An Efficient Authentication Protocol for Robust Security in Wireless Body Area Networks

Joshua Auko
Department of Computer science & software engineering
Jaramogi Oginga Odinga University of Science & Technology
Bondo, Kenya
jauko2015@gmail.com

Vincent Omollo Nyangaresi
Department of Computer science & software engineering
Jaramogi Oginga Odinga University of Science & Technology
Bondo, Kenya
vnyangaresi@jooust.ac.ke

Zaid Ameen Abduljabbar
Department of Computer Science
College of Education for Pure Sciences
University of Basrah
Basrah, Iraq
zaid.ameen@uobasrah.edu.iq

Zaid Alaa Hussien
Department of Management Information Systems
College of Administration and Economics
Southern Technical University
Basrah, Iraq
zaid.alaa@stu.edu.iq

Ali Hasan Ali
Department of Mathematics
College of Education for Pure Sciences
University of Basrah
Basrah, Iraq
Technical Engineering College
Al-Ayen University, Thi-Qar, Iraq
ali.hasan@uobasrah.edu.iq

Hamid Ali Abed AL-Asadi
Department of Computer Science
College of Education for Pure Sciences
University of Basrah
Basrah, Iraq
hamid.abed @uobasrah.edu.iq

2026 18th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) | 979-8-3315-5818-5/26/$31.00 ©2026 IEEE | DOI: 10.1109/ECAI69016.2026.11613774

***Abstract*— The ever increasing number of aging populace together with high number of chronic diseases has led to wide adoption of medical Internet of Things (IoT), such as Wireless Body Area Networks (WBANs). Through these networks, physiological data such as blood glucose, body temperature, blood pressure, and heart rate are collected and transmitted to remote medical professionals for analysis, diagnosis and treatment. However, the deployed open wireless channels and IEEE 802.15.6 standardized protocol have vulnerabilities that can easily compromise the patient data. Although many security solutions have been presented based on techniques such as certificates and bilinear-pairings, these algorithms have either high overheads or still have numerous security gaps. In this paper, a lightweight encryption protocol is presented. It is shown to incur the least computation costs and average communication overheads. In addition, it offers anonymity, untraceability, authentication, session key agreement, perfect key secrecy, revocability and conditional privacy. Moreover, it protects against node capture, session hijacking, denial of sleep, denial of service, key compromise, side-channeling, impersonation, eavesdropping, session key disclosure, privileged insider, tracking, offline guessing, forgery and non-repudiation.**

***Keywords*— BSU, WBAN, attacks, threat, algorithms, encryption.**

I. INTRODUCTION

A wireless body area network comprises of sensors and actuators which gather patient health information and transmit it to remote medical servers. A typical WBAN environment consists of the sensor nodes, medical professional and gateways. The gateway acts as a relay between the medical professionals and the sensors attached to the patient or elderly body [1]. These sensors are either implanted in the body, placed on the patient's body or in the vicinity of the patient. As explained in [2], the growing number of aging populace coupled with high number of chronic diseases has led to wide adoption of medical internet of things. Through the deployment of smart gadgets, WBANs and server-based platforms, patient data can be collected and transmitted in real-time to the cloud servers as well as medical experts. This physiological data may include blood glucose, body temperature, Electrocardiogram (ECG), blood pressure, heart rate and Electroencephalogram (EEG). The received data is then analyzed to facilitate diagnosis and treatment at any time and place [3]. Therefore, WBANs offers a cost-effective, efficient and reliable healthcare. In addition, WBANs enable medical experts to conveniently treat or attend to many patients. Apart from real-time patient monitoring, WBANs offer diagnostic support, medical administration and patient tracking [4-8]. In addition, the medical experts can offer targeted medical services in accordance with the received data [9]. Through the minimization of physical contacts between the patients and the medical staff, WBANs can prevent the spread of infectious diseases especially during pandemics.

However, numerous issues are yet to be solved in the WBAN environment to unleash its full potential. For instance, insecure communication channels used during data exchange exposes the data to numerous threats such as unauthorized access and user privacy leaks [9-10]. On the other hand, mobility and openness pose serious challenges to patient privacy due to possible adversarial intrusions and attacks. For instance, attacker may try to interrupt the communication process, modify or drop the transmitted messages [11]. In addition, adversaries can eavesdrop, intercept and tamper with transmitted data, or extract some sensitive patient information [12-14]. When patient data is corrupted, wrong diagnosis can be made and hence endangering patient life [15-16]. It is also possible to use the stolen patient information from the public channels to launch attacks such as impersonation, replay and Man-in-the-Middle (MitM) attacks [17]. Moreover, the mobile devices used by the medical experts or the sensors nodes may be stolen or lost and attackers can deploy power analysis techniques to extract the stored secrets. Afterwards, impersonations of these medical professionals or sensors can be attempted, which can lead to serious consequences [18]. As explained in [19], WBAN communications deploy the IEEE 802.15.6 standardized protocol which lacks forward secrecy and is vulnerable to impersonation attacks. The authors in [20] and [21] point out WBANs generate massive and real-time sensitive data which presents some challenges in its effective and timely management. Particularly, there is high energy consumption which results in inefficiencies [22]. Therefore, the usage of traditional cryptographic techniques will introduce further inefficiencies in an environment

979-8-3315-5818-5/26/$31.00 ©2026 IEEE

characterized by resource-limited sensor devices. There is therefore need for lightweight and privacy-preserving techniques to address these challenges. Although many lightweight schemes have been presented in literature, most of them are susceptible to attacks such as replay, modification, MitM and server spoofing [11].

There is therefore need for a robust and yet efficient authentication scheme for WBANs. It must preserve integrity, authenticity and confidentiality of information. This requires that security and privacy be upheld during processing and transmission over insecure channels [23-26]. In addition, authors in [27] identify data usability, mutual authentication, data integrity, attacks resilience, key agreement, backward and forward secrecy as being important considerations. The security of the WBANs authentication schemes directly affects patients' well-being [28-34]. As such, the proposed algorithm makes the following contributions:

- We develop an efficient encryption algorithm that leverages on only lightweight cryptographic primitives to protect data exchanges in wireless body area networks.
- Random numbers are incorporated in the derivation of security ephemerals so as to preserve untraceability.
- Network identities communicate using their pseudo-identities instead of their real identities so as to uphold anonymity of the communication process.
- We carry out comparative performance evaluation to show that our algorithm incurs the lowest computations overheads and moderate communication overheads..

II. Realted Works

Many schemes have been developed over the recent past in an effort to solve security issues in WBANs. For instance, a security scheme is presented in [35] to offer anonymity and protection against intermediate node impersonation attacks. However, it is still susceptible to intermediate node capture and hub node impersonation attacks [36]. To solve these challenges, Elliptic Curve Cryptography (ECC) based security solutions are presented in [37-43]. However, most of these schemes have numerous security issues. For instance, the protocol in [41] is defenseless against replay attacks [11]. In addition, ECC operations such as scalar multiplications are computationally intensive for WBAN sensors [44-46]. As such, some lightweight authentication schemes have been presented in [47-52]. Unfortunately, these schemes still have a number of shortcomings that hinder their deployment. For example, the protocol in [47] is vulnerable to sensor node capture and impersonation attacks [36] while the scheme in [48] cannot offer forward confidentiality [11]. On the other hand, the technique in [50] is vulnerable to Denial of Service (DoS), cannot offer perfect forward secrecy and session key agreement [53]. Similarly, the scheme in [2] is defenseless against key compromise, replay and impersonation attacks [54]. It also has anonymity and privacy concerns.

To address these issues, three-factor authentication protocols are introduced in [55] and [56]. However, the approach in [55] is susceptible to offline password guessing and ephemeral secret leakage attacks [56]. Similarly, the scheme in [56] cannot resist offline dictionary devaluation and privileged insider attacks [57]. To offer identity authentication, bilinear pairing-based security methods have been developed in [58] and [59]. However, the technique in [58] cannot offer mutual authentication and is vulnerable to client forgery attacks [60].

Similarly, the protocol in [59] fails to protect against client forgery attacks and can lead to de-synchronization of system logs [61]. Owing to the bilinear pairing operations, these schemes incur heavy computation overheads [62]. On its part, the scheme in [63] has clock de-synchronization, high control power and perfect forward secrecy challenges [64], while the protocol in [65] cannot protect against sensor impersonation attacks [66].

To preserve anonymity, authentication techniques are developed in [2] and [67]. However, the method in [2] is susceptible to offline identity guessing, replay and key compromise attacks [54], while the scheme in [67] is susceptible to brute-force guessing attacks [68]. In addition, it lacks perfect session key secrecy. On the other hand, the two-factor authentication protocol in [69] is vulnerable to session key disclosure, physical cloning, verification table leakage, privileged insiders and impersonation attacks [3]. To solve these issues, a Physical Unclonable Function (PUF)-based scheme is developed in [3]. However, PUF – based protocols have stability challenges [70]. Similarly, other PUF-based techniques are presented in [71-73]. Although PUF protects against physical cloning and tampering attacks they are still vulnerable to other attacks. To protect against sensor node capture attacks, a two-factor authentication scheme is presented in [74]. However, it is still vulnerable to other sensor node attacks [69].

III. Proposed Algorithm

This section presents the network model as well as the various phases of the proposed algorithm. The specific details are discussed in the following sub-sections.

A. Network Model

The major communicating entities in the proposed algorithm include the Gateway Node (*GWN*), Hospital Medical Server (*HMS*) and the Body Sensor Unit (*BSU*) as shown in Fig.1. Whereas the *BSU* collects the patient physiological data, the *GWN* acts as a relay between the BSU and the *HMS*.

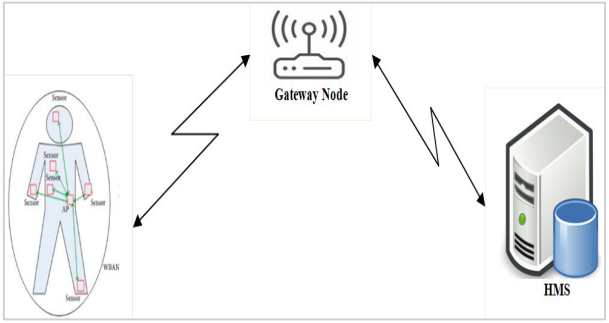

Fig. 1. Network model

Some of the collected data include *EEG*, blood glucose, body temperature, *ECG*, blood pressure and heart rate. Table I presents the symbols used throughout this paper. The major phases that are executed in the proposed algorithm include the system setup, registration, mutual authentication, session key agreement and finally the parameter update. The sub-sections below describe these phases in greater details.

B. System Setup Phase

This phase is executed by the *GWN* which receives and forwards messages from the *BSU* and *HMS*. Therefore, the *GWN* is believed to be sufficiently protected and hence is a trusted entity.

TABLE I. NOTATIONS

Symbol	Description
ID_{GWN}	Unique identity for the gateway node
SK_G	GWN secret key
ID_{HMS}	Unique identity for the HMS
ID_{NET}	Network identifier
HG_K	Common key shared between HMS & GWN
R_i	Random number *i*
PID_{HMS}	Pseudo-identity for the HMS
ID_{BSU}	Unique identity for the BSU
$Sess_H$	Session key derived at the HMS
$Sess_G$	Session key derived at the GWN
$Sess_B$	Session key derived at the BSU
PID_{BSU}	Pseudo-identity for the BSU
PW_i	Patient password for patient *i*
$\|\|$	Concatenation operation
$\oplus$	XOR operation
$h(.)$	Collision-resistant one way-way hashing function
$\tilde{A}$	Attacker

In this phase, the *GWN* generates its unique identity ID_{GWN} and secret key SK_G. This is followed by the selection of collision-resistant one way-way hashing function h (.) and derivation of network identity ID_{NET}.

C. Registration Phase

In this phase, all the body sensor units and hospital medical servers are registered at the *GWN*. To accomplish this, secure channels are deployed so that the exchanged parameters are protected from adversarial capture. The following 5 steps are required to register the *HMS* to the GWN.

Step 1: Each hospital medical server chooses its unique identity ID_{HMS}. Here, servers within the same network are identified with the network identity ID_{NET}.

Step 2: Each *HMS* derives common private key $HG_K = h(ID_{HMS}||SK_G||ID_{NET})$ which it shares with its corresponding *GWN*. It then composes registration message $Reg_1 = \{ID_{HMS}, HG_K\}$ that is sent over to the *GWN* through private channels.

Step 3: Upon getting registration message Reg_1 from the *HMS*, the *GWN* chooses some random nonces R_1 and R_2. Next, it generates pseudo-identity PID_{HMS} for each *HMS*.

Step 4: The *GWN* constructs registration response message $Reg_2 = \{ID_{GWN}, R_1, R_2, PID_{HMS}\}$ that is forwarded to the *HMS* over secured channels. Finally, the *GWN* stores parameter set $\{ID_{HMS}, PID_{HMS}, ID_{NET}, R_1, h(R_2)\}$ in its repository.

Step 5: After receiving message registration response message Reg_2, the *HMS* stores parameter set $\{ID_{GWN}, R_1, R_2, PID_{HMS}\}$ in its database.

To register the *BSU* to the *GWN*, we execute the following 5 steps.

Step 1: The *BSU* selects its unique identity ID_{BSU} and password PW_i. Next, it generates random nonce R_3.

Step 2: The *BSU* derives parameter $A_1 = h(PW_i||R_3)$ before composing registration message $Reg_3 = \{ID_{BSU}, A_1\}$. Finally, it forwards message Reg_3 to the *GWN* over protected communication channels.

Step 3: On receiving registration message Reg_3, the *GWN* checks its repository to determine whether identity ID_{BSU} has been used before. If this check turns positive, the *BSU* is prompted to generate a different identity. Otherwise, the *GWN* generates pseudo-identity PID_{BSU} for this particular *BSU*.

Step 4: The *GWN* generates random nonce R_4 for this particular *BSU*. It then stores value set $\{R_4, ID_{BSU}, A_1\}$ in its repository. Next, it derives security parameters $A_2 = h(PID_{BSU}||R_4||ID_{GWN}||SK_G||) \oplus A_1$ and $A_3 = h(ID_{BSU}||SK_G) \oplus h(ID_{BSU}||A_1)$. Finally, it constructs registration message $Reg_4 = \{PID_{BSU}, ID_{HMS}, ID_{GWN}, A_2, A_3\}$ that is transmitted over to the *BSU* over secured channels.

Step 5: After getting registration message Reg_4 from the *GWN*, the *BSU* computes values $A_4 = h(ID_{BSU}||PW_i) \oplus R_3$. It then stores parameter set $\{A_2, A_3, A_4, PID_{BSU}, ID_{GWN}\}$ in its memory. Algorithm 1 below summarizes the system setup and registration phases.

Algorithm 1: System setup and registration

Begin:
******System setup*******
1) Generate ID_{GWN} & SK_G
2) Choose h (.) & ID_{NET}
******** HMS registration *******
3) Select ID_{HMS}
4) Calculate HG_K
5) Create Reg_1
6) *HMS*→ *GWN*: { Reg_1}
7) Select R_1 & R_2
8) Derive PID_{HMS}
9) Compose Reg_2
10) *GWN* → *HMS*: { Reg_2}
11) Store $\{ID_{HMS}, PID_{HMS}, ID_{NET}, R_1, h(R_2)\}$ at *GWN*
12) Store $\{ID_{GWN}, R_1, R_2, PID_{HMS}\}$ at *HMS*
******** BSU registration *******
13) Choose ID_{BSU} & PW_i
14) Generate R_3
15) Calculate A_1
16) Construct Reg_3
17) *BSU*→ *GWN*: { Reg_3}
18) **If** ID_{BSU} is invalid **then:**
19) Halt registration
20) **Else:**
21) Generate PID_{BSU} & R_4
22) Store $\{R_4, ID_{BSU}, A_1\}$ in *GWN*
23) Compute A_2 & A_3
24) Compose Reg_4
25) *GWN* → *BSU*: { Reg_4}
26) Derive A_4
27) Store $\{A_2, A_3, A_4, PID_{BSU}, ID_{GWN}\}$ in *BSU*
28) **End if**
End

D. Mutual Authentication and Key Agreement

In this phase, the *BSU*, *GWN* and the *HMS* mutually verify the identities prior to setting up a session key to encrypt the communication process over the public channels.

Step 1: The *BSU* chooses the intended *HMS* then uses its unique identity ID_{BSU} and patient password PW_i to retrieve random nonce R_3 as $R_3^* = A_4 \oplus h(ID_{BSU}||PW_i)$ and parameter $A_1^* = h(PW_i||R_3^*)$.

Step 2: The *BSU* generates random nonce R_5. Next, it chooses the identity ID_{HMS} of the corresponding *HMS* before

deriving parameters $A_5 = A_2 \oplus A_1$, $B_1 = A_5 \oplus A_1 \oplus R_5$, $B_2 = ID_{HMS} \oplus h\ (ID_{BSU} || R_5)$ and $B_3 = h\ (PID_{BSU} || ID_{GWN} || ID_{HMS} || A_5 || ID_{BSU} || R_5)$. Finally, it composes authentication message $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$ and forwards it to the *GWN* over public channels.

Step 3: On receiving authentication message $Auth_1$, the *GWN* validates both ID_{GWN} and PID_{BSU} against their equivalents held in its repository. If this verification fails, the session is terminated. Otherwise, the *GWN* retrieves the corresponding value set $\{ID_{BSU}, R_4, A_1\}$ from its repository.

Step 4: The *GWN* computes parameters $A_5^* = h\ (PID_{BSU} || R_4 || ID_{GWN} || SK_G)$ and $R_5 = B_1 \oplus A_5^* \oplus A_1$. Next, it generates random numbers R_6 and R_7. This is followed by the retrieval of *HMS* unique identity ID_{HMS} as $ID_{HMS} = B_2 \oplus h\ (ID_{BSU} || R_5)$.

Step 5: *GWN* fetches random nonce R_1 from its repository and generates new pseudo-identity for the *HMS* as PID_{HMS}^*. This is followed by the computation of values $HG_K = h\ (ID_{HMS} || SK_G || ID_{NET})$, $B_4 = h\ (HG_K || ID_{GWN})$, $B_5 = (R_5 \oplus A_1) \oplus B_4 \oplus R_1$, $C_1 = R_6 \oplus B_4 \oplus ID_{HMS} \oplus R_1$, $C_2 = PID_{HMS}^* \oplus R_6 \oplus R_1$, $C_3 = h\ (R_6 || R_1 || B_4) \oplus R_7$ and $C_4 = h\ (PID_{HMS} || C_2 || C_3 || HG_K || R_5 \oplus A_1 || R_6)$. At the end, it constructs authentication message $Auth_2 = \{PID_{HMS}, R_5, A_1, B_5, C_1, C_2, C_3, C_4\}$ that is sent over to the *HMS* across public channels.

Step 6: Upon receiving authentication message $Auth_2$ from the *GWN*, the *HMS* validates the received PID_{HMS} against its equivalent in its repository. Basically, the authentication session is terminated if the two values do not match. Otherwise, the *HMS* derives $B_4 = h\ (HG_K || ID_{GWN})$, $(R_5 \oplus A_1) = B_5 \oplus B_4 \oplus R_1$, $R_6 = C_1 \oplus B_4 \oplus ID_{HMS} \oplus R_1$ and $C_4^* = h\ (PID_{HMS} || C_2 || C_3 || HG_K || R_5 \oplus A_1 || R_6)$.

Step 7: The *HMS* validates the derived C_4^* against the received C_4 in authentication message $Auth_2$. Here, the session is aborted if this validation turns negative. Otherwise, the *HMS* generates random nonce R_8. Next, it calculates $R_7 = h\ (R_6 || R_1 || B_4) \oplus C_3$, $PID_{HMS}^* = C_2 \oplus R_6 \oplus R_1$, $C_5 = R_6 \oplus B_4 \oplus R_2$, session key $Sess_H = h\ (R_5 \oplus A_1 || R_6 || R_8)$, $D_1 = h\ (HG_K || R_6) \oplus h(R_1) \oplus R_8$, $D_2 = h\ (C_5 || D_1 || Sess_H || ID_{HMS} || ID_{GWN} || R_8)$ and $R_1^* = h\ (R_1)$. It then stores parameter set $\{PID_{HMS}^*, R_7, R_1^*\}$. Finally, it composes authentication message $Auth_3 = \{C_5, D_1, D_2\}$ which is forwarded to the *GWN* over public channels.

Step 8: After getting authentication message $Auth_3$ from the *HMS*, the *GWN* retrieves R_1 from its repository and computes $R_1^* = h\ (R_1)$ as well as $R_2^* = R_6 \oplus B_4 \oplus C_5$. This is followed by the confirmation of whether $h(R_2)$ is equivalent to $h(R_2^*)$. Basically, the session is terminated if this condition does not hold. Otherwise, the *GWN* computes $R_8 = D_1 \oplus h\ (HG_K || R_6) \oplus R_1^*$ and session key as $Sess_G = h\ (R_5 \oplus A_1 || R_6 || R_8)$.

Step 9: The *GWN* derives $D_2^* = h\ (C_5 || D_1 || Sess_G || ID_{HMS} || ID_{GWN} || R_8)$ and validates it against value D_2 received in authentication message $Auth_3$. Next, it generates new pseudo-identity PID_{BSU}^* for the *BSU* and stores value set $\{PID_{HMS}^*, PID_{BSU}^*\}$ in its repository. This is followed by the substitution of R_1 with R_1^* and R_4 with $h\ (R_4)$.

Step 10: *GWN* derives $D_3 = h\ (PID_{BSU}^* || h(R_4) || ID_{GWN} || SK_G) \oplus h\ (R_5 || A_1)$, $D_4 = h(R_5 || ID_{BSU}) \oplus R_6$, $D_5 = h(R_5 || R_6 || A_1) \oplus R_8$, $E_1 = h\ (h(ID_{BSU} || SK_G) \oplus PID_{BSU}^*$ and $E_2 = h(Sess_G || ID_{BSU} || D_3 || PID_{BSU}^*)$. Finally, it constructs authentication message $Auth_4 = \{D_3, D_4, D_5, E_1, E_2\}$ that is transmitted over to the *BSU* over public channels.

Algorithm 2: Mutual authentication & key agreement

Begin:

1) Retrieve ID_{BSU} & PW_i
2) Derive R_3^* & A_1^*
3) Generate R_5
4) Generate ID_{HMS}
5) Calculate A_5, B_1, B_2, B_3
6) Construct $Auth_1$
7) *BSU*→ *GWN*: $\{Auth_1\}$
8) **If** ID_{GWN} & PID_{BSU} invalid **then**:
9) Abort session
10) **Else:**
11) Retrieve $\{ID_{BSU}, R_4, A_1\}$
12) Derive A_5^* & R_5
13) Generate R_6 & R_7
14) Derive ID_{HMS}
15) Retrieve R_1 & calculate PID_{HMS}^*
16) Compute HG_K, B_4, B_5, C_1, C_2, C_3 & C_4
17) Create $Auth_2$
18) *GWN* → *HMS*: $\{Auth_2\}$
19) **If** PID_{HMS} is invalid **then:**
20) Abandon session
21) **Else:**
22) Calculate B_4, $(R_5 \oplus A_1)$, R_6 & C_4^*
23) **If** $C_4^* \neq C_4$ **then:**
24) Abort session
25) **Else:**
26) Generate R_8
27) Compute R_7, PID_{HMS}^*, C_5, $Sess_H$, D_1, D_2 & R_1^*
28) Store $\{PID_{HMS}^*, R_7, R_1^*\}$ in *HMS*
29) Compose $Auth_3$
30) *HMS* → *GWN*: $\{Auth_3\}$
31) Retrieve R_1
32) Calculate R_1^* & R_2^*
33) **If** $h(R_2) \neq h(R_2^*)$ **then:**
34) Terminate session
35) **Else:**
36) Derive R_8, $Sess_G$ & D_2^*
37) **If** $D_2^* \neq D_2$ **then:**
38) Terminate session
39) Generate PID_{BSU}^*
40) Store $\{PID_{HMS}^*, PID_{BSU}^*\}$ in *GWN*
41) Replace $\{R_1, R_4\}$ with $\{R_1^*, h\ (R_4)\}$
42) Calculate D_3, D_4, E_1& E_2
43) Construct $Auth_4$
44) *GWN* → *BSU*: $\{Auth_4\}$
45) Derive R_6, R_8, PID_{BSU}^*, $Sess_B$ & E_2^*
46) **If** $E_2^* \neq E_2$ **then:**
47) Halt session
48) **Else:**
49) Set session key as $Sess_B = Sess_G$
50) Store $\{PID_{BSU}^*, E_2^*\}$ in *BSU*
51) **Endif**

End

Step 11: Upon receiving authentication message $Auth_4$ from the *GWN*, the *BSU* retrieves R_6 and R_8 by as $R_6 = D_4 \oplus h(R_5 || ID_{BSU})$ and $R_8 = D_5 \oplus h(R_5 || R_6 || A_1)$. Next, it derives $PID_{BSU}^* = E_1 \oplus h\ (h(ID_{BSU} || SK_G)$, session key $Sess_B = h\ (R_5 \oplus A_1 || R_6 || R_8)$ and $E_2^* =$

$h(Sess_B||ID_{BSU}||D_3||PID_{BSU}^*)$. This is followed by the confirmation of whether the derived E_2^* is equivalent to value E_2 received in authentication message $Auth_4$. On condition that this verification is successful, the *BSU* stores value set $\{PID_{BSU}^*, E_2^*\}$ in its memory and the session key is set as $Sess_B = Sess_G$. Algorithm 2 below summarizes these mutual authentication and key agreement procedures.

IV. Security Analysis

The main objective of this paper is to develop a light-weight encryption algorithm that offers improved security to the data exchanged in wireless body area networks. To show that the proposed algorithm is secure under the various threat models, the security functionalities provided by the developed encryption algorithm are discussed in this section. In addition, the attacks prevented by this algorithm are also described.

A. Anonymity

During the mutual authentication procedures, message exchange takes place over the open public communication channels. It is therefore important that the real identity of the *BSU* and *HMS* be protected from attacker $\tilde{A}$ who might be eavesdropping the communication network. During this process, four messages are exchanged. These messages include $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$, $Auth_2 = \{PID_{HMS}, R_5, A_1, B_5, C_1, C_2, C_3, C_4\}$, $Auth_3 = \{C_5, D_1, D_2\}$ and $Auth_4 = \{D_3, D_4, D_5, E_1, E_2\}$. It is evident that none of these messages contains the real identity of the *BSU* (ID_{BSU}) and *HMS* (ID_{HMS}). Instead, it is the pseudo-identity of the *BSU* (PID_{BSU}) and *HMS* (PID_{HMS}) that are exchanged over the public communication channels. As such, *BSU* and *HMS* anonymity are preserved.

B. Untraceability

Suppose that an attacker $\tilde{A}$ is interested in determining whether any message exchanged across the public channels belongs to a particular *BSU*. To achieve this, all the four messages $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$, $Auth_2 = \{PID_{HMS}, R_5, A_1, B_5, C_1, C_2, C_3, C_4\}$, $Auth_3 = \{C_5, D_1, D_2\}$ and $Auth_4 = \{D_3, D_4, D_5, E_1, E_2\}$ are intercepted. Here, R_5 is a random number, PID_{HMS} and PID_{BSU} are the *HMS* and *BSU* pseudo-identities respectively, ID_{GWN} is the real identity of the *GWN*, $A_1 = h(PW_i||R_3)$, $B_1 = A_5 \oplus A_1 \oplus R_5$, $B_2 = ID_{HMS} \oplus h(ID_{BSU}||R_5)$, $B_3 = h(PID_{BSU}||ID_{GWN}||ID_{HMS}||A_5||ID_{BSU}||R_5)$, $B_5 = (R_5 \oplus A_1) \oplus B_4 \oplus R_1$, $C_1 = R_6 \oplus B_4 \oplus ID_{HMS} \oplus R_1$, $C_2 = PID_{HMS}^* \oplus R_6 \oplus R_1$, $C_3 = h(R_6||R_1||B_4) \oplus R_7$, $C_4 = h(PID_{HMS}||C_2||C_3||HG_K||R_5 \oplus A_1||R_6)$, $C_5 = R_6 \oplus B_4 \oplus R_2$, $D_1 = h(HG_K||R_6) \oplus h(R_1) \oplus R_8$, $D_2 = h(C_5||D_1||Sess_H||ID_{HMS}||ID_{GWN}||R_8)$, $D_3 = h(PID_{BSU}^*||h(R_4)||ID_{GWN}||SK_G) \oplus h(R_5||A_1)$, $D_4 = h(R_5||ID_{BSU}) \oplus R_6$, $D_5 = h(R_5||R_6||A_1) \oplus R_8$, $E_1 = h(h(ID_{BSU}||SK_G) \oplus PID_{BSU}^*$ and $E_2 = h(Sess_G||ID_{BSU}||D_3||PID_{BSU}^*)$. It is clear that none of these messages contain plain-text *BSU* identity ID_{BSU} that can help an attacker $\tilde{A}$ to associate messages to a particular *BSU*. Although B_2, B_3, D_4, E_1 and E_2 contain ID_{BSU}, it is encapsulated in other parameters before being one-way hashed. Since it is computationally infeasible to reverse the one-way hashing function, an adversary is unable to retrieve ID_{BSU} from these variables.

C. Mutual Authentication

In the developed algorithm, all the three communicating entities (*BSU*, *GWN* and *HMS*) validate each other before exchanging any data. For instance, on receiving authentication message $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$ from the *BSU*, the *GWN* validates both ID_{GWN} and PID_{BSU} against their equivalents held in its repository. On the other hand, upon getting authentication message $Auth_2 = \{PID_{HMS}, R_5, A_1, B_5, C_1, C_2, C_3, C_4\}$, from the *GWN*, the *HMS* validates the received PID_{HMS} against its equivalent in its repository. In addition, the *HMS* validates the derived C_4^* against the received C_4 in authentication message $Auth_2$. Similarly, after getting authentication message $Auth_3 = \{C_5, D_1, D_2\}$ from the *HMS*, the *GWN* retrieves R_1 from its repository and computes $R_1^* = h(R_1)$ as well as $R_2^* = R_6 \oplus B_4 \oplus C_5$. This is followed by the confirmation of whether $h(R_2)$ is equivalent to $h(R_2^*)$. Additionally, the *GWN* derives $D_2^* = h(C_5||D_1||Sess_G||ID_{HMS}||ID_{GWN}||R_8)$ and validates it against value D_2 received in authentication message $Auth_3$. Finally, on receiving authentication message $Auth_4 = \{D_3, D_4, D_5, E_1, E_2\}$ from the *GWN*, the BSU computes $E_2^* = h(Sess_B||ID_{BSU}||D_3||PID_{BSU}^*)$. This is followed by the confirmation of whether the derived E_2^* is equivalent to value E_2 received in authentication message $Auth_4$. In all these authentication instances, the communication session is terminated upon failure of the verification process.

D. Key Agreement

To encipher the patient data collected by the *BSU*, it is important that the communicating entities setup a session key to encrypt the exchanged messages. In the developed algorithm, the *HMS* derives the session key as $Sess_H = h(R_5 \oplus A_1||R_6||R_8)$, while the *GWN* computes the session key as $Sess_G = h(R_5 \oplus A_1||R_6||R_8)$. Similarly, the BSU calculates the session key as session key $Sess_B = h(R_5 \oplus A_1||R_6||R_8)$. These session keys are utilized to ensure that the confidentiality and integrity of all messages exchanged over the public channels are upheld.

E. Revocability

In authentication schemes, it is important that all malicious users and devices are identified and eliminated from the network. Suppose that some malicious network entity has compromised patient password PW_i. Thereafter, an attempt is made to derive parameters such as $A_1 = h(PW_i||R_3)$, $A_4 = h(ID_{BSU}||PW_i) \oplus R_3$ and $R_3 = A_4 \oplus h(ID_{BSU}||PW_i)$. To curb this, the developed algorithm re-computes patient password as $PW_i^{New} = F_1 \oplus h(ID_{BSU}||R_5^{New})$, where $F_1 = PID_{BSU}^{New} \oplus h(ID_{BSU}||R_5^{New})$. If the malicious entity tries to authenticate using the old password, the *HMS* validates the derived C_4^* against the received C_4 in authentication message $Auth_2$, where $C_4^* = h(PID_{HMS}||C_2||C_3||HG_K||R_5 \oplus A_1||R_6)$. Since $PW_i \neq PW_i^{New}$,

this authentication will fail and hence *BSU* revocation will follow.

F. Conditional Privacy

Suppose that a given *BSU* or *HMS* has been compromised and the *GWN* is interested in tracking these entities for purpose of eliminating them from the network. During the registration phase, the *GWN* generates pseudo-identities PID_{HMS} and PID_{BSU} for the *HMS* and *BSU* respectively. Therefore, it can easily associate PID_{HMS} to ID_{HMS} stored in its memory. Similarly, it can associate a particular PID_{BSU} to ID_{BSU}. As such, conditional privacy is achieved by the proposed algorithm.

G. Node capture and Session Hijacking

Suppose that an attacker $\tilde{A}$ has captured a particular BSU_i and has managed to retrieve all the secret parameters stored in it. During the registration phase, the BSU_i stores value set $\{A_2, A_3, A_4, PID_{BSU}, ID_{GWN}\}$ in its memory. Using these parameters, an attempt is made to compromise the sessions of other network nodes, such as BSU_j. For instance, adversary $\tilde{A}$ may try to compose authentication message $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$ that is then forwarded towards the *GWN* over public channels. Here, $B_1 = A_5 \oplus A_1 \oplus R_5$, $B_2 = ID_{HMS} \oplus h\ (ID_{BSU} || R_5)$ and $B_3 = h\ (PID_{BSU} || ID_{GWN} || ID_{HMS} || A_5 || ID_{BSU} || R_5)$. It is clear that although the attacker has obtained values PID_{BSU} and ID_{GWN} from memory, access to B_1, B_2 and B_3 is still required. However, parameters A_1, A_5, R_5 as well as identities ID_{BSU} and ID_{HMS} are unavailable to the adversary. Consequently, these attacks are prevented by the developed algorithm.

H. Key Compromise

Let us assume that an adversary $\tilde{A}$ has compromised long-term secrets such as *GWN*'s secret key SK_G as well as common key HG_K shared between *HMS* and *GWN*. Next, an attempt is made to compromise the negotiated session keys $Sess_H = Sess_G = Sess_B = h\ (R_5 \oplus A_1 || R_6 || R_8)$. Here, R_5, R_6 and R_8 are random numbers while $A_1 = h\ (PW_i || R_3)$. Evidently, the derived session keys do not depend on either SK_G or HG_K. As such, the negotiated session keys are still secure in the face of active compromise of long-term secret keys.

I. Side Channeling and Impersonation

Suppose that an adversary $\tilde{A}$ is interested in impersonating sensor node *BSU*. To accomplish this, an attacker captures and retrieves secrets $\{A_2, A_3, A_4, PID_{BSU}, ID_{GWN}, PID_{BSU}^{*}, E_2^{*}\}$ stored in *BSU*'s memory. Next, the attacker tries to construct bogus message $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$ that is then forwarded to the *GWN*. Although PID_{BSU} and ID_{GWN} can be retrieved from *BSU* memory, the adversary still needs access to values B_1, B_2 and B_3. Here, $B_1 = A_5 \oplus A_1 \oplus R_5$, $B_2 = ID_{HMS} \oplus h\ (ID_{BSU} || R_5)$ and $B_3 = h\ (PID_{BSU} || ID_{GWN} || ID_{HMS} || A_5 || ID_{BSU} || R_5)$. It is clear that the values obtained from memory cannot help the adversary compute B_1, B_2 and B_3. Therefore, these attacks are prevented by the proposed algorithm.

J. Known Session Specific Temporary Information (KSSTI)

Let us assume that an adversary $\tilde{A}$ has access to the short term secrets such as random numbers. Afterwards, an adversary tries to derive the negotiated session keys $Sess_H = Sess_G = Sess_B = h\ (R_5 \oplus A_1 || R_6 || R_8)$, where $A_1 = h\ (PW_i || R_3)$. It is clear that although the adversary $\tilde{A}$ has access to short term session secrets such as random numbers R_3, R_5, R_6 and R_8, long term secret such as the patient password PW_i is still unavailable. Therefore, the developed algorithm effectively prevents this attack.

K. Eavesdropping and Session Key Disclosure

Supposing that an adversary is interested in eavesdropping the open public channels deployed to exchange messages between the *BSU* and the *HMS*. The ultimate goal is to obtain the derived session keys $Sess_H = Sess_G = Sess_B = h\ (R_5 \oplus A_1 || R_6 || R_8)$, where $A_1 = h\ (PW_i || R_3)$. In the proposed algorithm, messages $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$, $Auth_2 = \{PID_{HMS}, R_5, A_1, B_5, C_1, C_2, C_3, C_4\}$, $Auth_3 = \{C_5, D_1, D_2\}$ and $Auth_4 = \{D_3, D_4, D_5, E_1, E_2\}$ are transmitted over the public channels and hence can be intercepted by $\tilde{A}$. It is evident R_5 and A_1 can be obtained from the intercepted messages. However, $\tilde{A}$ still needs access to random numbers R_6 and R_8 which are derived at the *GWN* and *HMS* respectively. As such, the proposed algorithm is robust against these attacks.

L. Tracking Threats

Let us assume that adversary $\tilde{A}$ wants to track the patient using the messages exchanged over the public channels. During the entire authentication and key negotiation procedures, the patient's *BSU* transmits only one message, $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$. Here, $B_1 = A_5 \oplus A_1 \oplus R_5$, $B_2 = ID_{HMS} \oplus h\ (ID_{BSU} || R_5)$, $B_3 = h\ (PID_{BSU} || ID_{GWN} || ID_{HMS} || A_5 || ID_{BSU} || R_5)$ and $PID_{BSU}^{New} = F_1 \oplus h(ID_{BSU} || R_5^{New})$. It is clear that message $Auth_1$ does not any plain-text BSU identity ID_{BSU}. Any effort to extract this identity from B_2, B_3 and PID_{BSU}^{New} will fail due to the difficulty of reversing the one-way hashing function. As such, the proposed algorithm is robust against patient tracking.

M. Offline Guessing

Suppose that attacker $\tilde{A}$ has intercepted the previous session authentication messages $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$ sent from the *BSU* towards the *GWN*. Let us also assume that has retrieved value set $\{A_2, A_3, A_4, PID_{BSU}, ID_{GWN}\}$ stored in the *BSU*. Thereafter, an adversary tries to guess parameters $PID_{BSU}^{New} = F_1 \oplus h(ID_{BSU} || R_5^{New})$, B_1^{new}, B_2^{new} and B_3^{new} needed construct $Auth_1^{new}$ so as to authenticate at the *GWN* in the current session. Here, $B_1 = A_5 \oplus A_1 \oplus R_5$, $B_2 = ID_{HMS} \oplus h\ (ID_{BSU} || R_5)$ and $B_3 = h\ (PID_{BSU} || ID_{GWN} || ID_{HMS} || A_5 || ID_{BSU} || R_5)$. It is clear that none of the captured parameters can assist $\tilde{A}$ to correctly guess PID_{BSU}^{New}, B_1^{new} and B_2^{new}. Although $\tilde{A}$ is possession of PID_{BSU} and ID_{GWN}, access to ID_{HMS}, A_5, ID_{BSU} and R_5 is still required for the correct guessing of $ID_{HMS} || A_5 || ID_{BSU} || R_5$. Consequently, the developed algorithm thwarts any offline guessing attacks.

N. Non-repudiation

During the registration, the *GWN* receives registration message $Reg_1 = \{ID_{HMS}, HG_K\}$ from the *HMS*, generates *HMS* pseudo-identity PID_{HMS} before storing values $\{ID_{HMS}, PID_{HMS}, ID_{NET}, R_1, h(R_2)\}$ in its memory. Similarly, the GWN receives registration message $Reg_3 = \{ID_{BSU}, A_1\}$ from the BSU, generates pseudo-identity PID_{BSU} before storing parameter set $\{R_4, ID_{BSU}, A_1\}$ in its memory. During the authentication and key agreement phase, the *BSU* sends message $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$ towards the GWN. On the other hand, the HMS sends message $Auth_3 = \{C_5, D_1, D_2\}$ towards the *GWN*, where $C_5 = R_6 \oplus B_4 \oplus R_2$. Since $PID_{HMS}^{*} = C_2 \oplus R_6 \oplus R_1$, it follows that $R_6 = PID_{HMS}^{*} \oplus C_2 \oplus R_1$. As such, the *GWN* can easily link any of these messages to particular pseudo-identities and hence its real network entity. Therefore, network entities cannot deny having participated in any transaction.

V. Performance Evaluation

During the performance evaluation of WBAN security algorithms, computation and communication costs are frequently utilized. Therefore, these two performance measures are used to evaluate the performance of the developed algorithm. The specific details of these evaluations are described in the sub-sections below.

A. Computation Costs

To derive the computation of the developed algorithm, we take into consideration the time it takes to execute the various cryptographic operations during the mutual authentication and key agreement phase. During this phase, the *BSU* executes 10 one-way hashing operations, while the *GWN* and *HMS* execute 17 and 7 one-way hashing operations respectively. Therefore, the total computation cost of the proposed algorithm is 34 one-way hashing operations. According to studies by [3], one-way hashing (T_h) ≈ 0.00023ms, ECC scalar multiplication (T_m) ≈ 0.2226 ms, fuzzy extraction (T_{fe}) ≈ 0.268 ms and PUF operation (T_{puf}) ≈ 0.012 ms. Table II below shows the comparison of the computation cost of the proposed algorithm with other related algorithms.

TABLE II. Computation Costs

Algorithm	Derivation	Total (ms)
Lee et al. [3]	$19T_h + T_{fe} + T_{puf}$	0.23897
Xie et al. [12]	$18T_h + 6T_{pm}$	1.33974
Sammoud et al. [30]	$7T_h + 6T_{fe}$	1.60961
Khalid et al. [11]	$21T_h + 2T_m$	0.45003
Proposed	$34T_h$	0.00782

As shown in Table II, the algorithm developed by [30] incurs the highest computation costs of 1.60961 ms, which is followed by the scheme developed by [12] with computation costs of 1.33974 ms. The high computation overheads in these two schemes is due to ECC scalar multiplications and fuzzy extractions both of which are time-consuming. The algorithms developed by [11] and [3] incur computation overheads of 0.45003 ms and 0.23897 ms respectively. This is attributed to the relatively low fuzzy extraction and scalar multiplication operations carried out in these algorithms. On the other hand, the proposed algorithm incurs the lowest computation overhead of only 0.00782 ms. This is attributed to the fact that it executes only one-way hashing operations which are extremely lightweight.

B. Communication Costs

To derive the communication costs of the proposed algorithm, we consider the size of the messages exchanged during the mutual authentication and key agreement phase. In the proposed algorithm, messages $Auth_1 = \{PID_{BSU}, ID_{GWN}, B_1, B_2, B_3\}$, $Auth_2 = \{PID_{HMS}, R_5, A_1, B_5, C_1, C_2, C_3, C_4\}$, $Auth_3 = \{C_5, D_1, D_2\}$ and $Auth_4 = \{D_3, D_4, D_5, E_1, E_2\}$ are exchanged during this phase. Based on the values used by [11] and [3], ECC point = 320 bits, hashing output = 160 bits, timestamp = 32 bits, while random number, PUF challenge-response, identity and password are 64 bits each. Therefore, the size of these messages are computed as follows:

$Auth_1 = \{64+64+160+160+160 = 608 \text{ bits}\}$,
$Auth_2 = \{64+64+160+160+160+160+160+160 = 1088 \text{ bits}\}$,
$Auth_3 = \{160+160+160 = 480 \text{ bits}\}$ and
$Auth_4 = \{160+160+160+160+160 = 800 \text{ bits}\}$

Therefore, the total communication cost for the propose algorithm is 2976 bits. Table III shows the comparison of the obtained communication cost with other related algorithms.

TABLE III. Communication Costs

Algorithm	No. of messages	Total (ms)
Lee et al. [3]	4	2816
Xie et al. [12]	4	3936
Sammoud et al. [30]	3	1056
Khalid et al. [11]	6	800
Proposed	4	2976

As shown in Table III, the scheme by [11] incurs the lowest communication costs of only 800 bits. This is followed by the schemes by [30], [3] the proposed algorithm and the scheme by [12] whose communication costs are 1056 bits, 2816 bits, 2976 bits and 3936 bits respectively. Although the proposed algorithm incurs the relatively high communication costs, it offers numerous security features that are lacking in other algorithms. However, the other related algorithms have numerous security flaws as shown in Table IV below.

C. Security Features

In this sub-section, the security characteristics offered by the developed algorithm are demonstrated. Table IV presents the comparisons of the security supported by the proposed algorithm with their related algorithms. As shown in Table IV, the proposed algorithm offers the highest level of security compared with its peers. In overall, our security algorithm can protect the WBANs at the least computation costs and moderated communication overheads. It is therefore the most ideal for deployment in this environment where efficiency and robust security protection is key.

VI. Conclusion

Wireless body area networks provide a cost-effective, efficient and reliable healthcare in addition to enabling medical experts to conveniently treat or attend to many patients.

TABLE IV. SECURITY FUNCTIONALITIES

	[3]	[12]	[30]	[11]	Proposed
Security feature					
Anonymity	√	√	×	×	√
Untraceability	√	×	×	×	√
Authentication	√	×	√	√	√
Session key agreement	×	×	√	√	√
Perfect key secrecy	√	√	√	×	√
Revocability	×	×	×	×	√
Conditional privacy	×	×	×	×	√
Attacks prevented					
Node capture	×	√	×	×	√
Session hijacking	×	×	×	×	√
Denial of sleep	×	×	×	×	√
Denial of service	√	×	×	×	√
Key compromise	×	×	×	×	√
Side-channeling	×	×	×	×	√
Impersonation	√	√	√	√	√
KSSTI	×	×	×	×	√
Eavesdropping	×	×	×	×	√
Session key disclosure	√	×	×	×	√
Privileged insider	√	×	√	×	√
Tracking	×	×	×	×	√
Offline guessing	√	√	√	√	√
Forgery	×	×	√	×	√
Non-repudiation	×	×	×	×	√
	√ - Feature present × - Feature missing/not considered				

Apart from real-time patient monitoring, these networks offer diagnostic support, medical administration and patient tracking. It is also possible for medical experts to offer targeted medical services in accordance with the received data. Unfortunately, the sensitive patient information is transferred across the insecure public channels. This exposes the patient information to numerous attacks such as impersonation, replay and man-in-the-middle. These threats can endanger patient life and hence there is need to develop robust encryption schemes to secure these networks. In this paper, we have presented a lightweight encryption scheme that provides robust security at the lowest computation costs and average communication overheads. WBAN attacks such as node capture, session hijacking, denial of sleep, denial of service, key compromise, side-channeling, impersonation, KSSTI, eavesdropping, session key disclosure, privileged insider, tracking, offline guessing, forgery and non-repudiation are prevented. In addition, it supports anonymity, untraceability, authentication, session key agreement, perfect key secrecy, revocability and conditional privacy. It is therefore recommended for deployment in this environment due to its robust security features and efficiency. Future work in this domain revolves around further reduction of the proposed algorithm's relatively high communication costs.

REFERENCES

[1] G.B. Raja, "Advancements of IoT and sensor informatics in wearable, implantable, mobile, and remote healthcare," Academic Press (2025) 87-121.

[2] Z. Xu, C. Xu, W. Liang, J. Xu, H. Chen, "A lightweight mutual authentication and key agreement scheme for medical Internet of Things," IEEE Access, 7 (2019), 53922-53931.

[3] S. Lee, S. Kim, S. Yu, N. Jho, Y. Park, "Provably secure PUF-based lightweight mutual authentication scheme for wireless body area networks," Electronics 11 (2022) 1-29.

[4] A.I. Adamu, P.K. Donta, D.M. Ali, S. Sarang, G.M. Stojanović, S.S Sarnin, "A Systematic Literature Review of Advanced Machine Learning Techniques in Wireless Body Area Networks: Application, Challenges, and Future Directions," IEEE Access, 13, (2025) 194729-194778.

[5] M. Gupta, T. Mishra, "Healthconnect: A Comprehensive Overview of WBAN Integration in E-Healthcare," Security, Privacy, and Trust in WBANs and E-Healthcare (2024) 23-43.

[6] A. Bhattacharyya, H. Basumatary, M.K.D. Barma, "A Review on Next-Generation Wireless Health Monitoring System: Privacy and Protection," Procedia Computer Science 258 (2025) 3857-3866.

[7] S. Karthika, K.J. Gnanaselvi, "A review of forensics security hazards and challenges in WBAN and healthcare systems," Security, Privacy, and Trust in WBANs and E-Healthcare (2024) 63-82.

[8] V.O. Nyangaresi, M.A. Al Sibahee, Z.A. Abduljabbar, J. Ma, M.S. Khalefa, "Biometric-Based Packet Validation Scheme for Body Area Network Smart Healthcare Devices," 2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON), IEEE (2022) 726-731.

[9] B. Narwal, A.K. Mohapatra, "A survey on security and authentication in wireless body area networks," Journal of Systems Architecture 113 (2021) 101883.

[10] A.M. Almuhaideb, K.S. Alqudaihi, "A lightweight and secure anonymity preserving protocol for WBAN," IEEE Access 8 (2020) 178183-178194.

[11] H. Khalid, S.J. Hashim, S.M. Syed Ahmad, F. Hashim, M.A. Chaudhary, "Cross-SN: a lightweight authentication scheme for a multi-server platform using IoT-based wireless medical sensor network," Electronics 10 (2021) 790.

[12] Q. Xie, D. Liu, Z. Ding, X. Tan, L. Han, "Provably Secure and Lightweight Patient Monitoring Protocol for Wireless Body Area Network in IoHT," Journal of Healthcare Engineering 2023 (2023) 4845850.

[13] R.U. Rasool, H.F. Ahmad, W. Rafique, A. Qayyum, J. Qadir, "Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML," Journal of Network and Computer Applications 201 (2022) 103332.

[14] V.O. Nyangaresi, V. O. (2023). Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing 3(2023) 100154.

[15] F. Wu, L. Xu, S. Kumari, X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," Multimedia Systems 23 (2017) 195-205.

[16] M. Salayma, A. Al-Dubai, I. Romdhani, Y. Nasser, "Wireless body area network (WBAN) a survey on reliability, fault tolerance, and technologies coexistence," ACM Computing Surveys (CSUR) 50 (2017) 1-38.

[17] M. Rahman, H. Jahankhani, "Security vulnerabilities in existing security mechanisms for iomt and potential solutions for mitigating cyber-attacks," Information security technologies for controlling pandemics (2021) 307-334.

[18] M.S. Hajar, M.O. Al-Kadri, H.K. Kalutarage, "A survey on wireless body area networks: Architecture, security challenges and research opportunities," Computers & Security 104 (2021) 102211.

[19] J. Herbst, M. Rüb, S.P. Sanon, C. Lipps, H.D. Schotten, "Medical Data in Wireless Body Area Networks: Device Authentication Techniques and Threat Mitigation Strategies Based on a Token-Based Communication Approach," Network 4(2024) 133-149.

[20] V.O. Nyangaresi, J. Ma, "A formally verified message validation protocol for intelligent IoT E-health systems," 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), IEEE (2022) 416-422.

[21] W. Sun, Z, Cai, Y. Li, F. Liu, S. Fang, G. Wang, "Security and privacy in the medical internet of things: a review," Security and Communication Networks 2018 (2018) 5978636.

[22] Q. Liu, K.G. Mkongwa, C. Zhang, "Performance issues in wireless body area networks for the healthcare application: a survey and future prospects," SN Applied Sciences 3 (2021) 155.

[23] S. Iqbal, A. Nazish, " Security and Privacy Challenges in IoT Applications: A Focus on LoRaWAN Networks," Strengthening Industrial Cybersecurity to Protect Business Intelligence, IGI Global (2024) 180-208.

[24] H. Jahankhani, S. Kendzierskyj, O. Hussien, "Approaches and Methods for Regulation of Security Risks in 5G and 6G. In Wireless Networks: Cyber Security Threats and Countermeasures, Springer (2023) 43-70.

[25] S.M. Abdullahi, S. Lazarova-Molnar, "On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances," International Journal of Information Security 24(2025) 53.

[26] V.O. Nyangaresi, "Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks," Ad Hoc Networks 142 (2023) 103117.
[27] R. Somasundaram, M. Thirugnanam, "Review of security challenges in healthcare internet of things," Wireless Networks 27 (2021) 5503-5509.
[28] M. Yaghoubi, K. Ahmed, Y. Miao, "Wireless body area network (WBAN): a survey on architecture, technologies, energy consumption, and security challenges," Journal of Sensor and Actuator Networks 11(2022) 67.
[29] K.A. Delgado-Vargas, G. Gallegos-Garcia, P.J. Escamilla-Ambrosio, "Cryptographic Protocol with Keyless Sensors Authentication for WBAN in Healthcare Applications," Applied Sciences 13(2023) 1675.
[30] A. Sammoud, M.A. Chalouf, O. Hamdi, N. Montavont, A. Bouallegue, "A secure and lightweight three-factor authentication and key generation scheme for direct communication between healthcare professionals and patient's WMSN," 2020 IEEE Symposium on Computers and Communications (ISCC), IEEE (2020) 1-6.
[31] A.S. Rajasekaran, L. Sowmiya, A. Maria, R. Kannadasan, "A Survey on Exploring the Challenges and Applications of Wireless Body Area Networks (WBANs)," Cyber Security and Applications (2024) 100047.
[32] V.O. Nyangaresi, I.M. Al-Joboury, K.A. Al-sharhanee, A.H. Najim, A.H. Abbas, H.M. Hariz, "A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones," e-Prime-Advances in Electrical Engineering, Electronics and Energy (2024) 100471.
[33] N. Nigam, A. Agrawal, G. Sahoo, "Security issues and challenges in wireless body area networks: a comprehensive review," IEEE Access 11 (2023)14005–14024.
[34] M.A. Siddiqi, G. Hahn, S. Hamdioui, W.A. Serdijn, C. Strydis, "Improving the security of the IEEE 802.15. 6 standard for medical bans," IEEE Access 10 (2022) 62953-62975.
[35] C.M. Chen, B. Xiang, T.Y. Wu, K.H. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks," Applied Sciences 8(2018) 1074.
[36] S. Marandi, F. Moazami, A. Malekinezhad, "A lightweight and anonymous mutual authentication and key agreement scheme for WBAN," Peer-to-Peer Networking and Applications (2024) 1-17.
[37] A. Irshad, M. Sher, O. Nawaz, S.A. Chaudhry, I. Khan, S. Kumari, "A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme," Multimedia Tools and Applications 76(2017) 16463–16489.
[38] I. Azeem, A.C. Shehzad, X. Qi, L. Xiong, S.F. Mohammad, K. Saru, F. Wu, "An enhanced and provably secure chaotic map-based authenticated key agreement in multi-server architecture," Arabian Journal for Science and Engineering 43 (2018) 811-828.
[39] R. Amin, S.H. Islam, N. Kumar, K.K.R. Choo, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks," Journal of Network and Computer Applications 104 (2018) 133–144.
[40] V.O. Nyangaresi, H.M. Jasim, K.A.A. Mutlaq, Z.A. Abduljabbar, J. Ma, I.Q. Abduljaleel, D.G. Honi, "A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles," Electronics 12(2023) 3688.
[41] X. Li, J. Peng, M.S. Obaidat, F. Wu, M.K. Khan, C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," IEEE Systems Journal 14(2019) 39-50.
[42] Y.K. Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks," IEEE systems journal 13 (2018) 456-467.
[43] X. Li, J. Niu, S. Kumari, F. Wu, A.K. Sangaiah, K.K.K. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," Journal of Network and Computer Applications 103 (2018) 194–204).
[44] H. Timouhin, F. Amounas, M. Azrour, " New ECC-Based IoT Authentication Protocol for Securing RFID Systems," SN Computer Science 4(2023) 785.
[45] S. Hussain, S.S. Ullah, M. Uddin, J. Iqbal, C.L. Chen, "A comprehensive survey on signcryption security mechanisms in wireless body area networks," Sensors 22(2022) 1072.
[46] V.O. Nyangaresi, Z.A. Abduljabbar, J. Ma, M.A. Al Sibahee, "Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment," 2022 4th Global Power, Energy and Communication Conference (GPECOM), IEEE (2022) 569-574.
[47] A. Gupta, M. Tripathi, A. Sharma, "A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN," Computer Communications 160 (2020) 311-325.
[48] F. Wu, X. Li, A.K. Sangaiah, L. Xu, S. Kumari, L. Wu, J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," Future Generation Computer Systems 82 (2018) 727-737.
[49] M.N. Aman, K.C. Chua, B. Sikdar, "A light-weight mutual authentication protocol for IoT systems," 2017 IEEE global communications conference, IEEE (2017) 1-6.
[50] M. Zhao, X. Yao, H. Liu, H. Ning, " Physical unclonable function based authentication protocol for unit IoT and ubiquitous IoT," 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), IEEE (2016) 179-184.
[51] S. Prajapat, P. Kumar, S. Kumar, "A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks," Cluster Computing (2024) 1-17.
[52] V.O. Nyangaresi, G.K. Yenurkar, "Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks," High-Confidence Computing 4(2024)100178.
[53] X. Li, J. Niu, S. Kumari, F. Wu, K.K.R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," Future Generation Computer Systems 83 (2018) 607–618.
[54] B.A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," Wireless Personal Communications 117(2021) 47-69.
[55] R. Ali, A.K. Pal, S. Kumari, A.K. Sangaiah, X. Li, F. Wu, "An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring," Journal of Ambient Intelligence and Humanized Computing (2018) 1-22.
[56] M. Shuai, B. Liu, N. Yu, L. Xiong, "Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks," Security and Communication Networks 2019(2019) 8145087.
[57] J. Mo, Z. Hu, Y. Lin, "Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks," Security and Communication Networks 2020(2020) 5047379.
[58] L. Wu, Y. Zhang, L. Li, J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," Journal of medical systems 40 (2016) 1-12.
[59] C. Wang, Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," Journal of medical systems 39 (2015) 1-8.
[60] R. Chen, D. Peng, "Analysis and improvement of a mutual authentication scheme for wireless body area networks," Journal of medical Systems 43(2019) 19.
[61] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth," Journal of medical systems 40 (2016) 1-10.
[62] V.O. Nyangaresi, "Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography," Journal of Systems Architecture 133 (2022) 102763.
[63] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, K.K.R. Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," Computers & Electrical Engineering 61 (2017) 238-249.
[64] K. Sowjanya, M. Dasgupta, S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," International Journal of Information Security 19(2020) 129-146.
[65] X. Li, M.H. Ibrahim, S. Kumari, A.K. Sangaiah, V. Gupta, K.K.R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," Computer Networks 129 (2017) 429-443.
[66] A.M. Koya, P.P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," Computer networks 140 (2018) 138-151.
[67] A. Ostad-Sharif, M. Nikooghadam, D. Abbasinezhad-Mood, "Design of a lightweight and anonymous authenticated key agreement protocol

for wireless body area networks," International Journal of Communication Systems 32(2019) e3974.
[68] B.A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, M. Shafiq, "An improved lightweight authentication protocol for wireless body area networks," IEEE Access 8 (2020) 190855-190872.
[69] C.M. Chen, Z. Li, S.A. Chaudhry, L. Li, "Attacks and solutions for a two-factor authentication protocol for wireless body area networks," Security and Communication Networks 2021(2021), 3116593.
[70] V.O. Nyangaresi, N. Petrovic, "Efficient PUF based authentication protocol for internet of drones," 2021 International Telecommunications Conference (ITC-Egypt), IEEE (2021) 1-4).
[71] M.H. Mahalat, S. Saha, A. Mondal, B. Sen, "A PUF based light weight protocol for secure WiFi authentication of IoT devices," 2018 8th International symposium on embedded computing and system design (ISED), IEEE (2018) 183-187.
[72] F. Zhu, P. Li, H. Xu, R. Wang, "A lightweight RFID mutual authentication protocol with PUF," Sensors 19(2019) 2957.
[73] K. Mahmood, S. Shamshad, M. Rana, A. Shafiq, S. Ahmad, M.A. Akram, R. Amin, "PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication," Journal of Information Security and Applications 61 (2021) 102900.
[74] M. Fotouhi, M. Bayat, A.K. Das, H.A.N. Far, S.M. Pournaghi, M.A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," Computer Networks 177 (2020) 107333.