BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Certificateless Algorithm for Body Sensor Network and Remote Medical Server Units Authentication over Public Wireless Channels

Bahaa Hussein Taher[1] Muhammad Yasir[2] Abraham Isiaho[3] Judith N. Nyakanga[4*]

1. Huazhong University of Science & Technology, Wuhan, China
2. China University of Petroleum, Qingdao, China
3. Kaimosi Friends University College, Kaimosi, Kenya
4. Kenyatta National Hospital, Nairobi, Kenya

ARTICLE INFO

Article history
Received: 22 December 2021
Revised: 22 June 2022
Accepted: 5 July 2022
Published Online: 13 July 2022

Keywords:
Authentication
Body sensors
Security
Privacy
WBAN

ABSTRACT

Wireless sensor networks process and exchange mission-critical data relating to patients' health status. Obviously, any leakages of the sensed data can have serious consequences which can endanger the lives of patients. As such, there is need for strong security and privacy protection of the data in storage as well as the data in transit. Over the recent past, researchers have developed numerous security protocols based on digital signatures, advanced encryption standard, digital certificates and elliptic curve cryptography among other approaches. However, previous studies have shown the existence of many security and privacy gaps that can be exploited by attackers to cause some harm in these networks. In addition, some techniques such as digital certificates have high storage and computation complexities occasioned by certificate and public key management issues. In this paper, a certificateless algorithm is developed for authenticating the body sensors and remote medical server units. Security analysis has shown that it offers data privacy, secure session key agreement, untraceability and anonymity. It can also withstand typical wireless sensor networks attacks such as impersonation, packet replay and man-in-the-middle. On the other hand, it is demonstrated to have the least execution time and bandwidth requirements.

1. Introduction

Wireless Body Area Networks (WBAN) comprise of interconnected nano-sensors that are deployed to collect biomedical data from the patients. Thereafter, the sensed data are forwarded to the remote medical servers for analysis and appropriate action [1]. Some of the collected data may include body temperatures, blood pressure and sugar levels [2]. As described by Farooq, S. et al. [3], WBAN is a form of Wireless Sensor Network (WSN). The sensors in WBAN may be placed on the skin, in the vicinity of the

*Corresponding Author:
Judith N. Nyakanga,
Kenyatta National Hospital, Nairobi, Kenya;
Email: nyakinajudith@gmail.com

DOI: https://doi.org/10.30564/jcsr.v4i3.4258

patient or implanted in the patient's body [4]. During the transmissions from the patient side towards the hospital medical servers, wireless public channels [5] are utilized. This two-way communication allows remote monitoring and surveillance of the patients, elderly as well as the disabled population. In so doing, this technology boosts efficiency and safety, as well the reduction of associated healthcare costs. There is also some element of automated control of important healthcare parameters as well as movements, which are then forwarded to hospital servers for appropriate action [6]. In addition, this technology enhances pervasiveness, query handling as well as emergency healthcare services in a multi-hop topology. Moreover, timely intervention may serve to improve the patient's quality of life [7]. The increased demand for WBAN has led to the development of IEEE 802.15.6 communication standard. This allows for seamless connections among low power sensor devices and in so doing, expands the range of applications.

In spite of the many benefits that accrue from the deployment of WBANs, many security and privacy issues surround the deployment and usage of these networks. This is because of the sensitive and private nature of the data transmitted in open wireless channels. As such, any successful data compromise violates patient privacy, can inadvertently lead to misdiagnosis and erroneous treatment, as well as the endangering of patient life [7]. As discussed by Nyangaresi, V.O. et al. [8], WBAN is a special type of WSN and therefore inherits all security risks in these networks. The various attacks that can be launched in WBAN can be classified as internal, confidentiality breaches, external, active and passive [9]. Another significant requirement in WBAN is trust building among the participants such as medical staff, patients and healthcare providers. As such, high levels of trust are one of the critical success factors that serve to boost reliable data exchange among the communicating entities [4].

Based on the discussions above, it is evident that attackers can leak, misuse and corrupt the mission-critical WBAN data. This may lead to wrong medication, job loss or even humiliation [10]. Therefore, WBANs have serious privacy, security and trust threats that may hinder their full potential in the healthcare industry. As such, the secure exchange of medical data in the face of active and passive attacks is necessary but quite challenging. All these issues point to the necessity of protecting WBANs against unauthorized access as well as data compromise. In light of this, proper authentication among all the communicating entities serves as the first step towards security and privacy protection [11]. Any weak authentication facilitates illegal access to healthcare data including malicious modifications, deletion and insertion of bogus data. As explained above, all this can have devastating effects on the side of the patients. Although many authentication protocols [12] have been developed to offer security and privacy in communication networks, their deployment in WBANs is problematic due to the resource constrained nature of body sensors [13,14]. These limitations manifest themselves in form of computation abilities, battery power and memory. There is therefore need to encipher all the data before its transmission over insecure public channels. Since most of the body sensors may be implanted in the patient body, battery replacement presents some challenges. As such, it is critical for the authentication schemes to be energy-efficient. Therefore, this paper makes the following contributions:

- Temporary identifiers are deployed during information exchange to offer anonymity and prevent traceability attacks.
- Random numbers are incorporated in the transmitted data to offer freshness checks and hence protect against packet replays.
- Lightweight bitwise XOR and one-way hashing operations are utilized to enhance the efficiency of the developed algorithm. As such, it is shown that our algorithm has the least execution time and bandwidth requirements.
- Informal security analysis is carried out, which demonstrate that this algorithm can withstand numerous WBAN attacks.

The rest of this paper is organized as follows: Section 2 presents related work, while Section 3 provides a description of the proposed algorithm. On the other hand, Section 4 presents security analysis while Section 5 discusses the performance evaluation of this algorithm. Towards the end of this paper, Section 6 concludes the paper and gives future research directions.

2. Related Work

Many schemes have been put forward to offer protection to patient data exchanged over WBANs. For instance, to build trust among the WBAN participants, numerous blockchain-based protocols have been presented [15-18]. However, blockchain technology is computationally and memory intensive [19]. In addition, the scheme presented by Cheng, X. et al. [16] has not been evaluated in terms of communication costs and attack models. To provide authentication between two nodes and reduce storage costs, a security scheme is developed by Liu, X. et al. [20]. However, this scheme is not evaluated in terms of privacy and other attack scenarios. On the other hand, symmetric key based protocols have been introduced by Sammoud, A. et al. [21] and Renuka, K. et al. [22]. However, the scheme developed by Renuka, K. et al. [22] has high computation and execution time at the server side. Another secure and privacy preserving certificateless protocol is presented by Mwitende, G. et al. [23]. Unfortunately, this scheme has high computation overheads at the client-side. In addition, its analysis against security attacks is missing. To address these issues, an anonymous authentication scheme is introduced by Nyangaresi, V.O. et al. [24]. To offer mutual authentication, a three-factor scheme is presented by Sahoo, S.S. et al. [25]. Although this protocol has low communication and computation overheads, it is never evaluated against common security features such as non-repudiation, untraceability and unlinkability. Similarly, numerous security attacks analyses are missing in schemes developed by Pirbhulal, S. [26] and Peter, S. et al. [27]. To prevent traceability attacks against the user, a robust authentication scheme is presented by Wu, F. et al. [28]. However, significant security attacks analyses are not addressed in this approach. Similarly, resilience against eavesdropping, modifications, packet replays and Man-in-the-Middle (MitM) is not investigated in the protocol presented by Liu, J. et al. [29].

To offer secure data communication in WBAN, a digital signature based scheme is presented by Anwar, M. et al. [30]. The asymmetric key generation deployed here requires communicating entities to have pairs of private and public keys. This renders the algorithm quite inefficient and sophisticated [31]. To address this inefficiency challenge, an energy-efficient authentication protocol is presented by Chang, C.C. et al. [32]. Unfortunately, this protocol is not analyzed against various attack models. To provide conditional privacy, an authentication protocol is introduced by Tan and Chung [33]. However, this technique is vulnerable to Denial of Service (DoS) and impersonation attacks. On the other hand, anonymity preserving scheme that is capable of tracing malicious users is developed by Jegadeesan, S. et al. [34]. Unfortunately, this scheme is not evaluated against eavesdropping, MitM, impersonation and modification attacks. As explained by Shim, K.A. [35], impersonation and failure to offer non-repudiation and mutual authentication are key challenges for the scheme developed by Xiong and Qin [36]. To offer mutual authentication between a client and an access point, a scheme based on Elliptic Curve Cryptography (ECC) and bilinear pairing operations is introduced by Zhao, Z. [37]. However, this scheme is computationally intensive due to the deployed pairing operations [38]. To prevent MitM, impersonation, session hijacking and DoS attacks, an authentication approach is introduced by Zebboudj, S. et al. [39]. However, this protocol has not been analytically evaluated. On the other hand, an ECC based user authentication scheme is developed by Challa, S. et al. [40]. However, this protocol cannot withstand impersonation attacks.

Based on user biometrics, a retina-based security scheme is presented by Ullah, M.G. et al. [41]. Unfortunately, the authors fail to offer evaluation against security attacks. To address this challenge, mutual authentication protocols are introduced by Jiang, Q. et al. [42] and Abina, P. et al. [43]. However, the scheme developed by Jiang, Q. et al. [42] cannot withstand stolen verifier and packet replay attacks. On its part, the protocol by Abina, P. et al. [43] is susceptible to node compromise attacks. Similarly, the scheme presented by Zhou, L. et al. [44] is susceptible to packet replays, MitM, privileged-insider and impersonation attacks. To curb these security challenges, a certificate based authentication scheme is presented by Nyangaresi, V.O. et al. [45], while a user authentication protocol is presented by Farash, M.S. et al. [46]. However, vulnerabilities against offline guessing and impersonation attacks are serious issues in the scheme developed by Farash, M.S. et al. [46]. Similarly, the scheme introduced by Sharma, G. et al. [47] is susceptible to impersonation attacks. Anonymity is another important requirement that must be fulfilled in WBAN authentication protocols. As such, an anonymous authentication scheme is introduced by Javali, C. et al. [48]. Unfortunately, this scheme has very high computation costs. To solve this performance issue, a lightweight authentication protocol is developed by Wazid, M. et al. [49]. In addition, a device pairing scheme for shared key generation is developed by Javali, C. et al. [50]. However, the authors fail to evaluate this protocol against forgery, packet replays and DoS attacks. To address these security issues, an authentication technique is presented by Zhang, W. et al. [51]. This scheme is shown to be robust against tampering, impersonation and replay attacks. However, its design fails to consider inlinkability and anonymity.

The Physically Unclonable Function (PUF) presents another significant technology in the prevention of physical and side-channeling attacks. For instance, numerous PUF based schemes have been presented by different researchers [52-55]. However, PUF based schemes have stability issues. On the other hand, signature based schemes have also been developed to prevent non-repudiations. For instance, a lightweight distributed model based on signatures is introduced by Alaparthy and Morgera [56], while an energy-efficient scheme for key agreement and authentication is developed by Iqbal, J. et al. [57]. Unfortunately, many security attacks cannot be prevented in this protocol [57]. An authentication scheme for wearable sensors has been developed by Li, X. et al. [58]. However, this protocol lacks unlinkability and forward key secrecy [59]. To address these issues, an improved security and privacy-preserving technique is presented by Khan, H. et al. [60]. Similarly, an Advanced Encryption Standard (AES) based scheme that can offer strong forward key secrecy is introduced by He and Zeadally [61]. However, these schemes have key escrow problems in that the central node is required to store master keys as well as security parameters for all other nodes [62]. In addition, the protocol developed by He and Zeadally [61] cannot provide non-repudiation and protection against known secret key attacks. Although impersonation attacks are prevented in the protocol developed by He, D. et al. [63], this scheme cannot provide resilience against key escrow, non-repudiation, linkability and known secret key attacks.

To offer robust security protection, intrusion detection systems [64] and bilinear pairing based schemes developed by Wang and Zhang [65] and Xiong, H. [66] have been presented. Although this scheme by Wang and Zhang [65] offers anonymity, it fails to take into consideration storage overheads. In addition, both schemes have high computation complexities due to the bilinear pairings [67]. Smart cards present another important technique for WBAN authentication. In this regard, an efficient and privacy preserving scheme is developed by Chia-Hui and Yu-Fang [68]. However, this protocol cannot withstand stolen smart card, forgery, packet replays and offline guessing attacks. Group authentication-based protocols have also been developed to deal with security and privacy issues in WBANs. For instance, a group authentication scheme for sensor and personal digital assistant authentication is presented by Shen et al. [69]. However, this scheme cannot provide protection against packet replays, linkability, impersonation, MitM and packet replays. In addition, this scheme is vulnerable when some group members turn out to be malicious [70]. Although digital certificate based schemes can help address this challenge, certificate and public key management presents high complexity for body sensors.

3. The Proposed Algorithm

The medical staff, Trusted Authority (TA), Mobile Device (MD) and the body sensor (BS) are the major components in the proposed algorithm. As shown in Figure 1, the link between the body sensors and the medical staff's MD is an open wireless channel.

Here, the medical staff deploys the MD to access the body sensor data. On the other hand, the TA registers and issues the required security parameters to the body sensors and MDs to help them authenticate each other. Table 1 gives the notations used in this paper.

In term of execution, this algorithm comprises of four main phases, which include medical staff registration, sensor registration, authentication and session key agreement. These phases are explained in greater details in the sub-sections that follow.

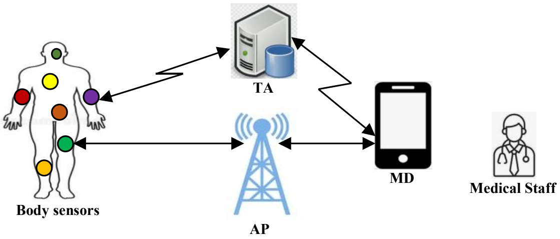

Figure 1. Network Model

Table 1. Notations

Symbol	Description
ID_M	Mobile device unique identity
ID_S	Body sensor unique identity
R_i	Random number *i*
TID_M	Mobile device temporary identifier
TID_A	Trusted authority temporary identifier
TID_B	Body sensor temporary identifier
SKi	Session keys
h(.)	Hashing operation
$\|\|$	Concatenation operation
$\oplus$	XOR operation

3.1 Medical Staff Registration

In this phase, any smart mobile device is deployed by the staff to register with the trusted authority before any access to patient information residing in the body sensors is granted. This is a four-step as shown below.

Step 1: The medical staff *Ui* chooses and inputs unique identity *IDM* and password *PWi* to the MD. Next, the MD constructs registration request message *RM1 = {IDM, PWi }* that is forwarded to the TA over some secure channels.

Step 2: Upon receiving *RM1* from the user's MD, the TA stores its contents in its database. Afterwards, it generates random number *R1* that it uses to derive security parameter $A1 = (IDM \oplus R1) \oplus PWi$.

Step 3: The TA generates *TIDM* as the user's mobile device temporary identity. Next, it computes parameter $A2 = R1 \oplus IDM$. Thereafter, it stores {*R1, TIDM*} in its database before sending parameter *A1* back to the user's MD.

Step 4: After getting *A1* from the TA, the MD computes nonce $R1^* = (A1 \oplus PWi) \oplus IDM$ and temporary identity $TIDM = R1^* \oplus IDM$. This is followed by the storing of parameter set $\{R1^*, TIDM\}$ in the MD's memory. Finally, the MD derives parameter $A3 = (PWi \| R1^*) \oplus TIDM$ that it stores in its memory.

3.2 Sensor Registration

In this phase, the sensor placed in the vicinity of the patient, implanted in the patient body or on the patient's skin need to register to the TA before forwarding the collected data to the medical staff. This is a three-step procedure as elaborated below.

Step 1: The body sensor extracts its identity IDS from memory. Afterwards, it generates random number $R2$. Next, it generates registration request message $RM2 =(IDS \| R2)$ that it forwards to the TA over private channels.

Step 2: On getting message $RM2$ from the body sensor, the TA extracts and stores parameter set $\{IDS , R2\}$ in its database. Next, the TA generates random number $R3$ that it utilizes to derive parameter $B_1 = (IDS \oplus R3) \oplus R1$ and its temporary identity $TIDA = R3 \oplus IDS$. Thereafter, the TA stores parameter set $\{R3, TIDA\}$ in its database. Lastly, the TA forwards authentication message $RM3 = \{B1\}$ over to the body sensor through some private channels.

Step 3: After getting message $RM3$ from the TA, the body sensor computes $R3^* = (B1 \oplus R2) \oplus IDS$. Finally, it derives its temporary identity as $TIDB = R3^* \oplus IDS$ before storing parameter set $\{R_2, R_3, TID_A\}$.

3.3 Authentication and Key Agreement Phase

In this phase, the medical staff and the body sensor execute mutual verification of each other before any access to the sensed data is permitted. This is a nine-step process as described below.

Step 1: The medical staff inputs password PWi to the MD after which it derives parameter $B2 = h\ (PWi \| R1) \oplus TIDM$. Next, the MD validates $B2$ against $A3$ that is stored in its memory. Provided that these two values are unequal, the session is terminated. Otherwise, the MD generates random number $R4$ which it uses to derive parameters $B3 = R4 \oplus PWi$ and $C1 = h\ (R1 \| PWi)$. Finally, it composes authentication message $AM1 = \{B3, TIDM, C1, TIDA\}$ that is sent to the TA as shown in Figure 2.

Step 2: On receiving message $AM1$ from the MD, the TA retrieves $R4$ from $B3$. Next, the freshness of random number $R4$ is verified. Here, the session is terminated if $R4$ fails the freshness check. Otherwise, the TA extracts $TIDM$ and $TIDA$ from its database and compares these values against the ones received in message $AM1$. Basically, the session is terminated when there is no match. Otherwise, the algorithm shifts to step 3 below.

Step 3: The TA derives parameter $C1^* = h\ (R1 \| PWi)$. It then retrieves $C1$ from its database and compares it against $C1^*$. If there is a mismatch, the session is terminated. Otherwise, the TA has successfully authenticated the user's MD. Next, the TA generates random number $R5$ that it uses to compute $C2 = (TIDA \oplus R5)$. Next, it computes $C3 = h\ (R2 \| R3)$ and session key $SK1$ that it masks in parameter $\phi = (SK1 \oplus R2) \oplus R5$. Thereafter, it derives and stores parameter $D1 = (R3 \oplus R2)$ in its database. Finally, it constructs authentication message $AM2 = \{C2, C3, TIDM, \phi, D1\}$ that it sends to the body sensor.

Step 4: After getting message $AM2$, the BS extracts $R5$ from $C2$ and validates its freshness. Here, the session is aborted if random number $R5$ fails the freshness check. Otherwise, the BS derives parameter $D2 = h\ (R2 \| R3)$ followed by its verification against $C3$. Essentially, the session is terminated if the two values do not match. Otherwise, the BS has successfully authenticated the TA.

Step 5: The BS extracts $SK1$ from ϕ as $SK1 = (\phi \oplus R5) \oplus R2$ followed by the generation of random number $R6$ that is employed to compute security parameters $D3 = (R6 \oplus TIDA)$, $E1 = h\ (R3^* \| R2 \| SK1)$ and $E2 = (R3 \oplus R2)$. Next, it retrieves $R3$ from $D1$ as $R3 = (D1 \oplus R2)$. It also computes new temporary identity $TIDB^* = R3^* \oplus IDS$ before storing parameter set $\{R2, R3, TIDB^*\}$ in its memory. Lastly, it composes authentication message $AM3 = \{D3, E1, E2\}$ and forwards it to the TA.

Step 6: On receiving message $AM3$ from the BS, the TA extracts random number $R6$ from $D3$ as $R6 = (D3 \oplus TIDA)$ and validates its freshness. Provided that this message passes the freshness check, the TA derives $E1^* = h\ (R3 \| R2 \| SK1)$. Next, parameter $E1^*$ is validated against $E1$ such that the BS is considered successfully authenticated by TA if this verification is successful. This also confirms the correctness of the derived session key $SK1$.

Step 7: The TA retrieves $R2$ from $E2$ as $R2 = (E2 \oplus R3)$ and derives $TIDB^* = R3 \oplus IDS$. Next, it stores parameter set $\{R3, TIDB^*\}$ in its database. Next, it generates random number $R7$ that it deploys to compute $E3 = IDM \oplus R7$. This is followed by the computation of MD's session key $SK2 = (\phi \oplus PWi) \oplus R7$.

It then generates random number $R8$ before computing $F1 = h\ (IDM \| PWi \| SK2 \| R7)$ and $F2 = (R8 \oplus PWi)$. Next, it derives temporary identifier $TIDMNew = R8 \oplus IDM$. Finally, it stores parameter set $\{R8, TIDMNew\}$ in its database and sends authentication message $AM4 = \{E3, SK2, F1, F2\}$ towards the MD.

Step 8: The MD retrieves random number $R7$ as $R7 = E3 \oplus IDM$ and validates its freshness. Provided that it passes this test, the MD derives session key $SK3 = (SK2 \oplus R7) \oplus PWi$ and parameter $F3 = h\ (IDM \| P$-

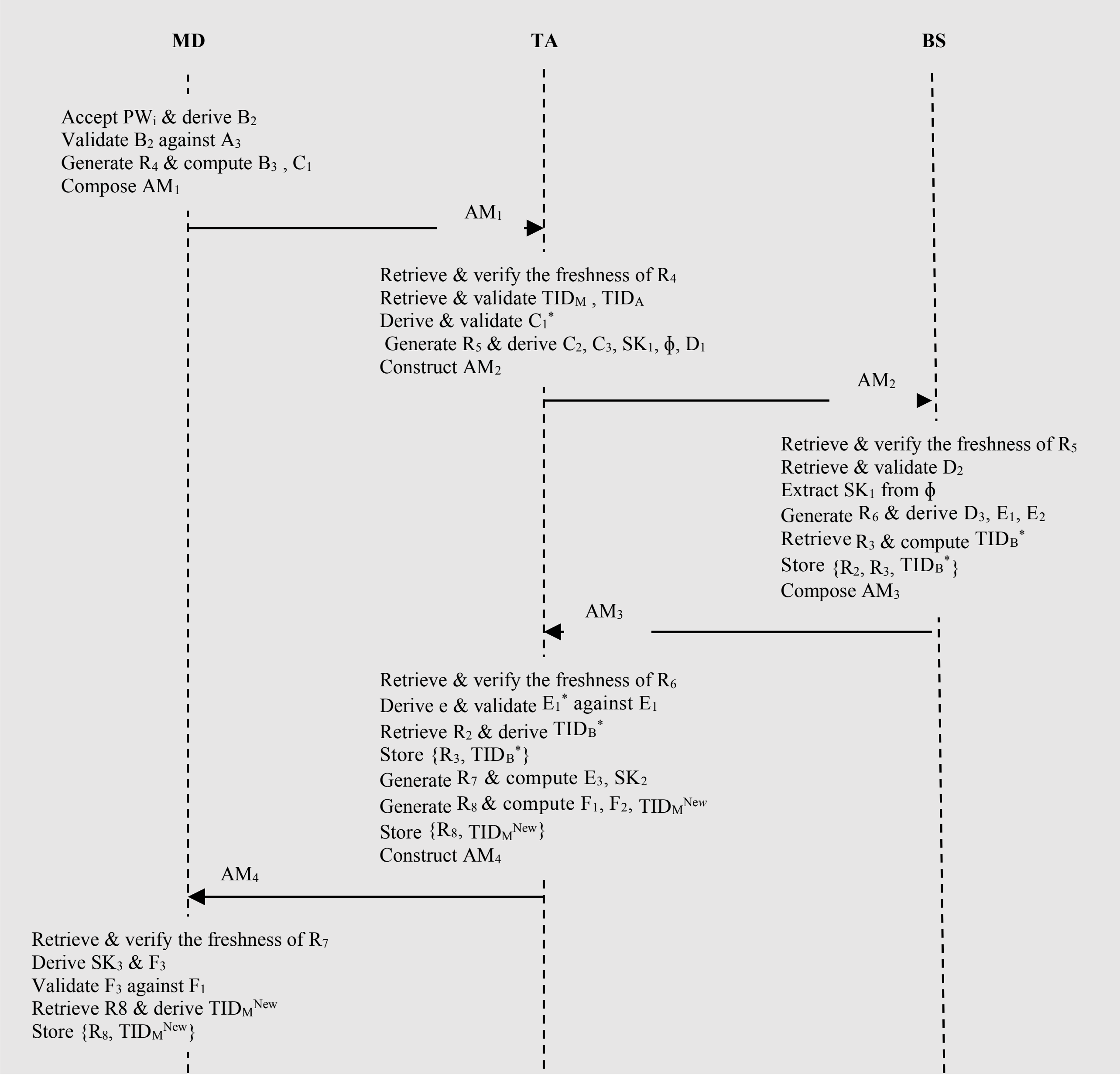
MD
TA
BS
Accept PW_i & derive B_2
Validate B_2 against A_3
Generate R_4 & compute B_3 , C_1
Compose AM_1
AM_1
Retrieve & verify the freshness of R_4
Retrieve & validate TID_M , TID_A
Derive & validate C_1^*
Generate R_5 & derive C_2, C_3, SK_1, ϕ, D_1
Construct AM_2
AM_2
Retrieve & verify the freshness of R_5
Retrieve & validate D_2
Extract SK_1 from ϕ
Generate R_6 & derive D_3, E_1, E_2
Retrieve R_3 & compute TID_B^*
Store $\{R_2, R_3, TID_B^*\}$
Compose AM_3
AM_3
Retrieve & verify the freshness of R_6
Derive e & validate E_1^* against E_1
Retrieve R_2 & derive TID_B^*
Store $\{R_3, TID_B^*\}$
Generate R_7 & compute E_3, SK_2
Generate R_8 & compute F_1, F_2, TID_M^{New}
Store $\{R_8, TID_M^{New}\}$
Construct AM_4
AM_4
Retrieve & verify the freshness of R_7
Derive SK_3 & F_3
Validate F_3 against F_1
Retrieve R8 & derive TID_M^{New}
Store $\{R_8, TID_M^{New}\}$

Figure 2. Authentication and Key Agreement Message Flows

Wi||SK3||R7). Thereafter, a comparison is made between *F3* and *F1* such that any match implies successful authentication between the MD and the TA. In addition, it indicates that the session key derived by the MD is valid.

Step 9: The MD retrieves *R8* from *F2* as *R8= (F2⊕ PWi)* and derives new temporary identity *TIDMNew = R8⊕IDM*. Finally, it stores parameter set *{R8, TIDMNew}* in its memory.

4. Security Analysis

In this section, informal security analysis is executed to show the robustness of the proposed algorithm against conventional WBAN attacks vectors. To accomplish this, the following theorems are formulated and proofed.

Theorem 1: Data privacy is assured in this algorithm

Proof: Suppose that the adversary captures messages *AM1 = {B3, TIDM, C1, TIDA}*, *AM2 = {C2, C3, TIDM, ϕ, D1}*, *AM3 = {D3, E1, E2}* and *AM4 = {E3, SK2, F1, F2}* that are exchanged during the authentication and session key agreement phase. Here, *B3 = R4⊕PWi*, *TIDM = R8⊕IDM*, *C1 = h (R1||PWi*), *TIDA = R3⊕ IDS*, *D3 = (R6⊕TIDA)*, *E1 = h (R3*||R2||SK1)*, *E2 = (R3⊕R2)*, *E3 = IDM⊕R7*, *SK2 = (ϕ⊕PWi*)*⊕R7*, *F1 = h (IDM||PWi||SK2||R7)* and *F2 = (R8⊕PWi)*. Clearly, the attacker is unable to obtain real information concerning the communicating entities because of the bitwise XOR and the collision-resistant one-way hashing operations. As such, an attacker is unable to read the contents of the exchanged messages.

Theorem 2: This algorithm can withstand packet replay attacks

Proof: The assumption made in this attack is that messages $R4^*$, *TIDM*, *C1* and *TIDA* have been captured by an adversary. Later on, an attempt is made to replay these messages to unsuspecting entities. Here, $R4 = B3 \oplus PWi$, $TIDM = R8 \oplus IDM$, $B3 = R4 \oplus PWi$, $C1 = h\ (R1 || PWi)$ and $TIDA = R3 \oplus IDS$. Evidently, all these messages contain random numbers whose freshness is checked at the receiver end. Upon the failure of the freshness checks, the session is terminated. Any modification of these random numbers will fail due to their masking in other parameters.

Theorem 3: This algorithm offers secure session key agreement

Proof: To secure the exchanged messages, the body sensor and the MD negotiate a session key to encipher all the exchanged messages. During this process, the trusted authority acts as an intermediary by providing the necessary keying parameters. After successful mutual authentication, the TA masks the body sensor session key *SK1* in security parameter $\phi = (SK1 \oplus R2) \oplus R5$ before transmitting it to the BS in message *AM2*. Similarly, the TA masks MD session key $SK2 = (\phi \oplus PWi) \oplus R7$ in parameter $F1 = h\ (IDM || PWi || SK2 || R7)$ before forwarding it to the MD in message *AM4*. Thereafter, the MD and the body sensor deploy these session keys to encrypt messages before coupling them to the public communication channels. Suppose that an attacker has captured both messages *AM2* and *AM4*. However, without knowledge of *R2, R5, PWi* and *R7*, the attacker cannot retrieve these session keys from the captured messages.

Theorem 4: Man-in-the-middle attacks are thwarted in this scheme

Proof: Suppose that an attacker has captured message $AM1 = \{B3, TIDM, C1, TIDA\}$. Next, an attempt is made to modify it so as to fool other communicating entities. Here, $B3 = R4 \oplus PWi$, $TIDM = R8 \oplus IDM$, $C1 = h\ (R1 || PWi)$ and $TIDA = R3 \oplus IDS$. However, the one-way hashing and bitwise XOR operations on these parameters imply that they cannot be easily altered. Similarly, messages *AM2*, *AM3* and *AM4* cannot be modified by an attacker.

Theorem 5: This scheme upholds untraceability and anonymity

Proof: The aim of the adversary here is to extract the identities of the communicating entities from the captured messages. Suppose that messages *AM1, AM2*, *AM3* and *AM4* have been successfully obtained by the attacker. Here, $AM1 = \{B3, TIDM, C1, TIDA\}$, $AM2 = \{C2, C3, TIDM, \phi, D1\}$, $AM3 = \{D3, E1, E2\}$ and $AM4 = \{E3, SK2, F1, F2\}$. Clearly, real identity information of the communicating entities is never sent in plaintext in all these messages. Instead, only temporary identities such as *TIDM* and *TIDA* are exchanged in these messages. In addition, these temporary identities are refreshed after every successful authentication process, such as in $TIDMNew = R8 \oplus IDM$. Therefore, the communication process in this algorithm is completely anonymous.

Theorem 6: Impersonation attacks are prevented in this scheme

Proof: Suppose that an attacker has captured message $AM2 = \{C2, C3, TIDM, \phi, D1\}$. Thereafter, an attempt is made to extract body sensor and user secret information to impersonate these two entities. However, $C2 = (TIDA \oplus R5)$, $C3 = h\ (R2 || R3)$, $TIDM = R8 \oplus IDM$, $\phi = (SK1 \oplus R2) \oplus R5$ and $D1 = (R3 \oplus R2)$ do not contain these secrets in plaintext. The utilization of one-way hashing and bitwise XOR operations impede any attempt to discern these secrets from the exchanged messages. The implication is that an attacker lacks real identities or secrets of the communicating entities. Therefore, any impersonation attack using message *AM2* or any other message will fail.

5. Performance Evaluation

In this section, we utilize execution time and bandwidth requirements to evaluate the performance of this algorithm.

5.1 Execution Time

The cryptographic operations carried out during the authentication and key agreement phase include three hashing operations (T_H) at the MD, $3T_H$ operations at the TA and $2T_H$ operations at the BS. The bitwise XOR operations are ignored since they have extremely low execution time compared with other cryptographic primitives. Therefore, the total execution time is $8T_H$ operations. Using the values by Srinivas, J. et al. [71], a single T_H operation takes 0.32 ms. As such, the total execution time for this algorithm is 2.56 ms. Table 2 presents the comparison of this execution time with other schemes.

Table 2. Execution time comparisons

Scheme	Operations	Time (ms)
[41]	$12T_H$	3.84
[44]	$36T_H$	11.52
[46]	$32T_H$	10.24
[47]	$23T_H$	7.36
[49]	$32T_H$	10.24
Proposed	$8T_H$	2.56

As shown in Figure 3, the scheme developed by Zhou, L. et al. [44] has the highest execution time, followed by the schemes developed by Farash, M.S. et al. [46] and Wazid, M. et al. [49] respectively. On the other hand, the protocol presented by Sharma, G. et al. [47] has the third highest execution time, while the scheme developed by Ullah, M.G. et al. [41] has the fourth highest execution time.

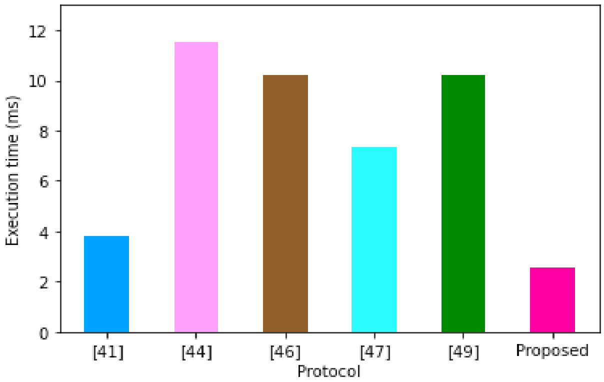

Figure 3. Execution time comparisons

It is evident that the proposed algorithm has the shortest execution time of only 2.56 ms. As such, it is the most ideal for deployment in computation power limited body sensors.

5.2 Bandwidth Requirements

To compute the number of exchanged bits, the four messages exchanged during the authentication and key agreement phase are considered. These messages include *AM1 = {B3, TIDM, C1, TIDA}*, *AM2 = {C2, C3, TIDM, ϕ, D1}*, *AM3 = {D3, E1, E2}* and *AM4 = {E3, SK2, F1, F2}*. Using the values by Srinivas, J. et al. [71], hashing output and ral identities are 160 bits long. On the other hand, random numbers and timestamps are 128 bits and 32 bits respectively. As such, the total size of these four messages is 2048 bits. Table 3 presents the bandwidth comparisons with other algorithms.

Table 3. Bandwidth comparisons

Scheme	Size (ms)
[41]	2528
[44]	3850
[46]	2752
[47]	2912
[49]	2400
Proposed	2048

Based on the plots in Figure 4, the scheme presented by Zhou, L. et al. [44] has the highest bandwidth consumption. This is followed by the approaches developed by Sharma, G. et al. [47], Farash, M.S. et al. [46], Ullah, M.G. et al. [41], Wazid, M. et al. [49] and the proposed algorithm respectively.

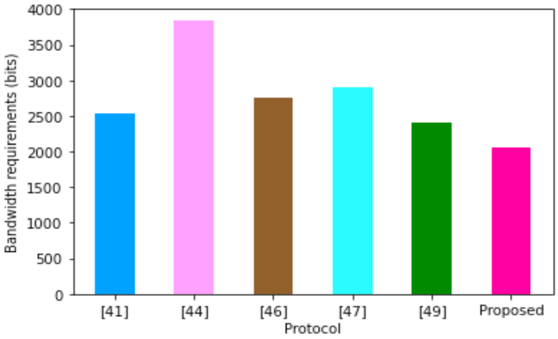

Figure 4. Bandwidth requirements comparisons

Therefore, the proposed algorithm offers strong security protection at the lowest bandwidth requirements.

6. Conclusions and Future Work

Strong security and privacy are critical requirements that must be implemented so as to boost the adoption of WBANs. As such, many protocols have been put forward to protect the mission-critical data exchanged between the body sensors and the remote hospital servers. However, many performance, security and privacy challenges have been noted in majority of the current schemes. Therefore, a truly secure and lightweight authentication algorithm is required to address these gaps. In this paper, a certificate-less authentication algorithm has been presented. Its security analysis has shown that it can offer session key agreement, data privacy, anonymity and untraceability. In addition, its resilience against impersonation, packet replay and man-in-the-middle attacks has been demonstrated. Since this approach has the least execution time and bandwidth requirement, it is the most suitable for deployment in WBANs. Future work will encompass the formal verification of the security features provided by this algorithm.

Conflict of Interest

There is no conflict of interest.

References

[1] Jabeen, T., Ashraf, H., Ullah, A., 2021. A survey on healthcare data security in wireless body area networks. Journal of Ambient Intelligence and Humanized Computing. pp. 1-14.

[2] Ali, S., Ashraf, H., Ramazan, M.S., 2020. An efficient cryptographic technique using modified Diffie-Hellman in wireless sensor networks. International Journal of Distributed Sensor Networks. 16(6), 24.

[3] Farooq, S., Prashar, D., Jyoti, K., 2018. Hybrid encryption algorithm in wireless body area networks (WBAN). Intelligent Communication, Control and Devices. Springer, Singapore. pp. 401-410.

[4] Mehmood, G., Khan, M.Z., Waheed, A., et al., 2020. A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. IEEE Access. 8, 131397-131413.

[5] Nyangaresi, V.O., 2021. ECC based authentication scheme for smart homes. 2021 International Symposium ELMAR, IEEE. pp. 5-10.

[6] Abidi, B., Jilbab, A., Mohamed, E.H., 2020. Journal of Medical Engineering & Technology. 44(3), 97-107.

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

[8] Nyangaresi, V.O., Abood, E.W., Abduljabbar, Z.A., et al., 2021. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. 2021 5th International Conference on Information Systems and Computer Networks (ISCON), IEEE. pp. 1-6.

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

[10] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., et al., 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal. 18(2), 113-122.

[11] Nyangaresi, V.O., Rodrigues, A.J., 2022. Efficient handover protocol for 5G and beyond networks. Computers & Security. 113, 102546.

[12] Fan, S., Li, K., Zhang, Y., et al., 2020. A hybrid chaotic encryption scheme for wireless body area networks. IEEE Access. 8, 183411-183429.

[13] Bashir, A., Mir, A.H., 2018. Securing communication in MQTT enabled Internet of Things with lightweight security protocol. EAI Endorsed Trans. Internet Things. 3(12), 1-6.

[14] Nyangaresi, V.O., Alsamhi, S.H., 2021. Towards secure traffic signaling in smart grids. in 2021 3rd Global Power, Energy and Communication Conference (GPECOM), IEEE. pp. 196-201.

[15] Bhattacharya, P., Tanwar, S., Bodkhe, U., et al., 2019. BinDaaS: blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Transactions on Network Science and Engineering. 8(2), 1242-1255.

[16] Cheng, X., Chen, F., Xie, D., et al., 2019. Blockchain-Based Secure Authentication Scheme for Medical Data Sharing. International Conference of Pioneering Computer Scientists, Engineers and Educators, Springer, Singapore. pp. 396-411.

[17] Xu, J., Meng, X., Liang, W., et al., 2020. A Hybrid Mutual Authentication Scheme Based on Blockchain Technology for WBANs. International Conference on Blockchain and Trustworthy Systems, Springer, Singapore. pp. 350-362.

[18] Gupta, R., Tanwar, S., Tyagi, S., et al., 2019. HaBiTs: Blockchain-based Tele-surgery Framework for Healthcare 4.0. 2019 international conference on computer, information and telecommunication systems (CITS), IEEE. pp. 1-5.

[19] Nyangaresi, V.O., Abduljabbar, Z.A., Al Sibahee, M.A., et al., 2021. Towards Security and Privacy Preservation in 5G Networks. 2021 29th Telecommunications Forum (TELFOR), IEEE. pp. 1-4.

[20] Liu, X., Jin, C., Li, F., 2018. An improved two-layer authentication scheme for wireless body area networks. Journal of Medical Systems. 42(8), 1-14.

[21] Sammoud, A., Chalouf, M.A., Hamdi, O., et al., 2020. A new biometrics-based key establishment protocol in wban: energy efficiency and security robustness analysis. Computers & Security. 96, 101838.

[22] Renuka, K., Kumari, S., Li, X., 2019. Design of a secure three-factor authentication scheme for smart healthcare. Journal of Medical Systems. 43(5), 133.

[23] Mwitende, G., Ye, Y., Ali, I., et al., 2020. Certificateless Authenticated Key Agreement for Blockchain-Based WBANs. Journal of Systems Architecture. 110, 101777.

[24] Nyangaresi, V.O., Abduljabbar, Z.A., Refish, S.H.A., et al., 2022. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference, Springer, Cham. pp. 325-340.

[25] Sahoo, S.S., Mohanty, S., Majhi, B., 2020. A secure three factor based authentication scheme for health care systems using IoT enabled devices. Journal of Ambient Intelligence and Humanized Computing. 12(1), 1419-1434.

[26] Pirbhulal, S., Zhang, H., Mukhopadhyay, S.C., et al., 2015. An efficient biometric-based algorithm using heart rate variability for securing body sensor networks. Sensors. 15(7), 15067-15089.

[27] Peter, S., Pratap Reddy, B., Momtaz, F., et al., 2016. Design of secure ECG-based biometric authentication in body area sensor networks. Sensors. 16(4), 570.

[28] Wu, F., Li, X., Sangaiah, A.K., et al., 2018. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems. 82, 727-737.

[29] Liu, J., Zhang, L., Sun, R., 2016. 1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks. Sensors. 16(5), 728.

[30] Anwar, M., Abdullah, A.H., Butt, R.A., et al., 2018. Securing data communication in wireless body area networks using digital signatures. Technical Journal. 23(02), 50-55.

[31] Nyangaresi, V.O., 2021. Provably Secure Protocol for 5G HetNets. in 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), IEEE. pp. 17-22.

[32] Chang, C.C., Lee, J.S., Wu, J.S., 2017. An Energy Conservation Authentication Scheme in Wireless Body Area Network. Communications of the CCISA. 23(4), 37-54.

[33] Tan, H., Chung, I., 2019. Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. IEEE Access. 7, 151459-151474.

[34] Jegadeesan, S., Azees, M., Babu, N.R., et al., 2020. EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access. 8, 48576-48586.

[35] Shim, K.A., 2018. Comments on "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks". IEEE Transactions on Information Forensics and Security. 15, 81-82.

[36] Xiong, H., Qin, Z., 2015. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE transactions on information forensics and security. 10(7), 1442-1455.

[37] Zhao, Z., 2014. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. Journal of Medical Systems. 38(2), 1-7.

[38] Nyangaresi, V.O., Ibrahim, A., Abduljabbar, Z.A., et al., 2021. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. in 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), IEEE. pp. 1-6.

[39] Zebboudj, S., Cherifi, F., Mohammedi, M., et al., 2017. Secure and efficient ECG-based authentication scheme for medical body area sensor networks. Smart Health. 3, 75-84.

[40] Challa, S., Wazid, M., Das, A.K., et al., 2017. Secure signature-based authenticated key establishment scheme for future iot applications. IEEE Access. 5, 3028-3043.

[41] Ullah, M.G., Chowdhary, B.S., Rajput, A.Q., et al., 2014. Wireless body area sensor network authentication using voronoi diagram of retinal vascular pattern. Wireless Personal Communications. 76(3), 579-589.

[42] Jiang, Q., Lian, X., Yang, C., et al., 2016. A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth. Journal of Medical Systems. 40(11), 1-10.

[43] Abina, P., Dhivyakala, K., Suganya, L., et al., 2014. Biometric Authentication System for Body Area Network. Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 3(3), 7954-7964.

[44] Zhou, L., Li, X., Yeh, K.H., et al., 2019. Lightweight iot based authentication scheme in cloud computing circumstance. Future Generation Computer Systems. 91, 244-251.

[45] Nyangaresi, V.O., Ogundoyin, S.O., 2021. Certificate Based Authentication Scheme for Smart Homes. 2021 3rd Global Power, Energy and Communication Conference (GPECOM), IEEE. pp. 202-207.

[46] Farash, M.S., Turkanovi´c, M., Kumari, S., et al., 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Networks. 36, 152-176.

[47] Sharma, G., Kalra, S., 2019. A lightweight user authentication scheme for cloud-IoT based healthcare services. Iranian Journal of Science and Technology, Transactions of Electrical Engineering. 43(1), 619-636.

[48] Wu, L., Zhang, Y., Li, L., et al., 2016. Efficient and anonymous authentication scheme for wireless body area networks. Journal of Medical Systems. 40(6), 1-12.

[49] Wazid, M., Das, A.K., Shetty, S., et al., 2019. LDA-KM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment. Sensors. 19(24), 5539.

[50] Javali, C., Revadigar, G., Libman, L., et al., 2015. SeAK: Secure authentication and key generation protocol based on dual antennas for wireless body area networks. International Workshop on Radio Frequency Identification: Security and Privacy Issues, Springer, Cham. pp. 74-89.

[51] Zhang, W., Qin, T., Mekonen, M., et al., 2018. Wireless body area network identity authentication protocol based on physical unclonable function. 2018 International Conference on Sensor Networks and Signal Processing (SNSP), IEEE. pp. 60-64.

[52] Nyangaresi, V.O., Petrovic, N., 2021. Efficient PUF based authentication protocol for internet of drones. in 2021 International Telecommunications Conference (ITC-Egypt), IEEE. pp. 1-4.

[53] Wang, W., Shi, X., Qin, T., 2019. Encryption-free Authentication and Integrity Protection in Body Area Networks through Physical Unclonable Functions. Smart Health. 12, 66-81.

[54] Xie, L., Wang, W., Shi, X., et al., 2017. Lightweight mutual authentication among sensors in body area networks through Physical Unclonable Functions. 2017 IEEE International Conference on Communications (ICC), IEEE. pp. 1-6.

[55] Tan, X., Zhang, J., Zhang, Y., et al., 2020. A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network. Tsinghua Science and Technology. 26(1), 36-47.

[56] Alaparthy, V.T., Morgera, S.D., 2018. A multi-level intrusion detection system for wireless sensor networks based on immune theory. IEEE Access. 6, 47364-47373.

[57] Iqbal, J., Umar, A.I., ul Amin, N., et al., 2017. Efficient Key Agreement and Nodes Authentication Scheme for Body Sensor Networks. International Journal of Advanced Computer Science And Applications. 8(7), 180-187.

[58] Li, X., Ibrahim, M.H., Kumari, S., et al., 2017. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks. 129, 429-443.

[59] Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O., 2022. Machine Learning Protocol for Secure 5G Handovers. International Journal of Wireless Information Networks. 29(1), 14-35.

[60] Khan, H., Dowling, B., Martin, K.M., 2018. Highly efficient privacy-preserving key agreement for wireless body area networks. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE. pp. 1064-1069.

[61] He, D., Zeadally, S., 2015. Authentication protocol for an ambient assisted living system. IEEE Communications Magazine. 53(1), 71-77.

[62] Nyangaresi, V.O., 2021. Hardware assisted protocol for attacks prevention in ad hoc networks. in International Conference for Emerging Technologies in Computing, Springer, Cham. pp. 3-20.

[63] He, D., Zeadally, S., Kumar, N., et al., 2016. Anonymous authentication for wireless body area networks with provable security. IEEE Systems Journal. 11(4), 2590-2601.

[64] Hady, A.A., Ghubaish, A., Salman, T., et al., 2020. Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access. 8, 106576-106584.

[65] Wang, C., Zhang, Y., 2015. New authentication scheme for wireless body area networks using the bilinear pairing. Journal of Medical Systems. 39(11), 1-8.

[66] Xiong, H., 2014. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Transactions on Information Forensics and Security. 9(12), 2327-2339.

[67] Nyangaresi, V.O., 2021. Lightweight key agreement and authentication protocol for smart homes. 2021 IEEE AFRICON, IEEE. pp. 1-6.

[68] Chia-Hui, L., Yu-Fang, C., 2016. Secure user authentication scheme for wireless healthcare sensor networks. Journal of Computers and Electrical Engineering. 59, 250-261.

[69] Shen, J., Chang, S., Shen, J., et al., 2018. A lightweight multi-layer authentication protocol for wireless body area networks. Future Generation Computer Systems. 78, 956-963.

[70] Nyangaresi, V.O., Moundounga, A.R.A., 2021. Secure Data Exchange Scheme for Smart Grids. in 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), IEEE. pp. 312-316.

[71] Srinivas, J., Das, A.K., Wazid, M., et al., 2018. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. IEEE Transactions on Dependable and Secure Computing. 17(6), 1133-1146.