Dynamic and Anonymous Authentication Protocol with Evaluation Mechanism for Telecare Medicine

Shisong Ni[1], Tianqi Zhou[2], Wenying Zheng[3], Yunpeng Song[4], Chin-Feng Lai[5]*

[1] School of Computer Science, Nanjing University of Information Science and Technology, China
[2] School of Information Science and Engineering, Zhejiang Sci-Tech University, China
[3] School of Computer Science and Technology, Zhejiang Sci-Tech University, China
[4] Industry Development Center of Zhejiang Province, China
[5] Department of Engineering Science, National Cheng Kung University, Taiwan
nshisong@126.com, tq_zhou@126.com, zhengwy0501@126.com, 33256491@qq.com, cinfon@ieee.org

Abstract

Telecare medicine is becoming a trend, due to the combination of traditional medicine and information technology. However, the online communication method leaves patient information at risk of being compromised. Therefore, a dynamic and anonymous authentication protocol for telecare medicine with evaluation mechanism is proposed in our paper. Dynamic and anonymity guarantees patient privacy and security. The differentiated evaluation mechanism not only improves the user's enjoyment of the experience but also reduces the pressure on the data of trusted authority (TA). Security analysis proves that attacks cannot break our protocol. Finally, our protocol is used to compare with other protocols. It is shown experimentally that our protocol has an advantage over other protocols in terms of computation cost.

Keywords: Telecare medicine, Anonymous authentication, Evaluation mechanism

1 Introduction

Recently, the rise of artificial intelligence has brought about significant changes in telecare medicine [1-2]. With the popularity of the Internet and advances in communication methods, telemedicine technology is changing telecare medicine in ways that have never been seen before [3]. This technology uses digital methods that break the boundaries of geography in traditional healthcare, allowing doctors and patients to communicate with each other without being constrained by time and location. While this approach brings more convenient and timely access to healthcare, it is accompanied by a series of security issues involving authentication [4-5].

In the telemedicine development, the communication eavesdropping between doctors and patients as well as the leakage of patients' private information have become larger security risks [6]. Therefore, assuring the confidentiality of communications and confirming the accuracy of the identities of the communicating parties become critical prerequisites for realizing telemedicine security [7]. It is urgently necessary to establish a reliable authentication protocol between doctors and patients [7-8].

In different application fields, several authentication protocols have been proposed [9-10]. However, these protocols have different security objectives. In telecare medicine, it is very important for patients that their personal privacy and sensitive information are not compromised [11-12]. The common anonymity protocols protect identities through a pseudonymization of the real name. Although this protects the patient's identity, some malicious adversaries will associate the patient's pseudonym and behavior. Therefore, telecare medicine protocols that feature dynamic and anonymity are necessary [13]. In addition, although authentication protocols are resistant to attacks by malicious users, some once well-intentioned users will change their behavior. To establish secure and reliable communication between doctors and patients, this paper proposes a dynamic and anonymous authentication protocol with evaluation mechanism for telemedicine [14-15].

1.1 Motivations

To establish secure and reliable communication between doctors and patients, our paper proposes a dynamic and anonymous authentication protocol for telecare medicine with evaluation mechanism.

- **Ensure patient privacy and security during telecare medicine.** Despite the temporal and spatial convenience telecare medicine brings to patients, the transmission of information over unsecured channels is prone to leakage. Thus, it is vital to be able to protect patient privacy.
- **Alleviating the pressure on TA to manage users.** TA is responsible for assisting in the authentication process between users, which may be mixed with some dishonest users who may intentionally disrupt the authentication process. In addition, the TA is also in charge of managing user information and is required to process a large amount of data. Therefore, a sound credibility evaluation mechanism can reduce the pressure on TA, and at the same time can better help users to realize a two-

*Corresponding Author: Yunpeng Song; Email: 33256491@qq.com
DOI: https://doi.org/10.70003/160792642026012701003

way choice among themselves.

1.2 Contributions

Combining the above description, we design a dynamic and anonymous authentication protocol for telecare medicine with evaluation mechanism by using a hash function, symmetric key, and evaluation mechanism. The contribution is as follows:

- **A dynamic and anonymous authentication protocol is designed to protect patient privacy in telecare medicine.** In the protocol, patients register using a pseudonym, which avoids the risk of compromising their real identity. Furthermore, the pseudonym is updated by the patient after each authentication is completed, which makes linking multiple behaviors to a single pseudonym impossible.
- **An evaluation mechanism has been designed, which takes the pressure off the TA to manage users.** Protocol management of malicious users becomes difficult because of the dynamic and anonymity approach. TA is introduced and symmetric encryption is utilized to implement patient tracking. By evaluating the behavior of patients and doctors, it can help them make better choices. Patients can avoid doctors with low reputation values (who might be guilty of violations). It is also easy and convenient for TA to manage the users who participate in the authentication. This practice reduces the pressure on credible organizations.
- **Protocol security is proven and performance is compared.** By security analysis, it is proved that our protocol is resistant to password-guessing attacks and Session-specific temporary information attacks, etc. Comparison with the protocols of Amin et al. [16], Chaudhry et al. [17], and Lei et al. [18] demonstrate that our protocol is more secure.

2 Related Work

Many authentication protocols have been proposed regarding patients to maintain their safety when performing telecare medicine. In 2013, Das et al. [19] designed a telemedical authentication protocol. This protocol utilizes the biohash setting as the user login authentication, which ensures the uniqueness of the user. In addition, trusted servers are used by the scheme to store the user identification table and update it with each session, which provides anonymity to the protocol. Although the scheme does a great deal in protecting user privacy, it cannot resist user impersonation attacks. In a single server, proposed a protocol for telecare medicine authentication with user anonymity was designed by Tan et al. [20]. The scheme guarantees user anonymity. In addition, the scheme also supports mutual authentication, which avoids user impersonation attacks. However, the scheme cannot deal with replay attacks. Subsequently, Chaung et al. [21] proposed a biohash authentication protocol under multiple servers. The multi-server structure alleviates the overhead of a single server. To achieve a lightweight protocol, random numbers and hashes are utilized. However, multiple servers don't always bring convenience, and some potential problems come with them. The protocol is not resistant to server spoofing attacks. In 2015, Chang et al. [22] proposed a two-factor authentication protocol to solve the problem of user identity exposure under multiple servers. However, the scheme will be vulnerable to offline password guessing attacks. In 2019 Zhang et al. [23] proposed a three-factor AKA protocol. The application of chaotic mapping allows the scheme to reach a balance between security and performance. The three-factor approach guarantees user login security. So, the protocol is more secure for communication over open channels. However, the protocol cannot resist offline password guessing attacks.

3 Preliminaries

This section describes the hash function and system model. The ability of the adversary is also defined.

3.1 Hash Function

Definition 1. For a function, the input can be of arbitrary length, but the length of the output is fixed. And the calculation of the function is one-way and the value of the original cannot be derived from the result. In addition, hash functions have extremely fast encryption or verification speeds. Finally, finding one that is different from the input value but the equal output value is computationally difficult.

3.2 System Model

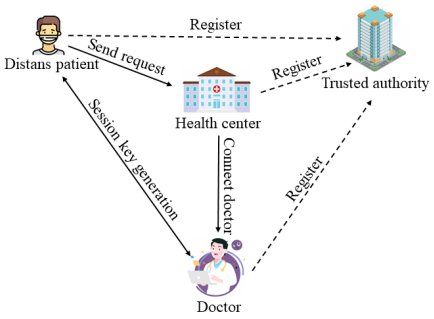

Figure 1. The system model of telecare medicine

Figure 1 shows the system model for telecare medicine. The system contains four entities: the patient, the doctor, the health center (HC), and the TA.

- The patient is the initiator of telecare medicine. Unregistered patients are potentially risky users. When a patient wants to access healthcare services, they need to first register with TA and then submit a telecare medicine request to HC.
- The doctor is a participant in telecare medicine.

Successfully registered doctors can reach authentication with their patients with the help of HC and thereafter provide online medical treatment to patients.

- HC is the facilitator of telecare medicine. Under the trusteeship of the TA, HC participates in the authentication of patients and doctors.
- TA is the controller of telecare medicine. The rest of the entities need to register with TA. The information of all the entities is also managed by the TA.

3.3 Adversary Model

Adversary ($\mathcal{A}$) capabilities in telehealth medicine are defined in our paper as follows.

1. $\mathcal{A}$ can eavesdrop, modify, delete, and insert fake messages on open channels in telecare medicine [24].
2. $\mathcal{A}$ can launch a offline password-guessing attack and an online password-guessing attack.
3. If $\mathcal{A}$ obtains the patient's lost mobile device, then it can decrypt the device and obtain the data contained therein.
4. When performing key security analysis, $\mathcal{A}$ is considered to be able to obtain the long-term secret value.
5. TA is trusted and it authorizes HC. TA and HC share a pair of symmetric keys in advance.

4 Protocol Description

In this section, the dynamic and anonymous authentication protocol for telecare medicine with evaluation mechanism is described in detail. To facilitate the understanding of our protocol, Table 1 lists the meaning of various symbols.

Table 1. Notations

Notations	Descriptions
P_i	i_{th} patient
D_j	j_{th} doctor
UID	Pseudony for patients
ID_i, PW_i	Identity and password of patient's respectively
ID_j, PW_j	Identity and password of doctor's respectively
$\mathcal{A}$	Adversary
HC	Health center
TA	Trusted authority
$h()$	One-way hash function
T_i	Timestamp
SK	Session key

4.1 Pre-setting Phase

TA generates a symmetric key. The hash function is generated and published.

4.2 Registration Phase

To enable telecare medicine, the patient needs to submit a registration request toward the TA. The registration process is shown in Figure 2:

Step 1. P_i chooses ID_i, PW_i, random numbers R and R_0. Then $UID = h(ID_i \oplus R)$ and $BPW_i = h(PW_i \| R_0)$ are calculated. Finally, ID_i, UID and BPW_i are sent to TA via a secure channel.

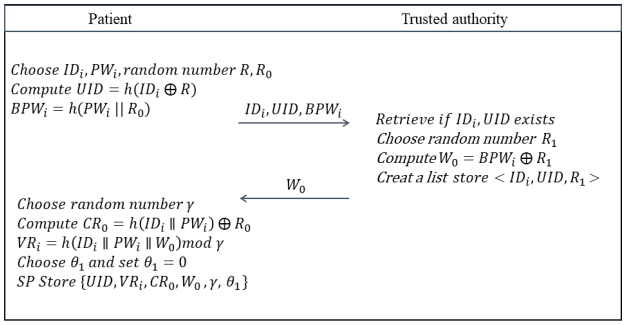

Figure 2. Patient registration phase

Step 2. TA retrieves whether ID_i and UID are in the database. Then, TA chooses a random number R_1, computers W_0=$BPW_i \oplus R_1$. Subsequently, a list is created that holds [D_i, UID, R_1]. Eventually, W_0 is sent to P_i.

Step 3. After receiving W_0, a random number γ is chosen by P_i. And then P_i computers CR_0=$h(ID_i||PW_i) \oplus R_0$ and VR_i=$h(ID_i||PW_i||W_0) mod\ \gamma$. Afterward, θ_1 is choosed by P_i and [ID, VR_i, CR_0, W_0, γ, θ_1] are stored in P_i mobile phone or device.

To realize online diagnosis, the doctor needs to submit a registration request to the TA. The registration process is shown in Figure 3.

Step 1. D_i chooses ID_j, PW_j and a random number R_2. Then BPW_j= $h(PW_j||R_2)$ is calculated. Finally, ID_j and BPW_j are sent to TA via a secure channel.

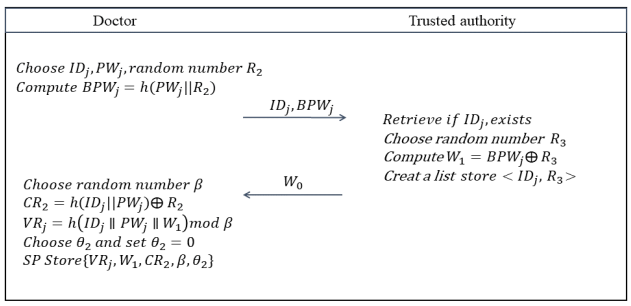

Figure 3. Doctor registration phase

Step 2. TA retrieves whether ID_j is in the database. Then, TA chooses a random number R_3, computers W_1= BPW_j=$\oplus R_3$). Subsequently, a list is created that holds [ID_j, R_3].

Step 3. After receiving W_1, a random number β is choosed by D_i. And then D_i computers $CR_2=h(ID_j||PW_j)\oplus R_2$ and $VR_j=h(ID_j||PW_j||W_1)mod\ \beta$. Afterward, θ_2 is choosed by D_i and $[VR_j, W_1, CR_2, \beta, \theta_2]$ are stored in D_i specialized equipment.

To alleviate data pressure on TA, HC submits registration requests to TA. After that, HC is responsible for managing the authentication of patients and doctors. The registration process is described below:

HC submits a registration request to TA. Then, TA puts the symmetric key into the key management module in HC.

4.3 Login and Authentication Phase

After all entities have successfully registered, P_i initiates an authentication request to HC when needed. The authentication and login process is shown in Figure 4:

Step 1. P_i tries to login using ID_i, PW_i. And then P_i computers $R_0=CR_0\oplus h(ID_i||PW_i)$ and $R_1=h(PW_i||R_0)\oplus W_0$. Next, whether $VR_i=h(ID_i||PW_i||W_0)mod\ \gamma$ is checked. If so, then P_i chooses a random number b and timestamp T_1, computers $SK_1=h(ID_i||b||R_1||T_1)$, $V_1=(SK_1||b)\oplus h(R_1||UID||T_1)$ and $V_{HC}=h(ID_j||R_1||SK_1||T_1)$. Eventually, $M_1=[UID, ID_j, V_1, V_{HC}, T_1]$s sent to HC.

Step 2. HC checks the freshness of T_1 after receiving M_1 from P_i. UID is symmetric encrypted and sent to TA. TA then decrypts and queries the $R_1^{'}$ corresponding to UID and sends it back to HC. Afterward, HC computers $(SK_1^{'}||b)=V_1\oplus h(R_1^{'}||UID||T_1)$ and checks whether $V_{HC}=h(ID_j||R_1^{'}||SK_1^{'}||T_1)$. If not, HC will report this behavior to TA. Subsequently, R_3 is sent to HC by TA. HC chooses a random number c and a timestamp T_2, computers $V_2=(SK_1^{'}||c)\oplus h(R_3||ID_j||T_2)$ and $V_D=h(ID_j||R_3||SK_1^{'}||T_2)$. Finally, $M_2=[V_2, V_D, T_2]$s sent to D_i.

Step 3. D_i needs to login a specialized computer before telecare medicine (the act of logging in only needs to be performed one time before telecare medicine, rather than one time for each P_i). D_i tries to login using ID_j, PW_j. And then D_i computers $R_2=CR_2\oplus h(ID_j||PW_j)$ and $R_3^{'}=h(PW_j||R_2)\oplus W_1$. Next, whether $VR_j=h(ID_j||PW_j||W_1)\ mod\ \beta$ is checked. If so, D_i first checks the freshness of T_2. Then computers $(SK_1||c)=V_2\oplus h(ID_j||R_3^{'}||T_2)$ and checks whether $V_D\oplus h(ID_j||R_3^{'}||(SK_1||T_2)$. If so, D_i chooses a random number d and timestamp T_3. Later $SK=SK_1\oplus SK_2$, $V_3=(SK_2||c)\oplus h(R_3^{'}||ID_j||T_3)$ and $V_{CH}=h(SK||R_3^{'}||SK_2||T_3)$ are calculated. Finally, $M_3=[V_3, V_{CH}, T_3]$ is ***sent*** to HC.

Step 4. HC checks the freshness of T_3 after receiving M_3 from P_i and chooses timestamp T_4. Then, $(SK_2^{'}||c)=V_3\oplus h(R_3||ID_j||T_4)$ and $SK=SK_1^{'}\oplus SK_2^{'}$ are calculated. Subsequently, HC checks if $V_{CH}=h(SK||R_3||SK_2^{'}||T_3)$. If not, HC will report this behavior to TA. Then, HC computers $V_4=(SK_2^{'}||b)\oplus h(R_1^{'}||ID_j||T_4)$ and $V_P=h(SK||SK_1^{'}||R_1^{'}||T_4)$, sends $M_4=[V_4, V_P, T_4]$ to P_i.

Step 5. After receiving M_4, P_i first checks the freshness of T_4, computers $(SK_2^{'}||b)=V_4\oplus h(R_1||ID_j||T_4)$ and $SK=SK_1\oplus SK_2^{'}$, then checks if $V_P=h(SK||SK_1||R_1||T_4)$. If so, SK is successfully established. To protect the security of P_i pseudonym, it is necessary to update the pseudonym. P_i chooses a new random R^{new} and computers $UID^{new}=h(UID\oplus R^{new})$. UID^{new} replaces UID in P_i devices. Finally, P_i sends UID^{new} to TA.

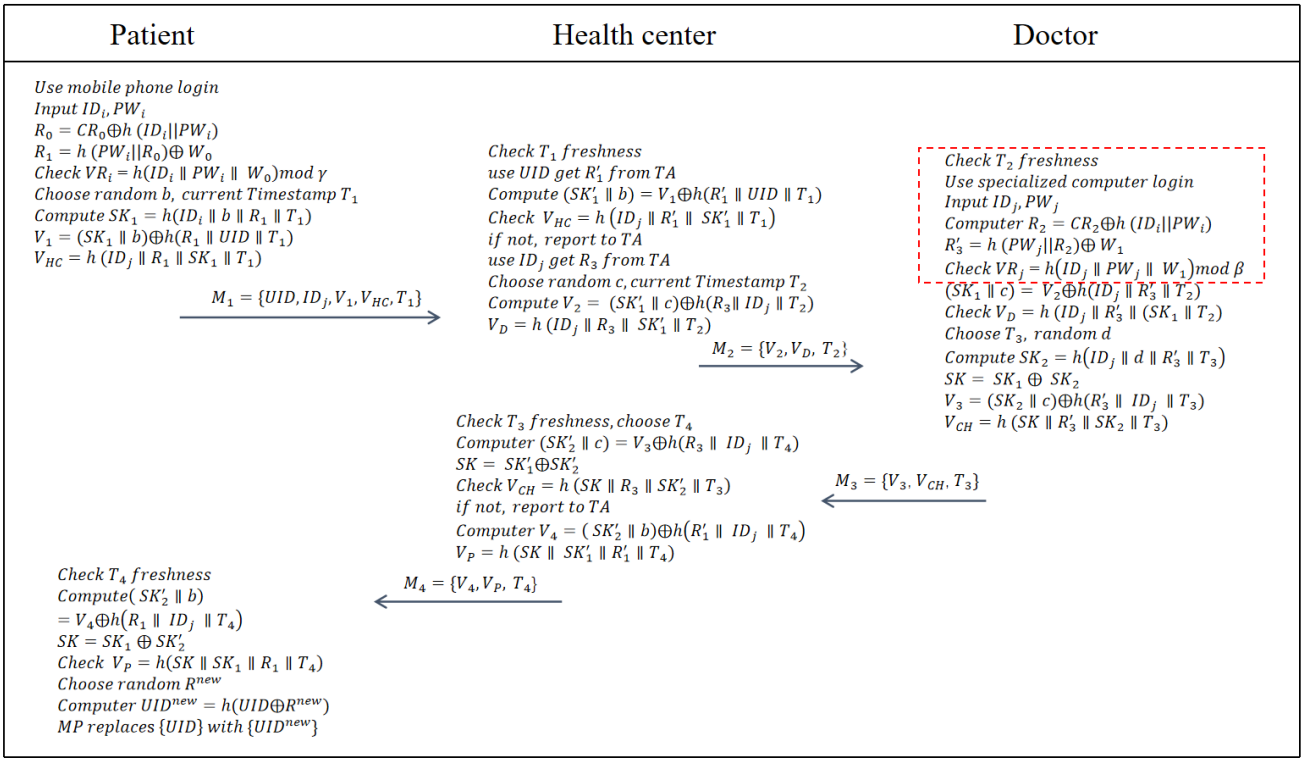

Figure 4. Login and authentication phase

4.4 Password Update Phase

The patient's password change process is as follows:

P_i first choose a random number R_0^{new}, γ^{new} and PW_i^{new}, computers $BPW_i^{new}=h(PW_i^{new}||R_0^{new})$, $CR_0^{new}=h(ID_i||PW_i^{new})\oplus R_0^{new}$, and $VR_i^{new}=h(ID_i||PW_i^{new}||W_0)mod\ \gamma^{new}$. Finally, [UID, VR_i^{new}, CR_0^{new}, W_0, γ^{new}, θ_1) are stored in P_i device.

4.5 Evaluation Phase

A good authentication protocol can resist unauthorized malicious user attacks. However, the protocol does not handle well with users who have been successfully registered or even have been behaving well, once their behavior changes. Thus, additional mechanisms are needed to counter that. Our protocol proposes a mechanism for evaluation patients and doctors. Behaviors are classified into three types: 1) m_0: An interaction is completed between the patient and the doctor. 2) m_1: Malicious interruption of the authentication process. For successfully registering the doctor and the patient, authentication may be interrupted for active or passive (e.g., loss of signal) reasons. 3) m_2: Breach of contract after the authentication process. Malicious breach of contract includes: the patient successfully registering with a doctor but being absent, and the doctor viewing private information that does not belong to their patients. Based on this, we designed an evaluation formula. Where n is the total number of times, i is the number of times m_i and $e^{-\frac{(n-i)}{i}}$ is the temporal decay.

$$s = s + \frac{e^{-\frac{(n-i)}{i}}\Sigma_{i=1}^{n}m_0 - e^{-\frac{(n-i)}{i}}\Sigma_{i=1}^{n}m_1 - e^{-\frac{(n-i)}{i}}\Sigma_{i=1}^{n}m_2}{n} \quad (1)$$

Traditional evaluation mechanisms typically discount users who engage in malicious behavior and gradually restore their evaluates after a period of time. However, this approach is not friendly to users who interact frequently and actively. Meanwhile, if malicious adversaries register multiple accounts and control these accounts to engage in destructive behavior over a period of time, traditional mechanisms are also difficult to effectively prevent. In Eq. (1), the temporal decay factor is introduced to modulate the effect of the user's latest behavior on the score. Users with normally good behavior will have relatively little impact on their scores when they commit a few acts of disruptive behavior. The differentiated treatment aims to protect those users who have been interacting positively, thus enhancing the system's perception of friendly users. Conversely, for users who engage in only malicious behavior, the system will gradually make authentication more difficult, making it more difficult to pass authentication. The strategy aims to effectively counter the problem of malicious users frequently registering multiple accounts and taking turns to engage in disruptive behavior. This enables the system to better identify and prevent such malicious behavior, thus protecting the overall stability of the system and the user experience.

5 Security Analysis

This section shows the security analysis of our protocol.

5.1 User Anonymity

According to the description in Section 3.3. $\mathcal{A}$ is not only able to eavesdrop on messages on the open channel, but also to gain access to information in P_i lost device. At this point, $\mathcal{A}$ obtains the UID from the open channel and also [UID, VR_i, CR_0, W_0, γ, θ_1] stored in the device. But $\mathcal{A}$ can't obtain the ID_i because $UID = h(ID_i\oplus R)$ is protected by receiving a hash and a random number R**.** So, our protocol provides user anonymity.

5.2 Privilege Insider Attack

Suppose there is a person within the TA who is trying to get the registration information. However, our protocol does not transmit ID_i to the TA in the registration phase, rather it transmits UID. Moreover ID_i cannot be computed from the UID. Therefore, our protocol is resistant to privileged insider attack.

5.3 Device Loss Attack

Suppose P_i login device is lost or stolen, and the information stored in it may be compromised. [UID, VR_i, CR_0, W_0, γ, θ_1] are obtained by $\mathcal{A}$. ID_i be not compromised in User Anonymity. In addition, PW_i does not exist in the device, so $VR_i = h(ID_i||PW_i||W_0)mod\ \gamma$ cannot be computed. Therefore, our protocol is resistant to device loss.

5.4 Impersonation Attack

Impersonation attacks are divided into three types.

Case 1: P_i impersonation. $\mathcal{A}$ intercepts M_1 and tries to re-forge M_1 to send to HC. However, since R_1 is a secret value between P_i and TA. $\mathcal{A}$ has no ability to obtain it. As a result, SK_1, V_1 and V_{HC} cannot be computed. Furthermore, suppose that M_4 is intercepted by $\mathcal{A}$ and $\mathcal{A}$ tries to falsify his identity to HC. However, the secrecy of R_1 causes SK_2 and SK computations to fail. Therefore, $\mathcal{A}$ cannot impersonate P_i at this stage.

Case 2: HC impersonation. $\mathcal{A}$ prevents D_i from receiving M_2 and tried to masquerade as HC. However, R_3 is a secret value between ID_i and TA, so $\mathcal{A}$ cannot compute V_2 and V_D. Furthermore, if $\mathcal{A}$ tries to forge M_4 and send it to P_i is impossible. Because both R_1 and b are unknown to $\mathcal{A}$. Therefore, $\mathcal{A}$ cannot impersonate HC at this stage.

Case 3: D_i impersonatio. $\mathcal{A}$ intercepts M_2 and tries to masquerade as D_i. However, without R_3, $\mathcal{A}$ cannot recover SK from V_2 and cannot pass V_D. Furthermore, if $\mathcal{A}$ intercepts M_3 and tries to forge it, but $\mathcal{A}$ does not have R_3, SK_1, and is unable to forge V_3 and V_{CH}. therefore, $\mathcal{A}$ cannot impersonate D_i at this stage.

5.5 Replay Attack

According to the description in Section 3.3, $\mathcal{A}$ is able to intercept M_1, … M_4. to launch a replay attack. After a period of time, $\mathcal{A}$ sends the message to the receiver. However, the timestamp checking prevents non-fresh messages from being accepted. Therefore, our protocol is able to resist replay attack.

5.6 Man-in-the-middle Attack

If $\mathcal{A}$ obtains all the information in P_i device and tries to launch a man-in-the-middle attack in our protocol. Then

$\mathcal{A}$ needs to prove the legitimacy of its identity to P_i, HC, and D_i. The absence of R_1 and R_3 prevents $\mathcal{A}$ from forging M_1, … M_4. But the absence of R1 and R3 prevents $\mathcal{A}$ from forging M_1, … M_4. Therefore, our protocol is resistant to man-in-the-middle attack.

5.7 Password Guessing Attack

According to the description in Section 3.3, $\mathcal{A}$ obtains one of the ID_i or PW_i, as well as the [UID, VR_i, CR_0, W_0, γ, θ_1] that exists in the device. At this point, $\mathcal{A}$ tries to go offline to enumerate the possible $< ID_i, PW_i >$ pairs. Due to the existence of γ, there is more than one possible correct $< ID_i, PW_i >$ pair. Thus $\mathcal{A}$ needs to login online to be sure. And the presence of θ_1 limits the number of online logins. Once θ_1 is more than 4, P_i account will be locked. So, our protocol can resistant to password guessing attack.

5.8 Forward Secrecy

After the current SK is successfully negotiated, suppose it is successfully obtained by $\mathcal{A}$. Then $\mathcal{A}$ tries to compute the previous SK. but since the random numbers b and d are involved, they are chosen randomly each round and the probability of a collision is negligible. So, $\mathcal{A}$ is not able to compute the previous SK. Thus, our protocols reach forward secrecy.

5.9 Ephemeral Secret Leakage Attack

Suppose all the temporary secret values (b, c, and d) of the authentication phase are leaked to $\mathcal{A}$, and $\mathcal{A}$ tries to compute the current SK. But since SK_1 requires the long-term secret value R_1, and SK_2 requires the long-term secret value R_3. so, SK is still not accessible to $\mathcal{A}$. Our protocol is resistant to ephemeral secret leakage attack.

6 Performance Analysis

In this section, our paper is compared with the papers of Amin et al. [16], Chaudhry et al. [17], and Lei et al. [18].

6.1 Comparison of Computation Cost

Table 2 gives the comparison results of our paper with protocols Amin et al. [16], Chaudhry et al. [17], and Lei et al. [18]. T_h, T_{se}, T_{mp}, and T_{ms} are the time spent on hash function, symmetric encryption/decryption, modular multiplication and scalar multiplication respectively. $\|$ and $\oplus$ are considered negligible.

Table 2. Computation cost

Protocols	P_i registration	Login and authentication
Amin et al. [16]	$3T_h + 2T_{se}$	$9T_h + 5T_{mp} + 2T_{se}$
Chaudhry et al. [17]	$6T_h$	$31T_h + 2T_{se}$
Lei et al. [18]	$6T_h$	$10T_h + 6T_{mp} + 1T_{ms}$
Ours	$5T_h$	$21T_h + 2T_{se}$

The above is a theoretical analysis of protocols. To evaluate the actual performance of protocols., Crypto ++ Library and Visual Studio C++ are used to simulate the computation cost of protocols. And CPU is i5-12400. In our experiments, we simulated each of the above operations 700 times. Then the average value was taken as the actual time. Finally, $T_h = 0.092ms$, $T_{se} = 0.067ms$, $T_{mp} = 3.868ms$, and $T_{ms} = 3.681ms$. It can be seen from Figure 5 that although our protocol is not the lowest in the registration phase. However, it has the lowest cost in the login and authentication phases from Figure 6. And also the final total cost is the lowest.

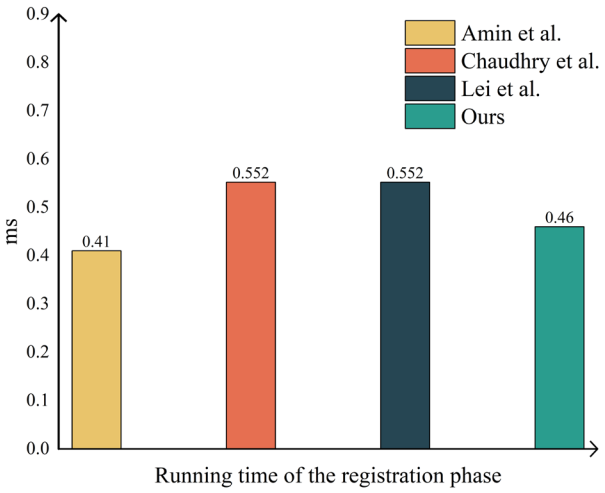

Figure 5. Running time of the registration phase

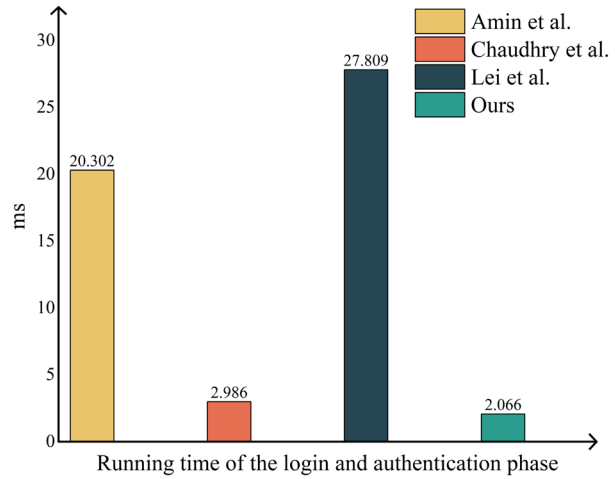

Figure 6. Running time of login and authentication phase

6.2 Comparison of Security

In Table 3 a comparison of the security of our paper with Amin et al. [16], Chaudhry et al. [17], and Lei et al. [18] are presented. Amin et al. [16]'s protocol is not resistant to Ephemeral secret leakage attack and man-in-the-middle attacks. Chaudhry et al. [17]'s protocol can not resistant to replay attack because the lack of timestamps and device loss attack. Since Lei et al. [18]'s protocol sends ID t the server during the registration phase, so, it is not resistant to privileged person attacks. Our protocols are highly secure and resistant to a range of attacks. In addition, the evaluate mechanism is unique to our protocol.

Table 3. Comparison of security

Security \ Protocols	Amin et al. [16]	Chaudhry et al. [17]	Lei et al. [18]	Ours
User anonymity	√	√	√	√
Privilege insider attack	√	√	×	√
Device loss attack	√	×	√	√
Impersonation attack	√	√	√	√
Replay attack	√	×	×	√
Man in the middle attack	×	√	√	√
Off-password guessing attack	√	√	√	√
Online-password guessing attack	×	×	√	√
Forward secrecy	√	√	√	√
Ephemeral secret leakage attack	×	×	×	√
Evaluate mechanism	×	×	×	√

6.3 Experimental

The basic requirement for authentication protocols is security. However. protocols are often assumed to operate in idealized environments that do not match the complex realities of the environment. In addition, it is difficult for humans to intuitively recognize whether a protocol is secure or not. Therefore, to verify the security of a protocol, AVISPA tool is used by us for simulation. The result is presented in Figure 7.

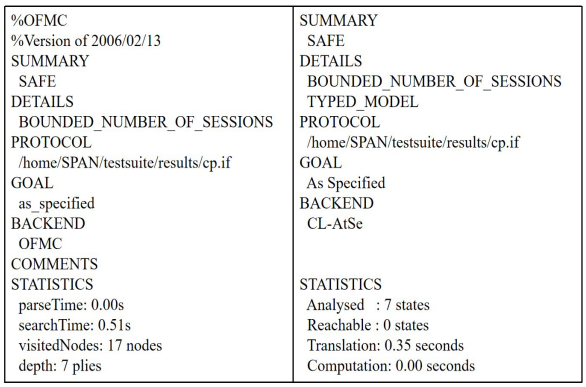

Figure 7. AVISPA result

7 Conclusion

An evaluation mechanism for dynamic and anonymous authentication protocol for telecare medicine is presented in our paper. Our protocol uses hash functions and symmetric encryption to secure the communication. Dynamic and anonymization is achieved for telecare medicine patients. In addition, an evaluation mechanism with differentiation is applied to alleviate TA data pressure. AVISPA proves that the protocol is secure. Finally, experiments also demonstrate that our protocol has less computation cost in the registration phase and login authentication phase.

Acknowledgment

The work is supported by the National Key Research and Development Program of China (No. 2023YFB2703700), the National Natural Science Foundation of China (Nos. U21A20465, 62302457), Zhejiang Provincial Natural Science Foundation of China under Grant Nos. LQ24F020009, LQ24F020012, and the Zhejiang Key Laboratory of Multidimensional Perception Technology Application and Cybersecurity (No. HIKKL-20230002).

References

[1] B. Chander, K. Gopalakrishnan, A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in Telecare medicine information system, *Computer Communications*, Vol. 191, pp. 425-437, July, 2022.

[2] J. Shen, A. Wang, L. Yan, Y. Ren, Q. Liu, Identity-based group devices authentication scheme for Internet of Things, *Proceedings of 11th EAI International Conference on Mobile Multimedia Communications*, Qingdao, China, 2018, pp. 45-55.

[3] M. Masdari, S. Ahmadzadeh, A survey and taxonomy of the authentication schemes in telecare medicine information systems, *Journal of Network and Computer Applications*, Vol. 87, pp. 1-19, June, 2017.

[4] G. J. Simmons, A survey of information authentication, *Proceedings of the IEEE*, Vol. 76, No. 5, pp. 603-620, May, 1988.

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, Y. Koucheryavy, Multi-factor authentication: A survey, *Cryptography*, Vol. 2, No. 1, Article No. 1, March, 2018.

[6] O. Mir, M. Nikooghadam, A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services, *Wireless Personal Communications*, Vol. 83, No. 4, pp. 2439-2461, August, 2015.

[7] D. B. He, J. H. Chen, R. Zhang, A more secure authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1989-1995, June, 2012.

[8] L. Zheng, Y. Zhang, R. Zhang, J. Chen, M. Cui, C. Song, An Improved Authentication Protocol in Telemedicine System, *Proceedings of Algorithms and Architectures for Parallel Processing: ICA3PP 2018 International Workshops*, Guangzhou, China, 2018, pp. 177-184.

[9] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, 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, January, 2018.

[10] J. Paul, R. S. Bhowmick, B. Das, B. K. Sikdar, A smart home security system in low computing IoT environment, *Proceedings of 2020 IEEE 17th India Council International Conference (INDICON)*, New Delhi, India, 2020, pp. 1-7.

[11] F. Rezaeibagha, Y. Mu, Practical and secure telemedicine systems for user mobility, *Journal of Biomedical Informatics*, Vol. 78, pp. 24-32, February, 2018.

[12] H. K. Sharma, T. Choudhury, A. Katal, J. S. Um, Security and Privacy issue in Telemedicine: Issues, Solutions, and Standards, in: T. Choudhury, A. Katal, J. S. Um, A. Rana, M. Al-Akaidi (Eds.), *Telemedicine: The Computer Transformation of Healthcare*, Springer, 2022, pp. 185-196.

[13] D. Zhang, S. Wang, Q. Zhang, Y. Deng, J. Wang, Blockchain-Based Mutual Authentication Protocol with Privacy Protection in Telemedicine, *Proceedings of Journal of Physics: Conference Series*, Vol. 2026, Article No. 012004, 2021.

[14] D. P. Spagnuelo, J. E. Martina, R. F. Custódio, R. Andrade, Multi-factor authentication in telemedicine systems, *Proceedings of The Fifth International Conference on EHealth, Telemedicine, and Social Medicine IARIA*, Nice, France, 2013, pp. 114-120.

[15] Z.-Y. Wu, Y.-C. Lee, F. Lai, H. C. Lee, Y. Chung, A secure authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1529-1535, June, 2012.

[16] R. Amin, S. H. Islam, G. Biswas, M. Khan, M. Obaidat, Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system, *Journal of Medical Systems*, Vol. 39, No. 11, pp. 1-20, September, 2015.

[17] S. A. Chaudhry, H. Naqvi, M. S. Farash, T. Shon, M. Sher, An improved and robust biometrics-based three factor authentication scheme for multiserver environments, *The Journal of Supercomputing*, Vol. 74, No. 8, pp. 3504-3520, August, 2018.

[18] C.-L. Lei, Y.-H. Chuang, Privacy protection for telecare medicine information systems with multiple servers using a biometric-based authenticated key agreement scheme, *IEEE Access*, Vol. 7, pp. 186480-186490, December, 2019.

[19] A. K. Das, A. Goswami, A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care, *Journal of Medical Systems*, Vol. 37, No. 3, pp. 1-16, June, 2013.

[20] Z. Tan, A user anonymity preserving three-factor authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, Vol. 38, No. 3, pp. 1-9, March, 2014.

[21] M.-C. Chuang, M. C. Chen, An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics, *Expert Systems with Applications*, Vol. 41, No. 4, pp. 1411-1418, March, 2014.

[22] I. P. Chang, T. F. Lee, T. H. Lin, C. M. Liu, Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks, *Sensors*, Vol. 15, No. 12, pp. 29841-29854, December, 2015.

[23] L. Zhang, S. Zhu, S. Tang, Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme, *IEEE Journal of Biomedical and Health Informatics*, Vol. 21, No. 2, pp. 465-475, March, 2017.

[24] H. Zhu, Y. Yuan, Y. Chen, Y. Zha, W. Xi, B. Jia, Y. Xin, A secure and efficient data integrity verification scheme for cloud-IoT based on short signature, *IEEE Access*, Vol. 7, pp. 90036-90044, June, 2019.

Biographies

Shisong Ni received the B.S. degrees from Nanjing University of science and technology of software, Nanjing, China, in 2021, where he is currently pursuing the M.S. degree with the School of Computer Science. His research interests include computer and network security, security systems, and cryptography.

Tianqi Zhou received her Ph.D. at Nanjing University of Information Science and Technology in 2023. From 2022 to 2023, she was a visiting Ph.D. student at Kyushu University. She is an Associate Professor at Zhejiang Sci-Tech University. Her research interests include public cryptography and cloud computing.

Wenying Zheng received the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2022. She is currently working with the School of Computer Science and Technology, Zhejiang SciTech University, Hangzhou, China. Her research interests include cloud storage security and network security.

Yunpeng Song received the master degrees in Detection Technology and Automation Equipment from Guangxi University in 2011, the abachelor's degree in Electronic Science and Technology from Zhengzhou University in 2003. He is presently serving as an engineer in Zhejiang Provincial Industry Development Center.

Chin-Feng Lai (Senior Member, IEEE) received the Ph.D. degree from National Cheng Kung University, Tainan, Taiwan, in 2010. He is a Professor with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China.