IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 6, Ser. 3 (Nov. – Dec. 2023), PP 19-23
www.iosrjournals.org

Provably Secure Authentication And Key Agreement Protocol For The Internet Of Things-Based Wireless BodyArea Network

Sunil Kumar Meena[1], Deepak Ranga[2], Dixit Kumar[2], And Sunil Prajapat[2*]
[1]*department Of Mathematics, Delhi Technological University, Delhi, India.*
[2]*srinivasa Ramanujan Department Of Mathematics, Central University Of Himachal Pradesh,India.,*

Abstract
The extensive utilization of mobile devices, sensors, wireless sensor networks, and the growing Internet of Things (IoT) has inspired the medical and healthcare communities to recruit IoT to measure, gather data, and communicate with patients. Wireless body area networks are prominent in the medical field. Wireless body area networks comprise several wirelessly communicating wear- able or implanted devices. These conventionally assemble the physical facts of the wearer and verbalize them to a server. Recently, many protocols have been proposed with security-assisted health data transfer techniques. As a result, we propose a reliable authentication technique for WBAN. In this technique, hash and X-OR operation topologies are being utilized. And we have also shown that the Burrows-Abadi-Needham (BAN) logic accuracy of the mutual authentication between the patient and medical server is demonstrated using common sense.
Keywords: *Internet of medical Things (IoMT), authentication, security, Wire- less body area networks.*

Date of Submission: 21-12-2023 Date of Acceptance: 31-12-2023

I. Introduction

In today's circumstances, the conception of a wireless body area network (WBAN) is taking control of the medical area. WBAN is a characteristic of sensor systems that associate humans with the health services they provide to interchange condemnatory health data. Health data contains important information about humans, their progenitive effects, behavioral details, etc. [1, 2]. The medical Internet of Things, formulated by the IoT and pharmaceutical industries, is growing quickly, and the WBAN is an essential part of it [3]. WBAN contains low-cost devices around the human body to assist in various applications, including medical. In WBAN, critical wearable and implanted devices observe various information from sensors deployed in the human body [4].

The WBAN sensor node should ensure that the body signal is reliably sensed, carry out the bare minimum of analysis on the detector, and then wirelessly transmit the pro- cessed signal to a nearby processing unit. Although, due to the typical characteristics of WBAN, it encounters a number of problems, including those relating to the quality of service (QOS), energy efficiency, privacy, and security [5]. WBAN health-observing systems fascinate researchers' observations. The WBAN is a new and promising tech- nology that will revolutionize people's healthcare experiences. WBAN health surveil- lance systems offer patients continuous monitoring of physiological signals in addition to their typical advantages of being affordable, reliable, and simplistic, which is highlybeneficial for the elderly population [6].

Wireless physiological data tracking to a system while using a communication con- nection to send essential real-time signs from wearable sensor apparatus to a central network supervisor. The patient's wireless devices gather physiological health indica- tors and immediately send the information to the doctors. WBAN enables its users to remain at home for small issues, decreasing the need for frequent hospitalizations, and to visit only when a significant health problem arises, lowering medicine costs [7].

Related Work

Back in 2012, an authentication protocol using electrocardiograms was put forward by Zhang *et al.* [8] so to reduce the optimization cost, but it failed to provide safety against Sybil, wormhole, and sink attacks, etc. Afterward, Liu *et al.* [9] provided a certificate- less signature ECC agreement and used bi-linear pairing to stand with forgery attacks and offer user anonymity. But later it was found that the Liu *et al.* [9] protocol could not provide security against impersonation and insider vulnerability.

Later, to provide great security, Das *et al.* [10] utilized biometric information in their protocol focusing on WBAN and used a symmetric key cryptosystem for rea- sonable computational cost. And provided security against various vulnerabilities, but could not satisfy user anonymity. Further, a bi-linear pairing authentication protocol was given by Jiang *et al.* [11] while using an asymmetric key cryptosystem for WBAN, but the computational cost was extensively high for the WBAN environment. Later, a to-factor authentication scheme was suggested by Wu *et al.* [12] in WBAN, but it failed to provide safety against stolen smart cards, password guessing, replay attacks, etc., and the optimization cost was not satisfied in the WBAN environment.Hence, in 2017, Arya *et al.* [13] put forward an enhanced user authentication agreement in the WBAN environment. And provide great resistance against insider, replay, plain text, fake sensor attacks, etc., which were inappropriate for frequently transmitting sensitive data in the respective environment. After that, mutual authentication and key agreement were recommended by Koya and Deepthi [14] to resist impersonation and forgery. And they claim their scheme is secure against various vulnerabilities but does not account for sensor node capture and replay attacks. To improve the performance and to re- solve the Koya and Deepthi [14] protocol vulnerabilities, Kompara *et al.* [15] came up with an alternative agreement. But the Kompara et al. [15] agreement could not ac- count for stolen smart cards or replay attacks, and even the computation cost was not satisfactory. Freshly, Xu *et al.* [16] proposed an authentication and key agreement pro- tocol to overcome the requirement, but it almost has a high communication cost and is also vulnerable to impersonation and stolen smart card attacks. Besides, it does not maintain user privacy. Hence, the authentication protocol for WBAN was presented by Fotouhi *et al.* [17] to reduce the computational overhead and preserve authenticity. Fur- ther, it is vulnerable to replay, stolen smart cards, and impersonation attacks. After that, Kasyoka *et al.* [18] proposed a certificate-less access agreement to preserve safety in WBAN.Moreover, it cannot maintain security against impersonation attacks. Further, the use of several operations will increase the computational value. Eventually, in 2021, an authentication scheme utilizing the hash function was put forward by Hussain *et al.* [19]. Although it was unable to safeguard the scheme from impersonation and replay attacks.

II. Elliptic Curve Cryptography

Due to its small weight and extremely tight closure, the elliptic curve over finite fields algebraic form, which serves as the substructure for the public key encryption method known as ECC, may furthermore be used to generate cryptographic keys more quickly, effectively and securely[20].F_q is designate an elliptic curve over the prime finite field F_q is given $v^2 = u^3 + \alpha u + \beta \mod q$, where $\alpha,\beta \in F_q$. F_q is an equation for an elliptic curve over F_q. Assuming that $'q'$ is an enormous prime integer. If $4\alpha^3 + 27\beta^2 \bmod q = 0$, the elliptic curve is believed to be non-singular. Of the use of indicates for every problem, a group of additive events with order q is composed. The operation of scale multiplication is described as $nP = P + P + ... + P$ (n $times$), where n $\in F_q$ is a positive integer, given a generator P of the group G [21]. Right here, we describe some intractable troubles as observed:

1. *Computational Diffe-Hellman Problem:* It is intractable to compute mnP if there factors P, mP , and nP are given, where $m, n \in F_q^*$ [20].
2. *Elliptic Curve Discrete Logarithm Problem:* Given that two factors are Q and P on

an elliptic curve, it is tough to locate m∈ F_q^*. Such that $Q = mP$.

System Modal

This section will review the device modal for the cautious technique, which includes three parties transmitting WBAN data. The following describes each participant's reg- istration, authentication, and key agreement phases.

Registration Center authority

The central trustworthy organization that registers patients must install the medical server under its control for registered patients to utilize the relevant service offered by the medical server. This is known as the registration center authority (RCA); the RCA maintains data about registered patients in a secure database and routinely transmits database data over a secure network to the installed medical server [22].

Medical Server

An entity must communicate the required information to make medical accom- modations to legitimate patients. Nevertheless, the medical server first verifies the legitimacy of the patient and the request by examining the patient's credentials and the request time stamp. The medical server also has direct access to the RCA database, utilized during the authentication stage.

1. **Patient** To determine the patient's health status, the patient utilizes a confidently sophisticated wearable contrivance to accumulate genuine-time health information from the patient's body and send it to the medical server to implement various cryp- tographic schemes for mutual authentication between the patient and the medical server for exchanging communication, which an impatiently smart wearable system accommodates as the patients.

Proposed Scheme

All the Notation used in this paper are given in the table 1.

Table 1: Notation used in the scheme.

Notation	Explanation
Pa_i	A Patient
ID_u PW_u SC_p SD_u MS_S PID_p	Identity of Pa_i Password of Pa_i Smart card of Pa_i
$x_p/b_p/c_S a_j$	Smart device of Pa_i Medical server
RCA DBR $PKSV$ A	A Pseudo identity of Pa_i
$t_1/t_3 t_2$	Generated random nonce for Pa_i and MS_S A large prime number
$\triangle T$	The Registration center authorityThe secure database of RCA Private key of MS_S
$\|$	An Attacker
$\oplus$	Time-stamp at Pa_i end Time-stamp at MS_S side
$h(.)$	Threshold time period Concatenation function Bit-wise XOR function One-way hash function
$H(.)$	Bio-Hash function

Initial Setup step

The registration center authority (RCA) generates a distinct hospital identifica- tion (ID_H) of 128 bits to establish a private key for medical server (MS_s) as $(PK_{MSS}) = h(R_{MSS} \| T_{MSS} \| ID_H)$, where T_{MSS} is the starting timestamp of server and R_{MSS} is a random nonce. RCA securely maintains PK$_{MSS}$ in the server and its databases. In addition, the server often establishes a secure channel connec- tion with RCA to obtain the most current database of freshly enrolled patients.

Patients Registration Step

A patient Pa_i enrolls with RCA to get future services from the server lawfully Pa_i then performs the subsequent moves through a secure channel.

(a) Pa_i choose ID_u, PW_u and Biometric feature 'B_p' and calculate $PB_p = PW_u \oplus H(B_p)$. Now,$Pa_i$ selects a random number x_p and compute a pseudo identity, $PID_p = h(x_p \| ID_u)$. After, that, (Pa_i) transfer $\{PID_p, PB_p\}$ to registrationcenter authority.

(b) the RCA calculate $A_i = h(PID_p \| PK_{MSS})$ where PK_{MSS} is a private key for the MS_s. After that compute $E_i = A_i \oplus h(PID_p \| PB_p)$. Now RCA generates a large prime number 'a_j' to calculate $G_i = E_i \oplus A_i \oplus h(a_j), F_i = h(E_i \| h(a_j) \| PK_{MSS})$. After that, RCA stores E_i, G_i, PID_p, and A_i in its secure database. Further, RCA saves E_i, G_i, and F_i in SC_p and installs it in a smartdevice (SD_u), and it sends this smart card to the Pa_i through a secure channel.

(c) After getting the smart card, Pa_i calculates one more parameter Z_i as $Z_i = ID_u \oplus PB_p \oplus x_p$. Then Pa_i store Z_i in the smart card and install it in the smart device (SD_u) for future communication.

Authentication and Key Agreement Step

Pa_i should establish their legality based on their credentials before requesting med-ical services from the MS_s or exchanging health data with it. To submit a message request to MS_s for user authentication, a smart device (SD_u) computes a message request. The suggested technique provides mutual authentication by having MS_s send a computed response message to Pa_i, confirming MS_s authenticity at Pa_i end if the request received is legitimate. If so, Pa_i's and MS_s's calculate a tempo- rary session key to communicate vital health information via a public channel. Thespecific actions are as follows.

(d) Pa_i insert ID_u, PW_u and Bio metric feature B_p into SD_u to compute $PB_p = PW_u \oplus H(B_p)$ and calculate $x_p = ID_u \oplus PB_p \oplus Z_i, PID_p = h(x_p \| ID_u)$.
After that, $A_i' = E_i \oplus h(PID_p' \| PB_p')$ and verifies $A_i' \stackrel{?}{=} A_i$. If both are equal, SD_u takes a random nonce 'b_p' to enumerate, h$(a_j) = G_i \oplus E_i \oplus A_i$,

$C_i = h(a_j) \oplus h(A_i \| PID_p) \oplus b_p$, $D_i = h(PID_p \| b_p \| A_i \| t_1)$, SD_u sends $\{PID_p, C_i, D_i, t_1\}$ towards the MS_s to prove the legality of Pa_i.

(e) MS_s does $\triangle T \leq t_2 - t_1$ to check the validity of $\{PID_p, C_i, D_i, t_1\}$. If valid, the MS_s calculate $h(a_j) = G_i \oplus E_i \oplus A_i$, $b_p = h(a_j) \oplus h(A_i \| PID_p) \oplus C_i$, $D_i' = h(PID_p \| b_p \| A_i \| t_1)$ to confirm $D_i' \overset{?}{=} D_i$. If both are equal, the MS_s generates a random number c_s. After that, MS_s's enumerate $R_i = h(c_s \| t_2) \oplus h(D_i \| h(a_j) \| b_p)$, $S_i = h(b_p \| h(c_s \| t_2) \| h(a_j) \| t_1)$. At the end, session key $K_{si} = h(PID_p \oplus h(a_j) \oplus h(c_s \| t_2) \oplus b_p)$ is computed by MS_s and transfer $\{R_i, S_i, t_2\}$ to SD_u for mutual authentication.

(f) SD_u verifies the validity of $\{R_i, S_i, t_2\}$ trough $\triangle T \leq t_3 - t_2$. If it is within $\triangle$T, then SD_u compute $h(c_s \| t_2) = h(D_i \| h(a_j) \| b_p) \oplus R_i$, $S_i' = h(b_p \| h(c_s \| t_2) \| h(a_j) \| t_1)$ for $S_i' \overset{?}{=} S_i$. If equal, then the SD_u calculates the session key $K_{pi} = h(PID_p \oplus h(a_j) \oplus h(c_s \| t_2) \oplus b_p)$. So, $K_{pi} = K_{si}$ is equal; this is how the session key is shared between SD_u and MS_s. Sensitive information is exchanged between SD_u and MS_s via session key, which is only valid for a short time. Both parties must go through the authentication steps again if p_i has expired.

III. Security Analysis

Informal Security Analysis

In this part, according to this security study's recommendations, we analyze the recom- mended protocols' protection and accuracy in light of server attacks. The recommended protocol is stated to be firmly closed against a number of possible attacks in the follow-ing section.

2. *The proposed scheme facilitates user anonymity:*

   The patient's anonymity indicates that the Pa_i identifying ID_u is private. Because 'A' must know the server's private key and the random nonces generated by both the patients and server to assess ID_u, our technique makes it easier for patients to maintain their anonymity. As a result, it is impossible to identify a patient who took part in the authentication. Additionally, they do not directly send ID_u among all public communication.

3. *The proposed scheme secures against an impersonation attack:*

   The recommended method allows for the possibility of impersonation attacks if an adversary 'A' can compile login credentials PID_p, C_i, and D_i on behalf of the le- gitimate patient and s/he obtains R_i, S_i and t_2 from MS_s to establish a connection for the transmission of health data. However, the following justification explains why A cannot execute this attack due to a lack of required values. To produce a new login request with the most recent timestamp, $'A'$ requires PID_p, C_i, D_i and t_1. If A modifies the time stamp and sends it to the MS_s, the MS_s check the time stamp, and the test is clear, but 'A,' however, disregard the MS_s side verification of $D_i' \overset{?}{=} D_i$, due to 'A' lack of h (a_j) and A_i. In A_i, we used password (PW_u) and bio-metric feature (B_p) such parameters are impossible to know by $'A'$, so A lack of sending a fake request is not an option. Consequently, the attacker is unable to launch an impersonation attack.

4. *The proposed scheme secures against offline password guessing attack:* Parameters E_i, G_i, F_i, Z_i can be stored on a smart card. If 'A' successfully steals the smart card even then, then none of the smart card's values hold the passworddirectly. The attacker 'A' must first determine $A_i = E_i \oplus h(PID_p \| PB_p)$, and then $PB_p = PW_u \oplus H(B_p)$. Even if PB_p passwords are kept, they are protected using X-OR operation and $H(B_p)$. Similarly, the patient's password PW_u is not sent in plain text. Consequently, a password-guessing attack using this approach isnot feasible in polynomial time.

5. *The proposed scheme secures against replay attack:*

   Consider a replay attack where the attacker endeavors to block or interrupt the transmission. So that a patient cannot connect to the MS_s or an attacker can- not engage in unlawful deportment by sending a message again. Each transmitted message includes a timestamp according to the proposed protocol among Pa_i and MS_s. When MS_s gets the request message from Pa_i, it does a $\triangle T \leq t_2 - t_1$ to verify the precision of the time. The session will be ended if this check fails. Fur- ther, Pa_i probably does check $\triangle T \leq t_3 - t_2$ to determine whether the challenge message from MS_s contains an incipient of time. Further, difficult parameters are computed utilizing the timestamp, preventing an attacker from doing destructive actions using an incipient timestamp. Therefore, the suggested protocol does not support a replay attack.

6. *The proposed scheme secures against smart-card lost attack:*

Assume that, A obtains the patient’s smart card in some manner and receives the values E_i, G_i, F_i, Z_i from it. Now that the {patient’s health} data may be unlaw- fully sent by connecting to the medical server using stored credentials from the smart card, a smart-card lost attack is conceivable. However, for attacker A to be aware of the secret data and parameters, $PB_p = PW_u \oplus H(B_p)$ is needed. There- fore, attacker A continues to be helpless in stealing the patient’s smart card. The suggested system, therefore, defends against a smart-card loss attack.

BAN Logic

In this section, the BAN logic of the proposed scheme. The notations used in the proof are included in the following table, along with their definitions.

Table 2: Notation of BAN Logic

Symbols	Description
$u1, u2$	Two principals
$r1, r2\, SK$	Two statementsThe session key$u1$
$u1 \mid\equiv r1\, u1 \mid$	believes $r1$ $u1$ once said $r1$ $u1$
$\sim r1\, u1 \Rightarrow$	controls $r1$ $u1 receives r1$ $r1$ is
$r1\, u1 \mid ¢\, r1$	fresh
$\#r1$ $(r1)K$	$r1$ is encrypted with K
SK	$u1$ and $u2$ have a shared key SK
$u1 \longleftrightarrow u2$	

IV. Conclusion

WBAN is emerging as a salient strategy in the healthcare field. This inductively sanc- tioning network allows transmitting the statistics from the medical patient to the medical server without barring any dislocation. WBAN promises a technological understanding that will revolutionize people’s healthcare experiences. In the WBAN, protection per- forms a principal function, as the neighborhood accommodates sensitive information that must be maintained confidentially. We cautioned for a better WBAN authentica- tion system. To show that it is tightly closed towards various Kenned assaults, we have informally explored its protection analysis. Using BAN logic, we confirmed that our protocol meets its protection objectives and presents secure authentication and key set- tlement between the user and host. The incrementation of the Internet of Things (IoT) will set up an incipient revolution for WBAN.

Bibliography

[1] Mohammad Yaghoubi, Khandakar Ahmed, And Yuan Miao. Wireless Body Area Network (Wban): A Survey On Architecture, Technologies, Energy Consumption, AndSecurity Challenges. Journal Of Sensor And Actuator Networks, 11(4):67, 2022.

[2] Okundu Omeni, Alan Chi Wai Wong, Alison J Burdett, And Christofer Toumazou. Energy Efficient Medium Access Protocol For Wireless Medical Body Area Sensor Networks. IEEE Transactions On Biomedical Circuits And Systems, 2(4):251–259,2008.

[3] A Vinny Mary And S Jerine. Wireless Body Area Network Transmissions For Iot- Based Healthcare Network: A Review. In IOP Conference Series: Materials ScienceAnd Engineering, Volume 983, Page 012017. IOP Publishing, 2020.

[4] Bahae Abidi, Abdelillah Jilbab, And Mohamed EL Haziti. Wireless Sensor Net- Works In Biomedical: Wireless Body Area Networks. In Europe And MENA Cooper- Ation Advances In Information And Communication Technologies, Pages 321–329. Springer, 2017.

[5] M Raj Kumar Naik And P Samundiswary. Wireless Body Area Network Security Issues—Survey. In 2016 International Conference On Control, Instrumentation, Communication And Computational Technologies (ICCICCT), Pages 190–194. IEEE, 2016.

[6] Saeideh Sadat Javadi And Mohammad Abdur Razzaque. Security And Privacy In Wireless Body Area Networks For Health Care Applications. Wireless Networks And Security: Issues, Challenges And Research Trends, Pages 165–187, 2013.

[7] Ibrahim Abdulai Sawaneh, Ibrahim Sankoh, And David Kanume Koroma. A Sur- Vey On Security Issues And Wearable Sensors In Wireless Body Area Network For Healthcare System. In 2017 14th International Computer Conference On Wavelet Active Media Technology And Information Processing (ICCWAMTIP), Pages 304–308. IEEE, 2017.

[8] Zhaoyang Zhang, Honggang Wang, Athanasios V Vasilakos, And Hua Fang. Ecg- Cryptography And Authentication In Body Area Networks. IEEE Transactions On Information Technology In Biomedicine, 16(6):1070–1078, 2012.

[9] Jingwei Liu, Zonghua Zhang, Xiaofeng Chen, And Kyung Sup Kwak. Certificate- Less Remote Anonymous Authentication Schemes For Wirelessbody Area Networks. IEEE Transactions On Parallel And Distributed Systems, 25(2):332–342, 2013.

[10] Ashok Kumar Das, Santanu Chatterjee, And Jamuna Kanta Sing. A New Biometric- Based Remote User Authentication Scheme In Hierarchical Wireless Body Area SensorNetworks. Adhoc & Sensor Wireless Networks, 28, 2015.

[11] Qi Jiang, Xinxin Lian, Chao Yang, Jianfeng Ma, Youliang Tian, And Yuanyuan Yang. A Bilinear Pairing Based Anonymous Authentication Scheme In Wireless Body Area Networks For Mhealth. Journal Of Medical Systems, 40:1–10, 2016.