Secure Equality Test Technique Using Identity-Based Signcryption for Telemedicine Systems
Mohammed Ramadan©, Member, IEEE, and Shahid Raza®, Senior Member, IEEE

Abstract—For telemedicine, wireless body area network (WBAN) offers enormous benefits where a patient can be remotely monitored without compromising the mobility of remote treatments. With the advent of high capacity and reliable wireless networks, WBANs are used in several remote monitoring systems, limiting the COVID-19 spread. The sensitivity of telemedicine applications mandates confidentiality and privacy requirements. In this article, we propose a secure WBAN-19 telemedicine system to overcome the pervasiveness of contagious deceases utilizing a novel aggregate identity-based signcryption scheme with an equality test feature. We demonstrate a security analysis regarding indistinguishable adaptive chosen-ciphertext attack (IND-CCA2), one-way security against adaptive chosen-ciphertext attack (OW-CCA2), and unforgeability against adaptive chosen-message attack (EUF-CMA) under the random oracle model. The security analysis of the scheme is followed by complexity evaluations where the computation cost and communication overhead are measured. The evaluation demonstrates that the proposed model is efficient and applicable in telemedicine systems with high-performance capacities.

Index Terms—Equality test, identity-based cryptography (IBC), signcryption, telemedicine, wireless body area networks (WBANs).

I. INTRODUCTION

The ongoing COVID-19 pandemic is one of many other world crises, such as global warming and economic crises, that are required extensive research work to be solved or mitigated. Technology has been involved in many life aspects, and information and communication technology (ICT) tools and innovations are developed since the beginning of this pandemic. Future emerging technologies, such as wireless body area networks (WBANs), wireless sensor networks (WSNs), and the Internet of Things (IoT) have been adopted widely as critical strategic solutions [1].

Telemedicine is a term invented in the 1970s that means “healing at a distance.” In 2007, the World Health Organization (WHO) standardized the definition of telemedicine as follows: “the delivery of healthcare services, where distance is the key factor, by all healthcare professionals using ICT to deal with medical information, including diagnosis, treatment, and prevention of diseases” [2]. Technically, telemedicine is a technology-based medical system that uses technical devices to allow remote healthcare data access securely. Thus, to enable periodic monitoring and continuous follow-up by sending sensitive health-related data collected using different WBAN nodes and implanted sensors in the body; to help decide if there is an urgent need for medical intervention. The diagnostic tools are essential due to the wide deployment and development of digital technologies. These monitoring services can be further improved by employing a wireless network that connects body sensors/nodes with remote healthcare providers through WBANs. Note that telemedicine refers to remote clinical services while telehealth for remote nonclinical services [3].

WBAN is a commonly implemented technique for remote monitoring, diagnoses, and intervention of patient health-related information via WBAN nodes such as embodied sensors. The key challenge with deploying emerging technologies within healthcare systems such as WBAN is to provide concrete security, including privacy preserving, confidentiality, integrity, and authentication is a significant challenge when deploying emerging technologies in healthcare systems. Security techniques and countermeasures are essential to efficiently address these concerns by considering all the limitations of implementing remote healthcare systems [4].

WBANs consist of various biological devices and sensors connected inside/around the body and can be wearable or in the surrounding area. These devices must have specific requirements for different purposes [5]. For instance, some devices can measure and monitor health conditions and physical symptoms, such as blood pressure, body temperature, heartbeats rate, respiratory rate, electrocardiogram (ECG), electromyogram (EMG), electroencephalogram (EEG), and blood glucose pollution level. The other devices/sensors for detecting responses to physiological and mental-related behaviors, such as fear, anxiety, and stress [6]. For the type of collected data, WBAN nodes manage to send the patient’s data to the corresponding physicians to provide real-time medical and diagnoses. Biokinet sensor collect human body movement-related data, while ambient sensors collect surrounding and ecological-related data [7]. See Fig. 1 for the overall WBAN model description.
As the patients of COVID-19 reach hospitals after diagnosis, they need close follow-up and monitoring to detect any deterioration or changes in their health condition. The healthcare professionals can then decide if there is a need for medical interventions, such as oxygen supplements or mechanical ventilation. Main symptoms, such as body temperature, pulse rate, blood pressure, level of awareness, repeated shaking, and chills are essential in the follow-up process. This collected data from patients required close contact with the patient’s body and the risk of infection exposure. Therefore, this article proposes a secure approach scheme for telemedicine systems providing secure remote diagnosis and follow-up techniques that can support the healthcare sector in maintaining social distancing and reduce the cost of personal protective equipment (PPE) [8].

The proposed WBAN-19 solution enables remote access to medical information and creates a wireless connection between the diagnosed medical data and the healthcare provider through WBAN sensors and to overcome the pervasiveness of COVID-19 [9]. The medical data must be secure, accurate, and preserve the privacy of patients’ information. Hence, security and privacy-preserving protocols are highly required to protect this sensitive medical information [10].

A. Related Work

Shamir [11] introduced identity-based cryptography (IBC), which solves the key management issues by eliminating the certificate authority (CA) and the public-key digital certificates. The user generates the public key using some of the user’s identity-related information that are publicly known. A trusted third party so-called private key generator (PKG) secretly generates the corresponding private keys for all users using a secret master key.

Boneh et al. [12] proposed an aggregate signature scheme that combines multiple signatures initiated by several users on different messages into a single aggregated short signature. The validation of this aggregate signature corresponds to the verification of every single signature used to generate the aggregated signature, i.e., the aggregated signature is valid if and only if all other signatures are valid and each signer signed its original message individually. The aggregation technique reduces resource usage regarding storage space and transmission capacity. Thus, it can be a significant use-case for resources-constrained systems. The first identity-based aggregate signcryption with formal security proof is given by Selvi et al. [13].

The first public key encryption with an equality test (PKEET) was introduced by Yang et al. [14], which is a public key encryption (PKE) scheme that enables an equality test process on encrypted data using public keys. In PKEET schemes, each user generates a trapdoor for equality tests to a third party called the equality tester (ET), which checking the equality among several ciphertexts without disclosing confidential information.

Lee et al. [15] presented a semi-generic PKE and an identity-based encryption scheme with an equality test technique. This approach considers some kind of access control for equality test over ciphertexts, and they only consider IND-CCA2 security for the PKE schemes in the random oracle model (ROM) under the hard assumptions of computational Diffie–Hellman (CDH) problems.

Wu et al. [16] researched and proposed an identity-based encryption scheme with an equality test technique for cloud computing systems. This scheme has a reasonably low computational cost Hash-To-Point function and claimed secure for one-way chosen identity and ciphertext attacks (OW-ID-CCA).

Shen et al. [17] proposed a secure and efficient identity-based aggregate signature scheme for WSNs that provides a data-integrity feature with respect to designated verification for WSN nodes. This scheme has relatively low computation and communication complexity, and it is claimed secure under the ROM.

Abouelkheir and El-Sherbiny [18] proposed a secure identity-based pairing-free aggregate signcryption scheme over the elliptic curve cryptographic (ECC). This proposed scheme is considered secure under the ROM providing confidentiality and unforgeability security requirements.

Finally, Xiong et al. [19] proposed a scheme to secure message classification services through identity-based signcryption with an equality test for the Internet of Vehicles (IoV). This scheme combines identity-based signcryption with an equality test feature (IBSC-ET). They set the cloud server to perform
the equality test process between two signcrypted ciphertexts using the same or different public keys. This scheme is considered secure using the ROM under the Diffie–Hellman hard assumptions.

Recently, many proposed approaches have been designed to provide identity-based encryption, equality test, aggregation, and signcryption techniques [20], [21], [22], [23], [24], [25], [26], [27], [28]. However, in this section, we only covered some of the more related to our proposed scheme.

**B. Our Contributions**

The proposed WBAN-19 solution provides a secure and efficient solution for the healthcare systems to overcome the spreading of the COVID-19 pandemic. The scheme remotely monitors and diagnoses the health conditions of COVID-19 cases by using the equality test feature under aggregate Identity-based signcryption. To our knowledge, there is no proposed scheme for telemedicine systems that is provably secure and can provide an aggregate signcryption with equality test feature under aggregate monitors and diagnoses the health conditions of COVID-19 spreading of the COVID-19 pandemic. The scheme remotely provides identity-based encryption, equality test, aggregation, and signcryption techniques [20], [21], [22], [23], [24], [25], [26], [27], [28]. However, in this section, we only covered some of the more related to our proposed scheme.

1) The proposed WBAN-19 scheme is a concrete solution for observing patients’ health conditions and suspicious cases based on COVID-19 symptoms and reporting them to the corresponding authorities. Also, the solution can provide an extensive healthcare system by observing and monitoring any diagnostic parameters.

2) The proposed WBAN-19 model provides an aggregated cryptosystem that supports the relevant medical authorities in achieving an equality test on ciphertexts through the trapdoor-test algorithm with authentication (signing algorithm) and confidentiality (encryption algorithm). The proposed approach is appropriate for monitoring and diagnosing contagious diseases, such as COVID-19 without revealing sensitive information or compromising users’ privacy.

3) We provide a complete performance evaluation analysis compared to other proposed schemes. The security analysis articulates that our scheme is secure against IND-ASC-CCA2, one-way security against adaptive chosen-ciphertext attack (OW-CCA2), and unforgeability against adaptive chosen-message attack (EUF-CMA) in the ROM.

4) Also, the evaluation affirms that the proposed approach is efficient, secure, and provides reasonable communication and computation cost.

5) Finally, the analysis comparisons and discussions demonstrate that our proposed scheme is secure, flexible, reliable, and compatible with telemedicine systems.

**C. Paper Organization**

The remainder of this article is organized as follows. Section II reviews some basics preliminaries and general notions related to the proposed scheme. Section III demonstrates the proposed system models and security definitions. In Section IV, we construct our proposed WBAN-19 scheme with detailed steps. In Section V, we provide a comprehensive security analysis for the proposed scheme. Subsequently, Section VI showed the performance evaluation of the proposed scheme with some comparisons and analysis. Finally, we summarized our article as a conclusion in Section VII.

**II. Preliminaries**

This section provides basic definitions, including bi-linear pairing and some hard assumptions.

**A. Bilinear Pairing**

Let $G_1$ and $G_2$ denote two cyclic groups whose orders are prime $p$. Let $R$ be a generator in $G_1$. A map $e : G_1 \times G_1 \rightarrow G_2$ is called a bi-linear pairing if it fulfills the following properties.

1) **Bilinearity:** For all $R, P \in G_1$ and $x, y \in \mathbb{Z}_p^*$, $e(xR, yP) = e(R, P)^{xy}$.

2) **Nondegeneracy:** $R, P \in G_1$ such that $e(R, P) \neq 1$.

3) **Computability:** For all $R, P \in G_1$, there always exists an algorithm to efficiently compute $e(R, P)$.

**B. Decision Diffie–Hellman Problem (DDH)**

Given $(g, g^x, g^y, Z) \in G_2$, where $x$ and $y$ are chosen randomly $x, y \in \mathbb{Z}_p^*$, the decision Diffie–Hellman problem (DDH) problem is to decide whether $Z = g^{xy}$.

There no exists a probabilistic polynomial-time algorithm to solve the DDH assumption with a nonnegligible probability.

**C. Computational Diffie–Hellman Problem**

Given $(P, xP, yP) \in G_1$, where $x$ and $y$ are chosen randomly $x, y \in \mathbb{Z}_p^*$, the computational Diffie–Hellman problem (CDHP) problem is to compute $xyP$.

There no exists a probabilistic polynomial-time algorithm to solve the CDHP assumption with a nonnegligible probability.

**D. Computational Bilinear Diffie–Hellman Problem**

Given $(P, xP, yP, zP) \in G_1$, where $x, y, z$ are chosen randomly $x, y, z \in \mathbb{Z}_p^*$, the computational bilinear Diffie–Hellman problem (CBDHP) problem is to compute $e(P, P)^{xyz}$.

There no exists a probabilistic polynomial-time algorithm to solve the CBDHP assumption with a nonnegligible probability.

**III. WBAN-19: Models Description**

**A. COVID-19 Application Model**

This section introduces the models description of our proposed WBAN-19 scheme which offers a secure lightweight cryptosystem with the equality test technique. It involves of logical multisteps algorithms as follows.

First, the medical sensors sense the patient body’s essential signals for medical checks. Then, the information gathered by WBAN sensors is encrypted (using an encrypted algorithm) and signed (using a signing algorithm), then transferred in an aggregated form (using an aggregation algorithm) to the medical server for processing this data. As described in Fig. 3, and after receiving the data, the medical server compares the equality of incoming data without revealing any sensitive information (using an equality test algorithm). If no symptoms
are detected in the patient’s health condition, then the system will respond by aborting the algorithm. The scheme concludes with another message sent to the medical server with the signcrypted message and later sent to be verified and decrypted in case of some symptoms are detected (checking the equality test) and required physicians intervention. Note that only end-users, i.e., patients and physicians could reveal medical sensitive information after the equality test process in case of potential symptoms.

On March 2020, the WHO declared COVID-19 a global pandemic. COVID-19 has varied from simple to mild symptoms to severe illness and mortality. According to the WHO, the most prevalent symptoms that are associated with COVID-19 include [29]:
1) fever;
2) cough;
3) shortness of breath.
These symptoms may become more severe in some people. The complete list of symptoms is still being investigated. Thus, doctors are learning new things about this virus every day. The following are some other symptoms of COVID-19.
1) Persistent pain or pressure in the chest.
2) Blue lips or face.
3) Excessive drowsiness.
4) Confusion.
Recently, we learned that COVID-19 might not first cause any symptoms for some people; and people may carry the virus for days or up to two weeks before noticing any symptoms. Therefore, it is important to observe other general signs to overcome the pervasiveness of the pandemic [30].

The proposed WBAN-19 solution is based on equality test comparisons among a set of parameters \(S_1, \ldots, S_8\); which are the (diagnosed values) sent by entities, and a set of parameters \(P_1, \ldots, P_8\); which are the values stored in the medical server at the hospital for (normal case values), with a threshold value to separate between normal health conditions and the critical ones. Fig. 2 shows the handshaking process for our proposed protocol. Note that a third party (PKG) is trusted for the signcryption process to generate the system parameters. In contrast, the third party (medical server) is non-trusted on the medical provider side to perform the equality test without revealing any medical data. The proposed security model is compatible with telemedicine systems for the following reasons: Using identity-based construction gives our proposed model more flexibility to be implemented in real use-case scenarios. The proposed models’ description shows more compatibility with telemedicine systems by using WBANs architecture. The complexity analysis shows more reliability to implement the proposed scheme within any real use-case scenarios. Finally, the comparison analysis shows the efficiency of our scheme compared to some other approaches.

### B. System Model

The proposed WBAN-19 model is an aggregated identity-based signcryption with a secure equality test technique for monitoring and observing the sensitive medical data. It consists of seven algorithms: 1) \(\text{Setup}\); 2) \(\text{KeyGen}\); 3) \(\text{Signcrypt}\); 4) \(\text{Aggregate}\); 5) \(\text{Unsigncrypt}\); 6) \(\text{Trapdoor}\); and 7) \(\text{Test}\). The public keys are the hash values of users’ identities, and all users can compute them. A trusted third party (PKG) calculates the private keys using the secret master key. Then, the private keys are generated and sent to the corresponding users by the PKG entity.

The general scheme description is as follows.

**Setup:** This algorithm runs by the security server, and it is a function in the secret parameters over identity-based cryptosystems.

<table>
<thead>
<tr>
<th>Physical Parameters</th>
<th>Diagnosed Values</th>
<th>Hospital Values</th>
<th>WBAN-19 Nodes/Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Body temperature</td>
<td>(S_1)</td>
<td>(P_1)</td>
<td>(N_1): Physiological Sensors</td>
</tr>
<tr>
<td>Heart rate</td>
<td>(S_2)</td>
<td>(P_2)</td>
<td>(N_2): Bio-sensors</td>
</tr>
<tr>
<td>Blood pressure</td>
<td>(S_3)</td>
<td>(P_3)</td>
<td>(N_3): Biokinetic Sensors</td>
</tr>
<tr>
<td>Respiratory rate</td>
<td>(S_4)</td>
<td>(P_4)</td>
<td>(N_4): Wearable Devices</td>
</tr>
<tr>
<td>Electromyogram (EMG)</td>
<td>(S_5)</td>
<td>(P_5)</td>
<td>(N_5): Body/Embodied Sensors</td>
</tr>
<tr>
<td>Electrocardiogram (ECG)</td>
<td>(S_6)</td>
<td>(P_6)</td>
<td>(N_6): RFID/Implanted Chips</td>
</tr>
<tr>
<td>Electroencephalogram (EEG)</td>
<td>(S_7)</td>
<td>(P_7)</td>
<td>(N_7): IEEE802.15.6 WSN Nodes</td>
</tr>
<tr>
<td>Blood glucose pollution level</td>
<td>(S_8)</td>
<td>(P_8)</td>
<td>(N_8): Smartphone Apps</td>
</tr>
</tbody>
</table>
**KeyGen:** This algorithm inputs system parameters and generates a pair of public/private keys.

**Signcrypt:** The user inputs system parameters, message \( M \), and the corresponding public/private keys as input and returns the signcrypted message.

**Aggregate:** This algorithm takes system parameters signcrypted messages and aggregates all signcrypted messages from all users combined.

**Unsigncrypt:** This algorithm takes system parameters, signcrypted messages, and the corresponding public/private keys; it performs the verification process.

**Trapdoor:** This algorithm runs by the users (physician/patient), and it is a function in the security parameters and the private key (secret key); it returns the corresponding trapdoor.

**Test:** This algorithm runs by the ET (security server), and it checks the health-related values as encrypted texts; it performs the equality test process. The equality test algorithm will check the health-related values as encrypted messages. This will be for the plaintext without revealing any ciphertexts as follows.

\[ S_1 \text{ is the first symptom, e.g., fever, the temperature for suspicious cases will be above 38}^\circ, \text{ and the normal temperature is } P_1 \leq 38^\circ. \]

\[ \text{Trapdoor}(S_1) = \text{Trapdoor}(P_1) \text{ holds.} \]

If yes, then abort, and report it as a normal case. Otherwise, check other symptoms.

\[ \text{Trapdoor}(S_1, \ldots, S_8) = \text{Trapdoor}(P_1, \ldots, P_6) \text{ holds.} \]

If yes, report it as a suspicious COVID-19. Otherwise, report it as a confirmed COVID-19 case.

### C. Security Model

This section defines the security models of the proposed WBAN-19 scheme. According to the NIST guidelines for the security assessment of communication protocols, three security models, namely OW-IND-ASC-CCA2, OW-IND-ASC-CCA2, and OW-IND-ASC-CCA2, are considered to prove the security of a protocol. The WBAN-19 scheme is OW-IND-ASC-CCA2 in the random oracle. The definition can be demonstrated by the following game:

**Definition 1:** The proposed WBAN-19 scheme is secure against IND-ASC-CCA2 in the random oracle if the advantage of \( A_1 \) to win against our proposed scheme is negligible. This definition can be demonstrated by the following game.

1. **Setup:** It runs by Ch to set the public parameters \( \text{params} \) and the master secret key \( s \). Ch gives \( \text{params} \) to \( A_1 \) and keeps \( s \) secret.
2. **Phase 1:** \( A_1 \) can adaptively have access to the following oracles.
3. **KeyGen-Queries:** \( A_1 \) makes a query in \( ID_i \), Ch answers with the corresponding private key \( X_{ID_i} \) to \( A_1 \).
4. **Unsigncrypt-Queries:** \( A_1 \) makes a query in the message \( M_i \) and the identities \( (ID_{iA}, ID_{iB}) \). \( A_1 \) sends the signcryption \( C_i \); it is valid, then Ch answers with the corresponding message \( M_i \).
5. **AggregateUnsigncrypt-Queries:** \( A_1 \) sends the aggregate signcryption \( C_{agg} \); if it is valid, then \( A_1 \) answers with all the corresponding messages \( M_i \), for \( (i = 1, 2, \ldots, n) \).
6. **Challenge:** After running the above queries adaptively, \( A_1 \) sends \( (M_0, M_1), (ID_A, ID_B) \) for \( (i = 1, 2, \ldots, n) \), then Ch checks if \( ID_B \) is one of the targeted identities. If not, Ch accepts. Otherwise, Ch chooses a random \( b_i \in \{0, 1\} \), for \( (i = 1, 2, \ldots, n) \) and signcrypts \( M_{b_i} \) using the sender’s private key \( X_{IDA} \) and the receiver's public key \( Q_{IDB} \), then Ch answers with the aggregate signcryption \( C_{agg} \) to \( A_1 \).
7. **Phase 2:** Same as in (Phase 1) except that \( A_1 \) cannot make unsigncrypt-query on the challenge aggregate signcryption \( C_{agg} \).
8. **Output:** \( A_1 \) outputs \( b'_i \) for \( (i = 1, 2, \ldots, n) \). \( A_1 \) wins the game if \( b'_i = b_i \) for \( (i = 1, 2, \ldots, n) \). The advantage of \( A_1 \) winning the game is negligible.

**Definition 2:** The plaintext remains secure knowing the trapdoor and the adversary's corresponding ciphertext. Accordingly, the WBAN-19 scheme is OW-CCA2 in the random oracle if the advantage of \( A_2 \) to win against our scheme, i.e., \( \Pr[M = M'] \) is negligible. This definition can be demonstrated by the following game.
1) Setup: Ch takes a security parameter $k$ as input to generate the system parameter params and sends it to $A_2$, then keeps the master key $s$ secure.

2) Phase 1: $A_2$ can adaptively have access to the following oracles.

3) KeyGen-Queries: Ch runs the KeyGen algorithm to generate the private key $X_{ID_i}$. Then, Ch sends it to $A_2$.

4) Trapdoor-Queries: Ch can get $X_{ID_i}$ and generate the corresponding trapdoor by executing the Trapdoor algorithm from the KeyGen-queries. Then, Ch sends it to $A_2$.

5) Unsigncrypt-Queries: Ch runs the Unsigncrypt algorithm. Then, Ch sends the plaintext $M_i$ to $A_2$.

6) Challenge: Ch chooses a plaintext $M^* \in M$ randomly and runs the Signcrypt algorithm to get the corresponding ciphertext $C$. Then, Ch sends it to $A_2$.

7) Phase 2: Ch answers similarly to Phase 1, except that $A_2$ cannot make queries on the secret key and the plaintext.

Definition 3: The proposed WBAN-19 scheme is secure against existentially EUF-CMA in the random oracle if the advantage of $A_3$ to win against our proposed scheme is negligible. This definition can be demonstrated as follows.

1) Setup: Ch runs the Setup algorithm to produce the system parameters params and sends it to $A_3$ while keeping the master key ($s$) secure.

2) KeyGen-Queries: $A_3$ creates queries on $ID_i$, then Ch sends the corresponding private key $X_{ID_i}$ to $A_3$.

3) Queries: The adversary can adaptively issue the following queries.

4) Signcrypt-Queries: $A_3$ can adaptively make queries on the signcryption of message $M_i$, then Ch sends the corresponding signcryption $C_{agg}$ to $A_3$.

5) Unsigncrypt-Queries: $A_3$ can adaptively query the signcrypted message $C_{agg}$, then Ch sends $M_i$ to $A_3$.

6) Output: $A_3$ outputs $ID^*$ with $C_{agg}^*$. If the result of the Unsigncrypt is valid, then $A_3$ wins the game with a negligible advantage.

IV. WBAN-19: SCHEME CONSTRUCTION

This section presents our proposed WBAN-19 scheme based on an identity-based cryptosystem with an aggregate signcryption with equality test features for the adequate security of remote medical monitoring systems. The private key is generated by a trusted third party (PKG) using the secret master key then sent to the corresponding users via a secure channel. The public key is the digest of the corresponding user’s identity and it is publicly known. Note that:

Entity A: WBAN-19 Nodes (Patients);
Entity B: WBAN-19 Nodes (Physician);

A. Scheme Description

The WBAN-19 scheme consists of seven algorithms:

1) Setup
2) KeyGen
3) Signcrypt
4) Aggregate
5) Unsigncrypt
6) Trapdoor
7) Test. The detailed description of our proposed scheme is as follows.

B. Correctness

The consistency of our proposed scheme can be demonstrated as follows.

1) Signcryption: $R'_i = e(X_{ID_i}, U_i)$
= e(sQ_{IDi}, r_iP) \\
= e(Q_{IDi}, r_iP_0) = R_i \\
M'_i = V_i ⊕ H_2(R_i) = H_2(R_i) ⊕ M_i ⊕ H_2(R_i) = M_i. \\
Then,
\[
e(W_{agg}, P) = e(\sum W_i, P) \\
= e(\sum r_i H_1(M_i) + H_3(U_i) · X_{IDi}, P) \\
= e(\sum r_i H_1(M_i) + H_3(U_i) · sQ_{IDi}, P) \\
= e(\sum r_i H_1(M_i), P) · e(\sum H_3(U_i) · sQ_{IDi}, P) \\
= \prod e(U_i, H_1(M_i)) · e(\sum H_3(U_i) · Q_{IDi}, P_0). \\
\]

2) **Equality Test:** 
\[
E_i = Z_i ⊕ H_2(e(U_i, T_{IDi})). \\
= (r_i · M_i) ⊕ H_2(R_i)^{\theta_i} ⊕ H_2(e(U_i, T_{IDi})). \\
= (r_i · M_i) ⊕ H_2(R_i)^{\theta_i} ⊕ H_2(e(U_i, X_{IDi})). \\
= (r_i · M_i) ⊕ H_2(e(U_i, X_{IDi})^\theta_i) ⊕ H_2(e(U_i, X_{IDi})^{\theta_i}). \\
= r_iM_i.
\]

V. WBAN-19: Security Analysis

The security model for our proposed WBAN-19 is an aggregate identity-based signcryption scheme with an equality test feature for secure medical monitoring systems. The following theorems present the security proof. Note: Ch denotes the Challenger. A_1, A_2: represent the Adversaries.

**Theorem 1:** The proposed WBAN-19 scheme is secure against indistinguishable adaptive chosen-ciphertext attack (IND-ASC-CCA2) in the ROM; if the CBDHP assumption holds.

**Proof:** Assume A_1 is an adversary against our scheme, and there exists a challenger Ch claims to solve the CBDHP problem in polynomial time and with a nonnegligible advantage. Thus, A_1 and Ch perform the following game.

1) **Setup:** The Challenger Ch runs this algorithm and generates the public parameters (params) as follows. Ch Chooses two groups, G_1 and G_2, then computer P_0 = sP and sends params to A_1.

2) **Phase 1:** For all the adversary queries, Ch answers as follows.

a) **H_1-Queries:** Ch selects Θ ∈ Z_q, such that 1 ≤ Θ ≤ q_{H_1}. A performs the Θth query on the targeted identity ID_{O_i}. If i = Θ, then Ch picks random value a_i ∈ Z_q and answers to A_1 with Q_{ID_i} = a_iβP. If i ≠ Θ, then Ch sets Q_{ID_i} = a_iP, and replies to A_1 with Q_{ID_i}. Ch adds (a_i, Q_{ID_i}, ID_i) into the list H_1-List.

b) **H_2-Queries:** Ch checks if R_i exists in H_2-List. If yes, Ch responds with μ_i = H_2(R_i) to A_1. Otherwise, Ch picks μ_i ∈ {0, 1}^* randomly and sends μ_i = H_2(R_i) to A_1, then adds (R_i, μ_i) into the list H_2-List.

c) **H_3-Queries:** Ch checks if U_i exists in H_3-List. If yes, then Ch responds with d_i = H_3(U_i) to A_1. Otherwise, Ch picks d_i ∈ Z_q randomly and sends d_i = H_3(U_i) to A_1, then adds (U_i, d_i) into the list H_3-List.

d) **KeyGen-Queries:** When receiving a query with X_{ID_i}. Then, Ch checks if i = Θ, Ch aborts. Otherwise, Ch recovers a_i from H_1-List, computes X_{ID_i} = a_iP_0, then sends X_{ID_i} to A_1.

e) **Unsigncrypt-Queries:** When receiving a query with C_{agg} and the receiver’s identity ID_B. If i ≠ Θ, then Ch returns M_i. If i = Θ, then Ch inputs C_{agg}, R_i, μ_i, from the above queries, computes M_i = V_i ⊕ μ_i, and checks if there exists at least n of ID_i and M_i corresponding to C_{agg}. If so, then abort. Otherwise, Ch verifies the equation. e(W_{agg}, P) = \prod e(U_i, H_1(M_i)) · e(\sum H_3(U_i) · Q_{IDi}, P_0), for(i = 1, . . . , n). If it holds, return M_i; otherwise, rejected.

3) **Challenge:** When receiving ID_B, ID_i, M_{0i}, M_{1i} for i = 1, 2, . . . , n, Ch check if ID_i = ID_Θ, then aborts. Otherwise, Ch randomly picks h ∈ [1, n] and checks if i = h. If not, Ch picks randomly b ∈ {0, 1} and signcrypts the message M_{bi} as follows:

\[
U_b^* = VP, V_b^* = H_2(R_i) ⊕ M_{bi}, and picks W_b^* and Z_b^*. \\
\]

Finally, Ch sends the challenge aggregate signcryption C_{agg} to A_1.

4) **Phase 2:** This phase is identical to Phase 1; the only difference is that A_1 cannot query the secret key and the plaintext of the targeted signcryption C_{agg}.

5) **Output:** A_1 outputs the guess b* ∈ {0, 1}^* then Ch obtains (a_1, R_1, μ_1) from the lists H_1-List and H_2-List. The following equation can achieve the BDH solution:

\[
R_i^{1/ai} = e(X_{ID_i}, U_i)^{1/ai} = e(VP, a_iqβP)^{1/ai}. \\
\]

**Analysis:** Assume that H_2-queries happen and there are n of R_i in H_2-List. Then, A_1 could recognize the challenge ciphertext C_{agg} is invalid. Then, Ch can solve the CBDHP problem with a nonnegligible advantage. Therefore, our WBAN-19 scheme is secure against IND-ASC-CCA2.

**Theorem 2:** The proposed WBAN-19 scheme is OW-CCA2 in the ROM; if the CDHP assumption holds.

**Proof:** Assume A_2 is an adversary against our scheme, and there exists a challenger Ch claims to solve the CDHP problem in polynomial time and with a nonnegligible advantage. Thus, A_2 and Ch perform the following game.

1) **Setup:** The challenger Ch runs this algorithm and generates the public parameters (params) as follows. Ch Chooses two groups, G_1 and G_2, then computer P_0 = sP and sends params to A_2.

2) **Phase 1:** For all the adversary queries, Ch answers as follows.

a) **H_1-Queries:** Ch checks if ID_{O_i} exists in H_1-List; if yes, Ch sends ID_i to A_2. Otherwise, Ch selects Θ ∈ Z_q. If i = Θ, then Ch picks random value a_i ∈ Z_q and answers to A_2 with Q_{ID_i} = a_iβP. If i ≠ Θ, then Ch sets Q_{ID_i} = a_iP, and replies to A_2 with Q_{ID_i}. Ch adds (a_i, Q_{ID_i}, ID_i) into the list H_1-List.

b) **H_2-Queries:** Ch checks if R_i exists in H_2-List. If yes, Ch responds with μ_i = H_2(R_i) to A_2. Otherwise, Ch picks μ_i ∈ {0, 1}^* randomly and sends μ_i = H_2(R_i) to A_2, then adds (R_i, μ_i) into the list H_2-List.

c) **H_3-Queries:** Ch checks if U_i exists in H_3-List. If yes, then Ch responds with d_i = H_3(U_i) to A_2. Otherwise, Ch picks d_i ∈ Z_q randomly and sends d_i = H_3(U_i) to A_2, then adds (U_i, d_i) into the list H_3-List.

d) **KeyGen-Queries:** When receiving a query with X_{ID_i}. Then, Ch checks if i = Θ, Ch aborts. Otherwise, Ch recovers a_i from H_1-List, computes X_{ID_i} = a_iP_0, then sends X_{ID_i} to A_2.
d) **KeyGen-Queries:** When receiving a query with $X_{ID_i}$. Then Ch checks if $i = \Theta$, Ch aborts. Otherwise, Ch recovers $a_i$ from $H_1$-List, computes $X_{ID_i} = a_iP_0$, then sends $X_{ID_i}$ to $A_2$.

e) **Trapdoor-Queries:** When receiving such query, if $i \neq \Theta$, Ch sends $(\gamma X_{ID_i})$ to $A_2$.

f) **Unsigncrypt-Queries:** When receiving a query with $C_i$ and the receiver’s identity $ID_B$, Ch inputs $C_i, R_i, \mu_i$, from the above queries, then computes $M_i = V_i \oplus \mu_i, E_i = \mu_i \oplus M_i$, then checks if:

$$e(W_{agg}, P) = \prod e(U_i, H_i(M_i)) \cdot e(\sum H_i(U_i) \cdot Q_{ID_i}, P_0), \text{ for } (i = 1, \ldots, n).$$

3) **Challenge:** When receiving a query on $ID^*\), Ch selects randomly $M^*_i \in \{0, 1\}^{*}, V^*_i \in \{0, 1\}^{*}, W^*_i \in \mathbb{G}_1, Z^*_i \in \{0, 1\}^{*},$ and $U^*_i = a_iP$, then Ch sends the targeted signcryption $C^*_i = (U^*_i, V^*_i, W^*_i, Z^*_i)$ to $A_2$.

4) **Phase 2:** This phase is identical to Phase 1 except that the Unsigncrypt-queries $A_2$ cannot make any queries on the challenge plaintext $M^*_i$.

5) **Output:** $A_2$ outputs the guess $M'_i \in \{0, 1\}^{*}$, then Ch obtains $(a_i, R_i, \mu_i)$ from the lists $H_1$-List and $H_2$-List. The following equation can achieve the CDHP solution:

$$U_i = a_iP, \text{ and } Z_i = a_i\mu_iP_0.$$ Therefore, Ch can solve the CDHP problem with a nonnegligible advantage, and the proposed WBAN-19 scheme is OW-CCA2.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>[35]</th>
<th>[36]</th>
<th>[37]</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signcrypt</td>
<td>$T_1 + 5T_2 + T_3 + 3T_4 = 20.199$</td>
<td>$5T_1 + 2T_2 + T_3 + 3T_4 = 25.706$</td>
<td>$6T_1 + 2T_2 + 6T_4 = 17.020$</td>
<td>$3T_1 + T_2 + T_3 + 4T_4 = 11.886$</td>
</tr>
<tr>
<td>UnsSIGNcryption</td>
<td>$4T_1 + 4T_3 + 5T_4 = 31.685$</td>
<td>$7T_1 + 2T_3 + 4T_4 = 22.530$</td>
<td>$3T_1 + 3T_3 + 3T_4 = 24.548$</td>
<td>$4T_3 + T_4 = 21.357$</td>
</tr>
<tr>
<td>Equality Test</td>
<td>$4T_1 + 2T_3 + 2T_4 = 21.366$</td>
<td>$2T_1 + 4T_3 + 2T_4 = 25.306$</td>
<td>$3T_2 + 4T_3 + 2T_4 = 29.085$</td>
<td>$3T_1 + T_4 = 16.020$</td>
</tr>
<tr>
<td>Total</td>
<td>$73.280$</td>
<td>$73.542$</td>
<td>$70.853$</td>
<td>$49.263$</td>
</tr>
</tbody>
</table>

**Table II: Comparisons of Computation Efficiency (MS)**

**VI. WBAN-19: PERFORMANCE EVALUATION**

**A. Computational and Communication Complexity**

Wireless networks have extremely restricted resources regarding power and bandwidth. The most significant concern is that these systems heavily consume this power through the computation cost and capacity overhead. We assess the performance of the WBAN-19 solution, mainly regarding the computation and communication complexities.

For the running time, we utilize PBC Library [31] and MIRACL Library [32], and the experimental computations in [33] and [34], with respect to the following specifications: PIV; Windows XP OS 64 (bits); 1 (GB) RAM; 3 (GHz) CPU. The running time for each operation is defined as follows.

1) **ECC Point Addition/Multiplication:** $T_1 = 1.970$ (ms).
2) **Exponentiation:** $T_2 = 2.573$ (ms).
3) **Bilinear Pairing:** $T_3 = 5.337$ (ms).
4) **General Hash Function:** $T_4 = 0.009$ (ms).
5) **Other lightweight (XOR, addition, etc.)** $\ll 0.001$ (ms) (Omitted).

The protocol overhead is another important factor in constrained environments such as WBAN systems. The proposed WBAN-19 scheme has an efficient overhead by reducing the size of transmitted data. We endorse the 80 (bits) security level, RSA with 1024 (bits), and ECC with 160 (bits). Assume that $|ID| = |M| = |Z_i| = |G_1| = |G_2| = 160$ (bits).

For any low-power systems such as WSNs. The power consumption, computation cost, and communication capacity can affect the performance due to the limited resources of such systems. Therefore, to improve the security level, we need to consider lightweight cryptosystems. Tables II and III demonstrate the computation cost and the communication overhead for our WBAN-19 scheme in comparison to the proposed schemes in [35], [36], and [37]. The security comparison in Table IV is carried against the proposed schemes in [38], [39], and [40]. This includes comparisons of the security features, security requirements, and the flexibility provided by each scheme.
TABLE III
COMPARISONS OF COMMUNICATION EFFICIENCY (BITS)

<table>
<thead>
<tr>
<th>Scheme</th>
<th>[35]</th>
<th>[36]</th>
<th>[37]</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signcryption</td>
<td>$3 + 640$</td>
<td>$3 + 800$</td>
<td>$2 + 640$</td>
<td>$Z^* = 800$</td>
</tr>
<tr>
<td>Equality Test</td>
<td>$5 + 960$</td>
<td>$5 + 1280$</td>
<td>$4 + 960$</td>
<td>$Z^* = 1280$</td>
</tr>
<tr>
<td>Total</td>
<td>1600</td>
<td>2080</td>
<td>1760</td>
<td>1120</td>
</tr>
</tbody>
</table>

TABLE IV
COMPARISONS OF SECURITY PROPERTIES

<table>
<thead>
<tr>
<th>Scheme</th>
<th>[38]</th>
<th>[39]</th>
<th>[40]</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual Authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Signcryption</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Aggregation</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>EUF-CMA Security</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IND-CCA2 Security</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OW-CCA2 Security</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Fig. 4. Comparisons of computation efficiency (ms).

B. WBAN Experiment

The IEEE 802.15.6—2012 is the standard for WBANs. It intends to update and assist new use cases while increasing the dependability support by such standards. This standard categorizes the WBAN into four main entities as follows [41].

1) WBAN Client: This could be WBAN users with implanted and wearable sensors/devices.
2) Mobile Device: This could be smartphones or any personal digital assistants (PDAs).
3) Medical Provider: This could be healthcare professionals or hospitals connected through a medical server.
4) Network Manager: This could be a trusted or semi-trusted third party (security server) that establishes and distributes secret and public parameters.

Also, IEEE Std. 802.15.6 defined the WBAN environment as follows.

1) Static: A single WBAN to serve a single patient in a specific environment.
2) Semidynamic: For elderly care with slow-moving capabilities.
3) Dynamic: Multiple WBANs to serve multiple users with fast-moving capabilities.

The proposed WBAN-19 scheme can be implemented in all possible WBAN environments since our proposed scheme is lightweight regarding the computational and communication complexities; with three entities involved (user A: patient aka WBAN user, user B: physician, and a medical/security server. We implemented an equality test and threshold methods for WBAN diagnoses algorithms and experiments. Fig. 2 shows two levels of diagnoses and healthcare decision making based on hospital and threshold values stored in the security/medical server, which is just compatible with the proposed model providing more flexibility and reliability to the proposed scheme.

There are several other algorithms that have been widely used in WBANs [42], [43]. These algorithms, such as blockchain-based techniques considered efficient and relatively secure. However, some of such lack fulfilling some security properties and features, such as signcryption as a one-logical algorithm, equality test as a diagnoses technique, aggregation for more efficiency, and provably security.

C. Comparisons Analysis

As shown in the above-mentioned evaluation for the WBAN-19 scheme, the computation cost and the communication overhead are improved compared to the other proposed schemes in [35], [36], and [37]. From Fig. 4, the computation cost in these references is (72.482 ms) in average. It is (49.263 ms) for our scheme. Thus, the total computational cost for our proposed WBAN-19 scheme is improved by (68%) compared to the other proposed schemes.

Fig. 5. Comparisons of communication efficiency (bits).
The communication overhead demonstrated in Fig. 5 and Table III indicates that our proposed scheme improves the communication overhead by (60%), from the approximate average overhead of (1800 bits) for the above-compared references to (1120 bits) for our proposed scheme.

As for security, the comparisons in Table IV show that our proposed scheme provides more security requirements, properties, and features than the proposed schemes in [38], [39], and [40]. Our scheme provides signcryption, equality test, and aggregation security properties as well as provable security under the ROM for EUF-CMA, IND-CCA2, and OW-CCA2 security models. The security versus functionality for our scheme shows more flexibility as several new features have been added to the WBAN-based COVID diagnoses system compared with other proposed schemes.

D. Results and Discussion

Pondering the security of current wireless networks such as WBANs, we can easily identify several vulnerabilities against different attacks. Security is an essential factor for wireless systems because they are meant to serve network users. Wireless technologies are also employed or associated with other applications, such as IoT, WSN, traffic control, e-health, smart grid, etc. [44]. According to the security analysis presented in Section V, the proposed approach allows WBAN-19 entities to authenticate each other and communicate securely before providing any services.

From the above analysis, the proposed WBAN-19 scheme is flexible, reliable, and compatible with telemedicine systems for the following reasons.

1) Using identity-based construction gives our proposed scheme more flexibility to be implemented in real use-case scenarios.

2) The proposed models’ description shows the compatibility of our scheme with telemedicine systems by using WBANs architecture.

3) The complexity analysis shows the reliability of our scheme, which can be implemented in any real use-case scenario.

4) The security analysis shows that the proposed scheme is secure under several provable security models.

5) Finally, the comparison analysis shows that our proposed scheme is more efficient than other proposed approaches.

As a result, the proposed WBAN-19 solution is secure and has low computational cost and communication overhead, achieving better performance than other proposed approaches. Furthermore, our proposed solution can be implemented efficiently by industrial sectors within the WBAN standardization and even by future technologies such as the upcoming 6G mobile networks [45], which is essential to reduce the stored data, transmission handshaking processes, delay, and bandwidth usage in these technologies to improve the battery life for better performance [46].

VII. CONCLUSION

WBAN-based applications can be employed widely in the healthcare sectors, allowing for a more flexible infrastructure for the daily monitoring of health parameters. It is an important security feature by providing privacy-preserving techniques to patients and hospitals and securing the sensitive information of healthcare systems. In this article, we proposed a novel security solution achieving equality test and aggregation techniques using identity-based signcryption construction for telemedicine systems. This solution aims to overcome the spreading of contagious diseases such as COVID-19 through WBAN-based telemedicine applications. The main advantage of this work is that it can be practically implemented in telemedicine systems securely using WBANs infrastructure. The performance evaluation and analysis showed that the proposed scheme is efficient and secure against several attacks considering adversarial models under some hard problem assumptions in the ROM. The gap in this article is to reduce the computational cost and communication overhead to a minimum. This can be achieved by using more lightweight public-key cryptosystems and providing aggregate group and ring signature schemes for some heterogeneous wireless networks (HWNs) applications. Also, our future work will focus on the security of telemedicine systems by developing homomorphic, multiparty computation, and private set intersection (PSI) techniques that can be efficiently implemented in lightweight WBAN-based telemedicine systems.

REFERENCES

Mohammed Ramadan (Member, IEEE) received the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2016. From 2017 to 2022, he worked as a Researcher, a Postdoctoral Fellow, and a Lecturer with the Research Institutes of Sweden, Stockholm, Sweden; UESTC; and Chengdu University of Information Technology, Chengdu. He is currently a Postdoctoral Researcher working on cryptography for decision systems with the Center for Information Security and Trust, IT University of Copenhagen, Copenhagen, Denmark. His current research interests include information security, cryptography, public-key cryptography, and wireless/mobile networks security.

Shahid Raza (Senior Member, IEEE) received the Master of Science degree in cybersecurity from KTH Sweden, Stockholm, Sweden, in 2009, and the Ph.D. degree in industrial from Malardalen University, Västerås, Sweden, in 2013. He is currently the Director of the Cybersecurity Unit, RISE Research Institutes of Sweden, Stockholm, and an Associate Professor with Uppsala University, Uppsala, Sweden. He is currently supervising four Ph.D. students as the main supervisor. His work on IoT security is published in prestigious journals and conferences, and only in last two years, he has received over 1700 citations on his IoT security papers. His research interests include security and privacy in IoT. For more information visit the link (http://shahidraza.net).