A lightweight and secure multilayer authentication scheme for wireless body area networks in healthcare system

Mohammad Fareed, Ali A. Yassin

Department of Computer Science, Education College for Pure Science, University of Basrah, Basrah, Iraq

Article Info	**ABSTRACT**
Article history: Received Mar 7, 2022 Revised Sep 18, 2022 Accepted Oct 14, 2022	Wireless body area networks (WBANs) have lately been combined with different healthcare equipment to monitor patients' health status and communicate information with their healthcare practitioners. Since healthcare data often contain personal and sensitive information, it is important that healthcare systems have a secure way for users to log in and access resources and services. The lack of security and presence of anonymous communication in WBANs can cause their operational failure. There are other systems in this area, but they are vulnerable to offline identity guessing attacks, impersonation attacks in sensor nodes, and spoofing attacks in hub node. Therefore, this study provides a secure approach that overcomes these issues while maintaining comparable efficiency in wireless sensor nodes and mobile phones. To conduct the proof of security, the proposed scheme uses the Scyther tool for formal analysis and the Canetti–Krawczyk (CK) model for informal analysis. Furthermore, the suggested technique outperforms the existing symmetric and asymmetric encryption-based schemes.
Keywords: Authentication Canetti-Krawczyk threat model Healthcare system Schnorr digital signature Scyther Wireless body area network	

Corresponding Author:

Mohammad Fareed
Department of Computer Science, Education College for Pure Science, University of Basrah
Basrah, Iraq
Email: pedupg.m.fareed@uobasrah.edu.iq

1. INTRODUCTION

Wireless technology advancements have had a favorable impact on practically every human existence in healthcare. Connecting the physical and digital worlds facilitates communication and access amongst network members, application services, and users as a whole [1]–[5]. The internet of things (IoT) relies heavily on wireless sensor network (WSN) technology [6], which consists of a group of wireless sensors. The wireless body area network (WBAN) is a perfect network for medical IoT devices, given the wide variety of WSNs available [7]–[9]. WBAN-based healthcare services might use to trace and gather healthy patient data remotely. The distance between a patient and a specialist doctor might impact his health [10]–[13]. However, the low level of hospital and the scarce of professional medical staff are common problems in most countries [14], [15]. Although this might be a concern, the remote healthcare system can assist in overcoming these issues. Remote healthcare is especially useful for long-term illnesses, including heart failure, diabetes, and chronic obstructive pulmonary disease (COPD) [16]. Chronic diseases are also becoming more common for healthcare providers who use remote monitoring and treatment technologies [17]. It is possible to monitor a patient's health state at any time/location in the remote healthcare system. Because the patient's health observes in real-time, the doctor can react swiftly and provide an early diagnosis if the patient's health state becomes critical, which is an additional benefit [18], [19]. Furthermore, remote healthcare monitoring enables patients to remain in their homes instead of spending money on costly healthcare facilities like hospitals or nursing homes [20], [21].

However, because remote healthcare services are vulnerable to many attacks, privacy and security are important in protecting this data as it is collected and sent [22]–[29]. The patient's life might be in danger if some of the attackers succeed in launching the assaults, and these unexpected tasks could be done through WBAN. As a result, authentication and key generation methods must protect remote healthcare applications. Many WBAN authentication techniques have been developed for healthcare applications. In particular, Zhu and Ma [30] an anonymous authentication system using smart cards is now in use, which uses a single message exchange to authenticate users while safeguarding their privacy. Although Lee *et al.* [31] proved that Zhu and Ma approach could not guarantee full user anonymity secrecy, they presented an improved protocol as a solution. Symmetric key cryptography, exclusive-or (XOR), and hashing operations are used in Zhu's and Lee's protocols. The elliptic curve cryptography (ECC) called by Memon *et al.* [32] serves as the base for an anonymous authentication method for site-based applications. Soon after, Reddy *et al.* [33] showed vulnerabilities of Memon *et al.*'s protocol focused on key compromised insider attacks, impersonation attacks, and insecure password changing part, and a difficult of imperfect mutual authentication. Reddy *et al.* [33] also proposed a two-factor authentication system based on smartcards and ECC. The Memon *et al.* [32] and the Reddy *et al.* [33] procedures rely on private key cryptosystem, especially ECC, to secure their communications. Khatoon *et al.* [34] and Ostad-Sharif *et al.* [35] independently suggested an ECC-based authentication and key agreement mechanism for the telemedicine information system. Khatoon *et al.* [34] aimed to offer patients safe and privacy-preserving identification utilizing biometrics, bilinear pairing-based, unlinkable, mutual authentication, and key agreement by using a fuzzy extractor. Ostad-Sharif *et al.* [35] created an anonymous and unlinkable authentication and key agreement mechanism that enabled formal security analysis via simulation and results from AVISPA. Ali *et al.* [36] have presented an authentication and access control technique for protecting wireless Healthcare WSNs in addition to their research efforts. According to AVISPA and burrows–abadi–needham (BAN) logic [37], Ali *et al.* protocol's is safe since it uses ECC and bilinear pairing.

Depending on primitives based on bilinear or ECC pairing has a higher computational cost than any other cryptosystem primitives, which is why they are high complexity on WBANs. An anonymous biometric-based authentication strategy based on chaotic maps was suggested by Khan *et al.* [38] to reduce the burden on the system. Based on hash functions and exclusive-or operations are used in Aman *et al.*'s Assuming that PUFs used in WBANs is an enormous strain on the system, even if Khan and Aman's protocols are operationally efficient. According to Xu and colleagues, WBANs may be securely authenticated and encrypted without the need for chaotic maps or PUFs [39]. Exclusive-OR and hash function operations are all that are needed to implement their system. Alzahrani *et al.* showed that Attacks like replaying and key compromise impersonation are possible with the Xu *et al.* protocol. Offline identity guessing attacks can also be done with this protocol [40]. For WBANs in healthcare applications, they developed an enhanced protocol. Furthermore, Alzahrani *et al.* does not ensure the unlinkability of patients since it utilizes the same identification of the access point in each session, even though it has a low computational cost and many benefits in terms of privacy and security issues. This study makes the following contributions:

− The proposed secure multilayer healthcare system works on a WBAN environment and secures the communication channels between the system's components see Figure 1;
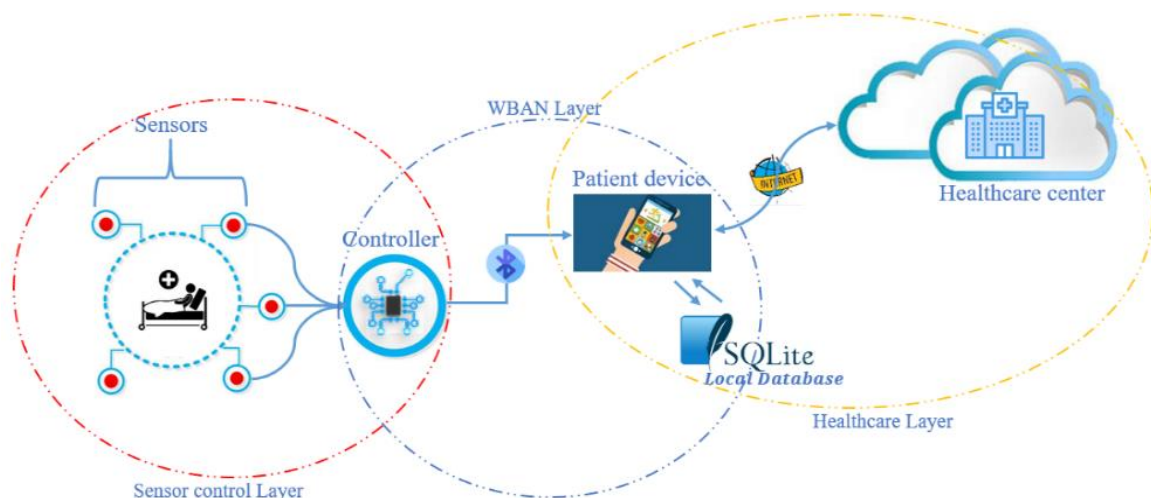

Figure 1. The organization of the multilayer healthcare system based on

− The suggested authentication scheme in the system relies on an XOR operation and a one-way hash function, which are lightweight compared to asymmetric cryptosystem operations. As a result, it is suited for use with WBANs in remote healthcare;
− The security analyses show that the suggested scheme offers both privacy and security for users. The formal security verification through the Scyther tool updates that the scheme can withstand malicious attacks; and
− Efficiency analysis is performed based on the complexity analysis of processing and communication. Comparison with related systems reveals that the suggested scheme is adequate for computing and communication efficiency.

2. PRIMITIVE TOOLS
2.1. Schnorr digital signature
Schnorr digital signatures have been presented to reduce the signature size of El-Gamal digital signatures [41]–[43]. It is a highly helpful, certified, and compact signature generator. Schnorr algorithm it's a three-function strategy:

Algorithm 1. Schnorr digital signature
KeyGen function:
Begin
        Step 1. Select two large prims $p \geq 2^{512}$ and $q \geq 2^{140}$ such that: $(p-1) \bmod q = 0$.
        Step 2. Choose $g \in \mathbb{Z}_p$ of order q, $g \neq 1$ & $g^q = 1 \bmod p$.
        Step 3. Pick $x \in \mathbb{Z}_q$ and $g^x \bmod p$.
        Step 4. *Private key = x*, and *Public key = y = $g^x \bmod p$*.
        Step 5. The public parts are (g, p, q, y).
End
Sign (g, x, M) function:
Begin
        Step 6. Choose $k \in \mathbb{Z}_q^*$ and set $r = g^k$.
        Step 7. Compute $e = H(r_{P_i} \| M)$ and $s = k + x * e$.
        Step 8. Send $(Sign_x(M) = \langle M, s, e \rangle)$ to the verifier.
End
Verify (M, e, s) function:
Begin
        Step 9. Set $r' = g^s y^{-e}$.
              $= g^{k+x*e} * g^{-x*e} = g^k$
        Step 10. IF $e \overset{?}{=} H(r' \| M)$; is true, the message is accepted; ELSE, it is rejected.
End

2.2. Scyther
Scyther is a tool used to verify, falsify, and analyze security protocols. It is a freely available and state-of-the-art tool that provides some novel features not offered by other tools. Novel features include the possibility of unbounded verification with guaranteed termination, ability to analyze infinite sets of traces in terms of patterns, and support for multi-protocol research. The tool provides a graphical user interface (GUI) that complements the command line and Python scripting interfaces. The GUI is aimed at users interested in verifying or understanding a protocol. The command line and scripting interfaces facilitate the use of Scyther for large-scale protocol verification tests [44].

2.3. Canetti-Krawczyk (CK) threat model
With the Canetti-Krawczyk (CK) model, the proposed scheme can be formally developed and analyzed. The proposed system should have many essential security properties [45]. In this paper, we used the following features: i) mutual authentication, ii) anonymity, iii) unlinkability, iv) smart factor, v) attack resistance, and vi) all channels are secure.

3. THE PROPOSED SCHEME
The proposed secure scheme on WBAN consists of three components: patient device (Pd_i), sensors ($S_{ij} = S_{i1}, S_{i3,\dots}, S_{in}$), and controller ($C_i$). Table 1 contains the necessary symbols used in this study. The work depends on the initialization, registration, login, and healthcare authentication phases. The registration phase involves registration of a new patient (P_i) in the global database (HCC). The login phase involves login, authentication, and verification of the system's components. The healthcare phase updates the patient's health status efficiently and securely through sensors. The main phases are explained.

Table 1. List of notations

Symbol	Description	Symbol	Description
HCC	Healthcare center.	$D_{T_{P_i}}$	temporary storage
HCC_{dp_k}	Specialist doctor	$D_{S_{P_{ij}}}$	Sensor data
Pd_i	Patient device.	$D'_{S_{P_{ij}}}$	Decrypted sensor data
P_i	Patient.	OTP	One time password
$S_{P_{ij}}$	Sensors.	FCI_{P_i}	Family contact info
$D_{S_{ij}}$	Encrypted $S_{P_{ij}}$ data	SMS_T	SMS token
C_{P_i}	Controller.	$f_{S_{P_{ij}}}$	Flag
FF_{P_i}	Flash file of P_i.	T_{P_i}	Login time
SK_{P_i}	Shared Key of P_i	$\oplus$	Exclusive or
$\mathbb{Z}$	Group of positive No.	T	Returns the current date and time
PW_{P_i}	P_i password	$\|$	Concatenation
CC_{P_i}	confirmation code	P and Q	Large primes number
$SQLite$	Local database	x	Private key
Pr_{HCC}	HCC private key	g	Random number $\in \mathbb{Z}$
Pu_{HCC}	HCC public key	y	Public key
Pr_{P_i}	P_i private key	M	message
Pu_{P_i}	P_i private key	NR_{P_i}	necessary recommendations
$H()$	Hash function	CR	Username combined with the sensor data sent

3.1. Initialization phase

At the moment, the HCC is responsible for configuring the system key and generating public and private keys (Pr_{HCC}, Pu_{HCC}) for signing data sent from the HCC to Pd_i based on the Schnorr digital signature. These steps are carried out as:
− HCC selects two prims p and q large numbers such that: $(p-1)\, mod\, q = 0$.
− HCC takes $g \in \mathbb{Z}_p$ of order q, $g \neq 1$ & $g^q = 1\, mod\, p$.
− HCC picks $x_{HCC} \in \mathbb{Z}_q$ and $g^{x_{HCC}}\, mod\, p$.
− $Pr_{HCC} = x_{HCC}$ and $Pu_{HCC} = g^{x_{HCC}} mod\, p$.

3.2. Registration phase

Here, the patient who wishes to register in the HCC performed the following steps:
Step 1. The patient registers his information (Full name (FN_{P_i}), Address (AD_{P_i}), Phone No. (PN_{P_i}), Email (EM_{P_i}), Family contact info (FCI_{P_i}), type of disease (TD_{P_i}), username (UN_{P_i}), password (PW_{P_i})), and compute H_{P_i} as anomaly method by using $H_{P_i} = H(PW_{P_i}\|UN_{P_i})$, then store the data to both the global database HCC and the local database $SQLLite$.
Step 2. HCC generates the shared key for patient ($SK_{P_i} \in \mathbb{Z}^*$) to enc/dec the sensitive medical data of $S_{P_{ij}}$.
Step 3. Embed the SK_{P_i} to the FF_{P_i} of the Controller C_{P_i} that uses this key to encrypt the sensor's data.
Step 4. HCC creates the Electronic Health Record (EHR_{P_i}) containing all the above medical information associated with the new patient.
Step 5. HCC generate public and private keys (Pr_{P_i}, Pu_{P_i}) for the signing data from the P_i to the HCC based on Schnorr digital signature as below:
− Pd_i selects two large prims p and q such that: $(p-1)\, mod\, q = 0$.
− Pd_i chooses $g \in \mathbb{Z}_p$ of order q, $g \neq 1$ & $g^q = 1\, mod\, p$.
− Pd_i picks $x_{HCC} \in \mathbb{Z}_q$ and $g^{x_{P_i}} mod\, p$.
− $Pr_{P_i} = x_{P_i}$ and $Pu_{P_i} = g^{x_{P_i}} mod\, p$.

3.3. Login phase

After completing the registration and access to the data showing interfaces, we'll go through how to log into the health application in this phase.
Step 1. P_i enters his login information (UN_{P_i} and PW_{P_i}) in the Pd_i.
Step 2. Pd_i computes the $H'_{P_i} = H(PW_{P_i}\|UN_{P_i})$.
Step 3. It compares the information (H'_{P_i}) with the H_{P_i} stored in the Pd_i local database ($SQLLite$).
Step 4. If the result is true, then Pd_i starts the application with the Healthcare phase. Otherwise, go to step 5.
Step 5: Pd_i computes $T = NOW()$ and sends $H''_{P_i} = H(H'_{P_i} \oplus T)$, T to the HCC through the internet. Since T cannot be repeated with a new login process, this feature has been used to prevent malicious attacks during the login process.

Step 6. HCC compares $H''_{P_i} \stackrel{?}{=} (H_{P_i} \oplus T)$ with and sends a confirmation code CC_{P_i} as a challenge to Pd_i using SMS token technique when the result of the current step is true. Otherwise, it terminates this phase.

Step 7. P_i enters the confirmation code CC'_{P_i} on his Pd_i and then sends to HCC.

Step 8. Upon receiving the information from P_i, HCC compares CC'_{P_i} with CC_{P_i}. If the comparison is correct, HCC sends registration information and SK_{P_i} to Pd_i.

Step 9. Pd_i saves registration information and SK_{P_i} in the $SQLite$. Figure 2 refers to the steps of the login authentication phase.
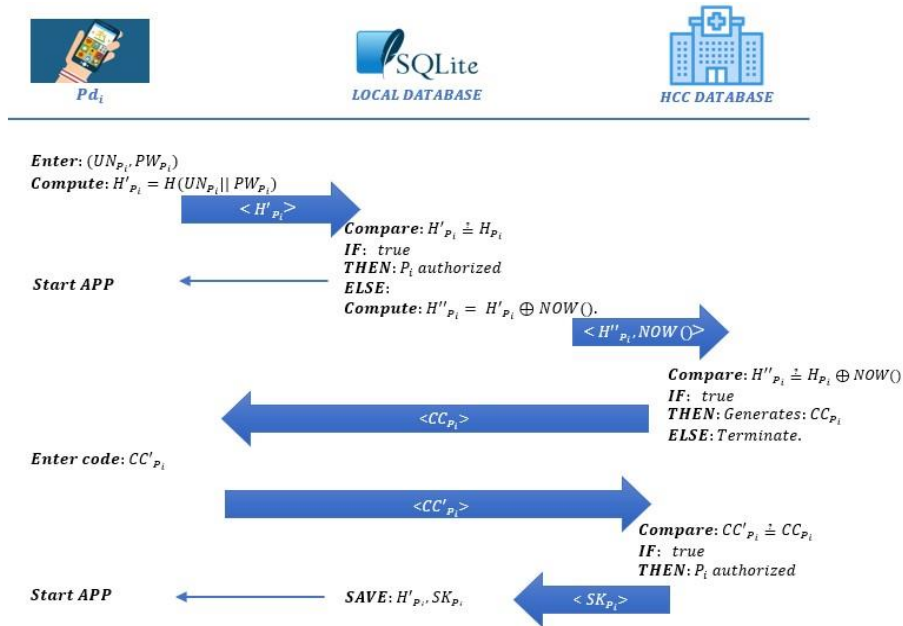

Figure 2. Login phase

3.4. Healthcare phase

After completing the registration and access to the data showing interfaces, we'll go through how to log into the health application in this phase. Currently, Pd_i is ready to receive and view the decrypted data of sensor $(D_{S_{P_{ij}}})$ as:

Step 1. In the first iteration, $S_{P_{ij}}$ sends data of each patient's sensor $D_{S_{P_{ij}}}$ to C_{P_i}. Then, C_{P_i} saves $D_{S_{P_{ij}}}$ in the temporary storage $D_{T_{P_i}}$. Where $D_{T_{P_i}}$ focuses on increasing the performance of C_{P_i}.

Step 2. C_{P_i} determines the severity of $D_{T_{P_i}}$ received by the $S_{P_{ij}}$ depended on three rules:

– If $D_{T_{P_i}}$ in the normal range, C_{P_i} sets $f_{S_{P_{ij}}} = 0$.

– If $D_{T_{P_i}}$ in the abnormal range, C_{P_i} sets $f_{S_{P_{ij}}} = 1$.

– If $D_{T_{P_i}}$ in the dangerous range, C_{P_i} sets $f_{S_{P_{ij}}} = 2$.

Step 3. C_{P_i} computes $E_{S_{P_{ij}}} = Enc_{SK_{P_i}}\left(D_{T_{P_i}} || f_{S_{P_{ij}}}\right)$ and sends $E_{S_{P_{ij}}}$ to the Pd_i.

Step 4. Pd_i receives $E_{S_{P_{ij}}}$ and performs $D'_{T_{P_i}} = Dec_{SK_{P_i}}(E_{S_{P_{ij}}})$. After that, Pd_i restores $f'_{S_{P_{ij}}}$ to determine the severity of health data by the following:

– If $f'_{S_{P_{ij}}} \stackrel{?}{=} 0$; then show the received data in the screen of Pd_i.

– If $f'_{S_{P_{ij}}} \stackrel{?}{=} 1$; then show the received data with a warning notification.

– If $f'_{S_{P_{ij}}} \stackrel{?}{=} 2$; then, show the received data with a danger notification and go to step 6.

Step 5. In the new iteration, $S_{P_{ij}}$ reads a new data of a patient's sensors $D_{S_{P_{ij}}}$ then sends to C_{P_i}. After that, C_{P_i} compares $D_{S_{P_{ij}}} \stackrel{?}{=} D_{T_{P_i}}$; if so, then return in the current step; otherwise, sets $D_{T_{P_i}} = D_{S_{P_{ij}}}$ and go to step 2.

Step 6. At this step, HCC contribute to the decision making of the patient's status. The Pd_i performs the following steps:

- Compute $CR = (E_{SP_{ij}} \| UN_{P_i})$.
- Choose $k_{P_i} \in \mathbb{Z}_q^*$ and set $r_{P_i} = g^{k_{P_i}}$.
- Compute $e_{P_i} = H(r_{P_i} \| CR)$ and $s_{P_i} = k_{P_i} + Pr_{P_i} * e_{P_i}$.
- Send $Sign_{Pr_{P_i}}(CR) = <CR, s_{P_i}, e_{P_i}>$ to HCC.

Step 7. HCC verifies whether the $Sign_{Pr_{P_i}}(CR)$ is valid or not by running $Verify_{Pu_{P_i}}(CR, s_{P_i}, e_{P_i})$.

- Set $r'_{P_i} = g^{s_{P_i}} y^{-e_{P_i}}$.
  $$= g^{k_{P_i} + Pr_{P_i}*e_{P_i}} * g^{-Pr_{P_i}*e_{P_i}}$$
  $$= g^{k_{P_i}}$$
- Compare $e_{P_i} \overset{?}{=} H(r'_{P_i} \| CR)$; if the result is true, go to step 8; Otherwise, terminate the current phase.

Step 8. HCC decrypts $E_{SP_{ij}}$ relied on $D'_{SP_{ij}} = Dec_{SK_{P_i}}(E'_{SP_{ij}})$, then analyses the patient's case, writes the necessary recommendations (NR_{P_i}) by the specialist doctor HCC_{dp_k}. Then save NR_{P_i} in the database and sign it using the following steps:

- Choose $k_{HCC} \in \mathbb{Z}_q^*$ and set $r_{HCC} = g^{k_{HCC}}$
- Compute $e_{HCC} = H(r_{HCC} \| NR_{P_i})$ and $s_{HCC} = k_{HCC} + Pr_{HCC} * e_{HCC}$.
- Send $Sign_{HCC}(NR_{P_i}) = <NR_{P_i}, s_{HCC}, e_{HCC}>$ to Pd_i and resend NR_{P_i} to FCI_{P_i} via SMS.

Step 9. Pd_i verifies whether the NR_{P_i} is correct or not based on the received s_{HCC}, e_{HCC} by running $Verify_{Pu_{HCC}}(NR_{P_i}, s_{HCC}, e_{HCC})$.

- Set $r_{HCC} = g^{s_{HCC}} y^{-e_{HCC}}$.
  $$= g^{k_{HCC} + Pr_{HCC}*e_{HCC}} * g^{-Pr_{HCC}*e_{HCC}}$$
  $$= g^{k_{HCC}}$$
- Compare $e_{HCC} \overset{?}{=} H(r_{HCC} \| NR_{P_i})$, if true, go to step 10; Otherwise, terminate the current phase.

Step 10. Pd_i shows NR_{P_i} with a danger notification on the screen of Pd_i and go to step 5. Figure 3 explains the healthcare phase and data transfer.
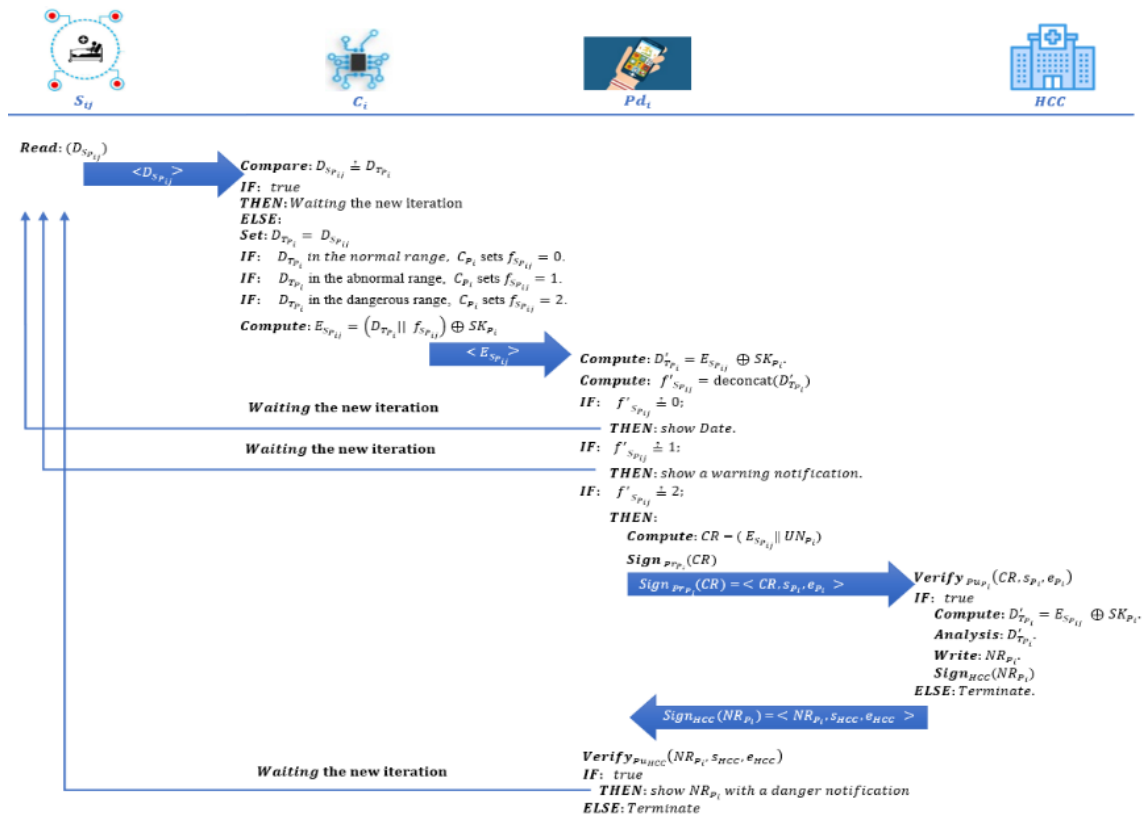

Figure 3. Healthcare phase

4. RESULTS AND DISCUSSION

This part analyzes the security of the proposed protocol using the Scyther tool and the CK model [37]-[40], [44] and shows how the protocol can achieve high levels of privacy and security than the alternatives. Scyther is an important tool for formal security analysis, but it only works if an attacker knows the decryption key to get the plaintext of the ciphertext. Scyther tool provides a lot of benefits:

- It is seen as an unbounded model for validating many security schemes, like authentication, verification, and access control.
- It lets you test the soundness of a proposed scheme for all possible behaviors, like attacks. To use any of the suggested schemes, we should write in the security protocol description language (SPDL), which defines protocols/schemes, supports expressions for encryption/decryption and signing, and sending/receiving events.

The GUI of Scyther is designed for anyone wanted to check or understand a protocol. To run large-scale protocol verification tests. The traditional system is implemented without the use of typical security features. Figure 4 shows the old system's flaws, as we have already shown.
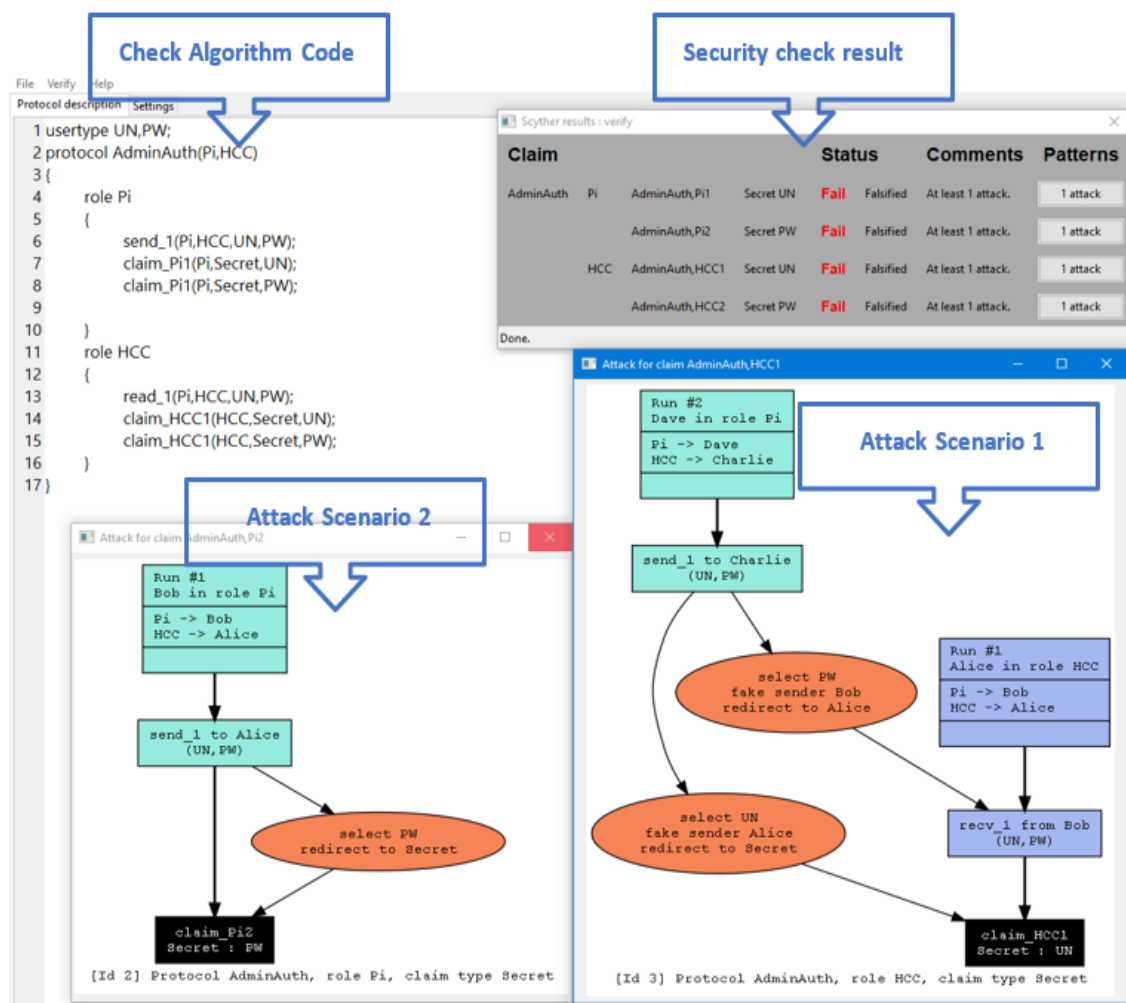

Figure 4. Weakness of the traditional system

4.1. Formal security analysis

Scyther is an important tool for formal security analysis, but it only works if an attacker knows the decryption key to get the plaintext of the ciphertext. Using symmetric key encryption, crypto-hash function, and digital signature, a secure system that overcomes the weaknesses of traditional systems has been developed. The results of the suggested system, which is resistant to well-known harmful attacks, are shown in Figure 5.
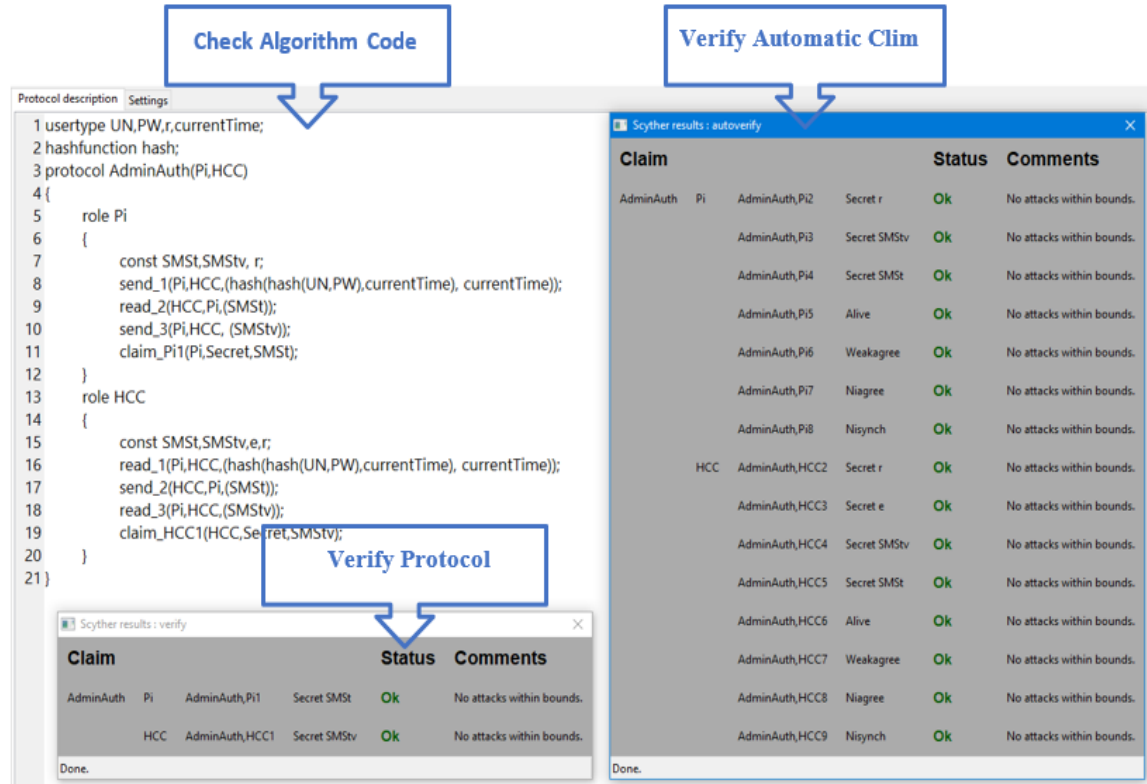
Figure 5. Verify protocol and automatic climes

4.2. Informal security analysis

The proposed scheme is capable of being formally developed and evaluated with the help of the CK model. The proposed system ought to possess a significant number of important security properties [45]. We review the most important security challenges that are present in this paper:

− Mutual authentication: HCC requires Pi to be genuine based on UN_{P_i}, PW_{P_i}, and CC, which is a message from Pi to HCC. HCC in the proposed system could authenticate only the legal Pi because a CK adversary needs to guess the information of login (UN_{Pi}, PW_{Pi}, T), compute $[H_{P_i} = H(H'_{P_i} \oplus T), T]$, and send it to HCC. It compares the received information with the data stored in the database, and if they are identical, it generates and sends the SMS token (CC) to Pi via PNO_{Pi}. Here, HCC can be considered as a trusted party. The attackers (Pi') fail to receive SMS_T from HCC because they do not own Pi's smartphone number PNO_{Pi}. Then, HCC terminates the authentication phase. In case of legitimate users (Pi), they enter CC' in the dialogue box and resubmit it to HCC. Finally, HCC compares $CC \overset{?}{=} CC'$ and if it matches, Pi is authorized.

− Anonymity: From the CK adversary's point of view, it is hard for an adversary to find out the user's identity and password. At the moment, it is necessary to check the identity of login information sent between system parts to show anonymity. The data in server is saved using SHA-256 hash function $[H(PW_{P_i} || UN_{P_i})]$, which has a robust relationship with the identity of entities. To do so, the adversary should know about breaking the SHA-256 hash function, which is not feasible. Therefore, the proposed system provides anonymity.

− Unlinkability: This feature focuses on preventing HCC from detecting if P_i has logged previously or not. This feature was applied in the proposed system by changing the value of $H''_{P_i} = H(H'_{P_i} \oplus T), T)$ for each login attempt of P_i. Since T is the value of the current date and time, it is impossible to repeat the value. Consequently, an adversary cannot link different logins with the same P_i.

− Smart factor: After the patient's first logon to the application, a secure connection session is opened by keeping the login information in the local database. This makes the system available in a smart and permanent way. This feature is used to reduce the burden of logging information during each login process. On deleting the application and changing the smartphone, the login information is deleted from the local database. This makes the process of entering information and security verification work.

− Attack resistance: Any malicious attack like the man-in-the-middle (MITM) attack [46], impersonation attack, insider attack, and replay attack is possible if a CK adversary finds a method to carry out the attack. For an impersonation attack related to mutual authentication, the attacker should learn the first-factor message (H', T) and confirmation code (CC) to masquerade as P_i and HCC respectively. Furthermore, these messages are linked to the knowledge of login information. So, the proposed scheme can prevent impersonation attacks. The MITM attack uses the same technique used by active eavesdropping. Here, we notice the mutual authentication provides. An attacker fails to get both UN_{P_i} and PW_{P_i} to compute H' because it uses a parameter (T) generated once for each login iteration. Assume that an attacker can access the current time T and login information to calculate H', but the attacker cannot have PNO_{P_i} to receive CC from HCC see Figure 6. Finally, the proposed scheme resists MITM attack, replay attack, impersonation attack, sniffing, hijacking, dictionary attack, and eavesdropping attack because an attacker is unable to get any benefit from parameters exchanged between P_i and HCC or establish an insider threat because CC is sent to the legal-patient's smartphone (PNO_{P_i}).

− All channels are secure: Since data transmitted through communication media is vulnerable to attack by an adversary, the proposed system secures all communication channels using encryption and digital signature. The data of $S_{P_{ij}}$ is encrypted $[Enc_{SK_{P_i}}\left(D_{T_{P_i}} || f_{S_{P_{ij}}}\right)]$ before being sent to PNO_{Pi}. Despite the short range of communication using Bluetooth technology, eavesdroppers will try to obtain the information. Data sent from PNO_{Pi} to HCC and data returned from the health institution to the phone are also signed using a Schnorr digital signature $(Sign_{pr}$ and $Verify_{pu})$. After reviewing the security challenges using the CK model, we compare our proposed system with similar works as shown in Table 2.
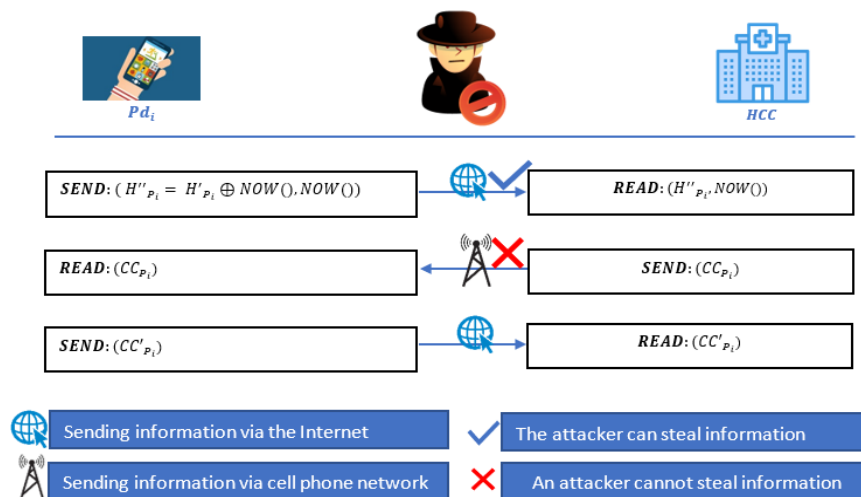

Figure 6. Scenario blocking malicious attacks

Table 2. Privacy and security feature comparison result

Protocol	Verification's time complexity	Result
[34]	$9T_h + 2T_{bp} + 2T_{sym} + 5T_{ecc}$	51.51
[35]	$14T_h + 2T_{sym} + 4T_{ecc}$	18.64
[38]	$11T_h$	0.88
[39]	$10T_h$	0.8
[40]	$10T_h$	0.8
[46]	$14T_h$	1.12
Proposed	$2T_{Sign} + 2T_{Verify}$	0.35

5. PERFORMANCE RESULTS

In this part, the protocol is compared to those in [34], [35], [38], [40], [41] to see how it performs in terms of computational and communication overheads. Moreover, any suggested protocol should be had balancing between performance and complexity of security. So, the WBANs prefers to use light security feature and preserve the privacy of health data. We notice that the proposed scheme can resist well-known attacks and achieves a good security feature compared with other related work.

5.1. Computation result

There are three phases in the proposed protocol: registration phase, login phase, and healthcare phase. We will concentrate on the computation requirements of the healthcare phase from the proposed system because the phase is the most frequently used one. To facilitate computation analysis, we define the computational requirements of a mathematical operation as T_m, a one-way hash function as T_h, symmetric key encryption and decryption as T_{sym}, an elliptic curve cryptosystem as T_{ecc} and a bilinear pairing operation as T_{bp}, and Schnorr digital signature, respectively, but do not consider the overhead of the exclusive-or operations as $T_\oplus$, [45], [47] which require a comparatively quite low overhead than any other operations. Table 3 the computational overhead comparison among the related protocols based on Table 4.

There are four hash operations and six mathematical operations in the proposed protocol, which is less time-consuming than the related works. Figure 7 shows the performance comparisons among the related system. We notice that our work achieves good result in the Table 4 explained the mechanism of arriving computation cost ($2T_{Sign}+2T_{Verify} ==> 0.35$) based on Table 3 [45]. Additionally, using digital signature operations (sign/verify) leads to obtain best result because these operations do not require extra time for encryption/decryption and the transferred data between mobile and server considers very critical and needs more efficiency and secrecy.

Table 3. Computation cost comparison result

Protocol	Verification's time complexity	Result
[34]	1472 $bits$	2 $messages$
[35]	2528 $bits$	2 $messages$
[38]	1760 $bits$	2 $messages$
[39]	3136 $bits$	4 $messages$
[40]	3136 $bits$	4 $messages$
[46]	3872 $bits$	4 $messages$
Proposed	1280 $bits$	3 $messages$

Table 4. Computation cost comparison result

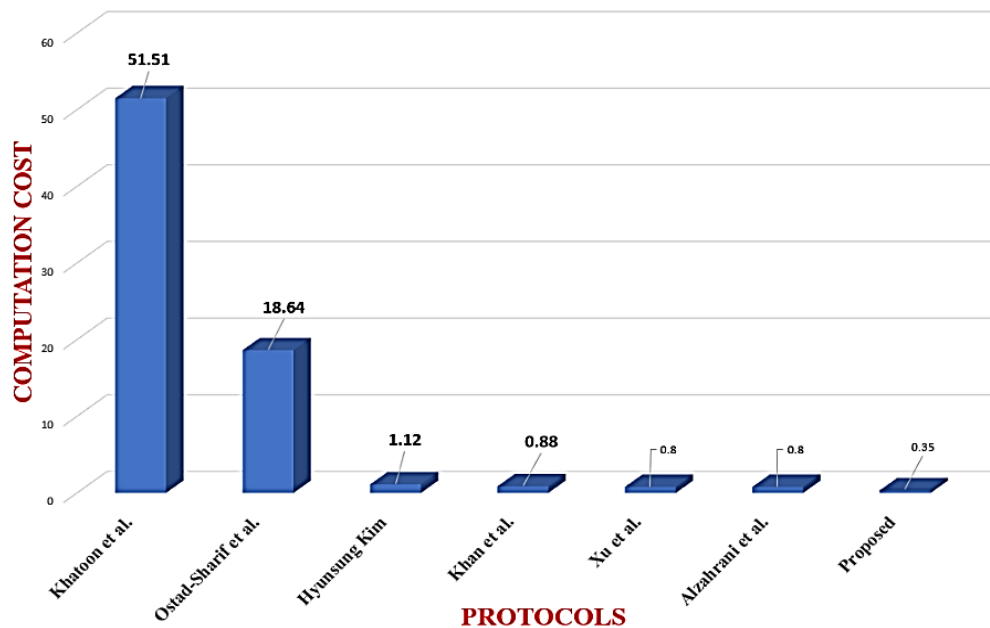|	[34]	[35]	[38]	[39]	[40]	[46]	Proposed
Mutual authentication	O	O	O	O	O	O	O
Anonymity	O	O	O	X	O	O	O
Unlinkability	O	O	O	X	X	O	O
Smart factors	X	X	X	X	X	X	O
All channels are secure	X	X	X	X	X	X	O
Attack resistance	X	X	X	X	X	O	O

Figure 7. Performance comparisons among the related

5.2. Communication result

We used seven different lengths for our communication analysis. Random numbers (128 bits), identification numbers (128 bits), a timestamp (32 bits), a hash function (160 bits), symmetric key encryption (256 bits), bilinear pairing (256 bits), and a Schnorr digital signature (512 bits) are all supported. Comparing the communication costs of the relevant protocols is shown in Table 5. Seven different lengths were used for the communication analysis random numbers (128 bits), identification numbers (128 bits), a timestamp (32 bits), a hash function (160 bits), symmetric key encryption (256 bits), bilinear pairing (256 bits), and a Schnorr digital signature (512 bits). Comparison of communication costs of relevant protocols is shown in Table 5.

In the proposed system, three exchange messages $S_{P_{ij}}$ data to Pd_i using symmetric key encryption, data sent from Pd_i to HCC using Schnorr digital signature, and vice versa are used in the communication processes. The total cost is 1280 bits and the lowest among related systems, as shown in Figure 8. Furthermore, the result relies on the potential of digital signature to reduce the transferred messages (three messages) between main components. The description of messages are:
- Message 1: C_i to Pd_i : Symmetric key encryption (256 bits).
- Message 2: Pd_i to HCC: Schnorr digital signature (512 bits).
- Message 3: HCC to Pd_i: Schnorr digital signature (512 bits).

Total of messages length: 1280.

Table 5. Comparing the communication cost with other related works

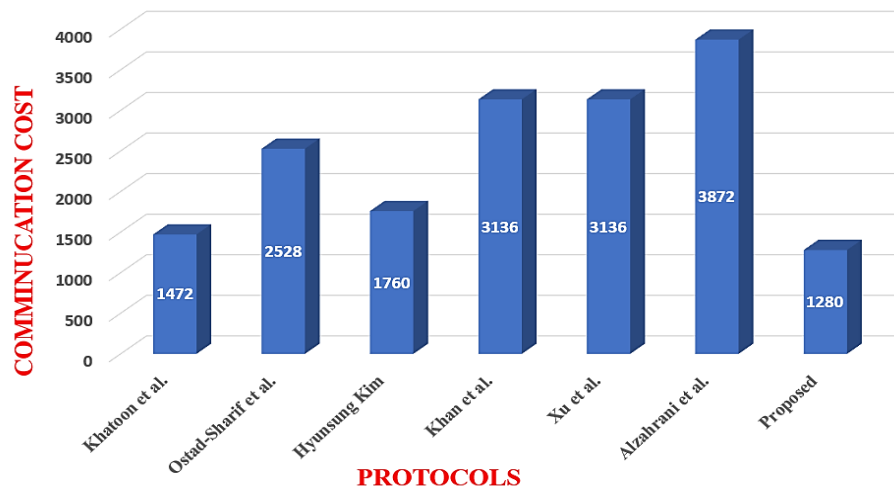| Operation	General meaning	Time
T_m	Mathematical operation	0.005
T_h	One-way hash function	0.08
T_{sym}	Symmetric key encryption	0.14
T_{ecc}	Elliptic curve cryptosystem	4.31
T_{bp}	Bilinear pairing operation	14.48
$T_{\oplus}$	Exclusive OR operation	negligible
T_{Sign}	$T_m + T_h$	0.085
T_{Verify}	$2T_m + T_h$	0.09

Figure 8. Communication cost comparison

6. CONCLUSION

This study proposes a secure and efficient multilayer healthcare system based on WBAN that preserves patients' privacy. It has many security features such as mutual authentication, anonymity, unlinkability, smart factor authentication, and secure data channels. Furthermore, it resists malicious attacks such as impersonation attack, MITM attack, replay attack, and insider attack. The healthcare server manages the primary operations in the system, which gives a high level of security, confidentiality, reliability, and efficiency in key management and distribution. Furthermore, the healthcare server stores health data in an anomaly manner. The proposed scheme was verified formally using the Scyther tool that guarantees that the

system is secure against well-known cyberattacks. The suggested system has low computational and communication costs. Moreover, a high level of security was achieved compared to other related systems.

REFERENCES

[1] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyber–physical systems," *Future Generation Computer Systems*, vol. 56, pp. 476–492, Mar. 2016, doi: 10.1016/j.future.2015.09.004.

[2] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4359–4373, May 2018, doi: 10.1109/TVT.2017.2780183.

[3] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V Vasilakos, "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," *IEEE Access*, vol. 5, pp. 25808–25825, 2017, doi: 10.1109/ACCESS.2017.2764913.

[4] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, Sep. 2020, doi: 10.1109/JSYST.2020.2991168.

[5] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Computing*, vol. 20, no. 3, pp. 2439–2450, Sep. 2017, doi: 10.1007/s10586-017-0848-x.

[6] M. A. Al Sibahee, S. Lu, Z. A. Hussien, M. A. Hussain, K. A.-A. Mutlaq, and Z. A. Abduljabbar, "The best performance evaluation of encryption algorithms to reduce power consumption in WSN," in *International Conference on Computing Intelligence and Information System (CIIS)*, Apr. 2017, pp. 308–312, doi: 10.1109/CIIS.2017.50.

[7] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-based applications in healthcare devices," *Journal of Healthcare Engineering*, vol. 2021, pp. 1–18, Mar. 2021, doi: 10.1155/2021/6632599.

[8] J. Paek, A. Gaglione, O. Gnawali, M. A. M. Vieira, and S. Hao, "Advances in mobile networking for IoT leading the 4th industrial revolution," *Mobile Information Systems*, vol. 2018, pp. 1–3, Dec. 2018, doi: 10.1155/2018/8176158.

[9] N. N. Malik, W. Alosaimi, M. I. Uddin, B. Alouffi, and H. Alyami, "Wireless sensor network applications in healthcare and precision agriculture," *Journal of Healthcare Engineering*, vol. 2020, pp. 1–9, Nov. 2020, doi: 10.1155/2020/8836613.

[10] N. Zhang *et al.*, "Spatial disparities in access to healthcare professionals in Sichuan: evidence from county-level data," *Healthcare*, vol. 9, no. 8, p. 1053, Aug. 2021, doi: 10.3390/healthcare9081053.

[11] B.-M. Park and H.-J. Lee, "Healthcare safety nets during the COVID-19 pandemic based on double diamond model: a concept analysis," *Healthcare*, vol. 9, no. 8, Aug. 2021, doi: 10.3390/healthcare9081014.

[12] Y. J. McDonald *et al.*, "Health service accessibility and risk in cervical cancer prevention: comparing rural versus nonrural residence in New Mexico," *The Journal of Rural Health*, vol. 33, no. 4, pp. 382–392, Sep. 2017, doi: 10.1111/jrh.12202.

[13] D. N. Kaluski *et al.*, "Health insurance and accessibility to health services among Roma in settlements in Belgrade, Serbia—the journey from data to policy making," *Health Policy and Planning*, vol. 30, no. 8, pp. 976–984, Oct. 2015, doi: 10.1093/heapol/czu101.

[14] R. Ganann, W. Sword, K. B. Newbold, L. Thabane, L. Armour, and B. Kint, "Influences on mental health and health services accessibility in immigrant women with post-partum depression: an interpretive descriptive study," *Journal of Psychiatric and Mental Health Nursing*, vol. 27, no. 1, pp. 87–96, Feb. 2020, doi: 10.1111/jpm.12557.

[15] R. Cookson, C. Propper, M. Asaria, and R. Raine, "Socio-economic inequalities in health care in England," *Fiscal Studies*, vol. 37, no. 3–4, pp. 371–403, Sep. 2016, doi: 10.1111/j.1475-5890.2016.12109.

[16] I. Bisio, F. Lavagetto, M. Marchese, and A. Sciarrone, "A smartphone-centric platform for remote health monitoring of heart failure," *International Journal of Communication Systems*, vol. 28, no. 11, pp. 1753–1771, Jul. 2015, doi: 10.1002/dac.2778.

[17] N. Kalid *et al.*, "Based on real time remote health monitoring systems: a new approach for prioritization 'large scales data' patients with chronic heart diseases using body sensors and communication technology," *Journal of Medical Systems*, vol. 42, no. 4, Mar. 2018, doi: 10.1007/s10916-018-0916-7.

[18] P.-Y. Wang, L.-I. Tsao, Y.-W. Chen, Y.-T. Lo, and H.-L. Sun, "'Hesitating and puzzling': the experiences and decision process of acute ischemic stroke patients with prehospital delay after the onset of symptoms," *Healthcare*, vol. 9, no. 8, Aug. 2021, doi: 10.3390/healthcare9081061.

[19] M. Z. U. Rahman, G. V. S. Karthik, S. Y. Fathima, and A. Lay-Ekuakille, "An efficient cardiac signal enhancement using time-frequency realization of leaky adaptive noise cancelers for remote health monitoring systems," *Measurement*, vol. 46, no. 10, pp. 3815–3835, Dec. 2013, doi: 10.1016/j.measurement.2013.07.009.

[20] S. Majumder, T. Mondal, and M. Deen, "Wearable sensors for remote health monitoring," *Sensors*, vol. 17, no. 12, Jan. 2017, doi: 10.3390/s17010130.

[21] D. Gu, G. Humbatova, Y. Xie, X. Yang, O. Zolotarev, and G. Zhang, "Different roles of telehealth and telemedicine on medical tourism: an empirical study from Azerbaijan," *Healthcare*, vol. 9, no. 8, Aug. 2021, doi: 10.3390/healthcare9081073.

[22] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113–122, Jul. 2017, doi: 10.1016/j.eij.2016.11.001.

[23] Q. Liu, K. G. Mkongwa, and C. Zhang, "Performance issues in wireless body area networks for the healthcare application: a survey and future prospects," *SN Applied Sciences*, vol. 3, no. 2, Feb. 2021, doi: 10.1007/s42452-020-04058-2.

[24] D. Formica and E. Schena, "Smart sensors for healthcare and medical applications," *Sensors*, vol. 21, no. 2, Jan. 2021, doi: 10.3390/s21020543.

[25] S. A. Tovino, "Privacy and security issues with mobile health research applications," *Journal of Law, Medicine and Ethics*, vol. 48, no. 1, pp. 154–158, Jan. 2020, doi: 10.1177/1073110520917041.

[26] H. Kim, "Research issues on data centric security and privacy model for intelligent internet of things based healthcare," *ICSES Transactions on Computer Networks and Communications (ITCNC)*, vol. 5, no. 2, 2019.

[27] H. Kim, "Research issues on data centric security and privacy model for intelligent internet of things based healthcare," *Biomedical Journal of Scientific and Technical Research*, vol. 16, no. 3, Mar. 2019, doi: 10.26717/bjstr.2019.16.002856.

[28] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, pp. 943–955, Jan. 2018, doi: 10.1016/j.future.2016.11.024.

[29] J. Vora *et al.*, "Ensuring privacy and security in E- health records," in *International Conference on Computer, Information and Telecommunication Systems (CITS)*, Jul. 2018, pp. 1–5, doi: 10.1109/CITS.2018.8440164.

[30]   J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 231–235, Feb. 2004, doi: 10.1109/TCE.2004.1277867.

[31]   C.-C. Lee, M.-S. Hwang, and I.-E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, Oct. 2006, doi: 10.1109/TIE.2006.881998.

[32]   I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced privacy and authentication: an efficient and secure anonymous communication for location based service using asymmetric cryptography scheme," *Wireless Personal Communications*, vol. 84, no. 2, pp. 1487–1508, May 2015, doi: 10.1007/s11277-015-2699-1.

[33]   A. G. Reddy, A. K. Das, E.-J. Yoon, and K.-Y. Yoo, "A secure anonymous authentication protocol for mobile services on elliptic curve cryptography," *IEEE Access*, vol. 4, pp. 4394–4407, 2016, doi: 10.1109/ACCESS.2016.2596292.

[34]   S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, "Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," *IEEE Access*, vol. 7, pp. 47962–47971, 2019, doi: 10.1109/ACCESS.2019.2909556.

[35]   A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC," *International Journal of Communication Systems*, vol. 32, no. 5, Mar. 2019, doi: 10.1002/dac.3913.

[36]   Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. K. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *Journal of Information Security and Applications*, vol. 52, Jun. 2020, doi: 10.1016/j.jisa.2020.102502.

[37]   M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, Dec. 1989, doi: 10.1098/rspa.1989.0125.

[38]   I. Khan, S. A. Chaudhry, M. Sher, J. I. Khan, and M. K. Khan, "An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data," *Journal of Supercomputing*, vol. 74, no. 8, pp. 3685–3703, Oct. 2018, doi: 10.1007/s11227-016-1886-5.

[39]   Z. Xu, C. Xu, H. Chen, and F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 14, Jul. 2019, doi: 10.1002/cpe.5295.

[40]   B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wireless Personal Communications*, vol. 117, no. 1, pp. 47–69, Mar. 2021, doi: 10.1007/s11277-020-07237-x.

[41]   C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, Jan. 1991, doi: 10.1007/BF00196725.

[42]   Z. Shao, "Fair exchange protocol of Schnorr signatures with semi-trusted adjudicator," *Computers and Electrical Engineering*, vol. 36, no. 6, pp. 1035–1045, Nov. 2010, doi: 10.1016/j.compeleceng.2010.03.005.

[43]   J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC Press, 2007.

[44]   C. J. F. Cremers, "The scyther tool: verification, falsification, and analysis of security protocols," in *International Conference on Computer Aided Verification*, vol. 5123, Springer Berlin Heidelberg, 2008, pp. 414–418.

[45]   H. Ryu and H. Kim, "Privacy-preserving authentication protocol for wireless body area networks in healthcare applications," *Healthcare*, vol. 9, no. 9, Aug. 2021, doi: 10.3390/healthcare9091114.

[46]   H. I. Nasser and M. A. Hussain, "Provably curb man-in-the-middle attack-based ARP spoofing in a local network," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 11, no. 4, pp. 2280–2291, Aug. 2022, doi: 10.11591/eei.v11i4.3810.

[47]   M. Alzuwaini and A. Yassin, "An efficient mechanism to prevent the phishing attacks," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 17, no. 1, pp. 1–11, Jun. 2021, doi: 10.37917/ijeee.17.1.15.

BIOGRAPHIES OF AUTHORS

Mohammad Fareed is M.Sc. student at University of Basrah, Education College for Pure Sciences, Computer Department. He received his BSc in computer science form University of Basrah, College of Science, Department of Computer Science, Iraq in 2016. His research interests include cyber security, cryptography, information technology, and security of systems. He can be contacted at my4irq@gmail.com or pedupg.m.fareed@uobasrah.edu.iq.

Ali A. Yassin is a Professor with the Department of Computer Science, College of Education for Pure Science, University of Basrah. He received the bachelor's and master's degrees from the University of Basrah, Basrah, Iraq, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China. His research interests include the security of cloud computing, image processing, pattern recognition, biometrics, data integrity, DNA cryptography, steganography, sharing data, graphical password, QR code, and soft computing can be contacted at email: alihas@upm.edu.my or Ali.Yassin@uobasrah.edu.iq.