Hindawi
Security and Communication Networks
Volume 2022, Article ID 1883293, 12 pages
https://doi.org/10.1155/2022/1883293

Research Article

Patient Family Binding and Authentication Scheme with Privacy Protection for E-Health System

Yuanyuan Zhang, Zhihao Huang, Qilong Zhu, and Lingzhe Meng

School of Computers, Hubei University of Technology, Wuhan 430068, China

Correspondence should be addressed to Yuanyuan Zhang; circle0519@hotmail.com

Received 3 April 2022; Accepted 1 July 2022; Published 8 August 2022

Academic Editor: Jawad Ahmad

The emergence of the E-health system has brought convenience to many chronically ill patients and elderly people with limited mobility. With the help of the E-health system, patients can upload their physiological data timely and get a diagnosis at home, which is more convenient and efficient as they do not have to line up in hospitals. In order to ensure this convenience while protecting patients' privacy, many schemes have been proposed which can help patient and medical server authenticate each other. However, considering these patients' inconvenience, sometimes family members need to participate in the patient's treatment process. So, the E-health system needs to provide a secure communication platform for the family members. At present, most of the authentication schemes for the E-health system only focus on the secure communication between the patient and the medical server, while ignoring the participation of family members. Moreover, in the E-health system, the permissions of family members and patient should be different, and the medical server needs to distinguish their permissions efficiently. In order to overcome these problems, we propose a patient family binding and authentication privacy protection scheme for the E-health system. In the scheme proposed by us, the medical server can efficiently assign different permissions to the family member and patient. And our scheme can allow patient to authorize their family members freely, and the increase in the number of family members will not impose additional burden on the server. At the same time, the authentication between the family member and the medical server does not require the participation of the patient. In addition, by comparing with other related schemes, we prove that our scheme has suitable efficiency and security performance in the E-health system.

1. Introduction

Before the emergence of the E-health system, disease monitoring and condition analysis of patients must be carried out in hospital, which means that patients should often take time from work to go to hospital for medical examination. However, limited medical resources do not allow a large number of patients to receive treatment in time, which undoubtedly brings a lot of inconveniences and risks. Especially in recent years, cardiovascular diseases have become the biggest killer threatening human health because they cannot be detected in time, and patients miss the best time of treatment. Nowadays, as people' living standards rise, people gradually realize the importance of health and they need a better E-health system in modern society. In this context, the E-health system is growing increasingly with the goal to reduce risks of death and implement real-time disease monitoring. The E-health system adopts advanced Internet of Things (IoT) technology and digital visualization mode, which makes limiting medical resources possible to be shared by more people. Generally, after mutual authentication between the patient and the medical server, the monitor devices close to or carried by the patient can transmit the real-time data (such as blood pressure, blood sugar, heart rate) to the medical server. After data have been received from the patient, the medical server will establish an electronic medical record (EMR) for each patient in order to provide data support for doctors to track a patient's condition [1]. The EMR includes doctor's orders, operation records, nursing records, which is helpful for doctors to

control the diseases. The E-health system is very intelligent to realize real-time health monitoring and provide effective reference value for doctors for diagnosis.

In the era of big data, privacy protection attracts people. Apart from patients who do not want their information to be abused, the medical server also does not want its data to be stolen. In the actual medical activities, medical institutions often use the E-health system to collect a large amount of medical-related data for diagnosis. These data cover all the basic information of patients with high confidentiality requirements, such as physical and disease information, family address, medical insurance, personal account. However, the monitor devices are connected wirelessly, which means these confidentiality data are transmitted in open network and will threaten the security of information greatly. Lots of sensitive data are transmitted on a public channel where the adversary may intercept the useful data by passive attack. Furthermore, the adversary may forge the EMR and forward the false EMR to the medical server; then, the medical server may draw incorrect conclusion and send a wrong diagnosis to the patient. And when this least expected thing happens, the patient may suffer more pains, even lose his life.

The message transmitted on public (insecure) networks is extremely vulnerable, in order to ensure the security of transmission in E-health system, a lot of schemes have been proposed [1, 2]. Zhang et al. proposed a dynamic authentication scheme for the E-health system [1] in 2018. In their paper, both patients and family members can register in the E-health system, but the authors did not clarify how family members login the system, it would be difficult to solve the problem of binding between family members and patients. If the family members log by using the same authentication scheme as the patient, it will be difficult for the server to distinguish the family member from the patient. In 2019, Karthigaiveni and Indrani [2] proposed an efficient authentication mechanism based on two-factor authentication, and they claimed that their scheme needs less computational cost. However, they also do not mention the involvement of family members.

In the former proposed E-health system scheme, the majority of schemes often consider the secure communication between patients and medical servers but neglect the important effect of family members in the E-health system. When family members want to care about the patient's condition, it is necessary for family members to participate in the E-health system. Therefore, how to let family members join the E-health system under the premise of ensuring secure communication is a problem worthy of in-depth study. In addition, family members and patients should have different rights in the E-health system. In the system, patients can upload, modify, and delete their own medical data and view doctors' diagnosis results. On the other hand, family members can view the patient's medical data and doctor's diagnosis results on the basis of the patient's authorization but cannot upload, modify, or delete the data.

In this study, we propose a patient family binding and authentication scheme with privacy protection for the E-health system, and the environment of the system is shown in Figure 1. The E-health system consists of patients, family members, and medical server. Our scheme contains a registration phase for patient, a binding phase for family member, and an authentication phase for the family member. Considering that there are already a lot of authentication schemes between patient and medical server, so our scheme is mainly introduced for family member authentication and focuses on solving the problem of patient-family member binding. Finally, the contributions of our scheme are as follows:

(i) We propose a binding scheme for the family member, which can bind the patient and the family member so that the family member can participate in the treatment process of the patient.

(ii) In our scheme, authentication between family member and medical server does not require the participation of patients.

(iii) One patient may have several family members that need to participate in the E-health system. In our scheme, the increase in the number of family members does not incur additional costs to the medical server.

(iv) The binding phase in our scheme between patient and their family members does not require the participation of medical server, which avoid the cost on remote information transmission. Moreover, because the only use of lightweight secures hash function, bytes connection and exclusive-or, our scheme has high-performance.

(v) Our scheme provides strong privacy protection for the E-health system, where it ensures the security of critical message.

The rest of our work is organized as follows: The related works are briefly analyzed in Section 2. We describe our proposed scheme in Section 3. In Section 4, we analyze the security of the proposed scheme. Section 5 discusses the performance comparison between ours and other schemes. In the end, Section 6 gives the conclusion.

2. Related Work

In this section, we will discuss related works for the E-health system. A number of authentication schemes [3–5] have been proposed for E-health system. In 1976, Diffie and Hellman [6] proposed a method to setup session key named Diffie-Hellman key exchange. On the basis of their scheme, many research articles [7–9] are proposed. Following that, several authentication schemes for E-health system have been developed.

A remote authentication scheme for health care has been introduced by Das and Goswami [10]. However, in 2015, Amin et al. [11] indicated several vulnerabilities of Das et al.'s scheme [10], for example, Das et al.'s scheme [10] is vulnerable to user impersonation attack and user anonymity problem. To isolate such problems, they offered a user mutual authentication scheme for E-health. However, Aghili et al. [12] discovered that the scheme of Amin et al. [11] was vulnerable to Dos attacks. Later, Aghili et al. further

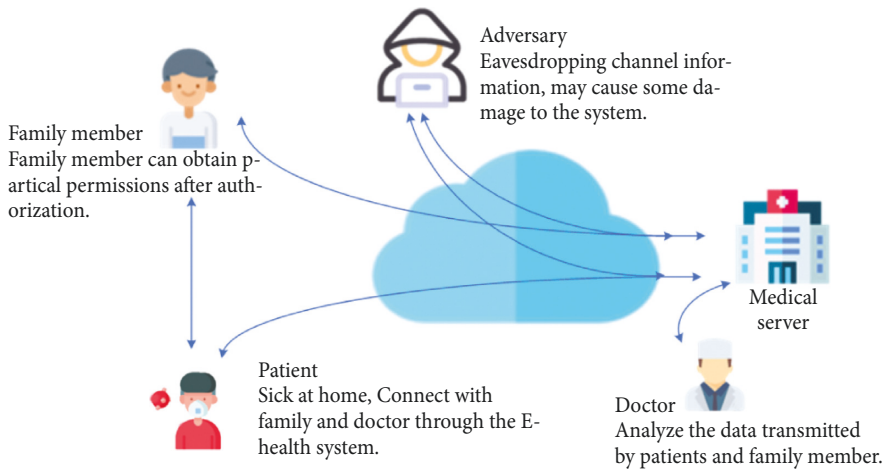

Figure 1: Environment of the scheme system.

presented a lightweight authentication scheme-based three-factor E-health system in 2019.

In order to overcome security flaws in the Session Initiation Protocol (SIP) authentication procedure, Yeh et al. [13] offered a secure authentication scheme based on Elliptic Curve Cryptography (ECC). Although, authors mentioned that their authentication procedure is shown to be more suitable for SIP applications. Unfortunately, Farash et al. [14] pointed that the authentication procedure presented by Yeh et al. [13] in 2016, cannot resist user impersonation and off-line password guessing attack, if the information in the smart card is stolen. As a remedy, they [14] further offered an authentication scheme for SIP-based ECC, which can provide the user anonymity and untraceability.

Mohit et al. [15] suggested a cloud computing for health care system in 2017, they proved that their scheme is more secure. In 2018, Zhang et al. [16] presented a dynamic authentication scheme for E-health system. Nevertheless, Aghili et al. [12] argued that Zhang et al.'s scheme is vulnerable to several attacks. To fix this, they further proposed lightweight authentication scheme by using three-factor scheme for E-health systems. Then 2017, Al-Saggaf et al. [17] introduced an authentication scheme for remote user by using smart cards, but according to Chen and Zhang [18], it fails to resist some secure attacks. To overcome these drawbacks, they put forward a biometric authentication scheme for E-health system, and proved that the scheme can satisfy the security requirements.

Wu et al. [19] designed a new authentication system which added the pre-computing method. The author claimed that their scheme will be more secure and efficient for Telecare Medicine Information Systems (TMIS). Although Wu et al.'s scheme is more secure than previous schemes, He et al. [20] declared that the method proposed by Wu et al. [19] had some security problems and proposed their improved solution. However, Wei et al. [21] pointed that neither Wu et al.'s [19] nor He et al.'s [20] scheme guarantee security and efficiency in the authentication scheme based on two-factor scheme. Then they offered an improved scheme and demonstrated the scheme is more secure and efficient.

After that, Yan et al. [22] suggested a secure authentication scheme which can be used on TMIS. They found that Tan [23] scheme cannot resist the Dos attack, and proposed their scheme to enhance security. However, Mir and Nikooghadam [24] showed that the method introduced by Yan et al. [22] still has some security faults. Then, an improved key agreement scheme based on biometrics for E-health services was presented by Mir and Nikooghadam [24] and the authors have shown that the solution is suitable for E-health services. But in 2019, Mehmood et al. [25] declared that there are some security flaws in Omid et al.'s scheme [24], and Omid et al.'s methods were susceptible to user impersonation attack. To fix all this, they offered a robust and efficient authentication scheme for E-health system. Unfortunately, Hosseini Seno and Budiarto [26] declared that Mehmood et al.'s [25] scheme is unsecure during the login and authentication process and they proposed a new scheme.

In 2019, Karthigaiveni and Indrani [2] introduced an efficient scheme with smart card and password by using Elliptic Curve Cryptography, and showed that their methods not only have better security but also have well computational cost. However, Chatterjee [27] scrutinized Kar et al.'s scheme [2] and declared some security defects in their scheme which lacks mutual authentication between the client and server. In 2020, Chatterjee [27] proposed an improved authentication scheme for health care applications. The author claimed that the scheme has higher security and efficiency.

In the past decade, many authentication protocols have been proposed to ensure system security. Regretfully, the former proposed schemes, which are about E-health system, mainly focus on improvement of security and efficiency but neglect the important effect of family members in the E-health system. The binding of family members can better serve patients and can improve the efficiency of diagnosis and providing binding and authentication service for family members can make the E-health system more practical. Furthermore, the E-health system should have good access control and excellent database performance.

3. Our Proposed Scheme

In order to ensure the security and efficiency of the E-health system operation, we propose a patient family binding and authentication privacy protection scheme. Our proposed scheme consists of three phases: registration phase for patient, binding phase for family member, and authentication phase for family member. By our scheme, family members can pay attention to the patient's medical data in time. The notations used in the proposed scheme are given in Table 1. Detailed descriptions of our scheme are as follows.

3.1. Registration Phase for Patients. In this phase of our scheme, a new patient PT will register with the medical server MS. The patient PT's authentication information is stored in the database of the medical server MS and a smart card, and the medical server MS issues the smart card to the patient PT. The detailed steps of the registration phase for patient are presented in Figure 2.

Step R1: firstly, the patient PT chooses identity ID_{PT} and password PW_{PT} which he/she can remember easily. Then, he/she generates a random number r_{PT} and uses it to calculate $M_1 = h(ID_{PT} \| PW_{PT} \| r_{PT})$. Next, patient PT respectively masks the identity ID_{PT} of patient and password PW_{PT} of patient with a random number r_{PT} by computing $R_{PT} = h(ID_{PT} \oplus PW_{PT}) \oplus r_{PT}$. Then, let $\{M_1, r_{PT}\}$ as a registration request message, the patient PT sends it to MS via secure channel.

Step R2: upon receipt of the request from the patient PT, the medical server MS firstly selects two identify labels id_{PT}, id_{FM} for the patient and family member, respectively. Then the medical server MS uses $PT's$ request information M_1 and MS's master key s to calculate $SC_{PT} = h(M_1 \| s)$. Afterwards, the medical server MS computes $MID_{PT} = h(M_1 \| id_{PT})$, $MID_{FM} = h(SC_{PT} \| id_{PT})$, $NID_{PT} = h(ID_{MS} \| M_1) \oplus id_{PT}$, $NID_{FM} = h(ID_{MS} \| id_{PT}) \oplus id_{FM}$ and $SC_{FM} = h(id_{FM} \| s)$, where ID_{MS} is identity information of medical server MS. Then the medical server uses SC_{FM} and SC_{PT} to calculate $L_{FM} = SC_{FM} \oplus SC_{PT}$, and uses SC_{PT}, $PT's$ random number r_{PT} to calculate $C_{PT} = r_{PT} \oplus SC_{PT}$. Next, the medical server chooses g where g is a generator of Z_P^* and P is a large prime. Finally, the medical server MS writes $\{MID_{PT}, MID_{FM}, SC_{PT}, id_{FM}, g\}$ into its database and stores $\{ID_{MS}, C_{PT}, NID_{PT}, NID_{FM}, L_{FM}, g\}$ into a smart card. Then the medical server MS sends the smart card which includes $\{ID_{MS}, C_{PT}, NID_{PT}, NID_{FM}, L_{FM}, g\}$ to the patient PT.

Step R3: the patient PT writes $\{R_{PT}\}$ into the smart card. After that, the registration phase for the patient is completed.

3.2. Binding Phase for Family Members. The binding of patient and family member can help the family member securely participate in the E-health system by performing the following steps. Figure 3 presents the detailed description of the binding phase.

Table 1: Notations used in our paper.

Notation	Description
PT	Patient
MS	Medical server of the E-health system
FM	Family of PT
ID_{MS}	Identity of MS
PW_{PT}	Password of PT
ID_{FM}	Identity of FM
PW_{FM}	Password of FM
r_{PT}	Random numbers generated by PT
$h(\cdot)$	Cryptographic one-way hash function
s	Master key of medical server
P	Large prime number
g	Generator of Z_P^*
$\|$	Concatenation operation
$\oplus$	Bitwise X-OR operation

Step A1: the patient PT chooses a secret information k and sends to family member in secure channel (for example, face to face).

Step A2: upon reception of the information k, the family member FM chooses his/her identity ID_{FM}, password PW_{FM}, then generates a random number r_{FM}, and uses the information k received from the patient PT to compute $I_{FM} = k \oplus r_{FM}$. After that FM sends I_{FM} to the patient PT.

Step A3: when receiving the message I_{FM}, patient PT inserts his/her smart card into the terminal card reader and inputs his/her identity ID_{PT} and password PW_{PT} in the smart card. Next, the smart card calculates $r'_{FM} = I_{FM} \oplus k$, $r'_{PT} = R_{PT} \oplus h(ID_{PT} \oplus PW_{PT})$, $SC'_{PT} = C_{PT} \oplus r'_{PT}$, $M'_1 = h(ID_{PT} \| PW_{PT} \| r'_{PT})$, $id'_{PT} = NID_{PT} \oplus h(ID_{MS} \| M'_1)$, $id'_{FM} = NID_{FM} \oplus h(ID_{MS} \| id'_{PT})$, $MID'_{FM} = h(SC'_{PT} \| id'_{PT})$, $N = L_{FM} \oplus MID'_{FM}$, $M_2 = N \oplus r'_{FM}$ and $M_3 = id'_{FM} \oplus h(N)$. After that, the smart card generates authorization information $Auth_{PT} = h(k \| M_2 \| M_3)$, and sends $\{M_2, M_3, Auth_{PT}\}$ to the family member.

Step A4: after receiving information $\{M_2, M_3, Auth_{PT}\}$ from patient PT, the family member FM verifies whether the equation $Auth_{PT} = h(k \| M_2 \| M_3)$ hold or not. If the verification is successful, the family member FM computes $N' = M_2 \oplus r_{FM}$, $id''_{FM} = M_3 \oplus h(N')$, $M_{FM} = h(ID_{FM} \| PW_{FM}) \oplus N'$ and stores $\{M_{FM}, id''_{FM}\}$ into he/she's smart card. Else, end the scheme.

3.3. Authentication Phase for Family Members. If a family member has completed the binding with a patient, he/she can log in to the medical server through the authentication phase. And a session key SK is negotiated by medical server MS and family member FM. Figure 4 presents the detailed description of the authentication phase.

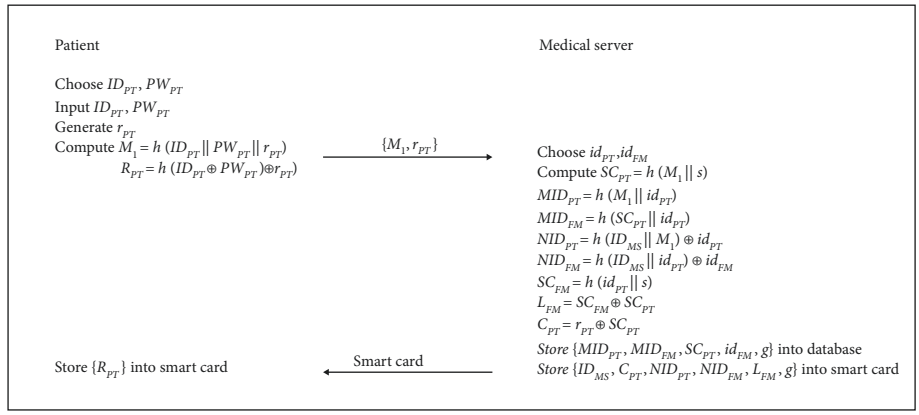

Figure 2: Details of the patient registration phase.

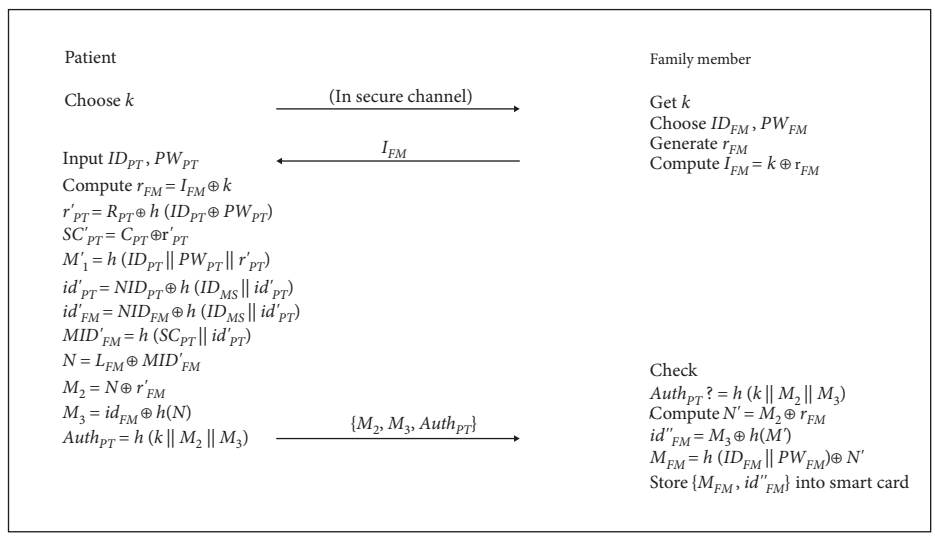

Figure 3: Details of the binding phase.

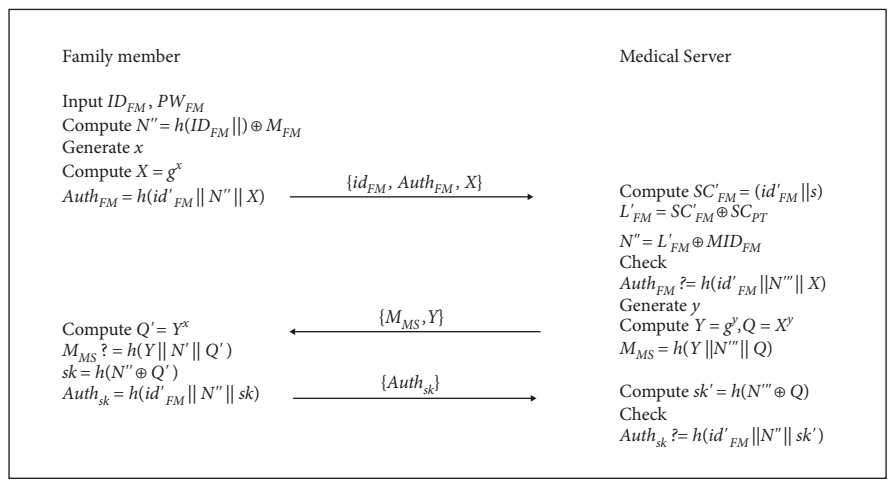

Figure 4: Details of the authentication phase.

Step C1: firstly, the family member FM inputs his/her identity ID_{FM} and password PW_{FM} into the smart card and calculates $N'' = h(ID_{FM} \| PW_{FM}) \oplus M_{FM}$. Next, the smart card generates a random number x and uses the information stored in it to calculate $X = g^x$ and $Auth_{FM} = h(id'_{FM} \| N'' \| X)$, and then sends $\{id'_{FM}, Auth_{FM}, X\}$ to the medical server MS.

Step C2: upon reception of information $\{id'_{FM}, Auth_{FM}, X\}$ from the family member FM, the medical server MS computes $SC'_{FM} = (id'_{FM} \| s)$, $L'_{FM} = SC'_{FM} \oplus SC_{PT}$, $N''' = L'_{FM} \oplus MID_{FM}$ and verifies whether the $Auth_{FM} = h(id_{FM}{}' \| N''' \| X)$ holds or not. If the verification is successful, the medical server MS generates a random number y, computes $Y = g^y$, $Q = X^y$, $M_{MS} = h(Y \| N''' \| Q)$ and sends $\{M_{MS}, Y\}$ as a verify message to the family member FM. Else, the MS will end the scheme.

Step C3: after receiving the verify message from the medical server, the family member FM computes $Q' = Y^x$, and then checks the equation $M_{MS}? = h(Y \| N'' \| Q')$. If the equation does not hold, it will end the scheme. Else, the family member FM computes the session key $sk = h(N'' \oplus Q')$. Then the family member FM uses the session key to compute $Auth_{sk} = h(id_{FM}{}' \| N'' \| sk)$ and sends $\{Auth_{sk}\}$ to medical server MS.

Step C4: on receiving $Auth_{sk}$ from the family member FM, the medical server MS computes $sk' = h(N''' \oplus Q)$ and checks the correctness of the $Auth_{sk}$ by comparing it with $h(id_{FM}{}' \| N''' \| sk')$. If the values are same, the medical server MS accepts the session key sk'. If the checking of $Auth_{sk}$ fails, the session will be terminated.

Finally, after the session key is negotiated, the family member FM and the medical server MS get sk and sk', respectively. The security proof process is as follows:

$$\begin{aligned} st &= h(N'' \oplus Q') \\ &= h(h(ID_{FM} \| PW_{FM}) \oplus M_{FM} \oplus Y^x) \\ &= h(h(ID_{FM} \| PW_{FM}) \oplus M_{FM} \oplus g^{xy}) \\ &= h(M_2 \oplus r_{FM} \oplus g^{xy}) \\ &= h(N \oplus Q) \\ &= (L_{FM} \oplus MID_{FM} \oplus Q) \\ &= h(N''' \oplus Q) \\ &= sk'. \end{aligned} \tag{1}$$

4. Security Analysis

In this section, we give a security analysis of our patient–family member binding scheme by using the real-or-random (RoR) model. In addition, we discuss the security of possible attacks.

4.1. Security Model. In this section, we use the random-or-real model [28] to prove that our authentication scheme is secure. The definitions of the model are presented as follows:

Participants: using $\mathcal{U}$ and $\mathcal{S}$ to respectively represent the set of user and the set of server. The set of all participants $\mathcal{P}$ is the union of $\mathcal{U} \cup \mathcal{S}$. We use $\mathcal{U}_i$ and $\mathcal{S}_j$ to represent the i-th member of $\mathcal{U}$ and the j-th member of $\mathcal{S}$.

Partnering: let the symbol $\Pi^{x_1}_{\mathcal{U}_i}$ and $\Pi^{x_2}_{\mathcal{S}_j}$, respectively represent the x_1-th instance of $\mathcal{U}_i$, the x_2-th instance of $\mathcal{S}_j$. If two instances $\Pi^{x_1}_{\mathcal{U}_i}$ and $\Pi^{x_2}_{\mathcal{S}_j}$ authenticate in the scheme and obtain the same no-null session identification ($si\ d$), then these two instances are called partner instances.

Freshness: in order to ensure freshness, there are two conditions needed to be met. First, the two partner instances can successfully negotiate a session key without being queried Reveal query. Second, the two partner instances can be only simulated by one of CorruptSC or CorruptDB query.

Adversary: an adversary $\mathcal{A}$ which in this model runs in polynomial time, and was given the attack ability by accessing the following queries:

(i) Execute $(\Pi^{x_1}_{\mathcal{U}_i}/\Pi^{x_2}_{\mathcal{S}_j})$: this query models passive attack in which the adversary $\mathcal{A}$ can obtain the message transmitted between instance $\Pi^{x_1}_{\mathcal{U}_i}/\Pi^{x_2}_{\mathcal{S}_j}$ and its partner instance.

(ii) Send $(\mathcal{P}, \mathcal{M})$: this query models active attack, such as replay attacks, impersonation attacks in which the adversary $\mathcal{A}$ may intercept or modify the massage sent to $\mathcal{P}$. The adversary $\mathcal{A}$ also can send a message $\mathcal{M}$ to $\mathcal{P}$ and can receive the output message.

(iii) Reveal $(\Pi^{x_1}_{U_i}/\Pi^{x_2}_{\mathcal{S}_j})$: this query allows A to gain the session key obtained by $\Pi^{x_1}_{U_i}$ (or $\Pi^{x_2}_{\mathcal{S}_j}$) and its partner after the current authentication. If this session key has not been defined or A has initiated a $Test$ query for the session key that needs to be guessed, then an empty result ($\perp$) is returned. Otherwise, A will receive the session key.

(iv) CorruptSC(u): adversary $\mathcal{A}$ in this query can simulate the smart card lost attack and uses this attack to get family member's smart card data.

(v) CorruptDB(s): adversary $\mathcal{A}$ in this query can simulate the stolen verifier attack.

(vi) Test(u/s): in this function, we test the security of the simulated session by flipping the coin $b \in \{0, 1\}$. The adversary sends an inquiry, and will return a session key if $b = 1$ or returned a same size binary random number if $b = 0$.

(vii) Hash(x): in this function, there is a table containing x and $h(x)$. Search for x in this table after receiving the query. If x exists, returns $h(x)$; otherwise, returns a random string as the hash value $h(x)$ and stores $\{x, h(x)\}$ in the table.

Semanticsecurity: if the adversary successfully guesses the value of b by nonnegligible advantage, the scheme fails to provide semantic security. To distinguish between the random number and the session key, the adversary can use the above-mentioned queries to increase the advantage of guessing. Let $A\ dv^{AKE}$ be the advantage of A in breaking the semantic security of the scheme. We use the notion Suc to denote the event that adversary successfully guesses the value of b. If $A\ dv^{AKE}$

is small enough to be ignored, then we say that our scheme is secure under the RoR model.

4.2. Formal Security Analysis

Theorem 1. *Let q_s, q_h, and q_t be the time of Send queries, Hash queries, guessing the master key s of medical server MS. And l is the length of s. Thus, we have*

$$Adv^{AKE}(A) <= \text{Max}\left\{\frac{q_s}{|I_1|\cdot|I_2|}, \frac{q_t}{2^l}\right\} + \frac{q_h^2}{2\cdot|H|} + \frac{q_s^2}{2^l}. \text{(Section 1).} \tag{2}$$

Here, I_1 and I_2 denote uniformly distributed dictionaries of user identity and user password. Then, the $|H|$, $|I_1|$ and $|I_2|$ denote the range size of hash function, I_1 and I_2.

Proof. A series of games $Gm_i\,(0 <= i <= 4)$ are completed in the proof to prove the security of our proposed scheme. In each game, $\mathscr{P}r[Suc_i]\,(0 <= i <= 4)$ represents the probability that the adversary successfully guesses a correct value of b in each Gm_i.

Gm_0: this starting game models a real attack scenario in RoR model by the adversary $\mathscr{A}$. We have

$$Adv^{AKE}(A) = \left|2\mathscr{P}r[Suc_0] - 1\right|. \tag{3}$$

Gm_1: according to the scheme, in order to increase the advantage of the adversary $\mathscr{A}$ successfully guessing the value of b, we add Execute(u, s) query in this game. In our scheme, the session key SK is computed by N and Q. The adversary $\mathscr{A}$ can obtain some messages through this query such as $\{id_{FM}', Auth_{FM}, X, M_{MS}, Y, Auth_{sk}\}$, but due to $N = L_{FM}'\oplus MID_{FM}$ and $Q = g^{xy}$, the adversary $\mathscr{A}$ cannot infer N and Q from above messages. Therefore, the adversary $\mathscr{A}$ cannot get additional advantage through the eavesdropping attack. Thus, we have

$$\mathscr{P}r[Suc_1] = \mathscr{P}r[Suc_0]. \tag{4}$$

Gm_2: in this game, the adversary $\mathscr{A}$ is considered to use Send$(\mathscr{P}, \mathscr{M})$ query to simulate active attack. If the adversary $\mathscr{A}$ wants to get the correct feedback message, he/she needs to calculate the correct $Auth_{FM} = h(id_{FM}'\|N''\|X)$, $M_{MS} = h(Y\|N''\|Q)$ and $Auth_{sk} = h(id_{FM}'\|N''\|sk)$, but the adversary cannot get N and Q, so they cannot calculate $Auth_{FM}$, M_{MS} or $Auth_{sk}$ and can only rely on guessing. According to the birthday paradox, the collision probability on the hash oracle is $q_h^2/2\cdot|H|$, and the collision probability of N requires guessing the value of master key s is $q_s^2/2^l$. Thus, we have

$$\mathscr{P}r[Suc_2] - \mathscr{P}r[Suc_1] <= \frac{q_h^2}{2\cdot|H|} + \frac{q_s^2}{2^l}. \tag{5}$$

Gm_3: in this game, the adversary $\mathscr{A}$ can use *Reveal* query to gain the session key obtained by $\Pi_{\mathscr{U}_i}^{x_1}$ or $\Pi_{\mathscr{S}_j}^{x_2}$ and its partner after the current authentication. But in our scheme, the session key is $sk = h(N''\oplus Q')$, where $Q' = X^y = Y^x$. The data $Q' = X^y = Y^x$ are updated after each communication. Therefore, the adversary $\mathscr{A}$ cannot get additional advantage through *Reveal* query. Thus, we have

$$\mathscr{P}r[Suc_3] = \mathscr{P}r[Suc_2]. \tag{6}$$

Gm_4: in this game, according to the definition of Freshness, the adversary $\mathscr{A}$ can only queries one of the CorruptSC and the CorruptDB oracle. So, it is discussed in the following two situations. □

Case 1. In this case, the adversary $\mathscr{A}$ can receive the data in smart card like $\{M_{FM}, id_{FM}'\}$ by the CorruptSC oracle. Afterwards, the adversary $\mathscr{A}$ wants to capture the user's session key $sk = h(N''\oplus Q')$, where $N'' = h(ID_{FM}\|PW_{FM})\oplus M_{FM}$ and $Q' = Y^x$. The adversary $\mathscr{A}$ in this case only has $\{M_{FM}, id_{FM}'\}$ which cannot calculate N'', so the adversary $\mathscr{A}$ needs to guess the value of $ID_{FM}\|ID_{FM}$. Since the scale of the dictionary is $|I_1|\cdot|I_2|$, we have

$$\mathscr{P}r[Suc_4] - \mathscr{P}r[Suc_3] <= \frac{q_s}{|I_1|\cdot|I_2|}. \tag{7}$$

Case 2. In this case, the adversary $\mathscr{A}$ can simulate a stolen verification table attack by queries in CorruptDB oracle. Then, the adversary $\mathscr{A}$ receives the server's data $\{MID_{PT}, MID_{FM}, SC_{PT}, id_{FM}\}$. According to the session key $sk = h(N''\oplus Q)$, the adversary needs to calculate $N'' = h(L_{FM}'\oplus M_{FM})$ which $L_{FM} = SC_{FM}\oplus SC_{PT}$ and $SC_{FM} = h(id_{FM}\|s)$. The adversary $\mathscr{A}$ can only get SC_{PT} and id_{FM} from above data. If the adversary $\mathscr{A}$ wants to calculate $SC_{FM} = h(id_{FM}\|s)$. The adversary $\mathscr{A}$ needs to guess the server's master key s. Thus, we have

$$\mathscr{P}r[Suc_4] - \mathscr{P}r[Suc_3] <= \frac{q_t}{2^l}. \tag{8}$$

In addition, all the random oracles are simulated. The adversary can take Test query one time to guess the bit b. Thus,

$$\mathscr{P}r[Suc_4] = \frac{1}{2}. \tag{9}$$

In summary, for the Case 1, combining (2)–(6) and (8), we have

$$Adv^{AKE}(A) <= \frac{q_h^2}{2\cdot|H|} + \frac{q_s^2}{2^l} + \frac{q_s}{|I_1|\cdot|I_2|}. \tag{10}$$

And for the Case 2, combining (2)–(8), we have

$$Adv^{AKE}(A) <= \frac{q_h^2}{2\cdot|H|} + \frac{q_s^2}{2^l} + \frac{q_t}{2^l}. \tag{11}$$

The adversary A can choose one of case as the Gm_3. Thus, we have $A\,dv^{AKE}(A) <= \mathrm{Max}\{q_s/|I_1| \cdot |I_2|, q_t/2^l\} + q_h^2/2 \cdot |H| + q_s^2/2^l$. In summary, the adversary cannot obtain additional advantage of guessing the correct coin b through the above games. Thus, it can be proved that our patient–family member binding scheme provides semantic security in RoR model.

4.3. Discussion on Possible Attacks. In this section, we discuss the strong privacy protection mechanism of our scheme against the most common attacks in E-health system.

4.3.1. Resist Smart Card Loss Attack. In this attack, the adversary could capture the message stored in a smart card and want to calculate important private data with that information. In our scheme, the adversary can capture information $\{M_{FM}, id_{FM}'\}$ from family member $FM's$ smart card and the information $\{R_{PT}, ID_{MS}, C_{PT}, NID_{PT}, NID_{FM}, L_{FM}\}$ from the patient $PT's$ smart card. After adversary obtaining smart card information $\{M_{FM}, id_{FM}'\}$, the adversary wants to calculate the value of $Auth_{FM}$. But due to the absence of a necessary values N'', the adversary cannot derive $Auth_{FM}$ to pass authentication. Furthermore, even if the adversary has also obtained the patient $PT's$ smart card information $\{R_{PT}, ID_{MS}, C_{PT}, NID_{PT}, NID_{FM}, L_{FM}\}$, the adversary cannot derive $N'' = L_{FM} \oplus MID_{FM}$ without MID_{FM}. So, the adversary cannot guess the value of $sk = h(N'' \oplus Q')$ without N''. The adversary cannot obtain the useful information to guess session key through the smart card attack. Thus, our scheme could provide security and against the stolen smart card attack successfully.

4.3.2. Resisting Off-Line Guessing Attack. Assuming that the adversary intercepted the data $\{I_{FM}, M_2, M_3, Auth_{PT}\}$ from binding phase, the $\{Auth_{FM}, id_{FM}, X, M_{MS}, Y\}$ from authentication phase, which transmitted over the insecure channel, attempted to launch an off-line guessing attack. However, none of the above data can be used to calculate ID_{PT}, PW_{PT} or ID_{FM}, PW_{FM}. Moreover, the identity and password always appear in pairs of the equations, and our scheme could ensure the anonymity for patient and family member. So, the adversary cannot obtain the identity and password of the patient and the family member. Since the private key s of the medical server is a high-entropy random number and is protected by a one-way hash function, the adversary cannot guess it. Thus, the off-line guessing attack cannot threaten our proposed scheme.

4.3.3. Resisting Replay Attack. In our scheme, if the adversary captures the message $\{id_{FM}', Auth_{FM}, X\}$ and replays it to medical server MS, the medical server MS will use the received X to calculate $Q^* = X^y$, then send Y and M_{MS}^*, which is calculated by Q^* to the adversary. But in the next step, the adversary needs to use the message M_{MS}^* to calculate $Auth_{sk}$. Because the calculation of $Auth_{sk} = h(id_{FM}' \| N'' \| sk)$ requires sk and the calculation of $sk = h(N'' \| Q')$ requires $Q' = Y^x$, the adversary cannot calculate Q' from the obtained message. So, he/she cannot pass the Verify by medical server MS. Then, if the adversary captures the message $\{M_{MS}, Y\}$ and wants to replay it to family member FM, the adversary also cannot be authenticated by family member FM. Because the verification message $M_{MS} = h(Y \| N'' \| Q')$ which is calculated with $Q' = Y^x$, and the random number x will refresh in every session. The adversary cannot get the value of x. Similarly, if the adversary captures the message $Auth_{sk}$ and replays it to medical server MS, it will not be authenticated by the medical server MS, because the value of $sk = h(N'' \oplus Q')$ is calculated by N'' and Q', the random number in Q' will change every time. The adversary also cannot pass the medical server's authentication. Obviously, the medical server MS and family member FM can resist the replay attack. Thus, the replay attack cannot threaten our proposed scheme.

4.3.4. Resisting Man-in-the-Middle Attack. In our proposed scheme, the session key sk is established in the authentication phase between the family member and the medical server. If the adversary interrupts the authentication request $\{id_{FM}', Auth_{FM}, X\}$ and computes a new request $\{id_{FM}^{'*}, Auth_{FM}^*, X^*\}$ to cheat the medical server, it will not successfully pass the medical server $MS's$ authentication, because the adversary cannot calculate the message $Auth_{FM} = h(id' \| N'' \| X)$ which is computed by N''. And same as the adversary intercepts the authentication message $\{M_{MS}, Y\}$ or $\{Auth_{sk}\}$, he/she also cannot calculate the message $\{M_{MS}^* = h(Y \| N'' \| Q'), Y^*\}$ or $\left\{Auth_{sk}^* = h(id_{FM}' \| N'' | sk)\right\}$ to pass the authentication without N''. Therefore, our scheme can resist man-in-the-middle attack.

4.3.5. Resisting Privileged Insider Attack. The insider attack means that the insider of system can access to obtain user-sensitive information. In our scheme, the adversary obtains the data $\{MID_{PT}, MID_{FM}, SC_{PT}, id_{FM}\}$ in the medical server database through privileged insider attack. In the authentication phase, the calculation of $N''' = L_{FM}' \oplus MID_{FM}$ requires $L_{FM}' = SC_{FM}' \oplus SC_{PT}$, but the adversary only has the data SC_{PT}. So, the adversary cannot derive L_{FM}'. Cause the adversary just has the data MID_{FM}, the adversary cannot drive $N''' = L_{FM}' \oplus MID_{FM}$. Therefore, our scheme can resist the privileged insider attack.

4.3.6. Perfect Forward Secrecy. This security feature can ensure security even if an adversary obtains all past session keys. As can be seen from our scheme, the session key is $sk = h(N'' \oplus Q')$, where $N'' = h(ID_{FM} \| PW_{FM}) \oplus M_{FM}$, $Q' = X^y = Y^x$. The sk is protected by the N'' and Q'. The data $Q' = X^y = Y^x$ is updated after each communication. Even if the adversary $\mathcal{A}$ knows the past session key, he/she is still impossible to compute the new session key of our

scheme. Therefore, our scheme can provide the perfect forward secrecy.

5. Performance Comparison

In this section, we compare the computation cost and function of our patient–family member binding scheme with other related authentication schemes [29–33]. Our proposed scheme has two main phases: (1) binding phase and (2) authentication phase. We use the computational cost (total time to perform all operations) to compare the performance. In order to evaluate the computational cost, let the following notions to represent time complexity:

(i) T_{ha}: time for performing a one-way hash operation

(ii) T_{sy}: time for performing a symmetric encryption/decryption operation

(iii) T_{ec}: time for performing an elliptic curve scalar point multiplication operation

(iv) T_o: time for performing an elliptic curve scalar addition operation

(v) T_{em}: time for a modular exponentiation operation

We evaluate the computation cost by using MIRACL C/C++ Library. The system used 64 bit Windows 10 operating system (CPU:2.3 GHz, RAM:8 GB). Based on the above system requirements, we get the average computation time of each cryptographic operation: $T_{ha} \approx 0.057ms$, $T_{sy} \approx 0.187ms$, $T_{ec} \approx 1.37ms$, $T_o \approx 0.91ms$, and $T_{em} \approx 1.89ms$.

In Table 2, we show the computational cost of the related schemes [29–33] and ours in the registration phase and authentication phase. During the evaluating process, due to the small amount of calculation, we can ignore the XOR and string concatenation. In registration phase, computational cost of ours needs $8T_{ha}$ whereas other related schemes which were proposed by Zhang et al. [29], Qu et al. [30], Qi and Chen [31], Karuppiah et al. [32], and Irshad et al. [33], respectively are $3T_{ha}$, $3T_{ha} + 2T_{ec} + 1T_o$, $3T_{ha}$, $4T_{ha}$, and $4T_{ha} + 1T_{sy} + 1T_{ec}$. We observe that Qu et al.'s scheme and Irshad et al.'s scheme requires more computational cost during the registration phase, because of T_{ec}/T_{sy} in their calculation. The methods used in Zhang et al.'s scheme, Qi-Chen's scheme and Kar et al.'s scheme have lower costs during the registration phase. As we have known, in the key agreement scheme, the scheme only needs to be registered once, but authentication phase will be run multiple times. Therefore, the computational cost of the registration phase has little effect on the overall scheme. During the authentication phase, computational cost of our scheme needs $9T_{ha} + 4T_{em}$, which costs less than other related schemes which were proposed by Zhang et al. [29], Qu et al. [30], Qi and Chen [31], Karuppiah et al. [32], and Irshad et al. [33]. Finally, the total computational cost of above schemes as follows:

(i) Zhang et al. [29]: $14T_{ha} + 2T_{sy} + 6T_{ec} = 9.39\,(ms)$

(ii) Qu et al. [30]: $16T_{ha} + 11T_{ec} + 6T_o = 21.442\,(ms)$

(iii) Qi and Chen [31]: $15T_{ha} + 6T_{ec} = 9.075\,(ms)$

(iv) Karuppiah et al. [32]: $19T_{ha} + 4T_{em} = 8.63\,(ms)$

(v) Irshad et al. [33]: $21T_{ha} + 12T_{ec} + 5T_{sy} = 18.57\,(ms)$

(vi) Ours: $17T_{ha} + 4T_{em} = 8.52\,(ms)$

In summary, our scheme has a great advantage on total costs which only needs $17T_{ha} + 4T_{em} = 8.52\,(ms)$. Our scheme has the best performance with low computational cost as compared with the other related schemes [29–33]. And more performance comparison of each scheme is shown in Figures 5–7.

In Figure 5, the two graphs respectively represent the time cost in the registration phase and the authentication phase of all schemes. In the left graph, we can see that in the registration phase, the computational cost of the Qu et al.'s scheme and Irshad et al.'s scheme is much bigger than other schemes. In the authentication phase (the right graph), Qu et al.'s scheme and Irshad et al.'s scheme requires large computational cost. Meanwhile, Zhang et al.'s scheme, Qi-Chen's scheme, Kar et al.'s scheme and ours perform well in the authentication phase. Besides, the computational cost of ours is lower than other schemes. Figure 6 shows the total time cost of those schemes and Figure 7 shows the comparison of computation cost of our proposed scheme with related schemes. From Figure 7, we can know that the number of users increases, our scheme still has good performance. In summary, our scheme shows better performance which needs lower computational cost than other related schemes.

We compare the proposed scheme with other related schemes in terms of different security attacks and parameters in Table 3. Zhang et al.'s [29] scheme cannot provide several security features such as fail to resist the stolen verifier attack [34]. Qu et al.'s [30] scheme focuses on preventing the impersonation attack but suffers from the off-line guessing attack and reply attack. Qi and Chen's [31] scheme ignores the user anonymity and suffers insider attack [32]. Karuppiah et al.'s scheme [32] cannot provide perfect forward security and cannot resist impersonation attack. Irshad et al.'s scheme [33] can resist most attacks but suffers impersonation attack [35].

Furthermore, compared with the scheme [29–33], our proposed scheme not only realizes the secure communication between the family member and the medical server, but also realizes advanced security attributes and strong security attack protection.

5.1. Future Works. We propose a binding scheme for the family member, which can bind the patient and the family member so that the family member can participate in the treatment process of the patient. In our paper, patients can only authorize one family member per binding phase. When multiple family members need to bind at the same time, a batch binding scheme is needed. Moreover, more and more scenarios use biometric authentication. In order to make it more convenient for patients and their families to complete the binding and the authentication, it is necessary to design a scheme that uses biometric characteristics to complete the

Table 2: Computational cost comparisons.

	Registration phase	Authentication phase	Total	Time (ms)
Zhang and Zhu [29]	$3T_{ha}$	$11T_{ha} + 2T_{sy} + 6T_{ec}$	$14T_{ha} + 2T_{sy} + 6T_{ec}$	9.39
Qu and Tan [30]	$3T_{ha} + 2T_{ec} + 1T_{o}$	$13T_{ha} + 9T_{ec} + 5T_{o}$	$16T_{ha} + 11T_{ec} + 6T_{o}$	21.442
Qi and Chen [31]	$3T_{ha}$	$12T_{ha} + 6T_{ec}$	$15T_{ha} + 6T_{ec}$	9.075
Karuppiah et al. [32]	$4T_{ha}$	$15T_{ha} + 4T_{em}$	$19T_{ha} + 4T_{em}$	8.63
Irshad et al. [33]	$4T_{ha} + 1T_{sy} + 1T_{ec}$	$17T_{ha} + 11T_{ec} + 4T_{sy}$	$21T_{ha} + 5T_{sy} + 12T_{ec}$	18.57
Ours	$8T_{ha}$	$9T_{ha} + 4T_{em}$	$17T_{ha} + 4T_{em}$	8.52

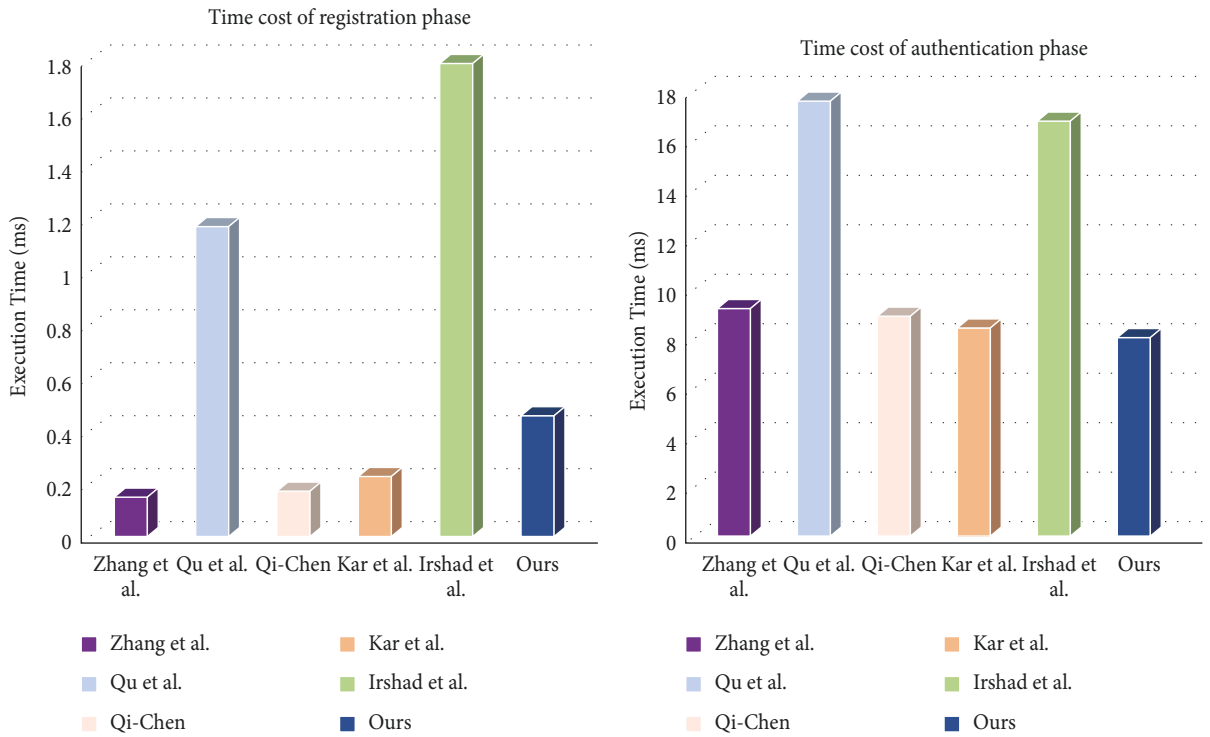

Figure 5: Computational cost comparison.

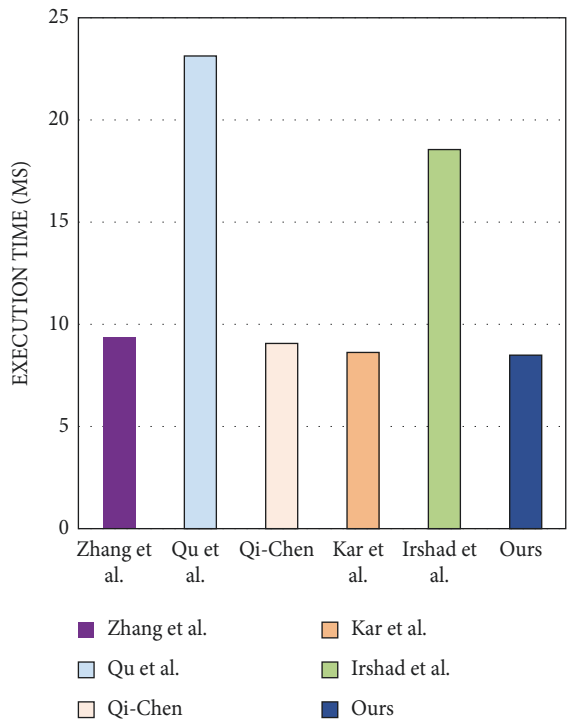

Figure 6: Total time cost.

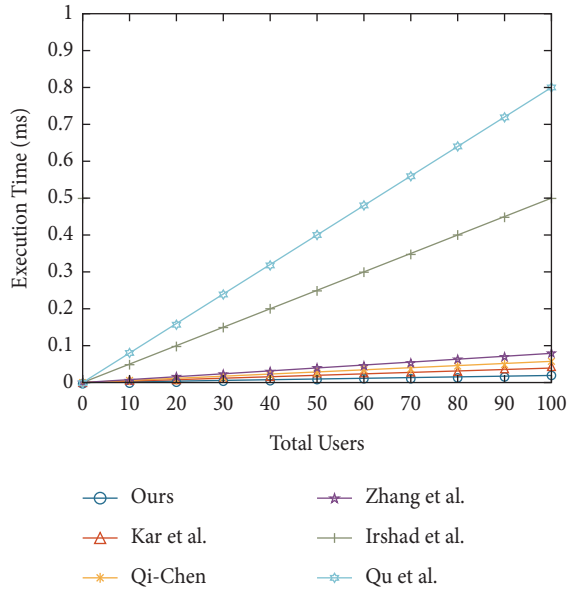

Figure 7: Computation cost for different numbers of users.

Table 3: Functionality comparison.

	[29]	[30]	[31]	[32]	[33]	Ours
User anonymity	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{N}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$
FM-MS authentication	$\mathscr{R}$	$\mathscr{R}$	$\mathscr{R}$	$\mathscr{R}$	$\mathscr{R}$	$\mathscr{Y}$
Key agreement	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$
Resistance to stolen verifier attack	$\mathscr{N}$	$\mathscr{R}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{R}$	$\mathscr{Y}$
Resistance to insider attack	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{N}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$
Resistance to off-line guessing attack	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$
Perfect forward security	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{N}$	$\mathscr{N}$	$\mathscr{Y}$	$\mathscr{Y}$
Resistance to impersonation attack	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{R}$	$\mathscr{N}$	$\mathscr{N}$	$\mathscr{Y}$
Resistance to replay attack	$\mathscr{N}$	$\mathscr{N}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$	$\mathscr{Y}$

$\mathscr{Y}$: means can resist the attack successfully or provide the security property, $\mathscr{N}$: means cannot resist the attack successfully or cannot provide the security property, and $\mathscr{R}$: means not refereed.

authentication. In the future, we will conduct further studies on batch binding and biometric authentication.

6. Conclusion

In this paper, through reviewed the previous papers, we find that most systems only consider the secure communication between the patient and the medical server, but ignore the important role of family member in the E-health system. In order to overcome this problem, we propose a patient family binding and authentication scheme with privacy protection for E-health system. In our scheme, not only patients can bind family member freely, but also the family member can timely process the diagnosis result when the patient is inconvenient. In addition, the increasing the number of family members will not cause additional burden on the medical server. Consequently, our scheme is proved to be efficient and secure.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China under grants Nos. 61701173, 61802445, 62072134, and U2001205, the Young Talents Project of Science and Technology Research Program of Hubei Education Department and under grant Q20211403, and the Key Research and Development Program of Hubei Province under grant 2021BEA163.

References

[1] 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.

[2] M. Karthigaiveni and B. Indrani, "An efficient two-factor authentication scheme with key agreement for iot based

e-health care application using smart card," *Journal of Ambient Intelligence and Humanized Computing*, no. 8, 2019.

[3] E. Lara, L. Aguilar, and J. A. García, "Lightweight Authentication Protocol Using Self-Certified Public Keys for Wireless Body Area Networks in Health-Care Applications," *IEEE Access*, vol. 9, 2021.

[4] J. Ryu, D. Kang, H. Lee, H. Kim, and D. Won, "A secure and lightweight three-factor-based authentication scheme for smart healthcare systems," *Sensors*, vol. 20, no. 24, p. 7136, 2020.

[5] Y. Chen and J. Chen, "A secure three-factor-based authentication with key agreement protocol for e-health clouds," *The Journal of Supercomputing*, vol. 77, pp. 1–22, 2020.

[6] W. Hellman and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, November 1976.

[7] J. Joux, "A one round protocol for tripartite diffie-hellman," in *Algorithmic Number Theory*, W. Bosma, Ed., Springer, Berlin, Germany, pp. 385–393, 2000.

[8] B.-L. Chen, W.-C. Kuo, and L.-C. Wuu, "Robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems*, vol. 27, no. 2, pp. 377–389, 2014.

[9] Y.-H. Chuang and C.-L. Lei, "An independent three-factor mutual authentication and key agreement scheme with privacy preserving for multiserver environment and a survey," *International Journal of Communication Systems*, vol. 34, p. e4660, 2000.

[10] A. K. Das and 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. 9948–10016, 2013.

[11] R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan, and Li Xiong, "Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems," *Journal of Medical Systems*, vol. 39, no. 11, pp. 1–21, 2015.

[12] S. Aghili, M. 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, pp. 410–424, 2019.

[13] H.-L. Yeh, T.-Ho Chen, and W.-K. Shih, "Robust smart card secured authentication scheme on sip using elliptic curve cryptography," *Computer Standards & Interfaces*, vol. 36, no. 2, pp. 397–402, 2014.

[14] M. Farash, S. Kumari, and M. Bakhtiari, "Cryptanalysis and improvement of a robust smart card secured authentication scheme on sip using elliptic curve cryptography," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4485–4504, 2016.

[15] P. Mohit, R. Amin, A. Karati, G. P. Biswas, and M. K. Khan, "A standard mutual authentication protocol for cloud computing based health care system," *Journal of Medical Systems*, vol. 41, no. 4, p. 50, 2017.

[16] L. Zhang, Y. Zhang, S. Tang, and L. He, "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, 2017.

[17] A. A. Al-Saggaf, "Key binding biometrics-based remote user authentication scheme using smart cards," *IET Biometrics*, vol. 7, no. 3, pp. 278–284, 2018.

[18] Li Chan and Ke Zhang, "Privacy-aware smart card based biometric authentication scheme for e-health," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1353–1365, 2021.

[19] Z. Yu Wu, Y. C. Lee, F. Lai, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, 2012.

[20] D. He, J. Chen, and R. Zhang, "A more secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989–1995, 2012.

[21] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3597–3604, 2012.

[22] X. Yan, W. Li, P. Li, J. Wang, X. Hao, and P. Gong, "A secure biometrics-based authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 37, no. 5, pp. 9972–9976, 2013.

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

[24] O. Mir and 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, 2015.

[25] Z. Mehmood, A. Ghani, G. Chen, and S. A. 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.

[26] S. A. Hosseini Seno and R. Budiarto, "An efficient lightweight authentication and key agreement protocol for patient privacy," *Computers, Materials & Continua*, vol. 69, 2021.

[27] K. Chatterjee, "An improved authentication protocol for wireless body sensor networks applied in healthcare applications," *Wireless Personal Communications*, vol. 111, no. 3, pp. 1–19, 2019.

[28] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proceedings of the International Workshop on Public Key Cryptography Public Key Cryptography - PKC 2005*, pp. 65–84, Springer, Les Diablerets, Switzerland, January 2005.

[29] L. Zhang and S. Zhu, "Robust ecc-based authenticated key agreement scheme with privacy protection for telecare medicine information systems," *Journal of Medical Systems*, vol. 39, no. 5, p. 49, 2015.

[30] J. Qu and X.-L. Tan, "Two-factor user authentication with key agreement scheme based on elliptic curve cryptosystem," *Journal of Electrical and Computer Engineering*, vol. 2014, no. 4, pp. 1–6, 2014.

[31] M. Qi and J. Chen, "An efficient two-party authentication key exchange protocol for mobile environment," *International Journal of Communication Systems*, vol. 30, no. 16, Article ID e3341, 2017.

[32] M. Karuppiah, A. K. Das, Li Li et al., "Secure remote user mutual authentication scheme with key agreement for cloud environment," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 1046–1062, 2019.

[33] A. Irshad, M. Sher, O. Nawaz, S. Chaudhry, I. Khan, and S. Kumari, "A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme," *Multimedia Tools and Applications*, vol. 76, no. 15, pp. 16463–16489, 2017.

[34] D. Dharminder, U. Kumar, and P. Gupta, "A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2531–2542, 2021.

[35] T. Limbasiya, S. Sahay, and B. Sridharan, "Privacy-preserving mutual authentication and key agreement scheme for multi-server healthcare system," *Information Systems Frontiers*, vol. 23, no. 4, pp. 835–848, 2021.