Computers, Materials & Continua
DOI:10.32604/cmc.2021.019051
Article

Tech Science Press

An Efficient Lightweight Authentication and Key Agreement Protocol for Patient Privacy

Seyed Amin Hosseini Seno[1], Mahdi Nikooghadam[1] and Rahmat Budiarto[2,*]

[1]Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad, 9177948974, Iran
[2]Department of Informatics, Faculty of Science and Technology, Universitas Alazhar Indonesia, Jakarta, 12110, Indonesia
[*]Corresponding Author: Rahmat Budiarto. Email: rahmat.budiarto@uai.ac.id
Received: 29 March 2021; Accepted: 30 April 2021

Abstract: Tele-medical information system provides an efficient and convenient way to connect patients at home with medical personnel in clinical centers. In this system, service providers consider user authentication as a critical requirement. To address this crucial requirement, various types of validation and key agreement protocols have been employed. The main problem with the two-way authentication of patients and medical servers is not built with thorough and comprehensive analysis that makes the protocol design yet has flaws. This paper analyzes carefully all aspects of security requirements including the perfect forward secrecy in order to develop an efficient and robust lightweight authentication and key agreement protocol. The secureness of the proposed protocol undergoes an informal analysis, whose findings show that different security features are provided, including perfect forward secrecy and a resistance to DoS attacks. Furthermore, it is simulated and formally analyzed using Scyther tool. Simulation results indicate the protocol's robustness, both in perfect forward security and against various attacks. In addition, the proposed protocol was compared with those of other related protocols in term of time complexity and communication cost. The time complexity of the proposed protocol only involves time of performing a hash function T_h, i.e.,: $O(12T_h)$. Average time required for executing the authentication is 0.006 seconds; with number of bit exchange is 704, both values are the lowest among the other protocols. The results of the comparison point to a superior performance by the proposed protocol.

Keywords: Authentication; key agreement protocol; tele-medical; Scyther; perfect forward secrecy

1 Introduction

With the rapid development and advancement of information technology, new Internet-based services have emerged, such as online banking, online medicine, and online training. Since all of these services utilize the potentially insecure environment of the Internet, the disclosure of important and sensitive information is a major concern for users.

Medical online service is one of the most sensitive Internet-based services, in which patient medical records are stored in databases and transmitted over the Internet. These records contain confidential information on patient illness and treatment. To take advantage of telemedicine, patients must register with a medical provider. After the initial registration process, whenever telemedicine services are accessed, the user and the server must authenticate to each other. If each party confirms the other party's identity, the two can reach a key agreement and exchange their messages through the shared key.

When Internet-based communications are not secure, it is very possible that an unauthorized party disclosures patient information and resulting violation of patient's privacy. To address this issue, many research works have focused on the security and authentication of telecommunications protocols [1–6]. Nevertheless, the proposed protocols are still lack of perfect forward secrecy feature. This research work attempts to address the issue and come up with a robust and efficient lightweight authentication and key agreement protocol for patient privacy in network communications by considering perfect forward secrecy. A robust protocol should be developed based on comprehensive analysis and evaluation on the security requirements. Thus, this work begins with investigating the existing relevant protocols to reveal the flaws and strengths then design the protocol in such a way to avoid the flaws.

The article is organized as follows. Section 2 reviews previous studies and Section 3 analyzes the Mehmood et al. [7] protocol. Section 4 proposes a secure and efficient protocol for authentication and key exchange which is resistant to various attacks. Section 5 deals with the security analysis of the introduced protocol, while Section 6 presents formal analysis using Scyther tool [8]. Then, Section 7 compares the proposed protocol with similar ones in terms of time complexity. Finally, Section 8 provides conclusion and discusses future work.

2 Related Works

In 2012, Wu et al. [9] introduced a "password and smart card" authentication protocol. However, in the same year, Debiao et al. [10] revealed that the Wu et al. protocol was not resistant to "insider and impersonation" attacks and so they introduced an improved protocol. Tan et al. [11] proposed a biometric-based authentication protocol for Telecare medical information system (TMIS), claiming it was resistant to all attacks and could meet various security needs. Finding that the Tan et al. [11] protocol was not immune to DoS and replay attacks, Arshad and Arshad et al. [12] introduced a new three-factor biometric-based protocol. In 2015, Giri et al. [13] demonstrated that the Khan et al. [14] protocol was not resistant to the Stolen-verifier attack and off-line password guessing attack and then developed an RSA encryption-based validation protocol to ward off this attack. When studying the Giri et al. [13] protocol in 2015, Amin et al. [15] discovered that it was vulnerable to insider and password guessing attacks and, thus, could not meet the security requirement of anonymity. In the same year, Arshad et al. [16] demonstrated that the Muhaya protocol [17] was not resistant to the Stolen-verifier attack and off-line password guessing attack and unable to meet the "perfect forward secrecy" security requirement, so Arshad et al. proposed an Elliptic-curve cryptography (ECC)-based authentication scheme for TMIS, in which the user is anonymous.

Chaudhry et al. [18] evaluated Amin and Biswas protocol [19] and reported its lack of resistance to stolen smart card attacks and an ineffective password change phase. They further improved the protocol.

Jiang et al. [19] examined the three-factor authentication protocol proposed by Lu et al. [20] and declared it to be vulnerable to password guessing and user and server impersonation attacks. After making enhancements to the three-factor protocol, they provided a more viable solution to the security issues proposed by Lu et al. [20]. Zhang et al. [21] presented a three-factor plan for medical service authentication, by then, Aghili et al. [22], showed to be at risk of DoS and insider attacks.

At the same time, Ostadsharif et al. [23] reviewed the protocols presented in [13,15] and found they were not resistant to key compromise impersonation attacks. In addressing this, they introduced a new protocol for authentication and key agreement between patients and medical practitioners. Later, Kumari et al. [24] reported that the protocol of Ostadsharif et al. [25] still failed to resist key compromise impersonation attacks. Furthermore, Khatoon et al. [26] presented a physician and medical practitioner authentication protocol, which Amintoosi et al. [4] reviewed the same year, concluding that its security did not provide perfect forward secrecy and was open to known-session-specific temporary information attacks.

Ravanbakhsh et al. [2] then came up with an interesting scheme for authentication and key agreement in telemedicine, which, although their design had several advantages, but their design could not meet the "perfect forward secrecy" and is not resistant to "known session-specific temporary information attack". Sowjanya et al. [27] examined the plan proposed by Li et al. [28] and concluded that the plan [28] has shortcomings such as not meeting the security requirements of Perfect Forward Secrecy. Also, He et al. [29] states that the plan in their other article [30] unable to meet the "perfect forward secrecy" security requirement Lastly, He et al. introduced a protocol for remote patient and physician authentication and claimed that it was resistant to all attacks and met various security requirements. The present study, nevertheless, proves that this protocol does not satisfy the security demands of perfect forward secrecy. Tab. 1 summarizes existing protocols and their issues in chronological time.

Table 1: Existing protocols and issues in chronological time

Year	Proposed protocol	Issues
2012	Password & smart card authentication [9]	Insider & impersonate attacks [10]
2013	Biometric-based authentication for TMIS [11]	DoS and Replay attacks [12], then proposed a new one, 2014
2013	Authentication scheme for healthcare services [14]	Stolen verifier & offline password guessing [13], 2015
2015	Robust RSA-based authentication for TMIS [13]	—Insider attack [15], then propose Improved RSA-based authentication —Key compromise impersonation attacks attack [23]
2015	Zhau's authentication scheme cryptanalyst for TMIS [17]	Stolen verifier and password guessing attacks [16], then propose ECC-based authentication protocol
2015	Improved RSA-based authentication [15]	—Key compromise impersonation attacks attack [23] —Stolen smart card attack & ineffective password change phase [18], then propose multi-server biometric authentication scheme

(Continued)

Table 1: Existing Protocols and issues in chronological time

Year	Proposed protocol	Issues
2015	3-factors authentication [20]	Password guessing & impersonation server [19]
2018	3-factor & dynamic authentication [21]	DoS & insider attacks [22], 2019
2015	Robust RSA-based authentication [13]	
2017	Enhanced 1-round authentication protocol for wireless body area networks with user anonymity [28]	Does not meet the security requirements of Perfect Forward Secrecy [27], 2020
2013	Improved remote user mutual authentication and session key agreement [30]	Missing perfect forward secrecy and is not resistant to known session-specific temporary information attack [29], 2016
2019	Privacy Preserved, Provable Secure, Mutually Authenticated Key Agreement [26]	Missing perfect forward secrecy [4], then propose ECC-based Authentication and Key Management, 2019
2019	Robust & efficient ECC-based mutual authentication [23]	Key compromise impersonation attack [24]
2019	Resistant to all attacks authentication and secure key management [7]	Missing perfect forward secrecy [this work]

3 Analyzing the Weaknesses of the Mehmood et al.'s Protocol

This section briefly reviews the protocol by Mehmood et al. [7] and analyzes the weaknesses of its security. Authentication and key authentication protocols usually include three phases: registration, authentication, and password change. According to Fig. 1, in the registration phase, the communication channel between the two channel entities is assumed to be secure. Furthermore, the parties communicate through a secure channel or in person. During the login and authentication process (Fig. 2), the channel is considered unsafe and the attacker can listen to the channel. Tab. 2 provides the symbols employed in Mehmood et al.'s protocol.

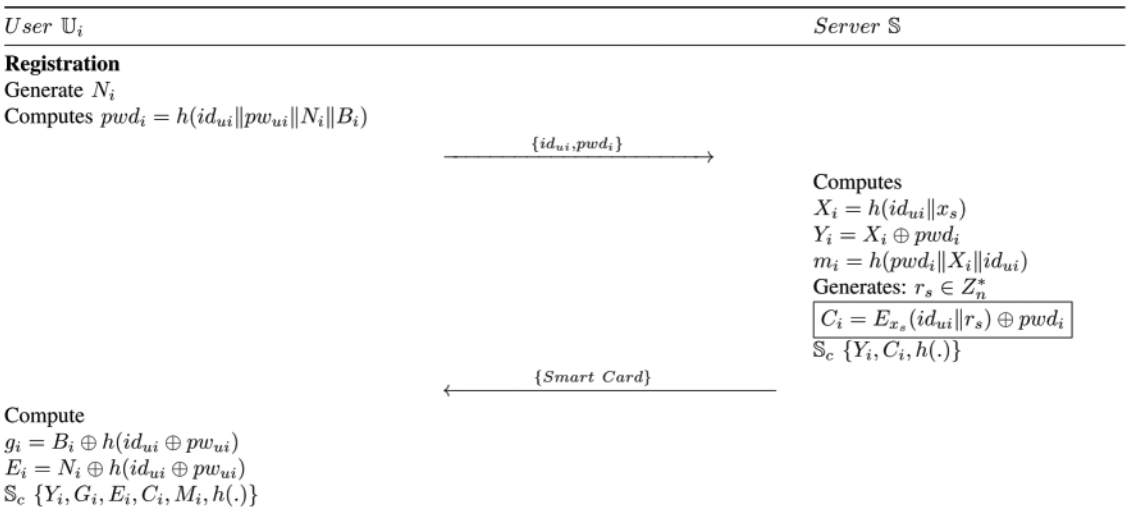

Figure 1: Registration phase of Mehmood et al. [7] protocol

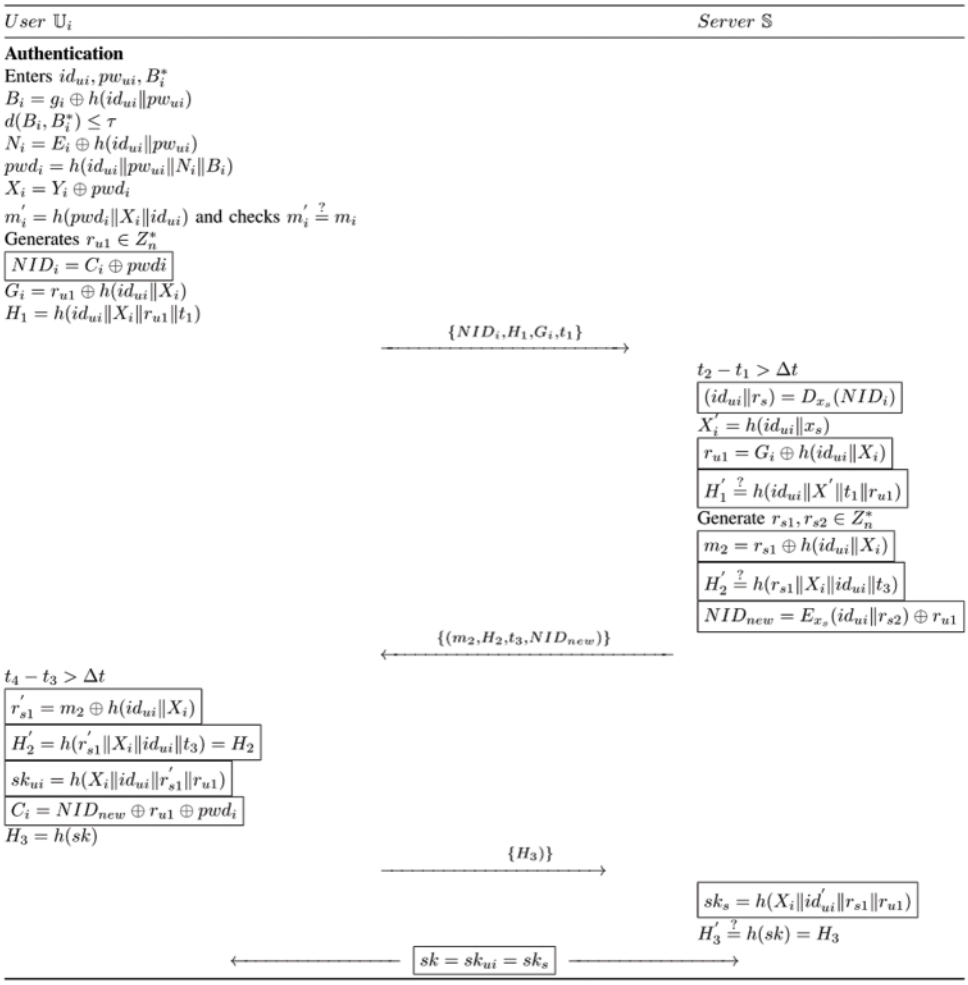

Figure 2: Authentication phase of Mehmood et al. [7] protocol

Table 2: Symbols used in Mehmood et al. [7] protocol

Symbol	Description	Symbol	Description
S, U_i	Server and user	x_s	Service provider confidential key
id_{ui}, pw_{ui}	User ID and password	H(.)	Hash function
r_{u1}, r_{s1}	Random numbers chosen by the parties	$\|$	Concatenation operation
B_i	User biometric parameter	$\oplus$	XOR operation
		Sc	User smart card

Mehmood et al. [7] presented a protocol for two-way authentication of patients and medical servers, declaring that it was resistant to most attacks and fulfilled various security needs. This section, however, proves that this protocol does not provide perfect forward secrecy and is vulnerable to DoS attacks.

3.1 Perfect Forward Secrecy

The security system of Perfect Forward Secrecy assumes that an attacker should not be able to access the session key even if long term parameters, such as the server's secret key, are compromised. However, if such a breach occurs in Mehmood et al.'s protocol, the attacker can, in fact, obtain the session key. To explain the matter, one can suppose that the attacker has the secret key of the server. Because parameter NID_i is exchanged on the public channel (an insecure channel), the attacker can decode this parameter and obtain id_{ui} and r_s. As assumed that the attacker already have had the server's secret key and now also to possess parameter id_{ui}, the attacker can then calculate X_i based on $X_i = h(id_{ui} \,||\, x_s)$. However, because there is a G_i parameter on the public channel in $r_{u1} = G_i \oplus h(id_{ui} \,||\, X_i)$ and the attacker had acquired X_i and id_{ui} in the previous steps, the attacker can now obtain r_{u1}.

Furthermore, due to the relationship $r_{s1} = m_2 \oplus h(id_{ui} \,||\, X_i)$ has parameter m_2 on the public channel and the attacker had obtained id_{ui} and X_i in the previous steps, the attacker is able to acquire r_{s1}. As a result, the attacker can procure the session key from relationship $SK = \mathrm{h}(X_i \,||\, id_{ui} \,||\, r_{s1} \,||\, r_{u1})$.

3.2 DOS Attack

When the user sends the first message to the server, the initial action taken before authentication is decryption, which is a demanding operation. During this strain on the server, the attacker can repeatedly send the message, thus ***keeping*** the server extremely busy and unable to respond to requests.

4 A Secure and Efficient Protocol for Authentication and Key Exchange

In order to address the drawbacks of Mehmood et al. [7] protocol, this work introduces a secure and efficient ECC-based protocol for authentication and key exchange. This scheme features registration, authentication, key agreement, and password update stages, for which a detailed description will be provided. Tab. 3 presents the symbols utilized in the proposed protocol.

Table 3: Symbols used in the proposed protocol

Symbol	Description	Symbol	Description
ID_i	User ID	s	Service provider confidential key
ID_s	Server ID	Sc	User smart card
pw_i	Password of $\mathrm{User_i}$	$\oplus$	XOR operation
SC	Smart Card	$\|\|$	Concatenation operation

4.1 Registration Phase

As seen in Fig. 3, during the registration process, the patient selects his/her own ID (ID_i) and a password (pw_i). Then, after selecting a random number, a_i, the proposed protocol computes A_i as $A_i = h(ID_i \,||\, pw_i \,||\, a_i)$ and finally sends A_i and ID_i to the server via a secure channel. Upon receiving a message from the patient, the server obtains parameters B_i, HID_i, D_i , Q_i, and G_i from relationships described in the following. In the registration process for each patient, the Q_i and d_i parameters are ultimately saved in the server's memory. Additionally, the D_i, B_i, G_i, b_i and

d_i parameters are stored in the patient's smart card, which is sent to the patient. The patient then adds the a_i and $W_i = G_i \oplus A_i$ parameter to the smart card and the registration process finishes.

Compute $HID_i = h(b_i \,||\, ID_i)$

Compute $B_i = h(A_i \,||\, HID_i)$

Selects random number d_i

Compute $D_i = h(B_i \,||\, ID_i \,||\, A_i)$

Compute $Q_i = h(HID_i \,||\, s)$

Compute $G_i = B_i \oplus Q_i$

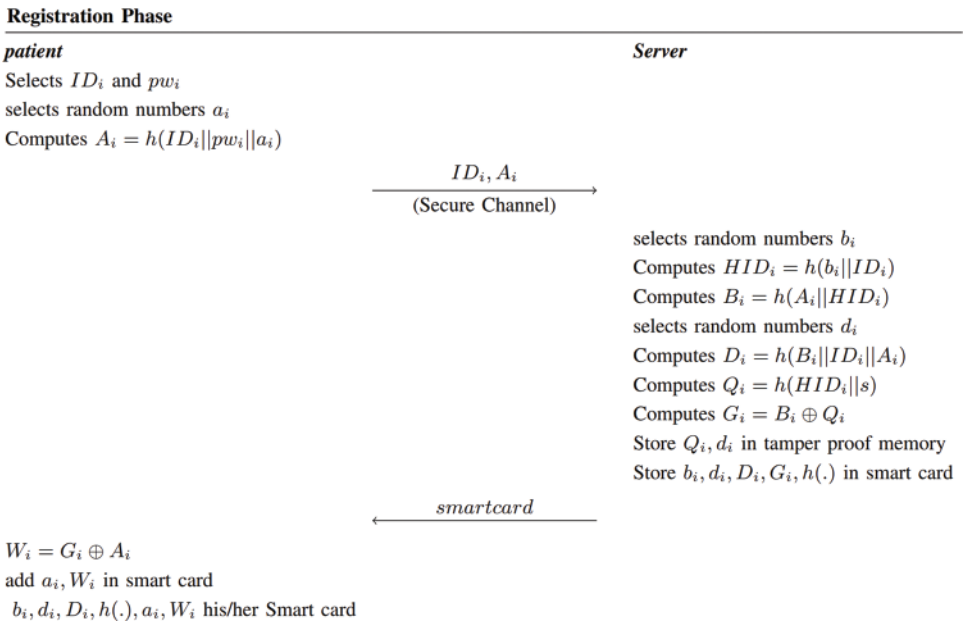

Figure 3: Registration phase of the proposed protocol

4.2 Login and Authentication Phase

In this phase, the patient and server authenticate each other, after which the patient can log into the server. As presented in Fig. 4, during the login and authentication stage of the proposed protocol, the patient inserts his/her smart card into the card reader and enters the correct *ID* and password. Initially, through the following relationships, the smart card is verified as belonging to the patient in question and, therefore, not stolen.

Enters his/her ID_i^* and pw_i^*

Compute $A_i^* = h(ID_i^* \,||\, pw_i^* \,||\, a_i)$

Compute $HID_i^* = h(b_i \,||\, ID_i^*)$

Compute $B_i^* = h(A_i \,||\, HID_i^*)$

Check $D_i = D_i^*$

Compute $G_i = W_i \oplus A_i$

Compute $Q_i = B_i \oplus G_i$

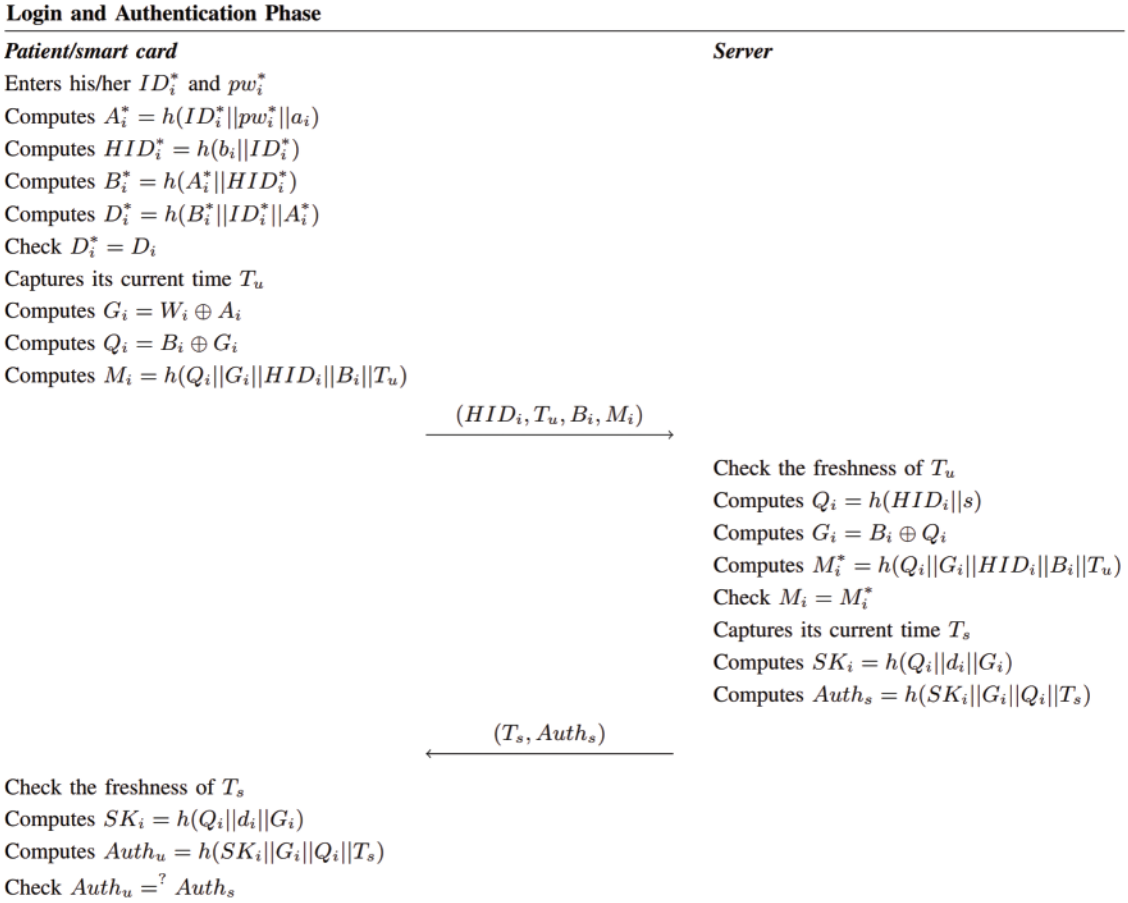

Figure 4: Login and authentication phase of the proposed protocol

At this point, parameter M_i is obtained from relation $M_i = h(Q_i \,||\, G_i \,||\, HID_i \,||\, B_i \,||\, T_u)$ and the timestamp (T_u) is selected. Finally, parameters M_i, T_u, B_i and HID_i are sent to the server.

As soon as it receives the patient's message, the server checks for its freshness. Possessing its own secret key, the server obtains parameter Q_i from the relation $Q_i = h(HID_i \,||\, s)$. Then, from the following relationships, the server determines whether the message received is fake or not; in other words, the authenticity of the patient message is verified.

Compute $Q_i = h(HID_i \,||\, s)$

Compute $G_i = B_i \oplus Q_i$

Compute $M_i^* = h(Q_i \,||\, G_i \,||\, HID_i \,||\, B_i \,||\, T_u)$

Check $M_i = M_i^*$

Now, the server selects the timestamp (T_s) and obtains the session key from the relationship $SK_i =$ h($Q_i \,||\, d_i \,||\, G_i$). Also acquired is parameter $Auth_s$ from the following relation. Finally, the

server sends $Auth_s$ and T_s to the patient.

$Auth_s = h\,(SK_i \,||\, G_i \,||\, Q_i \,||\, T_s)$

As soon as it receives the server's message, the patient checks for its freshness. After creating the session key from the following relationship, the patient authenticates the received message to verify its authenticity and identity. In this manner, the login and authentication phase of the proposed protocol finishes.

Compute $SK_i =$ h$(Q_i \,||\, d_i \,||\, G_i)$

Compute $Auth_s = h(SK_i \,||\, G_i \,||\, Q_i \,||\, T_s)$

Check $Auth_s =?Auth_u$

4.3 Change Password Phase

In this phase, the patient can securely change his/her password. To do so, the patient first enters the password (pw_i^*) as well as ID (ID_i^*). Then, the following relationships are computed to determine if the smart card belongs to the patient in question.

Compute$A_i^* = h(ID_i^* \,||\, pw_i^* \,||\, a_i)$

Compute$HID_i^* = h(b_i \,||\, ID_i^*)$

Compute $B_i^* = h(A_i \,||\, HID_i^*)$

Check $D_i = D_i^*$

At this point, the patient enters the new password (pw_i^{**}). The following relationships are computed and then parameter D_i^{**} replaces parameter D_i in the smart card.

Compute $A_i^{**} = h(ID_i^* \,||\, pw_i^{**} \,||\, a_i)$

Compute $HID_i^* = h(b_i \,||\, ID_i^*)$

Compute $B_i^{**} = h(A_i^{**} \,||\, HID_i^*)$

Compute $D_i^{**} = h(B_i^{**} \,||\, ID_i^* \,||\, A_i^{**})$

5 Security Analysis of the Proposed Protocol

The security parameters of the proposed protocol are discussed in the following sections.

5.1 Perfect Forward Secrecy

According to Nikooghadam et al. [31], the security measure of Perfect Forward Secrecy assumes that an attacker cannot obtain the session key even if the secret key of one of the parties is disclosed or if long term parameters are exposed. In the proposed protocol, the session key is equal to $SK_i =$ h$(Q_i \,||\, d_i \,||\, G_i)$, such that the attacker cannot access parameter d_i, even when it is able to acquire the secret key of the server. Since d_i is a random parameter, the attacker cannot obtain it.

5.2 Anonymity

In anonymity, it is presumed that the attacker cannot access the identity of the parties if it intercepts all messages transmitted on the public channel. In the proposed protocol, even if the attacker hears all messages transmitted on the public channel, it will not be able to obtain the parties' *IDs*.

5.3 Replay Attack

In the replay attack, the attacker is assumed to intercept an old message from the public channel and send it to the parties after a period of time. In the proposed protocol, such attack does not occur due to the use of time stamps and random parameters.

5.4 DoS Attack

A DoS attack occurs when a substantial operation, such as scalar multiplication, is performed by one of the two entities. The proposed protocol would not experience such an attack as no considerable jobs are undertaken, such as decoding or scalar multiplication.

5.5 User Impersonation Attack

Due to the two-way authentication between the patient and server, impersonation is not possible. One can consider the scenario in which the attacker sends fake parameters, i.e.,: M_i, T_u, B_i, and HID_i, instead of the main parameters. Since the attacker does not have the server's secret key, it is not able to obtain the Q_i parameter nor is feasible to continue.

5.6 Server Impersonation Attack

Since there is a session key within the $Auth_s$ parameter and $Auth_s$ is used for authentication, the attacker cannot obtain the session key and, therefore, cannot impersonate. Furthermore, with the output of the Scyther tool, there is also no possibility of impersonation attacks occurring.

5.7 Insider Attack

In the insider attack, it is assumed that the attacker is on the server side and intends to acquire the user password. Consequently, in the registration stage, the proposed protocol does not send the patient's password directly to the server. Therefore, the password is sent to the service provider in the form of $A_i = h(ID_i \,||\, pw_i \,||\, a_i)$. As a result, such an attack is not possible.

5.8 Password Guessing Attack

The assumption of the password guessing attack is that the user password cannot be guessed even if the attacker intercepts all the messages transmitted on the public channel. Because the user password is in the format of $A_i = h(ID_i \,||\, pw_i \,||\, a_i)$, it has been exchanged and, therefore, cannot be guessed.

5.9 Known-Session-Specific Temporary Information Attack

In this attack, it is presumed that the attacker cannot obtain nor construct the session key, even if it acquires random parameters. Furthermore, in the session key, there are long term parameters, such as Q_i. Therefore, if the attacker acquires random parameters, the long term parameters shall prevent this attack.

5.10 Stolen-Verifier Attack

The stolen-verifier attack assumes that it is not possible for the attacker to access the session key if it has acquired the parameters within the server memory or the smart card. In the proposed protocol, since the server's memory is tamper-proof, such parameters cannot be stolen. In addition, since there are no important parameters inside the smart card, the attacker cannot obtain the session key by stealing it.

6 Formal Security Analysis with Scyther

Scyther [8] is a powerful and effective tool for analyzing and identifying potential attacks and security protocol vulnerabilities. This official tool automatically analyzes protocol and scrutinizes its behavior when faced with most possible attacks. Implementation code Scyther tool is shown in Fig. 5.

Fig. 6 provides the output of the proposed protocol review by Scyther, i.e.,:

— The Niagree feature ensures the parties in communication are confident that messages are securely transmitted and in correct order between them.
— The Nisynch feature makes sure that messages exchanged between parties cannot be decrypted and resent.
— The Alive feature guarantees that the protocol steps are approved by the parties in communication.
— The Weakagree feature sees to it that the protocol does not impersonate.
— The secret property also ensures that the relevant parameter remains safe.

As shown in Fig. 6, the proposed authentication protocol provides all of the above features.

```
usertype TimeStamp;
hashfunction H1;
secret XOR: Function;
secret IDi,pwi,ai,bi,di,s;
macro Ai=H1(IDi,pwi,ai);
macro hidi=H1(bi,IDi);
macro Bi=H1(Ai,hidi);
macro Di=H1(Bi,IDi,Ai);
macro Qi=H1(hidi,s);
macro Gi=XOR(Bi,Qi);
protocol MAHDI(user,server)
{
role user                {
var Auths;
macro Ai=H1(IDi,pwi,ai);
macro hidi=H1(bi,IDi);
macro Bi=H1(Ai,hidi);
macro Dii=H1(Bi,IDi,Ai);
match(Dii,Di);
macro Mi=H1(Qi,Gi,hidi,Bi);
send_1(user,server, (hidi,Bi,Mi));
recv_2(server,user, (Auths));
macro Qi=XOR(Bi,Gi);
macro ski=H1(Qi,di,Gi);
macro Authu=H1(ski,Gi,Qi);
match(Authu,Auths);
claim (user, Alive ) ;
claim (user, Nisynch );
claim(user,Niagree);
claim(user,Weakagree);
claim(user, Secret, sk);
                        };
role  server
                        {
recv_1(user,server, (hidi,Bi,Mi));
macro Qii=H1(hidi,s);
macro Gii=XOR(Bi,Qii);
macro Mii=H1(Gii,Qii,hidi,Bi);
match(Mii,Mi);
macro ski=H1(Qii,di,Gi);
macro Auths=H1(ski,Gii,Qii);
send_2(server,user, (Auths));
claim (server, Alive ) ;
claim (server, Nisynch );
claim(server,Niagree);
claim(server,Weakagree);
claim(server, Secret, sk);
                                    };
};
```

Figure 5: Implementation code of Scyther

According to the material presented and evaluated by the usage of the Scyther tool, Tab. 4 compares the security of the proposed protocol with that of other similar protocols. Based on the information in this table, the proposed protocol is resistant to various attacks and meets various security requirements.

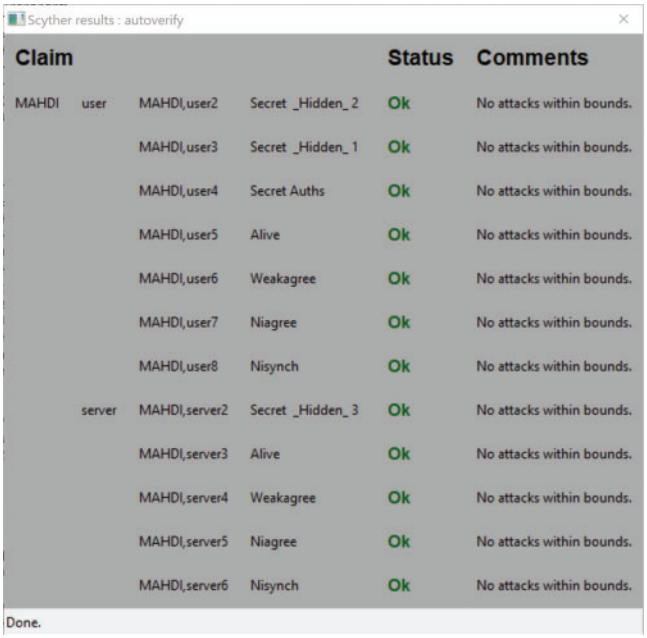

Figure 6: Evaluation of proposed protocol by Scyther tool [8]

Table 4: Security comparison

Attacks type	[26]	[21]	[7]	[16]	[17]	[2]	[29]	[28]	Proposed
Perfect forward secrecy	No	Yes	No	No	No	No	Yes	No	Yes
Anonymity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DOS attack	Yes	No	No	Yes	Yes	Yes	No [27]	Yes	Yes
Stolen-verifier attack	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
User impersonation attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Server impersonation attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password guessing attack	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Known-session-specific Temporary information attack	No	Yes	Yes	Yes	Yes	No	No [27]	Yes	Yes
Insider attack	Yes	No	Yes	Yes	Yes	Yes	Yes	No [27]	Yes

Notes: No: Not Resistant to Attack Yes: Resistant to Attack

7 Analysis and Validation Using BAN Logic

In this section, we analyze and validate our proposed design using BAN logic. The logical assumptions and rules of the Burrows–Abadi–Needham (BAN) logic, as well as the security objectives and ideal forms, are defined in (1) to (6). The symbols used are shown in Tab. 5.

$$\text{Message meaning rule is}: \frac{P \equiv P \overset{K}{\leftrightarrow} Q,\ P \lhd \{X\}K}{P| \equiv Q \sim X} \tag{1}$$

$$\text{The freshness rule is}: \frac{P| \equiv \#(X)}{P| \equiv (X,\ Y)} \tag{2}$$

$$\text{The nonce verification rule is}: \frac{P| \equiv \#(X),\ P| \equiv Q| \sim X}{P| \equiv Q| \equiv X} \tag{3}$$

$$\text{The jurisdiction rule is}: \frac{P| \equiv Q| \Rightarrow X,\ P| \equiv Q| \equiv X}{P| \equiv X} \tag{4}$$

$$\text{The belief rule is}: \frac{P| \equiv (X), P| \equiv (Y)}{P| \equiv (X,\ Y)} \tag{5}$$

$$\text{The H rule is}: \frac{P| \equiv \mathrm{Q} \sim \mathrm{H}(X), P \lhd X}{P| \equiv \mathrm{Q} \sim X} \tag{6}$$

Some assumptions are shown in Tab. 6.

Table 5: Symbols of BAN logic

Symbol	Description
$P\| \equiv X$	The principal P believes a statement X
$P \lhd X$	The principal P sees a statement X
$P\| \sim X$	The principal P once said a statement X
$P \Rightarrow X$	The principal P has jurisdiction over X
$\#(X)$	The message X is fresh
$P \equiv Q \overset{K}{\leftrightarrow} P$	The secret key K is used by P and Q for communicating
$\{X\}K$	The formula X is encrypted with the key K
$<X>K$	The formula X is XORed with the key K
$(X)K$	The formula X is hashed with the key K

Table 6: Assumptions

No.	Assumption	No.	Assumption
1	**A1:** $\mathrm{U_i}\| \equiv (\mathrm{U_i} \overset{d_i}{\leftrightarrow} S)$	5	**A5:** $S\| \equiv U_i \Rightarrow (U_i \overset{sk}{\leftrightarrow} S)$
2	**A2:** $\boldsymbol{S}\| \equiv (\mathrm{U_i} \overset{d_i}{\leftrightarrow} S)$	6	**A6:** $U_i\| \equiv S \Rightarrow (U_i \overset{sk}{\leftrightarrow} S)$
3	**A3:** $\mathrm{U_i}\| \equiv (\mathrm{U_i} \overset{Q_i}{\leftrightarrow} S)$	7	**A7:** $\mathrm{U_i}\| \equiv \#(T_u)$
4	**A4:** $\boldsymbol{S}\| \equiv (\mathrm{U_i} \overset{Q_i}{\leftrightarrow} S)$	8	**A8:** $S\| \equiv \#(T_s)$

Goals are as follows:

$\mathrm{U_i}\| \equiv (\mathrm{U_i} \overset{sk}{\leftrightarrow} S)$.

$S\| \equiv (\mathrm{U_i} \overset{sk}{\leftrightarrow} S)$.

Idealized forms are as follows:

Message 1: $\mathrm{U_i} \rightarrow S$: $((G_i, HID_\mathrm{i}, B_\mathrm{i}, T_u)_{Q_i}, (G_\mathrm{i})_{Q_i}, T_u, (\mathrm{ID_i})_{b_i})$.

Message 2: $S \rightarrow \mathrm{U_i}$: $(T_s, (\mathrm{U_i} \overset{sk}{\leftrightarrow} S, G_i, T_s)_{Q_i})$.

Based on the assumptions and logical rules of BAN logic, we analyze the ideal form of the proposed protocol as follows: According to the Message 1, we can obtain the following:

R1: $S \lhd ((G_i, HID_\mathrm{i}, B_\mathrm{i}, T_u)_{Q_i}, < G_\mathrm{i} >_{Q_i}, T_u, (\mathrm{ID_i})_{b_i})$.

Based on the assumption A2, and after applying the H rule to R1, R2 can be deduced as:

R2: $S| \equiv \mathrm{U_i}| \sim (G_i, HID_\mathrm{i}, B_\mathrm{i}, T_u)$.

Based on the assumption A7, and after applying the nonce verification rule H to R2, R3 can be deduced as:

R3: $S| \equiv \mathrm{U_i}| \sim (G_i, HID_\mathrm{i}, B_\mathrm{i})$.

Based on the Message 2, R4 can be deduced as:

R4: $\mathrm{U_i} \lhd (T_s, (\mathrm{U_i} \overset{sk}{\leftrightarrow} S, G_i, T_s)_{Q_i})$.

Based on the assumption A4, and after applying the H rule to R4, R5 can be deduced as:

R5: $\mathrm{U_i}| \equiv S| \sim (\mathrm{U_i} \overset{sk}{\leftrightarrow} S, G_i, T_s)$.

Based on the applying the nonce verification rule to R5, R6 can be deduced as:

R6: $U_i| \equiv S| \equiv (G_i)$.

Based on the assumptions A1, A3, A6, and the session key $\mathrm{sk} = \mathrm{h}\ (Q_i \parallel d_i \parallel G_i)$, R7 can be deduced as:

R7: $U_i| \equiv S| \equiv (U_i \overset{sk}{\leftrightarrow} S)$.

Based on the assumption A5, and after applying the jurisdiction rule to R7, R8 can be deduced (which is Goal1) as:

R8: $U_i| \equiv (U_i \overset{sk}{\leftrightarrow} S)$.

Based on the R3, assumptions A2, A4 and the session key $\mathrm{sk} = \mathrm{h}\ (Q_i \parallel d_i \parallel G_i)$, R9 can be deduced as:

R9: $\mathrm{S}| \equiv U_i| \equiv (U_i \overset{sk}{\leftrightarrow} S)$.

Based on the assumption A6, and after applying the jurisdiction rule to R9, R10 can be deduced (which is Goal2) as:

R10: $S| \equiv (U_i \overset{sk}{\leftrightarrow} S)$.

8 Analysis and Comparison of the Proposed Protocol's Time Complexity with Other Similar Protocols

Based on research work by He et al. [30] the computation time of a fuzzy extraction operation, the time of performing a hash function, the time of performing symmetric encryption/decryption, the time of performing ECC point multiplication, the time of performing ECC point addition operation, and the time of modular exponentiation operation is 0.063075, 0.0005, 0.0087, 0.063075, 0.000262, and 0.522 s, respectively and the symbol for each are listed in the Tab. 7. Furthermore, for the communication cost, we have considered the size of an identifier or timestamp to be 32 bits, a nonce to be 64 bits, an EC point to be 320 bits, and a hash output to be 256 bits.

Table 7: Symbols used to calculate time complexity and approximate time

Symbol	Description	Approximate time (ms)
T_f	Time of a fuzzy extraction operation	0.063075
T_h	Time of performing a hash function	0.0005
$T_{en/d}$	Time of performing symmetric & encryption/decryption	0.0087
T_{mu}	Time of performing a (ECC) point multiplication	0.063075
T_A	Time of performing a (ECC) point addition operation	0.000262
T_E	Time modular exponentiation operation	0.522

As exhibited in Tabs. 8 and 9, the proposed protocol performs better than or closer to similar protocols in the past. The importance of this issue is apparent when the proposed protocol is able to meet security requirements with less complexity than of most similar protocols.

Table 8: Time complexity of the proposed protocol and other similar protocols

Protocol	Time complexity	Approximate time (s)
Proposed protocol	$12T_h$	*0.006*
[7]	$19T_h + 3e/d$	*0.0356*
[26]	$12T_h + 2T_{en/d} + 5T_{mu}$	*0.3387*
[21]	$19T_h$	*0.0095*
[16]	$14T_h + 6T_{mu}$	*0.3854*
[17]	$12T_h + 2T_E$	*1.05*
[2]	$11T_h + 6T_{mu} + 1T_f$	*0.447*
[29]	$7T_h + 8T_{mu}$	*0.5081*
[28]	$4T_h + 5T_{mu}$	*0.3173*

Table 9: The number of messages exchanged on the channel at the authentication stage

Protocol	Message exchanged #	Bit exchanged #
Proposed protocol	2	704
Mehmood et al. [7]	3	1144
Ostadsharif et al. [25]	2	984
Zhang et al. [21]	3	1120
Arshad et al. [16]	3	1696
Bin Muhaya et al. [17]	3	1600
Ravanbakhsh et al. [2]	3	1248
He et al. [29]	2	960
Li et al. [28]	2	1120

9 Conclusion

Having done revealing flaws in perfect forward secrecy and preventing DoS attacks of authentication and key agreement scheme proposed by Mehmood et al, this work has proposed a secure

and ultra-lightweight protocol for medical services communication. The proposed protocol was analyzed in term of secureness and performance during the authentication stage was measured. Formal analysis using Scyther tool proves its robustness against various attacks, and demonstrates its ability to provide various security features. During the authentication stage, measurement results showed that the proposed protocol outperforms other existing protocol and achieves a satisfactory computational time and less number of bits in the exchanged messages. Telemedicine provides easy and secure access to patient information by physicians and access to the large number of specialist physicians needed by patients, even patients in remote and underprivileged areas, while saving time and money.

As future work, the proposed protocol can be implemented hardware-wise using the ARM and FPGA programming languages and the Cortex-M3 Microcontroller board, and the results can be reviewed.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services," *Wireless Personal Communication*, vol. 83, no. 4, pp. 2439–2461, 2015.

[2] N. Ravanbakhsh and M. Nazari, "An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 55–88, 2016.

[3] 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, pp. e3913, 2019.

[4] H. Amintoosi and M. Nikooghadam, "A novel provably-secure ECC-based authentication and key management protocol for telecare medical information systems," in *Proc. of 9th Int. Conf. on Computer and Knowledge Engineering*, Mashhad, Iran, pp. 85–90, 2019.

[5] N. Radhakrishnan and M. Karuppiah, "An efficient and secure remote user mutual authentication scheme using smart cards for telecare medical information systems," *Informatics in Medicine Unlocked*, vol. 16, no. 2, pp. 100092, 2019.

[6] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," *IEEE Access*, vol. 7, pp. 23514–23526, 2019.

[7] Z. Mehmood, A. Ghani, G. Chen and A. S. Alghamdi, "Authentication and secure key management in e-health services: A robust and efficient protocol using biometrics," *IEEE Access*, vol. 7, pp. 113385–113397, 2019.

[8] C. J. F. Cremers, "Scyther-semantics and verification of security protocols," Ph.D. Thesis. Eindhoven University of Technology, 2006.

[9] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2010.

[10] H. Debiao, C. Jianhua and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989–1995, 2011.

[11] Z. Tan, "An efficient biometrics-based authentication scheme for telecare medicine information systems," *Networks*, vol. 2, no. 3, pp. 200–204, 2013.

[12] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 12, pp. 1, 2014.

[13] D. Giri, T. Maitra, R. Amin and P. D. Srivastava, "An efficient and robust RSA-based remote user authentication for telecare medical information systems," *Journal of Medical Systems*, vol. 39, no. 145, pp. 770, 2014.

[14] M. K. Khan and S. Kumari, "An authentication scheme for secure access to healthcare services," *Journal of Medical Systems*, vol. 37, no. 4, pp. 201, 2013.

[15] R. Amin and G. P. Biswas, "An improved RSA based user authentication and session key agreement protocol usable in TMIS," *Journal of Medical Systems*, vol. 39, pp. 1–14, 2015.

[16] H. Arshad, V. Teymoori, M. Nikooghadam and H. Abbassi, "On the Security of a two-factor authentication and key agreement scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 39, no. 8, pp. 1, 2015.

[17] F. T. Bin Muhaya, "Cryptanalysis and security enhancement of Zhu's authentication scheme for telecare medicine information system," *Security and Communication Networks*, vol. 8, no. 2, pp. 149–158, 2014.

[18] S. A. Chaudhry, M. T. Khan, M. K. Khan and T. Shon, "A multiserver biometric authentication scheme for TMIS using elliptic curve cryptography," *Journal of Medical Systems*, vol. 40, no. 11, pp. article–no. 230, 2016.

[19] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang *et al.,* "Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1061–1073, 2017.

[20] Y. Lu, L. Li, H. Peng and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 39, no. 32, pp. 1, 2015.

[21] L. Zhang, Y. Zhang, S. Tang and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2018.

[22] S. F. Aghili, H. Mala, M. Shojafar and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT," *Future Generation Computer Systems*, vol. 96, no. 1, pp. 410–424, 2019.

[23] A. Ostad-Sharif, D. Abbasinezhad-Mood and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *Journal of Medical Systems*, vol. 43, no. 10, pp. 175, 2018.

[24] S. Kumari, P. Chaudhary, C.-M. Chen and M. K. Khan, "Questioning key compromise attack on Ostad-Sharif et al.'s authentication and session key generation scheme for healthcare applications," *IEEE Access*, vol. 7, pp. 39717–39720, 2019.

[25] A. Ostad-Sharif, M. Nikooghadam and D. Abbasinezhad-Mood, "Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks," *International Journal of Communication Systems*, vol. 32, no. 12, pp. e3974, 2019.

[26] 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.

[27] K. Sowjanya, M. Dasgupta and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *International Journal of Information Security*, vol. 19, no. 1, pp. 129–146, 2019.

[28] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah *et al.,* "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computers & Electrical Engineering*, vol. 61, pp. 238–249, 2017.

[29] D. He, S. Zeadally, N. Kumar and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[30] D. He, N. Kumar, M. Khan and J. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 4, pp. 811–817, 2013.

[31] M. Nikooghadam and H. Amintoosi, "Perfect forward secrecy via an ECC-based authentication scheme for SIP in VoIP," *Journal of Supercomputer*, vol. 76, no. 4, pp. 3086–3104, 2019.