IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 14, 2020, accepted February 25, 2020, date of publication March 3, 2020, date of current version March 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977968

EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs)

SUBRAMANI JEGADEESAN[1], MARIA AZEES[2], N. RAMESH BABU[3], UMASHANKAR SUBRAMANIAM[4], (Senior Member, IEEE), AND J. DHAFER ALMAKHLES[4], (Member, IEEE)

[1]Department of Electronics and Communication Engineering, M.Kumarasamy College of Engineering, Karur 639113, India
[2]Department of Electronics and Communication Engineering, GMR Institute of Technology, Rajam 532127, India
[3]M.Kumarasamy College of Engineering, Karur 639113, India
[4]Communications and Networks Engineering, Prince Sultan University, Riyadh 12435, Saudi Arabia

Corresponding author: N. Ramesh Babu (nrameshme@gmail.com)

ABSTRACT The recent advancement in wireless body area networks (WBAN) plays an important role in remote health care systems. However, these networks are suffering from data security and privacy threats. Lack of anonymous authentication and secure data communication leads to operation failure in WBAN. Computational cost and privacy preservation are the two major hindrances for anonymous authentication in many existing schemes. Therefore, a secure and efficient privacy-preserving anonymous authentication scheme is proposed to provide data security and privacy to the users with low computational and communication cost. The performance analysis and experimental simulation results ensure that our proposed anonymous authentication method outperforms the existing systems in terms of providing data security and privacy with less computational overhead.

INDEX TERMS Anonymous authentication, computational cost, conditional tracking, privacy preservation, wireless body area network.

I. INTRODUCTION

Ongoing advancements in wireless communication, design, and size of sensors help to form the short-range wireless networks in the human body to monitor the health, which is known as a Wireless Body Area Network (WBAN). It consists of different wireless sensors that are implanted in the human body, mainly for the continuous monitoring of the physical parameters. The physical parameter includes heartbeat level, body temperature level, blood pressure level, oxygen saturation, blood glucose and so on [1]. WBAN can be used for different medical and non-medical applications due to its remote monitoring ability. For example, it permits us to continuously monitor elderly people and chronically ill patients remotely [2]–[5]. WBAN is also used to analyze the automatic dosing in diabetics.

The WBAN follows two stages of communication. In the first stage, the sensor nodes collect the physical parameters and transmit them to the controller such as smartphones and Personal Digital Assistant (PDA). In the second stage, the controller transfers the collected information to the users and the network manager. Thereby, the controller acts as a gateway between WBAN and users. Thus the performance of healthcare is significantly improved through WBAN. Hence, there is no need for patients to visit the hospital frequently.

The collected health information is analyzed with the medical data and the treatment will be given to the patient based on the data analysis report. Since the health information about the patient is highly confidential, only the authorized doctors can access the medical information of a particular patient [5]. If the medical information is accessed by an unauthorized user, then it may be abused, distributed or it may be altered. As a result, it may lead to disastrous consequences for the patient. Therefore, it is important to provide data security to WBANs with less computational cost. The essential security requirements include user authentication, data integrity, and user privacy. For valid user communication, anonymous certificate and signatures should be shared and verified between

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran.

the doctor and patient. To track the misbehaving of the doctors in the system, an effective tracking mechanism is also required for WBANs.

In the proposed work, the efficient privacy-preserving anonymous mutual authentication scheme for WBANs is presented to meet the above-mentioned security requirements and challenges.

The main objectives of the proposed work are given below

- To ensure the legitimacy of the patients and doctors
- To provide the message integrity
- To develop a conditional tracking system to track the misbehaving doctors in the WBAN.

The rest of this paper is structured as follows. Detailed discussions of the recent works are presented in Section II. The system model and the necessary preliminaries to support the proposed work are given in section III. Section IV gives a detailed explanation of the proposed work. Security analysis of the Efficient Privacy-Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (EPAW) is presented in section V. In section VI, the proposed work is compared with existing works in terms of performance. Finally, section VII gives the conclusion of the proposed work.

II. RELATED WORKS

In many existing schemes, public-key cryptosystems (PKC) is used for remote authentication [6], [7]. Since PKC wants to calculate modular exponentiation, it may suffer from computation overhead. Therefore, these existing systems are not suitable for Ad-Hoc networks. Later, many alternative authentication methods have been proposed based on the elliptic curve cryptosystem (ECC) [8]–[10]. ECC provides better performance with a smaller key size [11]. For example, RSA uses 1024-bit to provide data security, but the same level of security can be achieved by 160-bit in the ECC method. However, the ECC-based system requires certification authority (CA) to maintain the certificate of the user which leads to high computational overhead.

Recently, many researchers are working towards RFID based anonymous authentication protocols to verify the legitimacy of RFID tags without revealing their real identities [12], [13]. But, many symmetric key cryptosystem based RFID authentication schemes [14]–[16] assumes RFID readers as fully trusted. Bichsel *et.al.* [17] scheme based on PKC, anonymous credentials is used to preserve the anonymity of tags against RFID tag readers. But, it consumes more computational cost and complexity in management. An efficient anonymous authentication method is proposed by Armknecht *et.al.* [18], but it needs an anonymizer to ensure anonymity. Therefore, it is clear that the recent RFID based authentication methods are not suitable for the remote monitored WBAN application. Further, the efficiency of ECC-based methods can be also improved by using the ID-based cryptosystem [19], particularly in ID-based

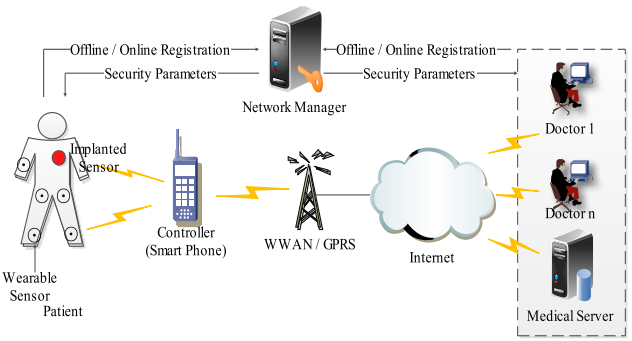

FIGURE 1. Overall system model.

signatures (IBS) [20]–[24]. In [20] authors proposed a certificate less public key cryptography to deal with the fundamental limitation of IBS-based methods. An efficient certificate less signature (CLS) method is proposed in [21], which is more efficient than IBS. But, a scheme which was proposed by Al-Riyami and Paterson [20] failed to attain the traceability.

The proposed work is different in two aspects comparing with existing authentication and privacy-preserving methods. First, the proposed method authenticates the users anonymously with less computational cost and preserves the actual identities of the user from other users. Next, the tracking mechanism gives conditional privacy by disclosing the actual identities of misbehaving doctors with very little cost in terms of computation.

III. SYSTEM OVERVIEW

The overall system model, the security requirements and the definitions of the bilinear pairing technique are described in this section.

A. OVERALL SYSTEM MODEL

The proposed WBAN comprises a network manager (*NM*), doctors and patients with monitoring sensors. The system model of the proposed EPAW method is shown in Fig. 1. In this method, *NM* is considered as a trusted system and all the users are required to register their credentials before starting to use the WBAN system. In this method, the registration is performed using *NM* offline mode, i.e., the doctors and the patient should directly contact the *NM* and register by submitting their required details such as name, address, mobile number, etc. to get the WBAN services. The WBAN comprises of lightweight sensor nodes, which are wearable as well as implanted and are connected with the controller through wireless nature. The controller is considered to be trusted for storing the patient's health information, secret key, etc. It collects the patient's health information such as heartbeat, body temperature, blood pressure, blood glucose level and oxygen saturation from various sensors and transfers the messages to the doctors in an emergency or on-demand basis. The actual identity of the doctor and the patient is only known by the *NM*, in case of dispute, *NM* can disclose the doctor's actual identity.

B. IMPORTANT SECURITY REQUIREMENTS FOR WBAN

The main objective of the proposed work is to provide secure and efficient privacy-preserving anonymous authentication to fulfill the following security requirements:

1 ***Authentication and Data integrity:*** If a doctor wants to access the patient's health information from the WBAN, he/she should be anonymously authenticated by the WBAN before starting the communication. To preserve the integrity of transferring information in WBAN, an anonymous signature is attached to each transferring messages.
2 ***Identity privacy-preserving:*** To preserve the privacy of patients from different security attacks, the actual identification of the patient's data should be kept secret in the WBAN system.
3 ***Traceability:*** In case of any dispute or misbehavior, the *NM* has the ability to obtain the doctor's actual identification through its anonymous certificate and disclose the real information to all other users in the WBAN.

C. BILINEAR PAIRING

Let G_1, G_2 and G_T represent a multiplicative cyclic group of prime order p. Let m_1 denotes generator of G_1, m_2 be a generator of G_2 and ψ be an isomorphism from G_2 to G_1 such that $\psi(m_2) = m_1$. $e : G_1 \times G_2 \rightarrow G_T$ is a bilinear map and the properties of bilinear pairing are described as follows,

1. Bilinear: $e(m_1^a, m_2^b) = e(m_1, m_2)^{ab}$ for all $m_1 \in G_1, m_2 \in G_2$ and $a, b \in Z_p^*$.
2. Non-degeneracy: $e(m_1, m_2) \neq 1G_T$.
3. Computability: There exists an efficient algorithm to simply compute the bilinear map $e : G_1 \times G_2 \rightarrow G_T$.

IV. PROPOSED METHOD

The proposed method consists of three phases such as system initialization, registration and EPAW anonymous mutual authentication.

A. SYSTEM INITIALIZATION

Initially, the *NM* selects two random numbers $p, q \in z_p^*$ that are preserved secretly to calculate the public keys effectively. Next, the *NM* choose a cryptographic hash function: $H : \{0,1\}^* \rightarrow Z_p^*$. The *NM* also chooses a private key as $S_{NM} \in Z_p^*$ and calculates its public-key as $U_{NM} = m_1^{S_{NM}+p}$ Where m_1 is the generator of G_1. Finally, the *NM* distributes the system parameters to the users $param = (p, G_1, G_2, G_T, m_1, U_{NM}, H, e)$.

B. REGISTRATION

Step 1: In the registration phase, the doctor D_j is required to register with the *NM*. Once the D_j has registered in the *NM* successfully, then the *NM* selects the private key as $S_{D_j} \in Z_p^*$ and calculates the corresponding doctor public key as $U_{D_j} = m_1^{S_{D_j}+q}$. Next, the *NM* transmit the S_{D_j} to the doctor through the secure channel and it announces U_{D_j} at the public.

Step 2: Similarly, for the patient P_j, *NM* selects the random number $S_{P_j} \in Z_p^*$ as a private key and generates its corresponding public key as $U_{P_j} = m_1^{S_{P_j}+p}$. Next, the *NM* sends S_{P_j} to the patient secretly through the secure channel and it announces U_{P_j} to the public.

Step 3: After that, the *NM* provides the license (WL_{D_j}) to every doctor D_j to access the health information of the patient securely, where $WL_{D_j} = U_{D_j}^p * m_1^p$.

The *NM* maintains ($id - D_j$, $U_{D_j}^{p*q}$) in the checklist, where $id - D_j$ is the identification of 'D_j' assigned by the *NM* during the registration.

TABLE 1. Notation and its description.

Notation	Description
G_1, G_2 and G_T	Multiplicative cyclic groups
m_1	Generator of G_1
e	Bilinear map
p	Large prime number
ψ	Isomorphism
NM	Network Manager
p, q	Random number selected by NM to compute public keys
S_{NM}	Network Manager Private Key
U_{NM}	Network Manager Public Key
$H()$	One-way hash function
D_j	Doctor j
S_{D_j}	Private Key of Doctor j
U_{D_j}	Public Key of Doctor j
P_j	Patient j
S_{P_j}	Private Key of Patient j
U_{P_j}	Public Key of Patient j
WL_{D_j}	WBAN License for Doctor j
$id - D_j$	Identity of Doctor j
x_j	One-time private key of the patient for mutual authentication
y_j	One-time public key of the patient for mutual authentication
k_j	One-time private key of the doctor for mutual authentication
l_j	One-time public key of the doctor for mutual authentication
CR_{P_j}, CR_{D_j}	One-time Anonymous Certificate of the patient and the doctor
sig	One-time Anonymous Signature

C. ANONYMOUS AUTHENTICATION

1) PATIENT TO DOCTOR ANONYMOUS AUTHENTICATION

In this section, the anonymous authentication is performed between the patient and the doctor to communicate sensitive health information securely and to avoid communication with malicious users. To preserve the privacy of patients from other

WBAN users, the P_j uses one time secret key for verification. If the patient gets the service from the doctor once through WBAN, then the validity of an authentication key will get over. The patient wants to get service from the doctor through WBAN again; he/she needs to come across a fresh authentication process.

Step 1: The P_j first selects a random number x_j from a set of 'X' random numbers $x_1, x_2, \ldots, x_X \in Z_p^*$ as a one-time private key and then calculate the corresponding public key as $y_j = m_1^{x_j+S_{P_j}}$ for $j = 1, 2, \ldots, X$.

Step 2: For each one-time public key y_j, the patient calculates the one-time anonymous self-generated certificate CR_{P_j} as follows:

a. The patient randomly selects $k_1 \in Z_p^*$ and calculates a_1 and a_2 where $a_1 = m_1^{S_{P_j}}$ and $a_2 = m_1^{S_{P_j}+k_1}$.
b. Then, calculates the challenger $c = H(y_j \parallel a_1 \parallel a_2 \parallel U_{NM})$ and also P_j computes a_1' and a_2' where $a_1' = m_1^{x_j-k_1}$ and $a_2' = \frac{1}{m_1^{x_j}}$.
c. Finally, set $CR_{P_j} = \{y_j \parallel a_1' \parallel a_2' \parallel c\}$ as the one-time anonymous self-generated certificate.

Step 3: To maintain the integrity of a patient's health data d, the P_j computes the signature as $sign = m_2^{\frac{1}{x_j+S_{P_j}+H(d)}}$ and transmit the following data to the doctor D_j $data = (d \parallel sign \parallel y_j \parallel CR_{P_j} \parallel T_P)$, where T_P is the current timestamp.

Step 4: After receiving $data = (d \parallel sign \parallel y_j \parallel CR_{P_j} \parallel T_P)$, the doctor D_j first checks the freshness of T_P value. If not, D_j simply terminates the connection. Next, D_j checks the validity of the information source and data integrity as follows.

The D_j first calculates

$$a_1'' = y_j \times a_2'$$
$$a_2'' = \frac{y_j}{a_1'}$$

Finally, D_j computes $c' = H(y_j \parallel a_1'' \parallel a_2'' \parallel U_{NM})$. If $c = c'$, then the y_j and CR_{P_j} crosses the verification and the patient authenticated by the receiver successfully.

Proof of Correctness:

The challenger computed by P_j and D_j should be equal, i.e, $a_1'' = a_1$ and $a_2'' = a_2$.

$$\begin{aligned} a_1'' &= y_j \times a_2' \\ &= m_1^{x_j+S_{P_j}} \times \frac{1}{m_1^{x_j}} \\ &= m_1^{x_j+S_{P_j}-x_j} \\ &= a_1 \end{aligned}$$

and

$$\begin{aligned} a_1'' &= \frac{y_j}{a_1'} \\ &= \frac{m_1^{x_j+S_{P_j}}}{m_1^{x_j-k_1}} \\ &= m_1^{x_j+S_{P_j}-x_j+k_1} \\ &= m_1^{S_{P_j}+k_1} \\ &= a_2 \end{aligned}$$

Step 5: Once the certificate is verified, then the doctor validates the integrity of d as follows:

$$e(y_j.m_1^{H(d)}, sign) = e(m_1, m_2)$$

If it holds, then the data d is accepted by the doctor, it will be rejected otherwise.

Proof of Correctness:

$$\begin{aligned} e(y_j.m_1^{H(d)}, sig) &= e(m_1^{x_j+S_{P_j}}.m_1^{H(d)}, m_2^{\frac{1}{x_j+S_{P_j}+H(d)}}) \\ &= e(m_1^{x_j+S_{P_j}+H(d)}, m_2^{\frac{1}{x_j+S_{P_j}+H(d)}}) \\ &= e(m_1, m_2). \end{aligned}$$

where, the $e(m_1, m_2)$ value can be pre-calculated.

2) DOCTOR TO PATIENT ANONYMOUS AUTHENTICATION

In this section, the anonymous authentication is performed to transfer the medical data from the doctor to the patient in a secure manner and to avoid communication with malicious users. To preserve the privacy of a doctor from other users, the D_j uses one time secret key for verification. If the doctor enters into the WBAN and accessed the information once, then the validity of an authentication key will get over. The doctor wants to access the information from WBAN again; he/she needs to come across a fresh authentication process. Note that, if a user D_j is compromised by an adversary, then the NM will withdraw to broadcasting the information to the particular user D_j.

Step 1: The D_j first selects a random number k_j from a set of 'K' random numbers $k_1, k_2, \ldots, k_K \in Z_p^*$ as a one-time private key and then calculates the corresponding public key as $l_j = m_1^{k_j+S_{D_j}}$ for $j = 1, 2, \ldots, K$.

Step 2: For each one-time public key l_j, the doctor calculates the one-time anonymous self-generated certificate CR_{D_j} as follows:

a. The doctor randomly selects $t_1, t_2 \in Z_p^*$ and calculates b_1 and b_2.
   Where $b_1 = m_1^{t_2+S_{D_j}}$ and $b_2 = m_1^{t_1+k_j}$
b. Then, D_j calculates the challenger $c = H(l_j \parallel b_1 \parallel b_2 \parallel U_{NM})$ as well as b_1' and b_2' where $b_1' = m_1^{t_2-t_1}$ and $b_2' = \frac{1}{m_1^{-t_1-S_{D_j}}}$.
c. Finally, sets $CR_{D_j} = \{l_j \parallel b_1' \parallel b_2' \parallel c\}$ as the one-time anonymous self-generated certificate.

Step 3: To maintain the integrity of a prescribed medical data 'md', the doctor computes the signature $sig = m_2^{\frac{1}{k_j+S_{D_j}+H(md)}}$ and transmits the following value to the patient P_j, $data = (md \parallel sig \parallel l_j \parallel CR_{D_j} \parallel T_D \parallel WL_{D_j})$.

Step 4: After receiving $data = (md \parallel sig \parallel l_j \parallel CR_{D_j} \parallel T_D \parallel WL_{D_j})$, P_j checks the freshness of T_D. If not, P_j simply

terminates the connection. Next P_j checks the validity of the information source and data integrity as follows.

The P_j first calculates

$$b_1'' = b_1' \times b_2'$$
$$b_2'' = b_2' \times l_j$$

and then the patient checks the challenger $c' = H(l_j \parallel b_1'' \parallel b_2'' \parallel U_{NM})$. If $c = c'$, then the l_j and CR_{D_j} crosses the verification and the doctor D_j is authenticated by the patient successfully.

Proof of Correctness:

The challenger value generated by the doctor and the patient should be the same. i.e., $b_1'' = b_1$ and $b_2'' = b_2$.

$$\begin{aligned} b_1'' &= b_1' \times b_2' \\ &= m_1^{t_2 - t_1} \times \frac{1}{m_1^{-t_1 - S_{D_j}}} \\ &= m_1^{t_2 - t_1} \times m_1^{t_1 + S_{D_j}} \\ &= m_1^{t_2 - t_1 + t_1 + S_{D_j}} \\ &= m_1^{t_2 + S_{D_j}} \\ &= b_1 \\ b_2'' &= b_2' \times l_j \\ &= \frac{1}{m_1^{-t_1 - S_{D_j}}} \times m_1^{k_j - S_{D_j}} \\ &= m_1^{t_1 + S_{D_j} + k_j - S_{D_j}} \\ &= m_1^{t_1 + k_j} \\ &= b_2 \end{aligned}$$

Step 5: Once the certificate is verified, then the patient validates the integrity of *md* as follows:

$$e(l_j.m_1^{H(md)}, sig) = e(m_1, m_2)$$

If it holds, then the medical data *md* is accepted by the patient. Otherwise, it will be rejected.

Proof of Correctness:

$$\begin{aligned} e(l_j.m_1^{H(md)}, sig) &= e(m_1^{k_j + S_{D_j}}.m_1^{H(md)}, m_2^{\frac{1}{k_j + S_{D_j} + H(md)}}) \\ &= e(m_1^{k_j + S_{D_j} + H(md)}, m_2^{\frac{1}{k_j + S_{D_j} + H(md)}}) \\ &= e(m_1, m_2). \end{aligned}$$

where, the $e(m_1, m_2)$ value can be pre-calculated.

Step 6 (Conditional Tracking): If the received medical data '*md*' from the doctor who is having a license WL_{D_j} has been doubtful, then the *NM* has the ability to track the actual identity $id - D_j$, by seeing the record $(id - D_j, U_{D_j}^{p*q})$ in the tracking list.

$$\frac{(WL_{D_j})^q}{m_1^{p*q}} = \frac{(U_{D_j}^p * m_1^p)^q}{m_1^{p*q}} = \frac{U_{D_j}^{p*q} * m_1^{p*q}}{m_1^{p*q}} = U_{D_j}^{p*q}$$

V. SECURITY ANALYSIS

This section presents both the informal and formal security analysis of the proposed EPAW method.

A. INFORMAL SECURITY ANALYSIS

In EPAW, to execute an impersonation attack, the opponent needs to find the one-time key of the authentic user and the private key of the user which is distributed by the *NM*. Also, the opponent cannot compromise the registration process. Since it is implemented directly in offline mode. Hence, the proposed work is more secure from the impersonation attack.

- ***Authentication and Data Integrity:*** To ensure data integrity, the signature attached to every data before the transmission. For anonymous and secure mutual authentication, anonymous certificate is attached with each data before the transmission. In the proposed work, the signature is appended on data d is defined as $sig = m_2^{\frac{1}{x_j + S_{P_j} + H(d)}}$. sig is depends on the one-time private key x_j and the patient private key S_{P_j} which are known only to the particular patient P_j. Therefore, it is very difficult for the attacker to forge the signature without knowing the one-time private key x_j and patient private key S_{P_j}. Similarly CR_{P_j} is depends on one-time private key x_j and patient private key S_{P_j}. Therefore, it is very difficult for an adversary to forge the certificate. Moreover, the value x_j will get changed from time to time. Even if the intruder found the one-time private key x_j, it is not possible for his/her to generate CR_{P_j}, without knowing the patient private key S_{P_j}. If P_j need continuous monitoring, then the health information of P_j should be communicated to doctors after appending signature and certificate with the information to ensure the data integrity and source authentication. Hence, we can avoid the impersonation attack [9] with the nature of data integrity and source authentication.
- ***Conditional Privacy Preservation:*** In the proposed EPAW scheme, the patient and doctors can protect their actual identities from other users by using their anonymous certificates and signatures. But, the *NM* has the ability to track the actual identity of a doctor by using its anonymous certificate. For example, when a doctor transmits bogus data to the patient with their anonymous certificate, the *NM* can verify the message content. If the message content is found as bogus, then *NM* will collect the anonymous certificate of the bogus information and maps it with the tracking list. From the mapping, the *NM* can track the actual identification of a doctor efficiently. Afterward, the *NM* can reveal the privacy of the doctor and withdraw that doctor from WBAN.
- ***Anonymity:*** It is computationally hard to find the real source of the information by using the proper *sig* and CR_{P_j}. Therefore, the opponent cannot identify the source of the message from *sig* and CR_{P_j}.

- ***Nonrepudiation:*** The user (patient and doctor) cannot repudiate after sending the data. Because, when the user P_j or D_j receives the information from the opponent P_j or D_j, they can verify the authenticity of the user using the certificate CR_{P_j} and they can ensure the integrity of the received information using the signature. When a dispute occurs, the user can contact *NM* with the information. *NM* can trace the actual identity of the user by using the received information. After that, the *NM* can disclose the privacy of the particular user and withdraw the user from the WBAN.
- ***Replay Attack:*** The timestamp values are included during each data communication between patient and doctor. The information transferred from patient to doctor is $data = (d \parallel sig \parallel y_j \parallel CR_{P_j} \parallel T_P)$. Once the data is received by the doctor, he/she will check the freshness of T_P. If it is true, the doctor will accept the received data. Otherwise, he/she will simply reject the received data. Similarly, the information transferred from the doctor to the patient is $data = (md \parallel sig \parallel l_j \parallel CR_{D_j} \parallel T_D \parallel WL_{D_j})$. After receiving the data, P_j will check the freshness of T_D. If it holds, P_j will accept the data. Otherwise, received data is rejected by the P_j. So, it is easy for the verifier to detect the replay attack. Therefore, our proposed scheme is secure against the replay attack.
- ***Unlinkability:*** The *sig* and CR_{P_j} are calculated depends on the randomly chosen one-time private key x_j. Also, the value of x_j gets changed from time to time. Therefore, the one-time private key x_j generates new *sig* and CR_{P_j} for each communication. Hence, it is very difficult for the intruder to find the source of information except *NM* during the data communication between WBAN users.
- ***Bogus message attack:*** All the entities in the WBAN validate the correctness of the received messages by using the attached signature. During the signature verification, the received message has to pass the verification test. Otherwise, the entity will reject the message immediately. Hence, the proposed EPAW scheme is secure against the bogus message attack.

B. BAN LOGIC BASED FORMAL SECURITY ANALYSIS

Burrows, Abadi and Needham developed BAN logic for analyzing the authentication protocols [33]. The BAN logic is very simple and easy to understand and use. It will find the security vulnerability of the protocol.

Postulates of BAN logic:

- ***Rule 1 (R1): Message-meaning rule***

$$\frac{\text{P believes Q} \xleftrightarrow{\text{K}} \text{P,P sees } \{\text{X}\}_{\text{K}}}{\text{P believes Q said X}}$$

P believes *Q* has said *X* if *P* believes the key *K* is the shared key with *Q* and *P* sees *X* is encrypted by *K*.

- ***Rule 2 (R2): Nonce – Verification rule***

$$\frac{\text{P believes fresh(X), P believes Q said X}}{\text{P believes Q believes X}}$$

P believes *Q* believes *X* if *P* believes *X* is sent currently and *Q* has said *X*.

- ***Rule 3 (R3): Jurisdiction rule***

$$\frac{\text{P believes Q controls X, P believes Q believes X}}{\text{P believes X}}$$

P believes *X* if *P* believes *Q* has the jurisdiction for *X* and *P* believes *Q* believes *X*.

- ***Rule 4 (R4): Decomposition rule***

a) $\dfrac{\text{P sees (X,Y)}}{\text{P sees (X)}}$

b) $\dfrac{\text{P believes fresh (X)}}{\text{P believes fresh (X,Y)}}$

c) $\dfrac{\text{P believes (X,Y)}}{\text{P believes (X)}}$

Various postulates are used for decomposing messages and for verifying their freshness. Informally, (a) *P* can detect *X* if it observes all (b) Combination of *X*, *Y* is fresh if one of the components is fresh and (c) Combination of various message components implies belief in them individually.

- ***Protocol proof using BAN logic***

1. As per message-meaning rule (R1)

$$\frac{\text{D}_j \text{ believes D}_j \overset{CR_{P_j}}{\longleftrightarrow} \text{P}_j, \text{D}_j \text{ sees } \{data\}_{CR_{P_j}}}{\text{D}_j \text{ believes P}_j \text{ said } \{data\}}$$

2. According to nonce verification rule (R2)

$$\frac{\text{D}_j \text{ believes fresh } (\text{T}_D), \text{D}_j \text{ believes P}_j \text{ said } \{data\}}{\text{D}_j \text{ believes P}_j \text{ believes } \{data\}}$$

3. As per rule 3 (R3)

$$\frac{\text{D}_j \text{ believes P}_j \text{ controls } \{data\}, \text{D}_j \text{ believes P}_j \text{ believes } \{data\}}{\text{D}_j \text{ believes } \{data\}}$$

4. As per rule 4 (R4)

$$\text{D}_j \text{ believes D}_j \overset{CR_{P_j}}{\longleftrightarrow} \text{P}_j$$

5. According to message meaning rule (R1)

$$\frac{\text{P}_j \text{ believes P}_j \overset{CR_{D_j}}{\longleftrightarrow} \text{D}_j, \text{P}_j \text{ sees } \{data\}_{CR_{D_j}}}{\text{P}_j \text{ believes D}_j \text{ said } \{data\}}$$

6. According to nonce verification rule (R2)

$$\frac{\text{P}_j \text{ believes fresh } (\text{T}_P), \text{P}_j \text{ believes D}_j \text{ said } \{data\}}{\text{P}_j \text{ believes D}_j \text{ believes } \{data\}}$$

7. As per rule 3 (R3)

$$\frac{\text{P}_j \text{believes D}_j \text{controls } \{data\}, \text{P}_j \text{believes D}_j \text{believes} \{data\}}{\text{P}_j \text{believes } \{data\}}$$

8. As per rule 4 (R4)

$$P_j \text{ believes } P_j \overset{CR_{D_j}}{\longleftrightarrow} D_j$$

9. P_j believes D_j believes $P_j \overset{CR_{D_j}}{\longleftrightarrow} D_j$

Because, P_j believes fresh (T_P), so we can acquire P_j believes fresh ($T_P + 1$).

Therefore, we can get P_j believes fresh ($\{T_P + 1\}\, CR_{P_j}$).

Because,

$$P_j \text{ believes } CR_{P_j}),\ P_j \text{ sees } \{T_D + 1\}\, CR_{D_j}).$$

10. According to rule 1 (R1)

$$P_j \text{ believes } D_j \text{ said } \{T_D + 1\}\ CR_{D_j}).$$

11. As per rule 2 (R2)

$$P_j \text{ believes } D_j \text{ believes } \{T_D + 1\}\ \ CR_{D_j}).$$

Finally, we can get

$$P_j \text{ believes } D_j \text{ believes } P_j \overset{CR_{D_j}}{\longleftrightarrow} D_j$$

Similarly, we can get

$$D_j \text{ believes } P_j \text{ believes } P_j \overset{CR_{P_j}}{\longleftrightarrow} D_j$$

C. FORMAL SECURITY VERIFICATION USING AVISPA TOOL

In this section, we have discussed about the widely used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, the security verification and the simulation results of the proposed EPAW method in AVISPA tool.

In the AVISPA tool, the High-Level Protocol Specification Language (HLPSL) is used to verify the designed protocol. First the HLPSL code is converted into the Intermediate Format (IF) then it is given to one of the four backend's (On-the-fly model checker, Constraint-Logic-based Attack Searcher, SAT-based Model- Checker and Tree Automata-based protocol analyzer) as input [34]. The IF produces the Output Format (OF). The OF gives a security verification result after the detailed analysis of the designed protocol. The OF consists of several divisions such as [34].

- SUMMARY: It gives the result as the designed protocol is safe or unsafe or the analysis is inconclusive.
- DETAILS: It gives a detailed explanation about why the designed protocol is safe or on what basis the designed protocol is unsafe or why it is inconclusive.
- PROTOCOL: It gives the detailed HLPSL specification of the designed protocol in the intermediate format.
- GOAL: It explains the goal (security verification of the designed protocol) which is being performed in the AVISPA tool.
- BACKEND: It gives the details of the backend (any one out of four) which is used for the security verification.
- STATISTICS & COMMENTS: This section gives a detailed explanation of the possible vulnerability to the designed protocols along with relevant comments.

```
% OFMC
% Version of 20012/07/20
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\program~5\SPAN\testsuite\results\device
_accesscontrol.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 57.42s
  visitedNodes: 27544 nodes
  depth: 6 plies
```

FIGURE 2. Security verification result in AVSPA (under OFMC backend).

For our proposed work, we have used the Security Protocol Animator (SPAN) for the simulation. The OFMC backend is used for taking simulation results. The simulation result is shown in Fig. 2.

D. SECURITY COMPARISON

In this section, the security properties of the proposed EPAW scheme are compared with existing schemes. Security property comparisons of different schemes are listed in Table 2.

The symbol ✓ indicates that the scheme under consideration satisfies the specific security property. The symbol × indicates that the scheme under consideration does not satisfy the specific security property. Hu *et al.* [35] and Cagalaban and Kim [36] scheme does not achieve privacy, anonymity and also they have unlinkability problem. Braeken *et al.* [37] scheme does not satisfy the confidentiality, nonrepudiation and unlinkability properties. Liu *et al.* [27] scheme has the confidentiality and unlinkability problem. The proposed EPAW scheme satisfies all the security properties under consideration.

VI. PERFORMANCE ANALYSIS

In this section, the performance of the proposed EPAW method is evaluated in terms of computational cost to verify the certificate, signature appended to the message and the communication cost.

A. COMPUTATIONAL COST COMPARISON

The computational cost is referred to the total time needed to verify both signature and certificate for user authentication and to verify the data integrity. The performance of the proposed EPAW method is compared with many other existing methods J. Liu et al. Scheme [27], Z. Zhao et al. Scheme [28],

TABLE 2. Comparison of security.

Security	Schemes				
	C.Hu et al.	G.Caga laban et al.	A.Brae ken et al.	J.Liu et al.	Propos ed
Authentication	✓	✓	✓	✓	✓
Confidentiality	✓	✓	×	×	✓
Data integrity	✓	✓	✓	✓	✓
Privacy preservation	×	×	✓	✓	✓
Anonymity	×	×	✓	✓	✓
Nonrepudiation	✓	✓	×	✓	✓
Replay attack	✓	✓	✓	✓	✓
Unlinkability	×	×	×	×	✓

TABLE 3. Computational cost to perform signature and the certificate verification process of different schemes.

Method	For verifying '1'signature and certificate	For verifying 'n' signature and certificate
J. Liu et al. Scheme	$4T_h + 5T_m + 3T_p$	$4nT_h + 5nT_m + (2n+1)T_p$
Z. Zhao et al. Scheme	$11T_h + 9T_m + 3T_{se}$	$11nT_h + 9nT_m + 3nT_{se}$
L. Wu et al. Scheme	$7T_h + 8T_m + T_p + 2T_{se}$	$7nT_h + 8nT_m + nT_p + 2nT_{se}$
J. Shen et al. Scheme	$9T_h + 13T_m$	$9nT_h + 13nT_m$
D. Boneh et al. Scheme	$2T_h + 4T_p$	$2nT_h + (2n+2)T_p$
Z. Gong et al. Scheme	$2T_h + 5T_p$	$2nT_h + (4n+1)T_p$
Proposed Scheme	$T_h + 2T_m + 2T_p$	$nT_h + 2nT_m + (1+n)T_p$

L. Wu et al. Scheme [29], J. Shen et al. Scheme [29], S. S. Al-Riyami et al. Scheme [20], X. Chen et al. Scheme [21], Z. Zhang et al. Scheme [24], D. Boneh et al. Scheme [31] and Z. Gong et al. Scheme [32]. Let T_p is the time needed to perform a pairing operation, T_h is the time taken to perform a one-time hash operation and T_m is the time needed to perform the point multiplication operation. The time is taken for performing the exponential operation in G_1 and G_2 are represented as T_{e1} and T_{e2}.

From Table 3, it is proved that the proposed EPAW method consumes a very low computational cost to perform the signature and certificate verification process compared with other existing methods. Since, the proposed EPAW method consumes only $2T_p$, $2T_m$ and T_h to perform a single signature and certificate verification process.

Hence, the proposed EPAW method takes 5.9 ms to verify a single signature and certificate comparing

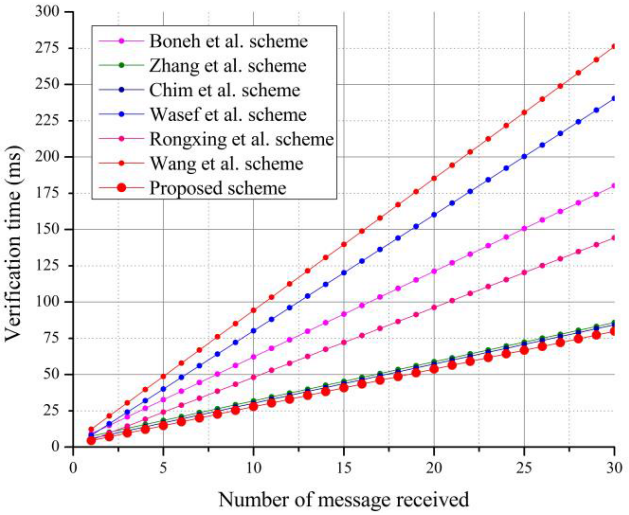

FIGURE 3. Signature and certificate verification time comparison.

with J. Liu et al. Scheme (15.6 ms), Z. Zhao et al. Scheme (30.06 ms), L. Wu et al. Scheme (20.74 ms), J. Shen et al. Scheme (24.31ms), D. Boneh et al. Scheme (11.8 ms), Z. Gong et al. Scheme (13.4 ms). It is observed that, in the signature and the certificate verification process T_p and T_h are the most time-consuming operation. The proposed EPAW method takes two pairing operations to verify the single signature and it takes $(1 + n)$ pairing operations to verify 'n' signatures. Hence, the proposed method consumes very less computational cost compared with other existing methods.

To determine the exact calculation time of the proposed anonymous mutual authentication method, we have chosen a 2-GHz computer system with 4-GB memory capacity, running Cygwin 1.7.35–15 [24] with the GCC version 4.9.2 for our proposed scheme. Each output is analyzed for more than 100 simulation runs and then the average values of the output are taken into account. In our simulation, the time parameters T_p, T_h and T_m are measured and it is calculated as 1.6 ms (milliseconds), 2.7 ms, and 0.001 ms, respectively. The time required to perform an exponential operation T_{e1} and T_{e2} is calculated as 0.7 ms and 0.6 ms respectively. Table 3, shows the computational cost of the signature and certificate process of J. Liu et al. Scheme, Z. Zhao et al. Scheme, L. Wu et al. Scheme, J. Shen et al. Scheme, D. Boneh et al. Scheme, Z. Gong et al. Scheme and proposed EPAW methods.

Fig.3 shows the received message (n) and its verification time in millisecond (ms). It is observed that, when 'n' is more, our proposed EPAW method is more efficient than the other existing methods and consumes very less time for the verification process, compared with other existing schemes.

From Fig. 3, it is very clear that the proposed EPAW method takes only takes 87.64 ms to verify 30 numbers of signatures and certificates comparing with J. Liu et al. Scheme (281.7 ms), Z. Zhao et al. Scheme (601.38 ms), L. Wu et al. Scheme (414.96 ms), J. Shen et al. Scheme (486.26 ms), D. Boneh et al. Scheme (175.2 ms), Z. Gong et al. Scheme (237.6 ms).

TABLE 4. Total computation time of various schemes.

Method	Time required to generate the signature and certificate	Time required to verify the signature and certificate
D. Boneh et al. Scheme	$13T_m + 6T_p$	$T_h + 11T_m + 3T_p$
Z. Gong et al. Scheme	$T_h + 2T_p + 4T_m$	$2T_h + 5T_p$
S. S. Al-Riyami et al. Scheme	$T_h + T_p + T_e + 2T_m$	$T_h + 4T_p + T_e + T_m$
X. Chen et al. Scheme	$T_h + 3T_m$	$T_h + 4T_p + T_e + 2T_m$
Z. Zhang et al. Scheme	$T_h + 3T_e$	$2T_h + 4T_p$
Proposed Scheme	$T_h + 4T_{e1} + T_{e2}$	$T_h + 2T_m + 2T_p$

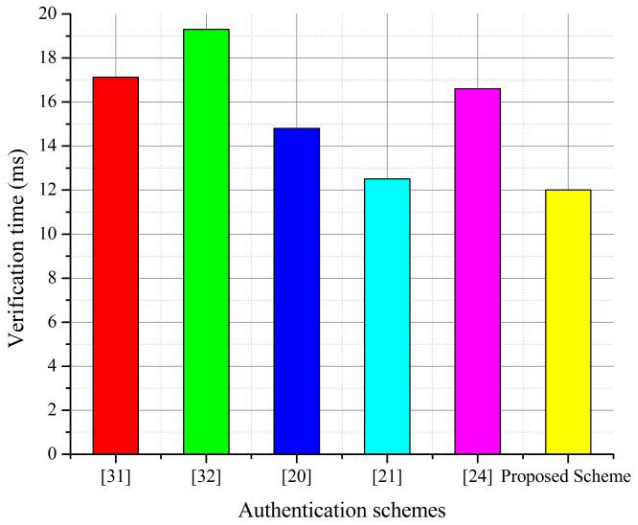

FIGURE 4. Total computational time of different authentication schemes.

To analyze the computational cost of anonymous authentication in EPAW, we have considered the computational cost as T_{gen}^{sen} and T_{verify}^{rec}. T_{gen}^{sen} is the time needed to produce one anonymous signature and certificate by the sender and T_{verify}^{rec} is the time needed to validate single anonymous certificate and signature by the receiver. For the proposed EPAW method, the total computational time (TCT) for the anonymous authentication T_{TCT} is calculated as:

$$T_{TCT} = T_{gen}^{sen} + T_{verify}^{rec}$$

In this study, TCT of the proposed method is compared with the existing method and it is tabulated in Table 4. From Fig. 4, we can see that the TCT of our EPAW is better than the other existing methods.

B. COMMUNICATION COST COMPARISON

To calculate the communication cost of the proposed scheme, we have assumed that $d = md = 160$ *bits*, the patient and doctors self generated certificate is $CR_{P_j} = CR_{D_j} = 160$ *bits*, the patient and doctors signature as $sign = sig = 160$ *bits*, the public keys of patient and doctors is $y_j = l_j = 320$ *bits*, the time stamp added by the patient and doctors is $T_P = T_D = 32$ *bits* and the license of doctors associated with the particular WBAN is $WL_{D_j} = 160$ *bits* [38]. In the proposed EPAW scheme, two messages $data = (d \parallel sign \parallel y_j \parallel CR_{P_j} \parallel T_P)$ and $data = (md \parallel sig \parallel l_j \parallel CR_{D_j} \parallel T_D \parallel WL_{D_j})$ are communicated between the patient and doctor for authentication. These two messages consume 832 bits (from patient to doctor) and 992 bits (from doctor to patient). Totally, the proposed EPAW scheme requires 1824 bits as a communication cost for a single communication. Communication cost comparison of EPAW scheme with other existing scheme are shown in Table 5. The total communication cost required for the D. Boneh et al. Scheme, Z. Gong et al. Scheme, S. S. Al-Riyami et al. Scheme, X. Chen et al. Scheme and the Z. Zhang et al. Scheme are 3842 bits, 3532 bits, 1536 bits, 3040 bits and 2112 bits respectively. The proposed EPAW scheme consumes second less communication cost compared with the other existing schems.

TABLE 5. Comparison of communication cost of various schemes.

Method	Number of Messages	Total Communication Cost (bits)
D. Boneh et al. Scheme	03	3842
Z. Gong et al. Scheme	03	3532
S. S. Al-Riyami et al. Scheme	02	1536
X. Chen et al. Scheme	03	3040
Z. Zhang et al. Scheme	02	2112
Proposed Scheme	02	1824

VII. CONCLUSION

In this study, a new EPAW scheme is proposed to provide secure and efficient data transmission in WBAN. In the EPAW scheme, doctors are anonymously authenticated by the controller efficiently before sending the patient health information. The EPAW scheme takes the very little cost for signature and certificate authentication and it is essential for the WBAN environment. Also, it gives an effective privacy and tracking system to disclose the actual identification of the malicious user to improve the WBAN performance. During the signatures, certificate verification and communication the proposed work performs better than that of existing works.

REFERENCES

[1] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Netw.*, vol. 140, no. 1, pp. 138–151, Jul. 2018.
[2] A. A. Omala, K. P. Kibiwott, and F. Li, "An efficient remote authentication scheme for wireless body area network," *J. Med. Syst.*, vol. 41, no. 2, Feb. 2017, Art. no. 25.
[3] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4777–4803, Nov. 2016.

[4] A. A. Omala, I. Ali, and F. Li, "Heterogeneous signcryption with keyword search for wireless body area network," *Secur. Privacy*, vol. 1, no. 5, p. e25, Sep. 2018.

[5] K. Suriyakrishnaan and D. Sridharan, "Reliable packet delivery in wireless body area networks using TCDMA algorithm for e-Health monitoring system," *Wireless Pers. Commun.*, vol. 103, no. 4, pp. 3127–3144, Dec. 2018.

[6] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 231–235, Feb. 2004.

[7] K.-A. Shim, "Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9211–9212, Oct. 2019.

[8] S. Jegadeesan, M. Dhamodaran, M. Azees, and S. S. Shanmugapriya, "Computationally efficient mutual authentication protocol for remote infant incubator monitoring system," *Healthcare Technol. Lett.*, vol. 6, no. 4, pp. 92–97, Aug. 2019.

[9] Y. Xie, S. Zhang, X. Li, Y. Li, and Y. Chai, "CasCP: Efficient and secure certificateless authentication scheme for wireless body area networks with conditional privacy-preserving," *Secur. Commun. Netw.*, vol. 2019, no. 1, pp. 1–13, Jun. 2019.

[10] X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang, and Y. Zhang, "CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2019.2927219.

[11] S. Jegadeesan, M. Azees, P. M. Kumar, G. Manogaran, N. Chilamkurti, R. Varatharajan, and C.-H. Hsu, "An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications," *Sustain. Cities Soc.*, vol. 49, no. 1, Aug. 2019, Art. no. 101522.

[12] X. Zhang, J. Zhao, L. Mu, Y. Tang, and C. Xu, "Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber–physical systems," *Pervas. Mobile Comput.*, vol. 56, pp. 18–28, May 2019.

[13] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1018–1025, Mar. 2013.

[14] S. Piramuthu, "Lightweight cryptographic authentication in passive RFID-tagged systems," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 38, no. 3, pp. 360–376, May 2008.

[15] E. Cesena, H. Löhr, G. Ramunno, A.-R. Sadeghi, and D. Vernizzi, "Anonymous authentication with TLS and DAA," in *Trust and Trustworthy Computing* (Lecture Notes in Computer Science), vol. 6101. Berlin, Germany: Springer-Verlag, Apr. 2010, pp. 47–62.

[16] M. Burmester, T. Van Le, B. De Medeiros, and G. Tsudik, "Universally composable RFID identification and authentication protocols," *ACM Trans. Inf. Syst. Secur.*, vol. 12, no. 4, pp. 1–33, Apr. 2009.

[17] P. Bichsel, J. Camenisch, T. Groß, and V. Shoup, "Anonymous credentials on a standard java card," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, May 2009, pp. 600–610.

[18] F. Armknecht, L. Chen, C. Wachsmann, and A.-R. Sadeghi, "Anonymous authentication for RFID systems," in *Radio Frequency Identification: Security and Privacy Issues* (Lecture Notes in Computer Science), vol. 6370. Berlin, Germany: Springer-Verlag, May 2010, pp. 158–175.

[19] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 196. Berlin, Germany: Springer-Verlag, Apr. 1984, pp. 47–53.

[20] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology—ASIACRYPT* (Lecture Notes in Computer Science), vol. 2894. Berlin, Germany: Springer-Verlag, May 2003, pp. 452–473.

[21] X. Chen, F. Zhang, and K. Kim, "A new ID-based group signature scheme from bilinear pairings," in *Proc. WISA*, in Lecture Notes in Computer Science, vol. 2908. Berlin, Germany: Springer-Verlag, Jun. 2003, pp. 585–592.

[22] X. Li, K. Chen, and L. Sun, "Certificateless signature and proxy signature schemes from bilinear pairings," *Lithuanian Math. J.*, vol. 45, no. 1, pp. 76–83, Jan. 2005.

[23] M. C. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *Computational Intelligence and Security* (Lecture Notes in Computer Science), vol. 3802. Berlin, Germany: Springer-Verlag, May 2005, pp. 110–116.

[24] *Cygwin: Linux Environment Emulator for Windows*. Accessed: Dec. 3, 2019. [Online]. Available: http://www.cygwin.com/

[25] C. J. Wang, D. Y. Long, and Y. Tang, "An efficient certificateless signature from pairings," *Int. J. Netw. Secur.*, vol. 8, no. 1, pp. 96–100, Jan. 2009.

[26] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, Sep. 2004.

[27] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Trans. Parallel Distrib. Syst*, vol. 25, no. 2, pp. 332–342, Feb. 2014.

[28] Z. Zhao, "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 38, no. 2, Feb. 2014, Art. no. 13.

[29] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *J. Med. Syst.*, vol. 40, no. 6, Jun. 2016, Art. 134.

[30] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *J. Netw. Comput. Appl.*, vol. 106, no. 1, pp. 117–123, Mar. 2018.

[31] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer-Verlag, 2003, pp. 416–432.

[32] Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificateless aggregate signatures from bilinear maps," in *Proc. 8th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/ Distrib. Comput. (SNPD)*, vol. 3, Jun. 2007, pp. 188–193.

[33] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[34] AVISPA. (2019). *Automated Validation of Internet Security Protocols and Applications*. Accessed: Oct. 2019. [Online]. Available: http://www.avispa-project.org/

[35] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 37–46, Sep. 2013.

[36] G. Cagalaban and S. Kim, "Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption," in *Proc. 13th Int. Conf. Adv. Commun. Technol.*, Seoul, South Korea, Feb. 2011, pp. 863–867.

[37] A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "EDAAAS: Efficient distributed anonymous authentication and access in smart homes," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 12, Dec. 2016, Art. no. 155014771668203.

[38] X. Zeng, G. Xu, X. Zheng, Y. Xiang, and W. Zhou, "E-AUA: An efficient anonymous user authentication protocol for mobile IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1506–1519, Apr. 2019.

SUBRAMANI JEGADEESAN received the B.E. degree in electronics and communication engineering from Periyar University, Salem, India, in 2004, the M.E. degree in communication systems from the Anna University of Technology, Coimbatore, India, in 2009, and the Ph.D. degree from the Faculty of Information and Communication Engineering, Anna University, Chennai, in 2016. He is currently an Associate Professor with the M. Kumarasamy College of Engineering, Karur, India. His main thirst research areas include energy management in wireless sensor networks and network and information security.

MARIA AZEES received the B.E. degree in electronics and communication engineering and the M.E. degree in applied electronics from the St. Xavier's Catholic College of Engineering, Nagercoil, India, which is affiliated under Anna University, Chennai, India, in 2011 and 2013, respectively, and the Ph.D. degree in the faculty of information and communication engineering from Anna University, Chennai, in 2017. He is currently a Senior Assistant Professor with the GMR Institute of Technology, Rajam, India. He has already published the research articles in some of the reputed journals, such as the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *Cluster Computing* (springer), and *IET intelligent transport systems*. His research interests include security in wireless sensor networks and VANETs.

N. RAMESH BABU received the B.E. degree in electrical and electronics engineering from Bharathiyar University, the M.E. degree in applied electronics from Anna University, and the Ph.D. degree from VIT University. He is currently a Professor and the Principal with the M. Kumarasamy College of Engineering, Karur, India. He has authored or coauthored more than 60 publications in reputed international journals and conferences. His research areas include wind speed forecasting, optimal control of wind energy conversion systems, solar energy, power electronics, and application of soft computing techniques in electrical engineering. He is an Associate Editor of IEEE Access Journal and also an Editorial Board Member of three other journals.

UMASHANKAR SUBRAMANIAM (Senior Member, IEEE) worked as an Associate Professor and the Head with VIT Vellore and a Senior R&D and Senior Application Engineer in the field of power electronics, renewable energy, and electrical drives. He is currently an Associate Professor with the Renewable Energy Laboratory, College of Engineering, Prince Sultan University, Saudi Arabia. He has more than 15 years of teaching, research and industrial R&D experience. Under his guidance 24 P.G students and more than 25 U.G students completed the senior design project work, and also, six Ph.D. scholars completed doctoral thesis as a Research Associate. He is also involved in collaborative research projects with various international and national level organizations and research institutions. He has published more than 250 research papers in national and international journals and conferences. He has also authored/coauthored/contributed 12 books/chapters and 12 technical articles on power electronics applications in renewable energy and allied areas. He is a member of IACSIT, IDES, and ISTE. He received the Danfoss Innovator Award-Mentor, from 2014 to 2015 and from 2017 to 2018. and the Research Award from VIT University, from 2013 to 2018. He received the INAE Summer Research Fellowship for the year 2014. He has taken charge as the Vice Chair of the IEEE Madras Section and the Chair of the IEEE Student Activities, from 2018. From 2014 to 2016, he was an Executive Member of the IEEE MAS Young Professional, IEEE Madras Section, where he has been the Vice Chair since 2017. He is an Editor of *Heliyon* (Elsevier).

DHAFER ALMAKHLES (Member, IEEE) received the B.E. degree in electrical engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in 2006, and the master's degree (Hons.) and the Ph.D. degree from The University of Auckland, New Zealand, in 2011 and 2016, respectively. Since 2016, he has been with Prince Sultan University, Saudi Arabia. He is currently an Assistant Professor with the Department of Communications and Networks Engineering. He is also the Director of Science and Technology Unit and the Leader of the Renewable Energy Laboratory, PSU. He has authored many published articles in the area of control systems. He served as a Reviewer for many journals including the IEEE Transactions on Fuzzy Systems, *Control of Network Systems*, *Industrial Electronics*, *Control Systems Technology*, the IEEE Control Systems Letters, and the *International Journal of Control*. His research interests include the hardware implementation of control theory, signal processing, networked control systems, nonlinear control design, unmanned aerial vehicle (UAV), and renewable energy.