in $N'_i \overset{?}{=} N_i$ verification at SER side, as T_1 is used N_i, whereas T'_1 is considered for N'_i computation (based on the received values from $\boldsymbol{A}$). In another case,

Fig. 5 The proposed patient password change phase

Patient (P_i)	**RCA**
Inserts ID_{P_i} and PW_{P_i} $A_i = h(ID_{P_i} \oplus PW_{P_i} \oplus Z_i)$ $R'_i = h(ID_{P_i}\|\|A_i\|\|Z_i)$ $R_i = R_i$ or not $h(a_i) = W_i \oplus A_i \oplus R'_i$ $Y_i = h(A_i\|\|R'_i\|\|h(a_i)\|\|T_1)$ $UNID_{P_i} = h(ID_{P_i}\|\|R'_i\|\|S_i)$	
$\xrightarrow{\{UNID_{P_i}, Y_i, T_1\}}$	
	$\Delta T \leq T_2 - T_1$ $h(a_i) = W_i \oplus R_i \oplus A_i$ $Y'_i = h(A_i\|\|R_i\|\|h(a_i)\|\|T_1)$ $Y'_i \overset{?}{=} Y_i \Rightarrow$ Ask for $PW^N_{P_i}$
$A^N_i = h(ID_{P_i} \oplus Z_i \oplus PW^N_{P_i})$ $R^N_i = h(ID_{P_i}\|\|A^N_i\|\|Z_i)$ $\alpha_i = h(T_1\|\|T_3\|\|h(a_i)\|\|R'_i) \oplus A^N_i$ $\beta_i = (R^N_i\|\|\|\|ID_{P_i}) \oplus$ $h(T_1\|\|A_i\|\|h(a_i)\|\|A^N_i)$ $\gamma_i = h(A^N_i\|\|R^N_i\|\|h(a_i)\|\|T_1\|\|T_3)$	
$\xrightarrow{\{\alpha_i, \beta_i, T_2\}}$	
	$A^N_i = \alpha_i \oplus h(T_1\|\|T_3\|\|h(a_i)\|\|R'_i)$ $(R^N_i\|\|ID_{P_i}) = \beta_i \oplus$ $h(T_1\|\|A_i\|\|h(a_i)\|\|A^N_i)$ $\gamma'_i = h(A^N_i\|\|R^N_i\|\|h(a_i)\|\|T_1\|\|T_3)$ $\gamma'_i \overset{?}{=} \gamma_i$ $S^N_i = h(R^N_i \oplus h(a_i) \oplus K_{SER})$ $W^N_i = A^N_i \oplus R^N_i \oplus h(a_i)$ $UNID_{P_i} = h(ID_{P_i}\|\|R^N_i\|\|S^N_i)$ Updates SC_i and its secure database
$\xleftarrow{\{SC_i\}}$	

A needs $UNID_{P_i}$, M_i, and N_i to generate a new login request with the fresh time-stamp. *A* can use $UNID_{P_i}$, but s/he does not have $h(a_i)$ and A_i, restricting to send a forged request. Hence, *A* cannot perform an impersonation attack in the suggested mechanism. □

Proposition 2 *LAKA can withstand a session key disclosure attack.*

Proof This attack is executed to apply malicious activities (i.e., change in information, bogus message, and erroneous data) in the system. The proposed protocol is designed based on the key agreement concept between a patient and the medical server and thus, *A* should know/calculate the session key (SK_{P_i}), which is computed as $h(UNID_{P_i} \oplus h(a_i) \oplus h(c_i||T_2) \oplus b_i)$ in the proposed system. We consider that *A* takes $UNID_{P_i}$ from a public channel, but s/he cannot get/compute $h(c_i||T_2)$, $h(a_i)$, and b_i Besides, the session key is valid for a temporary period. Thus, both should again calculate the session key to exchange health data if it is expired. Since *A* does not have all required credentials to compute SK_{P_i} anyhow, s/he cannot launch a session key disclosure attack in the proposed scheme. □

Proposition 3 *The suggested mechanism is secure against a modification attack.*

Proof If *A* can do any changes in messages, and the receiver believes on the modified messages, then s/he succeeds to apply a modification attack. In the proposed scheme, both (P_i and *SER*) exchange messages by using the computed session key mutually. Therefore, *A* requires the session key parameters ($UNID_{P_i}$, $h(a_i)$, $h(c_i||T_2)$, and b_i). Since $\boldsymbol{A}$ is not able to calculate the session key in the proposed scheme (discussed in Section 5.2), it is not feasible for an adversary to modify health data in the suggested mechanism while transferring messages. □

Proposition 4 *The proposed protocol can withstand a replay attack.*

Proof An adversary performs a replay attack to delay or stop messages so a patient cannot connect with the medical server or an adversary can re-transmit messages again to illegal activities. In the suggested protocol, we have used time-stamp concept to verify the freshness of obtained messages at the receiver end based on ΔT. If any received message is beyond ΔT, then the receiver discards it immediately. Further, different parameters are computed using time-stamp during its computation, not allowing an adversary to perform malicious activities by using a fresh time-stamp. Therefore, a replay is not applicable in the proposed mechanism. □

Proposition 5 *LAKA is secure against a smart card lost attack.*

Proof If $\boldsymbol{A}$ gets or steals smart card (SC_i) of P_i, and s/he can establish a connection with the medical server by using saved parameters in SC_i on behalf of P_i to transmit bogus/erroneous health data illegally, then a smart card lost attack is possible in the system. SC_i includes R_i, S_i, W_i, and Z_i. In the authentication and key agreement phase, P_i and SER transfers $UNID_{P_i}$, M_i, N_i, O_i, and X_i. Thus, we assume that $\boldsymbol{A}$ have all the mentioned parameters. In LAKA, $\boldsymbol{A}$ should recompute $M_i(= b_i \oplus h(A_i||UNID_{P_i}) \oplus h(a_i) \oplus T_1)$ and $N_i(= h(UNID_{P_i}||b_i||T_1||A_i))$ so that SER accepts his/her request and sends $\left\{O_i, X_i, T_2\right\}$. To compute M_i and N_i, $\boldsymbol{A}$ should know A_i and $h(a_i)$, as s/he manages $UNID_{P_i}$, b_i, and T_1. However, it is not feasible for an attacker to know/get A_i and $h(a_i)$ due to unavailability of essential parameters. Therefore, $\boldsymbol{A}$ cannot calculate M_i and N_i to perform forgery in the system. Hence, the proposed scheme resists to a smart card lost attack. □

Proposition 6 *The proposed mechanism can withstand a plain-text attack.*

Proof If messages are exchanged without applying any cryptographic operations, then an adversary an opportunity to apply this attack to understand transferred information because s/he can capture transmitted messages from a public channel. The proposed scheme is designed using a one-way hash function, and both (patient and the medical server) should initially generate a mutual session key to exchange vital data in the proposed mechanism. Since the session key is computed freshly for each session, and it is computed based on common agreed parameters for a temporary period. Thus, an adversary does not have required parameters to compute a session key, as discussed in Section 5.2. Therefore, an adversary is not able to learn information from the transferred messages. □

Proposition 7 *The suggested scheme is secure against a man-in-the-middle attack.*

Proof If $\boldsymbol{A}$ can understand transferred information in a public channel, then this attack is performed in the system. However, the proposed protocol is constructed to transfer message using the mutual session key. Thus, $\boldsymbol{A}$ needs this session key to understand transferred health data, but s/he cannot compute the session key as discussed in Section 5.2. Therefore, it is not feasible for an adversary to perform a man-in-the-middle attack in the proposed scheme. □

Proposition 8 *User privacy is satisfied in the proposed protocol.*

Proof If an adversary or a registered patient cannot derive the identity or other information of another patient from a common channel communication, then the system satisfies user privacy. In the suggested scheme, P_i sends $\left\{UNID_{P_i}, M_i, N_i, T_1\right\}$ to SER over a public channel, whereas SER sends $\left\{O_i, X_i, T_2\right\}$ to P_i via an insecure channel. Here, T_1 and T_2 are timestamps. Since $UNID_{P_i}$, M_i, N_i, O_i, and X_i calculated using one-way hash function, it is not feasible to retrieve any value from these hash computed variables. Hence, $\boldsymbol{A}$ does not find any information or identity of a patient, which loses user privacy. Therefore, the proposed scheme achieves user privacy in the system. □

Table 2 shows the comparison for different security attacks and user privacy. We have compared the proposed scheme with to understand security effectively among recent relevant mechanisms. We have used different notations in Table 2, which are as follows. $\boldsymbol{P_1}$: User privacy; $\boldsymbol{P_2}$: Impersonation; $\boldsymbol{P_3}$: Modification; $\boldsymbol{P_4}$: Man-in-the-middle; $\boldsymbol{P_5}$: Smart card lost; $\boldsymbol{P_6}$: Replay; $\boldsymbol{P_7}$: Session key disclosure; $\boldsymbol{P_8}$: Plain-text; ✓: Resists; N: Insecure;

6 Performance Analysis

We present various performance results in this section to understand the implementation efficiency of the proposed scheme. WBAN devices (i.e., medical server and smart wearable device) are different in the system configuration, such as storage, communication, and processing power. Furthermore, wearable devices connect with the medical server to transmit crucial health data. Hence, it is required to consider execution cost, power consumption, storage cost, computation time, and communication overhead for rapid data exchanges in WBAN [34, 35, 22]. We discuss on each measure as follows.

Table 2 Security Comparison for Relevant Authentication and Key Agreement Schemes

Scheme	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
[25]	✓	✓	✓	✓	×	×	✓	✓
[26]	✓	✓	✓	✓	×	×	✓	✓
[27]	×	×	✓	✓	×	✓	✓	✓
[28]	✓	×	✓	✓	×	×	✓	✓
[29]	✓	×	✓	✓	NA	×	NA	✓
[30]	✓	×	✓	✓	✓	×	✓	✓
Proposed	✓	✓	✓	✓	✓	✓	✓	✓

6.1 Execution Cost

When a patient wants to connect with the medical server to transfer health data over a common channel. Thus, both (patient and medical server) should perform different operations, and it is called as the execution cost. We count the required number of one-way hash ($T_{h(\cdot)}$) and Elliptic curve cryptography (T_{EC}) operations in the registration phase as well as for the authentication and key agreement phase. If this number is high in the scheme, then it requires more time in the implementation. The registration phase is executed once, whereas the authentication and key agreement phase is performed every time. Thus, it is more important to have less execution cost during the authentication and key agreement phase. The execution time for one $T_{h(\cdot)}$ and T_{EC} is 0.0529 milliseconds (*ms*) and 3.0179 *ms* respectively on Raspberry Pi 3B, which has the system configuration as Boardcom BCM2837 64bit Quad Core 1.2 GHz processor, 2.5 A power supply, 1 GB RAM, and 5 V input. We count the computation time for [25–30], and the proposed scheme. To do a comparison, the execution cost and computation time are described in Table 3 for [25–30], and the proposed mechanism. From Table 3, we notice that the proposed scheme needs less execution cost compared to [25, 28, 29], and [30].

6.2 Storage and Communication Costs

When a patient is registered with the *RCA*, some parameters are saved in SC_i. The cost of these saved values is called as the storage cost. During the authentication and key agreement phase, a patient and the medical server exchange different parameters to establish a connection to transfer health data, and it is called as the communication cost. The storage cost is one-time cost in the registration phase, and the communication cost is required in the authentication and key agreement phase. Thus, it is essential to have less communication cost in the scheme. Both costs (storage and communication) are measured in bytes. One-way hash ($h(\cdot)$), time-stamp (T), ECC (EC), and identity (ID) takes 32 bytes (as SHA-256), 8 bytes, 64 bytes, and 12 bytes respectively [36]. We count the storage and communication costs for [25–30], and the proposed protocol, discussed in Table 4. It is also displayed in Fig. 6 for better understanding the efficiency of each protocol. The communication cost requirement of the proposed scheme is reduced at least 57 % than [25–29], and [30]. The storage cost requirement is maximally increased 15 % than [27] and [28], but it is less in the proposed scheme compared to [25, 26, 29], and [30]. Since the storage cost is a one-time cost, it is less important than the communication overhead. In [29], the

Table 3 Execution cost and computation time comparison for relevant authentication and key agreement schemes

Scheme	Registration	Authentication and Key Agreement
Koya et al. [25]	$2T_{h(\cdot)} \approx 0.1058\ ms$	$15T_{h(\cdot)} \approx 0.7935\ ms$
Kompara et al. [26]	$1h(\cdot) \approx 0.0529\ ms$	$8h(\cdot) \approx 0.4232\ ms$
Xu et al. [27]	$2h(\cdot) \approx 0.1058\ ms$	$13h(\cdot) \approx 0.6877\ ms$
Fotouhi et al. [28]	$4h(\cdot) \approx 0.2116\ ms$	$30h(\cdot) \approx 1.5870\ ms$
Kasyoka et al. [29]	$4T_{h(\cdot)} + 4T_{EC} \approx 12.2832\ ms$	$4T_{h(\cdot)} + 5T_{EC} \approx 15.3011\ ms$
Hussain et al. [30]	$20T_{h(\cdot)} \approx 1.0580\ ms$	$18T_{h(\cdot)} \approx 0.9522\ ms$
Proposed	$8T_{h(\cdot)} \approx 0.4232\ ms$	$13T_{h(\cdot)} \approx 0.6877\ ms$

Table 4 Communication and storage cost comparison for relevant protocols

Scheme	Communication	Storage
Koya et al. [25]	$14h(\cdot)+2T$	$4h(\cdot)+2ID$
Kompara et al. [26]	$12h(\cdot)+1T+2ID$	$4h(\cdot)+3ID$
Xu et al. [27]	$14h(\cdot)+4T+2ID$	$3h(\cdot)+1ID$
Fotouhi et al. [28]	$16h(\cdot)+3ID$	$3h(\cdot)+2ID$
Kasyoka et al. [29]	$2h(\cdot)+1EC$	$2EC+1ID$
Hussain et al. [30]	$17h(\cdot)+4ID+8T$	$4h(\cdot)+4ID$
Proposed	$5h(\cdot)+2T$	$4h(\cdot)$

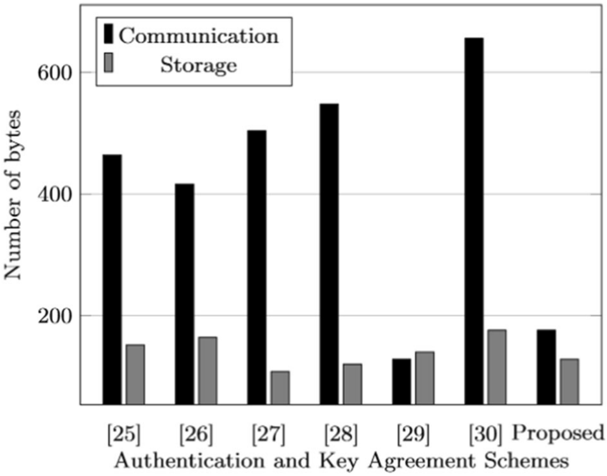

Fig. 6 Communication and storage cost comparison for authentication schemes

communication cost is 128 bytes. However, the communication cost is more in [25–28], and [30] than the proposed mechanism.

6.3 Power Consumption

When a patient and the medical server performs different operations to establish a connection, they require some amount of power during the computation, and it is called the power consumption. It is calculated as $P_C = P_M * T_{Exe}$, where P_C = power consumption, P_M = CPU maximum power (which is 12.5 V for Raspberry Pi 3B), and T_{Exe} = computation time. The power consumption is measured in millijoule (mJ), and it is dependent on the computation time [36]. We calculate the power consumption for [25–30], and proposed protocol. The power consumption comparison is shown in Fig. 7, where the power consumption in [29] is very high comparatively because the computation time is high than other relevant schemes.

When we consider security, privacy, and computational resources together, the proposed scheme is resistant to impersonation, modification, session key disclosure, replay, man-in-the-middle, and smart card lost attacks, and it also satisfies user privacy. Further, the proposed protocol collectively requires less computational resources for the execution cost,

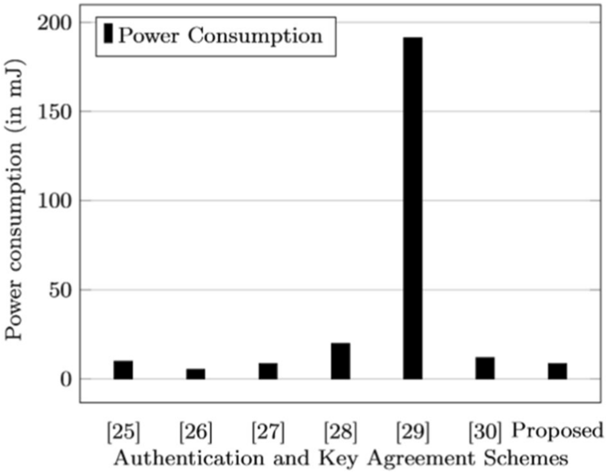

Fig. 7 Power consumption for related WBAN authentication mechanisms

storage cost, power consumption, and communication cost compared to recent relevant schemes.

7 Conclusion

We have proposed an efficient authentication and key agreement scheme (named LAKA) for WBAN to achieve different security and privacy requirements. The suggested scheme is resistant to various attacks, such as impersonation, plain-text, modification, smart card lost, replay, man-in-the-middle, and session key disclosure. Furthermore, it achieves user privacy while sending crucial information over a common channel. The proposed protocol is constructed using a low-cost function (i.e., SHA-256), and thus, it comparatively requires less execution cost, computation time, and power consumption. The performance results show that the suggested mechanism needs around 57% less communication overhead and 15% less storage cost. Therefore, the proposed system is effective in different performance measures and also achieves important security and privacy requirements for WBAN.

The proposed scheme is designed for WBAN, and thus, it is required to protect the data exchange system against future security attacks to preserve patient's health data from unauthorized access. In the future, we shall come up with a new parsing algorithm for categorizing the information, communication mechanism to resist future cyberattacks and improve performance results.

Author Contributions Mukesh Soni (Manuscript writing; Protocol design; Introduction; Literature Survey; Security analysis; Performance analysis;), Dileep Kumar Singh (Security analysis; Performance analysis; Manuscript proof-reading;)

Declarations

Conflict of interest I declare that I do not have any type of conflicts of interes

Code Availability We have used Python language to find the execution time of one-way hash operation

References

1. Seyedi, M., Kibret, B., Lai, D. T., & Faulkner, M. (2013). A survey on intrabody communications for body area network applications. *IEEE Transactions on Biomedical Engineering, 60*(8), 2067–2079.
2. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications Surveys & Tutorials, 16*(3), 1658–1686.
3. Sobin, C. C. (2020). A survey on architecture, protocols and challenges in IoT. *Wireless Personal Communications, 112,* 1383–1429.
4. Jindal, F., Jamar, R., & Churi, P. (2018). Future and challenges of internet of things. *International Journal of Computer Science Information Technology, 10*(2), 13–25.
5. Limbasiya, T., & Karati, A. (2018). Cryptanalysis and improvement of a mutual user authentication scheme for the Internet of Things. In: *2018 International Conference on Information Networking (ICOIN)*, (pp. 168-173). https://doi.org/10.1109/ICOIN.2018.8343105.
6. Chakraborty, C., Gupta, B., & Ghosh, S. K. (2013). A review on telemedicine-based WBAN framework for patient monitoring. *Telemedicine and e-Health, 19*(8), 619–626.
7. Arif, A., Zubair, M., Ali, M., Khan, M. U., & Mehmood, M. Q. (2019). A compact, low-profile fractal antenna for wearable on-body WBAN applications. *IEEE Antennas and Wireless Propagation Letters, 18*(5), 981–985.
8. Sharma, A., & Kumar, R. (2019). A constrained framework for context–aware remote E–healthcare (CARE) services. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.3649.
9. Kadhim, K. T., Alsahlany, A. M., Wadi, S. M., & Kadhum, H. T. (2020). An overview of patient's health status monitoring system based on Internet of Things (IoT). *Wireless Personal Communications, 114,* 2235–2262.
10. He, D., Ye, R., Chan, S., Guizani, M., & Xu, Y. (2018). Privacy in the Internet of Things for smart healthcare. *IEEE Communications Magazine, 56*(4), 38–44.
11. Shingala, M., Patel, C., & Doshi, N. (2018). An improve three factor remote user authentication scheme using smart card. *Wireless Personal Communications, 99*(1), 227–251.
12. Limbasiya, T., & Doshi, N. (2017). An analytical study of biometric based remote user authentication schemes using smart cards. *Computers & Electrical Engineering, 59,* 305–321.
13. Cavallari, R., Martelli, F., Rosini, R., Buratti, C., & Verdone, R. (2014). A survey on wireless body area networks: Technologies and design challenges. *IEEE Communications Surveys & Tutorials, 16*(3), 1635–1657.
14. Hussain, M., Mehmood, A., Khan, S., Khan, M. A., & Iqbal, Z. (2019). Authentication techniques and methodologies used in wireless body area networks. *Journal of Systems Architecture, 101,* 101655.
15. Sharma, A., Tomar, R., Chilamkurti, N., & Kim, B. G. (2020). Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics, 9*(10), 1609.
16. Narwal, B., & Mohapatra, A. K. (2021). A survey on security and authentication in wireless body area networks. *Journal of Systems Architecture*, *113*, 101883. https://doi.org/10.1016/j.sysarc.2020.101883.
17. Zhang, Z., Wang, H., Vasilakos, A. V., & Fang, H. (2012). ECG-cryptography and authentication in body area networks. *IEEE Transactions on Information Technology in Biomedicine, 16*(6), 1070–1078.
18. Liu, J., Zhang, Z., Chen, X., & Kwak, K. S. (2013). Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Transactions on parallel and distributed systems, 25*(2), 332–342.
19. Das, A. K., Chatterjee, S., & Sing, J. K. (2015). A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks. *Ad-hoc & Sensor Wireless Networks, 28*(3/4), 221–256.
20. Jiang, Q., Lian, X., Yang, C., Ma, J., Tian, Y., & Yang, Y. (2016). A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth. *Journal of medical systems, 40*(11), 231.
21. Wu, F., Xu, L., Kumari, S., & Li, X. (2017). An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. *Multimedia Systems, 23*(2), 195–205.
22. Li, T., Zheng, Y., & Zhou, T. (2017). Efficient anonymous authenticated key agreement scheme for wireless body area networks. *Security and Communication Networks, 2017,* 1–8.
23. Arya, A., Reddy, C., & Limbasiya, T. (2017). An improved remote user verification scheme in wireless body area networks. *Procedia Computer Science, 113,* 113–120.
24. He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2016). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal, 11*(4), 2590–2601.

25. Koya, A. M., & Deepthi, P. P. (2018). Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. *Computer Networks, 140,* 138–151.
26. Kompara, M., Islam, S. H., & Holbl, M. (2019). A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. *Computer Networks, 148,* 196–213.
27. Xu, Z., Xu, C., Liang, W., Xu, J., & Chen, H. (2019). A lightweight mutual authentication and key agreement scheme for medical Internet of Things. *IEEE Access, 7,* 53922–53931.
28. Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks, 177*(107333), 1–16.
29. Kasyoka, P., Kimwele, M., & Angolo, S. M. (2020). Towards an efficient certificateless access control scheme for wireless body area networks. *Wireless Personal Communications, 115*(2), 1257–1275.
30. Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2021). Performance enhancement in wireless body area networks with secure communication. *Wireless Personal Communications, 116*(1), 1–22.
31. Limbasiya, T., Soni, M., & Mishra, S. K. (2018). Advanced formal authentication protocol using smart cards for network applicants. *Computers & Electrical Engineering, 66,* 50–63.
32. Madhusudhan, R., & Mittal, R. C. (2012). Dynamic ID-based remote user password authentication schemes using smart cards: A review. *Journal of Network and Computer Applications, 35*(4), 1235–1248.
33. Dang, Q. (2015). Secure Hash Standard, Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD [online]. https://doi.org/10.6028/NIST.FIPS.180-4.
34. Li, F., Han, Y., & Jin, C. (2016). Cost-effective and anonymous access control for wireless body area networks. *IEEE Systems Journal, 12*(1), 747–758.
35. Ibrahim, M. H., Kumari, S., Das, A. K., Wazid, M., & Odelu, V. (2016). Secure anonymous mutual authentication for star two-tier wireless body area networks. *Computer Methods and Programs in Biomedicine, 135,* 37–50.
36. Limbasiya, T., & Das, D. (2019). Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication. *IEEE Systems Journal, 14*(1), 520–529.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Mukesh Soni is a Ph.d. Research Scholar in the Department of Computer Science and Engineering at Jagran lakecity University, Bhopal, India . He Has completed his Bachelor's in Information Technology from Gyan Ganga Institute of Technology & Management, Bhopal, India in 2011, and a Masters in Computer Science & Engineering from MANIT, Bhopal, India in 2015. He is associated with NPTEL (IIT Project) as a Quality Control Person since 2019. He is also a SPOC(Single point of contact) coordinator with the NPTEL learning project since 2019. He has Qualified GATE examination in the year of 2012,2013,2014,2015,2018, and 2020 and received India Book of

Record for this in 2020, also qualified UGC NET examination in 2014. His research interests include Applied Cryptography, Information Security, and Network Security. He has published a total of 13 research papers in IEEE/Springer Conferences, Scopus/SCIE Journals, and 16 papers in National and International Journals . He has published 9 Indian Patents and 9 International Patents. He has received a total of 9 Awards like the Young Scientist awards, Young faculty award, Best faculty award, International Goal Achiever Award, NPTEL start awards, NPTEL believer award, Award Appreciation for Excellent performance in the field of Computer Science & Engineering, Award for Contribution to Student Development by different organizations. He is associated as a member reviewer in different peer-reviewed journals like Advances in Science, Technology and Engineering Systems Journal, International Journal of Advanced Study and Research Work, Journal of Emerging Technologies and Innovative Research, International Journal of Creative Research Thoughts, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, International Research Journal on Advanced Science Hub. He is also a member of many International and National professional bodies like IEEE, Asia Society of Researcher, Scientific and Technical Research Association (STRA), "International Association of Engineers Institute for Engineering Research and Publication, Scholars Academic & Scientific Society.

Dileep Kumar Singh is associated with Jagran Lakecity University Bhopal, from August2014 and currently working as Head, JLU School of Engineering & Technology, JagranLakecity University Bhopal, M.P., India. He is an ICarnegie certified trainer for theSoftwareDevelopment Program of Carnegie Mellon University, USA. He is leading the ICTgroup of Jagran Lakecity University for the Tuning India Project of European Union. He ishaving around 16 years of vast experience in academics, research and administrations atreputed colleges and university of India. Prior to Jagran Lakecity University Bhopal, he hasserved as a Head of Department for 5 years in one of the reputed Engineering College inBhopal. He has obtained his B Tech degree in CSE from Government Engineering CollegeBilaspur in 2004 and after qualifying GATE exam, completed his M Tech with specialization inInformation Security from NIT Bhopal (MANIT). He has obtained his Ph. D. in CSE from NITBhopal. His fields of interests are information security, machine learning, data structure, weband mobile applications development. He has presented and published over 15 researchpapers in the reputed journals which include Scopus/SCIE journals and various national andinternational conferences include IEEE conferences and also has published 3 Patents andorganized National and International level Conferences. He is a member of ISCA (IndianScience Congress Association).He has received various awards including the CII(Confederation of Indian Industry) SIS "TECH GURU" Award-2017, from Honorable minister,technical education and the ambassador of Colombia, "Pratibhavan Chhatra" award byBhartiya Redcross Society, "Active participation in Research work", awarded and Certificationof appreciation continuously for 6 times and also the "most interesting faculty" award underthe "Prerak Award" based on students voting.