sensors

MDPI

Article

An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System

Chun-Ta Li [1], Tsu-Yang Wu [2,3,*], Chin-Ling Chen [4,5,*], Cheng-Chi Lee [6,7] and Chien-Ming Chen [8]

1 Department of Information Management, Tainan University of Technology, 529 Zhongzheng Road, Tainan 71002, Taiwan; th0040@mail.tut.edu.tw
2 Fujian Provincial Key Laboratory of Big Data Mining and Applications, Fujian University of Technology, Fuzhou 350118, China
3 National Demonstration Center for Experimental Electronic Information and Electrical Technology Education, Fujian University of Technology, 3 Xueyuan Road, Fuzhou 350118, China
4 Department of Computer Science and Information Engineering, Chaoyang University of Technology, 168 Jifeng East Road, Taichung 41349, Taiwan
5 School of Information Engineering, Changchun University of Technology, Changchun 130600, China
6 Department of Library and Information Science, Fu Jen Catholic University, 510 Jhongjheng Road, New Taipei 24205, Taiwan; cclee@mail.fju.edu.tw
7 Department of Photonics and Communication Engineering, Asia University, 500 Lioufeng Road, Taichung 41354, Taiwan
8 Harbin Institute of Technology Shenzhen Graduate School, Shenzhen University Town, Xili, Nanshan District, Shenzhen 518055, China; chienming.taiwan@gmail.com
* Correspondence: wutsuyang@gmail.com (T.-Y.W.); clc@mail.cyut.edu.tw (C.-L.C.)

Received: 28 May 2017; Accepted: 21 June 2017; Published: 23 June 2017

Abstract: In recent years, with the increase in degenerative diseases and the aging population in advanced countries, demands for medical care of older or solitary people have increased continually in hospitals and healthcare institutions. Applying wireless sensor networks for the IoT-based telemedicine system enables doctors, caregivers or families to monitor patients' physiological conditions at anytime and anyplace according to the acquired information. However, transmitting physiological data through the Internet concerns the personal privacy of patients. Therefore, before users can access medical care services in IoT-based medical care system, they must be authenticated. Typically, user authentication and data encryption are most critical for securing network communications over a public channel between two or more participants. In 2016, Liu and Chung proposed a bilinear pairing-based password authentication scheme for wireless healthcare sensor networks. They claimed their authentication scheme cannot only secure sensor data transmission, but also resist various well-known security attacks. In this paper, we demonstrate that Liu–Chung's scheme has some security weaknesses, and we further present an improved secure authentication and data encryption scheme for the IoT-based medical care system, which can provide user anonymity and prevent the security threats of replay and password/sensed data disclosure attacks. Moreover, we modify the authentication process to reduce redundancy in protocol design, and the proposed scheme is more efficient in performance compared with previous related schemes. Finally, the proposed scheme is provably secure in the random oracle model under ECDHP.

Keywords: elliptic curve cryptography (ECC); Internet of Things (IoTs); medical care system; smart cards; user authentication; wireless sensor networks (WSNs)

1. Introduction

As more network technologies and smart devices have been developed, many IoT (Internet of Things) applications have been proposed, such as transportation and logistics services, healthcare services and a variety of smart environment (home, office, plant) domains. IoT is going to create a world where physical things can be seamlessly integrated into communication networks in order to provide autonomous and intelligent services for improving human beings' life. In general, the IoT system involves three components: a sensing unit contains a large number of sensors, actuators and mobile terminals to sense physical environments; a network layer includes all network techniques with heterogeneous network configurations for data transmission; intelligent computing offers expected services or applications to IoT end users by mining and analyzing data processors.

IoT-based wireless sensor networks have been getting considerable attention from a variety of domains, such as environmental monitoring, intelligent appliances in daily living, medical care services, etc. Due to the ranking of the most common diseases in advanced countries having changed to chronic and cardiovascular diseases, the demands for medical care of such patients have increased substantially in hospitals and healthcare institutions. For the development of medical care services in hospitals and healthcare institutions, IoT-based WSNs technology is used to supplement physiological collection and measurement, enabling doctors, caregivers and families to examine the physiological conditions of patients remotely at anytime and anyplace through the Internet [1–6]. On the basis of IoT employed for medical care service in hospitals or healthcare institutions, WSNs enable sensing and collecting the physiological parameters of patients periodically, transmitting the acquired data to the authorized medical personnel, enabling professional doctors and medical personnel to monitor patients' health conditions in real time and providing patients with appropriate medical care and medical treatment.

To apply IoT-based WSNs to medical care services successfully, ensuring the personal privacy of patients and preventing malicious network intrusion are paramount. Undoubtedly, the foundation of security is to authenticate the legitimacy of remote users and ensure the integrity of data transmissions [7–12]. In the last decade, a diversity of user authentication schemes in WSNs have been presented. In 2006, Wong et al. [13] introduced an efficient user authentication scheme for WSNs using lightweight hashing functions and XOR operations. In 2007, Tseng et al. [14] pointed out the vulnerability of Wong et al.'s scheme to replay, forgery and password guessing attacks. Furthermore, in 2008, Lee [15] showed that the computational overheads of Wong et al.'s scheme are not suitable for resource-constrained sensor nodes. In 2009, Das [16] suggested a two-factor (namely the password and smart card) authentication mechanism for WSNs, which not only prevents a series of security threats, but also achieves efficiency in terms of computational overheads. However, Huang et al. [17] and Li et al. [18] pointed out the vulnerability of Das's scheme to off-line password guessing, user impersonation, node impersonation and unknown user attacks and that it does not provide the property of user anonymity. In 2012, Yoo et al. [19] pointed out the vulnerability of Huang et al.'s scheme to insider and parallel session attacks and that it does not provide mutual authentication between system participants. In 2013, Xue et al. [20] presented a temporal-credential-based authentication scheme for resource-constrained WSNs, and the authors claimed that their scheme provides relatively more security criteria without increasing system overheads too much in terms of communication, computation and storage. Parallel to Xue et al.'s work, in the same year, Li et al. [3] cryptanalyzed that Xue et al.'s scheme cannot withstand off-line password guessing, stolen-verifier, privileged insider, many logged-in users' and stolen smart card attacks, and the above security threats make Xue et al.'s scheme inapplicable to practical WSN applications.

In order to design a secure and two-factor user authentication scheme for wireless healthcare sensor networks, Liu and Chung [21] in 2016 proposed a bilinear pairing-based [22] authentication scheme, and Figure 1 illustrates the comprehensive structure of the IoT-based medical care system, which could be applied in hospitals or healthcare institutions. When patients live in hospitals or healthcare institutions, they wear smart clothes in which body sensors are embedded in the piece of

clothing and collect their physiological parameters (such as blood pressure, heartbeat, body pulse, electrocardiography and body temperature). Therefore, the users (such as doctors, caregivers, families and friends) in the medical care system can remotely inquire and monitor physiological information on patients with the help of trust authority. Before accessing the system, users must register with the trusted authority in person. After successful registration, the trusted authority issues a smart card to the user, and he/she can then use his/her smart card and mobile devices (such as smart phone, PDA, laptop and tablet computer) to log into the medical care system. After successful authentication, the user can access the sensed data of patients measured from sensor nodes within a limited time. Nevertheless, in this paper, we present a cryptanalysis of Liu–Chung's authentication scheme and indicate that their scheme is susceptible to the password disclosure, replay, sensed data disclosure, sensed data forgery, off-line password guessing and stolen smart card attacks. To solve the above-mentioned security problems, we present an improved version of Liu–Chung's authentication scheme using ECC, and we prove that the proposed scheme is secure under the elliptic curve discrete logarithm problem (ECDLP) and the elliptic curve Diffie–Hellman problem (ECDHP). In addition, by designing the mechanism of dynamic identity in the authentication process, we can build an extended scheme with user anonymity. User anonymity [23–25] means that a remote user's real identity will be masked during the login session, and he/she cannot be linked or traced by any outsiders. Furthermore, the correctness of mutual authentication between participants has been proven in the random oracle model under ECDHP. Finally, the proposed scheme requires lower computational overheads compared with other ECC-based schemes, and this advantage makes our scheme more suitable and practical for IoT-based medical care systems.

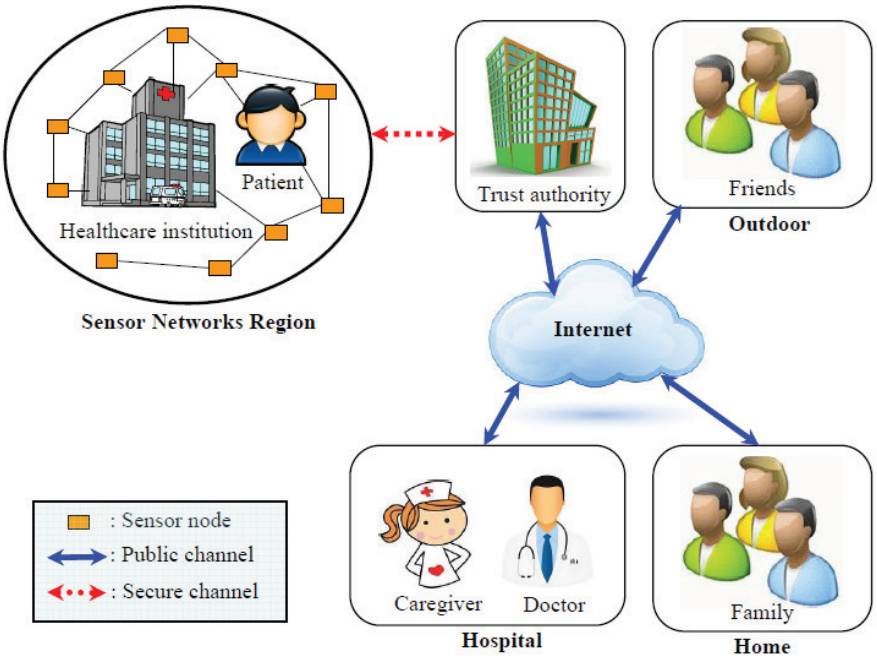

Figure 1. The IoT-based medical care system [21].

The rest of the paper is organized as follows. In Section 2, a brief review of Liu–Chung's authentication scheme is provided. In Section 3, security weaknesses developed to attack Liu–Chung's scheme are presented. In Section 4, the improved scheme is proposed. Security and performance analyses of our proposed scheme are presented in Sections 5 and 6, respectively. Section 7 concludes this paper.

2. Review of Liu–Chung's Authentication Scheme

This section briefly reviews Liu–Chung's authentication scheme [21], and their scheme consists of five phases, including: setup phase, registration phase, login phase, verification phase and access control and encryption phase. For convenience of description, the terminology and notations used in the paper are summarized as follows:

- U_i: The user.
- TA: The trusted authority.
- S: The sensor nodes deployed in hospitals and healthcare institutions.
- ID_i: The identity of U_i.
- PW_i: The password of U_i.
- $h(\cdot)$: A one-way hash function.
- $\hat{e}(a, b)$: The bilinear pairing function using parameter a and parameter b.
- a: A private parameter generated by TA.
- T_L: The login time of U_i.
- T_{now}: The current time.
- T_u: The time limit on the legal access to S by the user U_i.
- ΔT: The transmission delay.
- m: The sensed data collected from S.
- $||$: The message concatenation.
- $\oplus$: The XOR operation.

2.1. Setup Phase

In this phase, the trusted authority TA selects a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ and $P_0 \in G_1$ and generates two one-way hash functions $H_1 : \{0,1\}^* \rightarrow G_2$ and $H_2 : G_2 \rightarrow \{0,1\}^*$, where G_1 is an additive cyclic group of points on an elliptic curve E over F_p, G_2 is a multiplicative cyclic group of a finite field F_p^* and p is a large prime, such that $q|p-1$ for some great prime q. Then, TA selects the secret key $S_0 \in Z_q^*$ and publishes the parameter $P_{pub} = S_0 \times P_0$.

2.2. Registration Phase

In this phase, the user registers with the trusted authority TA through a secure channel to be a legal user. The details of registration phase are as follows:

Step 1: U_i registers an authenticated identity ID_i with TA and sets password PW_i.
Step 2: U_i sends $< ID_i, PW_i >$ to TA.
Step 3: TA computes $Q_{priv} = S_0 \times U_{pub}$, where $U_{pub} = U_{priv} \times P_0$ and $U_{priv} \in Z_q^*$ are U_i's public parameter and secret key, respectively.
Step 4: TA stores the parameters $< h(\cdot), Q_{priv}, ID_i, PW_i, a >$ in U_i's smart card, where a represents a private parameter generated by TA and all of the sensor nodes of TA include a.
Step 5: TA issued the smart card to U_i.

2.3. Login Phase

In this phase, the user inserts his/her smart card into the device and inputs ID_i and PW_i. Then, the smart card performs the following steps:

Step 1: The smart card checks the ID_i and PW_i entered by U_i matches those stored in the smart card. If yes, the smart card executes Step 2. Otherwise, the smart card terminates this phase.
Step 2: The smart card computes $r = h(ID_i||PW_i||a)$ and $Sig = r \times Q_{priv}$.

Step 3: The smart card sends $< Sig, r, T_L, ID_i >$ to TA through a public channel, where T_L represents U_i's login time to the TA.

2.4. Verification Phase

When TA receives the login request $< Sig, r, T_L, ID_i >$ from U_i, TA authenticates U_i through the following steps:

Step 1: TA checks the validity of ID_i and verifies if $\hat{e}(P_0, Sig) = \hat{e}(P_{pub}, r \times U_{pub})$. If yes, TA approves the request of U_i and executes Step 2. If no, TA rejects the request of U_i.

Step 2: TA checks if $T_{now} - T_L < \Delta T$. If yes, TA executes Step 3. Otherwise, it means that the login time exceeds the transmission delay, and the login request is rejected by TA.

Step 3: TA generates a random number b and computes $E = h(b \oplus U_{pub})$. Then, TA sends E to U_i through a public channel.

Step 4: TA sends $< T_u, b, ID_i >$ to all of the sensor nodes S through a secure channel and notifies S that U_i is legal. Note that T_u represents the time limit on the legal access to sensor node data by U_i.

2.5. Access Control and Encryption Phase

When the user U_i is authenticated as legal, U_i can legally access sensed data m in S within a limited time, and U_i and S perform the following steps:

Step 1: U_i inserts his/her smart card into the device and inputs ID_i and PW_i. Then, the smart card verifies whether ID_i and PW_i inputted matches the data stored in the card. If yes, the smart card executes Step 2.

Step 2: The smart card computes $C = h(a||ID_i) \oplus E$.

Step 3: The smart card sends $< C, ID_i, T' >$ to S through a public channel, where T' represents a timestamp.

Step 4: Upon receiving $< C, ID_i, T' >$ from U_i, S verifies if $T_{now} - T' < \Delta T$ and $T_{now} = T_u$. If yes, S executes Step 4.

Step 5: S computes $C' = h(a||ID_i) \oplus h(b \oplus U_{pub})$ and checks whether $C = C'$. If yes, the sensed data m will be transmitted, and S executes Step 5. If no, S terminates this session.

Step 6: S computes $M = m \oplus H_2(\hat{e}(U_{pub}, P_{pub}))$.

Step 7: S sends M to U_i through a public channel.

Step 8: U_i uses the secret parameter Q_{priv} and the public parameter P_0 to perform the following calculation to obtain m:

$$\begin{aligned} m &= M \oplus H_2(\hat{e}(Q_{priv}, P_0)) \\ &= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \oplus H_2(\hat{e}(Q_{priv}, P_0)) \\ &= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \oplus H_2(\hat{e}(S_0 \times U_{pub}, P_0)) \\ &= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \oplus H_2(\hat{e}(U_{pub}, P_0)^{S_0}) \\ &= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \oplus H_2(\hat{e}(U_{pub}, S_0 \times P_0)) \\ &= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \\ &= m \end{aligned}$$

Figure 2 shows the schematic of Liu–Chung's authentication scheme for the IoT-based medical care system.

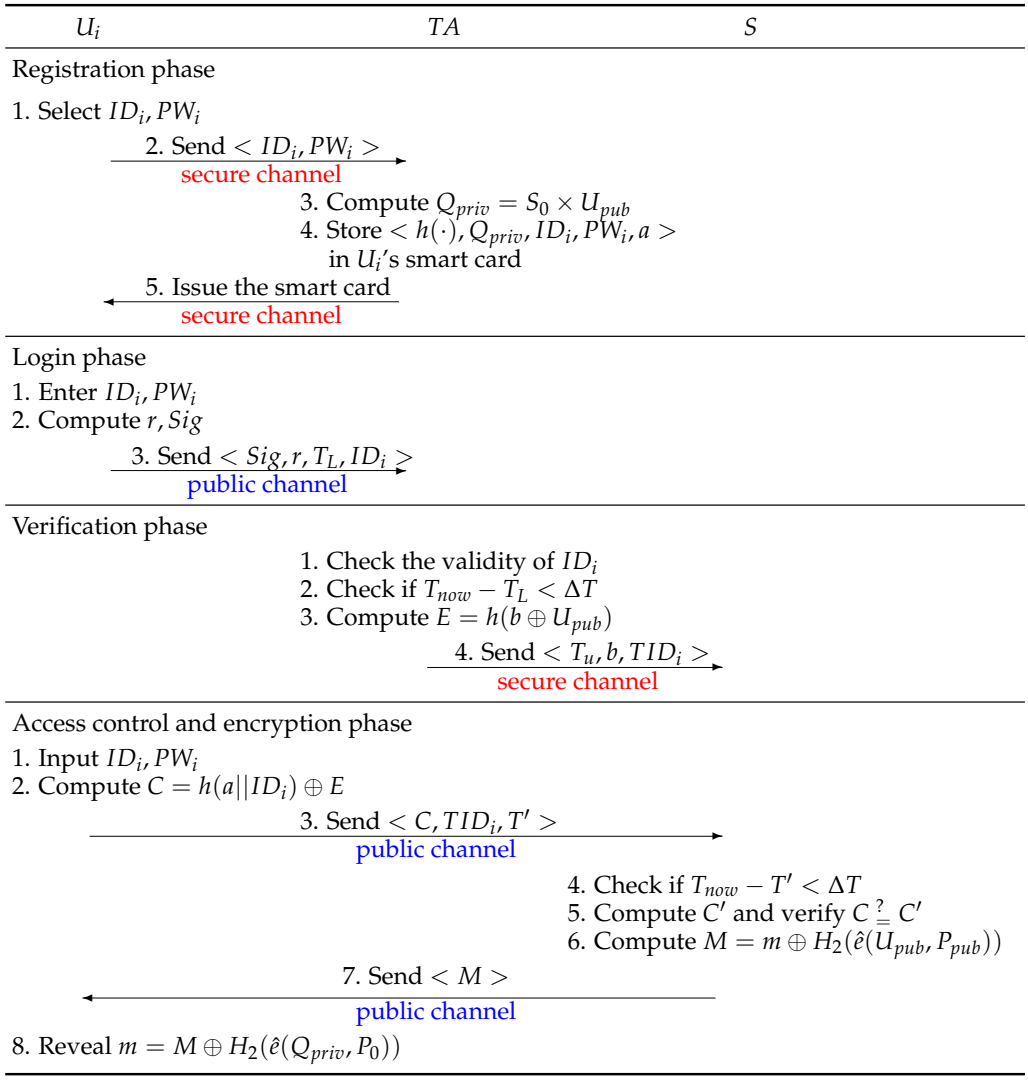

Figure 2. The schematic of Liu–Chung's authentication scheme for IoT-based medical care system.

3. Weaknesses of Liu–Chung's Authentication Scheme

In this section, we present the security weaknesses of Liu–Chung's scheme. We show that their scheme has some security problems and that an attacker U_a can mount different types of attacks on Liu–Chung's scheme.

3.1. Password Disclosure Attacks

In real environments, the user may register with a number of remote services by using a common password PW and the identity ID for his/her convenience. Thus, the privileged-insider of TA may try to use the knowledge of user's PW and ID to access another remote services. In the registration phase of Liu–Chung's scheme, U_i registers to TA by sending (ID_i, PW_i). Therefore, U_i's sensitive password PW_i will be revealed by the privileged-insider of TA.

3.2. Replay Attacks

In the login phase of Liu–Chung's scheme, although the transmitted login message $< Sig, r, T_L, ID_i >$ includes timestamp T_L, however, the other login parameters $< Sig, r, ID_i >$ of U_i are unchanged. Thus, an attacker U_a could replay the eavesdropped messages, such as U_i's login request $< Sig, r, T'_L, ID_i >$ with U_a's current login time T'_L. Finally, U_a can bypass the timestamp checking and replay attacks cannot prevented in Liu–Chung's scheme.

3.3. Sense Data Disclosure Attacks

In the access control and encryption phase of Liu–Chung's scheme, the sensor node S sends the encrypted sensed data M to U_i through an insecure channel. Due to the public U_{pub} of U_i and the public P_{pub} of TA, once an attacker U_a eavesdrops the encrypted sensed data M from the public channel, U_a can perform the following calculation to obtain m without knowing Q_{priv}:

$$\begin{aligned} m &= M \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \\ &= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \oplus H_2(\hat{e}(U_{pub}, P_{pub})) \\ &= m \end{aligned}$$

Finally, Liu–Chung's scheme cannot prevent sensed data disclosure attacks.

3.4. Sense Data Forgery Attacks

In the access control and encryption phase, we found that Liu–Chung's scheme allows the attacker U_a to forge a fake sensed data m' for the user U_i, and U_i wrongly believes he/she has received the physiological conditions of the patients. The sensed data forgery attacks on Liu–Chung's scheme are as follows:

(1) When the sensor node S sends $M = m \oplus H_2(\hat{e}(U_{pub}, P_{pub}))$ to the user U_i, U_a intercepts the message M.
(2) U_a maliciously forges a fake sensed data m' and computes $M' = m' \oplus H_2(\hat{e}(U_{pub}, P_{pub}))$, where U_{pub} and P_{pub} are public parameters of U_i and TA, respectively. Then, U_a sends M' to the user U_i.
(3) Upon receiving the message M', U_i uses the secret parameter Q_{priv} and the public parameter P_0 to obtain $m' = M' \oplus H_2(\hat{e}(Q_{priv}, P_0))$.

Therefore, the attacker U_a can control the sensed data that occur between the user U_i and the sensor nodes S.

3.5. Stolen Smart Card Attacks

Usually, the smart card of the user U_i is equipped with tamper-resistant hardware. However, if U_i's smart card is lost or stolen, the attacker U_a may obtain all of the sensitive parameters stored in its memory by monitoring the power consumption of the smart card [26]. Assume that U_a obtains the smart card of U_i and extracts the parameters $< h(\cdot), Q_{priv}, ID_i, PW_i, a >$ stored inside it. U_a then can make a valid login request with ease. For example, U_a uses $h(\cdot)$, ID_i, PW_i, a and Q_{priv} and computes $r = h(ID_i||PW_i||a)$ and $Sig = r \times Q_{priv}$. Finally, U_a can make a valid login request to impersonate U_i by sending $< Sig, r, T'_L, ID_i >$ to the trusted authority TA, where T'_L is the current login time of U_a.

3.6. Off-Line Password Guessing Attacks

Since Liu–Chung's authentication scheme is executed in the open network environment, then we assumed that an attacker U_a can eavesdrop the communication channels between U_i and TA in the login phase. Moreover, we assumed that U_a was a legitimate user in the medical care system, and he/she can extract the parameter a by launching power analysis attack [26]. Thus, U_a could guess U_i's password through the following steps.

(1) U_a eavesdrops the message $< Sig, r, T_L, ID_i >$ sent by a legal user U_i, where $r = h(ID_i||PW_i||a)$.
(2) U_a guesses a password PW_a and computes $r_a = h(ID_i||PW_a||a)$ in an off-line manner.
(3) U_a checks whether r_a is equal to r or not. If it is equal, U_i's sensitive password is successfully guessed. Otherwise, U_a repeats Steps (1) and (2) until the correct password is found.

From the above descriptions, we conclude that U_a could derive U_i's password through an off-line manner, and Liu–Chung's authentication scheme could not succeed against the off-line password guessing attacks.

4. The Proposed Scheme

This section proposes the new and improved lightweight user authentication scheme for medical care tailored for the Internet of Things environment. The proposed scheme is based on Liu–Chung's scheme; thus, it tackles and eliminates all of the previously-mentioned security problems and vulnerabilities of their scheme. As Liu–Chung's scheme, the proposed scheme also consists of five phases: setup, registration, login, verification and access control and encryption. Figure 3 shows the schematic of our proposed scheme for the IoT-based medical care system.

U_i	TA	S
Registration phase		
Select ID_i, PW_i, r		
Compute $R_i = h(ID_i \|\| PW_i \|\| r)$		
	Send $< ID_i, R_i >$ secure channel →	
	Check the validity of ID_i Compute V_i, W_i	
	← Issue the smart card secure channel	
Store X_i, Y_i into smart card		
Login phase		
Input ID_i, PW_i		
Compute r', V_i', Y_i'		
Verify $Y_i \stackrel{?}{=} Y_i'$		
Compute M_i, N_i, O_i, Q_i		
	Send $< M_i, Q_i, T_L >$ public channel →	
Verification phase		
	Check if $T_{now} - T_L < \Delta T$ Compute N_i', V_i, O_i' Verify $O_i \stackrel{?}{=} O_i'$ Compute E, RM	
	← Send $< RM >$ public channel	Send $< T_u, b, TID_i >$ secure channel →
Compute $h(N_i) \oplus RM$		
Check the validity of ID_i		
Access control and encryption phase		
Input ID_i, PW_i		
Check the validity of ID_i, PW_i		
Compute $C = h(a \|\| TID_i \|\| T') \oplus h(E)$		
	Send $< C, TID_i, T' >$ public channel →	
		Check if $T_{now} - T' < \Delta T$ Compute C' Verify $C \stackrel{?}{=} C'$ Compute $M = m \oplus SK$
	← Send $< M >$ public channel	
Reveal $m = M \oplus SK$		

Figure 3. The schematic of our proposed scheme for IoT-based medical care system.

4.1. Setup Phase

In this phase, the trusted authority TA selects an elliptic curve E over F_p and a base point P_0 over the E and chooses a secure one-way hashing function $h(\cdot) : \{0,1\}^* \rightarrow \{0,1\}^l$, where p is a large prime such that $q|p-1$ for some great prime q and l means the length of the output. In addition, TA chooses the secret key $S_0 \in Z_q^*$ and computes its public key $P_{pub} = S_0 \times P_0$. Finally, TA keeps S_0 securely and publishes $< E, q, P_0, P_{pub}, h(\cdot) >$ as system parameters.

4.2. Registration Phase

In this phase, the user registers with the trusted authority TA through a secure channel to be a legal user, and the details of registration phase are as follows:

Step 1: U_i registers an authenticated identity ID_i and password PW_i with TA and chooses a random number r for computing $R_i = h(ID_i||PW_i||r)$.

Step 2: U_i sends the registration request $< ID_i, R_i >$ to TS through a secure channel.

Step 3: TA checks whether ID_i has been registered or not. If ID_i has not been registered, TA computes $V_i = h(ID_i||S_0||a)$ and $W_i = V_i \oplus R_i$. Then, TA stores the parameters $< W_i, a, E, q, P_0, P_{pub}, h(\cdot) >$ in U_i's smart card and issued the smart card to U_i, where a represents a private parameter generated by TA and all the sensor nodes of TA include a.

Step 4: U_i computes $V_i = W_i \oplus h(ID_i||PW_i||r)$, $X_i = r \oplus h(ID_i||PW_i)$ and $Y_i = h(V_i||r||h(ID_i||PW_i))$ and stores $< X_i, Y_i >$ into the smart card. Finally, U_i's smart card contains the parameters $< Y_i, X_i, W_i, a, E, q, P_0, P_{pub}, h(\cdot) >$.

4.3. Login Phase

In this phase, the user inserts his/her smart card into the device and inputs ID_i and PW_i. Then, the smart card executes the following steps:

Step 1: The smart card checks the ID_i and PW_i entered by U_i matches those stored in the smart card. First, the smart card computes $r' = X_i \oplus h(ID_i||PW_i)$, $V_i' = W_i \oplus h(ID_i||PW_i||r')$ and $Y_i' = h(V_i'||r'||h(ID_i||PW_i))$ and verifies whether $Y_i = Y_i'$. If it holds, the smart card executes Step 2. Otherwise, the smart card terminates this phase.

Step 2: The smart card generates a random number α and computes $M_i = \alpha \times P_0$, $N_i = \alpha \times P_{pub}$, $O_i = h(ID_i||V_i'||T_L)$ and $Q_i = h(N_i) \oplus (ID_i||O_i)$ and sends $< M_i, Q_i, T_L >$ to TA through a public channel, where T_L represents U_i's login time to the TA.

4.4. Verification Phase

When TA receives the login request $< M_i, Q_i, T_L >$ from U_i, TA authenticates U_i through the following steps:

Step 1: TA checks if $T_{now} - T_L < \Delta T$. If yes, TA executes Step 2. Otherwise, it means that the login time exceeds the transmission delay, and the login request will be rejected by TA.

Step 2: TA computes $N_i' = S_0 \times M_i$ and $(ID_i||O_i) = Q_i \oplus h(N_i')$ and checks if user's ID_i is recorded by TA. If yes, TA executes Step 3. Otherwise, the login request is denied by TA.

Step 3: TA goes on to compute $V_i = h(ID_i||S_0||a)$ by using the identity ID_i and checks that the decrypted O_i is the same as computed $O_i' = h(ID_i||V_i||T_L)$. If no, the session is aborted by TA. Otherwise, TA computes $E = h(b \oplus TID_i)$ and $RM = h(N_i') \oplus (ID_i||TID_i||T_u||E)$ sends the response message $< RM >$ to U_i through a public channel, where b represents a random number and TID_i represents a temporary identity for the user U_i.

Step 4: TA sends $< T_u, b, TID_i >$ to all of the sensor nodes S via a secure channel and notifies S that the temporary identity TID_i is legal in the next access control and encryption phase.

Step 5: When U_i receives $< RM >$ from TA, U_i authenticates TA by computing $(ID_i||TID_i||T_u||E) = h(N_i) \oplus RM$ and checks that the decrypted ID_i is involved in RM or not. If yes, U_i confirms that TA is legal and the parameters TID_i, T_u and E will be used in access control and encryption phase. Otherwise, U_i ends this session. Note that TID_i and E must be kept secret by U_i and temporarily stored into U_i's smart card until the end of the access control and encryption phase.

4.5. Access Control and Encryption Phase

When the user U_i is authenticated as legal, U_i can legally access sensed data m in S within a permitted time T_u, and U_i and S perform the following steps:

Step 1: In this step, the executed operations are the same as Step 1 of the login phase.

Step 2: The smart card calculates $C = h(a||TID_i||T') \oplus h(E)$ and sends $< C, TID_i, T' >$ to S through a public channel, where T' represents a timestamp.

Step 3: Upon receiving $< C, TID_i, T' >$ from U_i, S verifies if $T_{now} - T' < \Delta T$ and $T_{now} \subseteq T_u$. If yes, S executes Step 4.

Step 4: S computes $C' = h(a||TID_i||T') \oplus h(h(b \oplus TID_i))$ by using the b transmitted by TA and the temporary identity TID_i of the user to examine whether $C = C'$. If yes, the validity of U_i is authenticated by S, and the sensed data m will be transmitted by S. If no, S terminates this session.

Step 5: S computes the session key $SK = h(E \oplus a \oplus T_u)$ and encrypts the sensed data by computing $M = m \oplus SK$. Then, S sends $< M >$ to U_i through a public channel. Note that the session key SK provides a secure channel for protecting data transmission between S and U_i.

Step 6: When U_i receives $< M >$ from S, U_i uses the parameters (E, a, T_u) to calculate the session key $SK = h(E \oplus a \oplus T_u)$ and decrypts the sensed data m by computing $m = M \oplus SK$.

Note that SK should be frequently updated when U_i's T_u is expired. If so, U_i returns to the login and verification phases for requesting a new T_u with TA. Finally, a new SK will be established and updated among U_i and S in the access control and encryption phase.

5. Security Analysis of the Proposed Scheme

In this section, we analyze the security of our proposed scheme, and show that it is able to prevent the above-mentioned weaknesses in Liu–Chung's scheme. The security of the proposed scheme is based on the collision-free one-way hash function and two hard problems: the elliptic curve discrete logarithm problem (ECDLP) and the elliptic curve Diffie–Hellman problem (ECDHP), defined as follows:

ECDLP: Given a base point P over an elliptic curve E and a random variable $b \in Z_q^*$, it is computationally infeasible to find out an integer solution a such that $b = aP$.

ECDLP: Given three parameters $P, aP, bP \in Z_q^*$, it is computationally infeasible to compute $abP \in Z_q^*$.

We analyze and summarize the main security advantages of our proposed scheme as follows.

5.1. Resistance to Password Disclosure and Password Guessing Attacks

In the registration phase, the user's password PW_i is used in the message $R_i = h(ID_i||PW_i||r)$. Although the privileged-insider of TA can obtain the message R_i and the identity ID_i of the user, it is unable to know the user's sensitive password PW_i due to r being randomly selected by the user, and PW_i is protected by $h(ID_i||PW_i||r)$. Note that deriving PW_i from $h(ID_i||PW_i||r)$ is equal to implementing the brute-force attack to crack the one-way hashing function. Moreover, during the login, verification and access control and encryption phases, neither the smart card nor the transmitted messages include user's password PW_i. Hence, the proposed scheme eliminates the possibility of password disclosure and password guessing attacks.

5.2. Resistance to Replay Attacks

The timestamps and random numbers are common countermeasures to prevent replay attacks in the authentication process. Since the messages $< M_i, Q_i, T_L >$ and $< C, TID_i, T' >$ contain freshly generated timestamps T_L and T' and these timestamps are also embedded in the protected messages $Q_i = h(N_i) \oplus (ID_i||h(ID_i||V_i'||T_L))$ and $C = h(a||TID_i||T') \oplus h(E)$, thus each participant first checks the freshness of timestamps received and verifies whether the same timestamps are present in the transmitted messages. Hence, this design discards the possibility of replay attacks in our proposed scheme.

5.3. Resistance to Sensed Data Disclosure Attacks

In the access control and encryption phase of the proposed scheme, the sensed data m is embedded in the encrypted message $M = m \oplus SK$, and m is well-protected via high-entropy session key $SK = h(E \oplus a \oplus T_u)$. Here, we assume that U_a can obtain the parameter a from a legal smart card and can eavesdrop the transmitted messages $< C, TID_i, T' >$ and $< M >$ from the public channels between the user U_i and the sensor nodes S. U_a can use the collected parameters to compute $h(a||TID_i||T')$ and $C \oplus h(a||TID_i||T')$ and derive $h(E)$. However, without having the knowledge of secrets E and T_u, an attacker U_a cannot derive SK from $h(E)$ because of the irreversibility of the secure one-way hashing function.

On the other hand, during the login phase of the proposed scheme, we assume that the parameter $M_i = \alpha \times P_0$ and the public key $P_{pub} = S_0 \times P_0$ of TA are disclosed. However, the secret parameter $N_i = \alpha \times P_{pub} = \alpha S_0 P_0$ cannot be calculated by U_a since the random number α is unknown due to the infeasibility of deriving them from M_i by solving ECDLP. Moreover, during the access control and encryption phase, a unique and fresh secret parameter N_i is computed in each new session using the random parameter α and the private key S_0. Due to the difficulties of ECDHP, U_a cannot derive N_i from M_i and P_{pub}, and thus, the protection of fresh secret parameter $h(N_i)$ does not allow U_a to gain E and T_u from RM. Therefore, U_a cannot successfully derive m from M by computing $m = M \oplus h(E \oplus a \oplus T_u)$, and the confidentiality of the sensed data m is guaranteed in the proposed scheme.

5.4. Resistance to Sensed Data Forgery Attacks

In the access control and encryption phase of the proposed scheme, the sensor node S first authenticates the user U_i by verifying whether $C' = h(a||TID_i||T') \oplus h(h(b \oplus TID_i)) = C$. Due to the protection of using timestamp T' and the secret parameters a and $h(b \oplus TID_i)$, no one can forge a valid message $< C, TID_i, T' >$ to pass S's verification. In addition, we assume that the attacker U_a intercepts the response message M and tries to generate a legitimate message $M' = m' \oplus h(E \oplus a \oplus T_u)$ with fake sensed data m'. However, since U_a does not know the secret parameters E and T_u, it cannot generate the legitimate message $< M' >$. Thus, the proposed scheme could withstand the sensed data forgery attacks.

5.5. Resistance to Stolen Smart Card Attacks

Suppose that the smart card of U_i is lost or stolen. The attacker U_a could get the stored parameters $< Y_i, X_i, W_i, a, E, q, P_0, P_{pub}, h(\cdot) >$ and try to impersonate U_i to successfully login to the trusted authority TA. U_a can first guess a candidate identity ID_i^* and password PW_i^* and compute $r^* = X_i \oplus h(ID_i^*||PW_i^*)$ $V_i^* = W_i \oplus h(ID_i^*||PW_i^*||r^*)$ and $Y_i^* = h(V_i^*||r^*||h(ID_i^*||PW_i^*))$. The way for U_a to learn PW_i is to find out the correct pair (ID_i^*, PW_i^*) such that $Y_i = Y_i^*$. In the proposed scheme, we assume the probability of guessing ID_i composed of exact l characters and PW_i composed of exact m characters is approximately $\frac{1}{2^{6l+6m}}$. This probability is negligible, and U_a has no feasible way to derive ID_i and PW_i of the user U_i in polynomial time.

5.6. Resistance to Off-Line Password Guessing Attacks

In the proposed scheme, we assume that an attacker U_a could eavesdrop all of the transmission messages $< M_i, Q_i, T_L >$, $< RM >$, $< C, TID_i, T' >$ and $< M >$ between U_i, TA and S. However, neither the smart card, nor the transmission messages include U_i's password PW_i. Therefore, the proposed scheme could withstand the off-line password guessing attack.

5.7. Provision of the Efficient Login Phase

In order to illustrate the verification mechanism during the login phase, three cases are taken into consideration. Case 1 assumed U_i inputs a correct identity ID_i and incorrect password PW_i^*. Case 2 assumed U_i inputs an incorrect identity ID_i^* and correct password PW_i. Case 3 assumed U_i inputs incorrect identity ID_i^* and incorrect password PW_i^*.

Case 1: After the user inputs (ID_i, PW_i^*), the smart card computes $r^* = X_i \oplus h(ID_i||PW_i^*)$, $V_i^* = W_i \oplus h(ID_i||PW_i^*||r^*)$ and $Y_i^* = h(V_i^*||r^*||h(ID_i||PW_i^*))$ and verifies $Y_i \stackrel{?}{=} h(V_i^*||r^*||h(ID_i||PW_i^*))$. In fact, the verification cannot pass as $Y_i \neq h(V_i^*||r^*||h(ID_i||PW_i^*))$, and the smart card immediately terminates the session.

Case 2: After the user inputs (ID_i^*, PW_i), the smart card computes $r^* = X_i \oplus h(ID_i^*||PW_i)$, $V_i^* = W_i \oplus h(ID_i^*||PW_i||r^*)$ and $Y_i^* = h(V_i^*||r^*||h(ID_i^*||PW_i))$ and verifies $Y \stackrel{?}{=} h(V_i^*||r^*||h(ID_i^*||PW_i))$. Furthermore, the verification cannot pass as $Y \neq h(V_i^*||r^*||h(ID_i^*||PW_i))$, and the smart card immediately terminates the session.

Case 3: After the user inputs (ID_i^*, PW_i^*), the smart card computes $r^* = X_i \oplus h(ID_i^*||PW_i^*)$, $V_i^* = W_i \oplus h(ID_i^*||PW_i^*||r^*)$ and $Y_i^* = h(V_i^*||r^*||h(ID_i^*||PW_i^*))$ and verifies $Y \stackrel{?}{=} h(V_i^*||r^*||h(ID_i^*||PW_i^*))$. Similarly, the verification cannot pass as $Y \neq h(V_i^*||r^*||h(ID_i^*||PW_i^*))$, and the smart card immediately terminates the session.

5.8. Provision of User Anonymity

Based on the design of our proposed scheme, the excellent property of user anonymity can be guaranteed at every phase. We cleverly mask the real identity of U_i via a public channel, and no attacker can compromise U_i's real identity by launching security attacks. First, in the login phase, U_i's real identity is included in $Q_i = h(N_i) \oplus (ID_i||O_i)$. Thus, U_a cannot reveal Q_i without $h(N_i)$. Additionally, in the verification and access control and encryption phases, the temporary identity TID_i is generated and utilized to replace U_i's identity transmitted among the user and the sensor nodes. That is to say, all of the identities are transmitted in cipher format instead of plaintext, and these temporary identities will be randomized at each new session. As a result, our proposed scheme can provide the property of user anonymity.

5.9. Provision of Mutual Authentication

In the login phase of the proposed scheme, only the legitimate user can know the secret parameter $V_i = h(ID_i||S_0||a)$ to generate a legal O_i. Therefore, in Step 3 of the verification phase, TA can authenticate U_i by checking if the decrypted O_i is equal to the computed O_i'. Moreover, in Step 5 of the verification phase, only the legal TA can own the secret key S_0 to compute the common secret parameter $h(N_i)$. As a result, U_i can authenticate TA by decrypting RM and checking if the revealed ID_i is involved in RM.

On the other hand, in the access control and encryption phase, only the legal user can obtain the secret parameter $h(E)$ to generate a legal C. Thus, in Step 4 of the access control and encryption phase, S can authenticate U_i by checking if the received C is equal to the computed C'. Additionally, in Step 5 of the access control and encryption phase, only the participated S can calculate the common session key $SK = h(E \oplus a \oplus T_u)$ to encrypt the sensed data by computing $M = m \oplus SK$. Finally, U_i can also authenticate S by establishing the common session key SK and checking if the sensed data m are involved in M by decrypting $m = M \oplus SK$.

5.10. Provision of Session Key Security

Since the common session key SK is only shared and established among the user U_i and the sensor nodes S, in order to establish a secure and authenticated channel for late successive transmission, the session key SK not only ensures confidentiality, but also achieves authenticity of participants and messages. Based on the design of session key $SK = h(E \oplus a \oplus T_u)$, E is used for verifying the integrity of the transmitted messages, whereas T_u is used for preventing possible replay and misuse service attacks. As a result, the session key security and data confidentiality can be provided in the proposed authentication scheme.

6. Security Proof of the Proposed Scheme

Here, we follow similar techniques to demonstrate the security of our scheme in the random oracle model [27–30] and under the elliptic curve Diffie–Hellman problem (ECDHP).

6.1. Adversarial Model

We assume an adversary $\mathcal{A}$ is a probabilistic polynomial time algorithm and allowed to issue the following queries to some oracles. Note that an oracle has multiple instances $\prod_{\mathcal{U}}^{j}$, where $\mathcal{U}$ denotes participants and $j \in \mathbb{N}$. Here, we set $\mathcal{U} \in \{U_i, TA, S\}$ and may use $\mathcal{A}$ to simulate the proposed scheme via issuing queries.

1. $Send(\prod_{\mathcal{U}}^{j}, m)$ query: Upon receiving this query with message m, instance $\prod_{\mathcal{U}}^{j}$ follows the proposed scheme and then returns the result to $\mathcal{A}$.
2. $Hash(\prod_{\mathcal{U}}^{j}, m)$ query: Upon receiving this query with message m, instance $\prod_{\mathcal{U}}^{j}$ returns a random value to $\mathcal{A}$.
3. $Corrupt(\prod_{U_i}^{j}, U)$ query: $\mathcal{A}$ may query user U's password. Upon receiving this query, instance $\prod_{U_i}^{j}$ returns a password PW_U to $\mathcal{A}$. Note that this query models the forward secrecy of session key.
4. $Reveal(\prod_{\mathcal{E}\in\{U_i,S\}}^{j})$ query: $\mathcal{A}$ may query the previous established session keys. Upon receiving this query, instance $\prod_{\mathcal{E}\in\{U_i,S\}}^{j}$ returns a previous session key to $\mathcal{A}$, if it has accepted. Otherwise, $\prod_{\mathcal{E}\in\{U_i,S\}}^{j}$ returns a random string to $\mathcal{A}$. Note that this query models the knowing the session key attack of session key.
5. $Test(\prod_{\mathcal{E}\in\{U_i,S\}}^{j})$ query: $\mathcal{A}$ may only issue this query once. Upon receiving this query, instance $\prod_{\mathcal{E}\in\{U_i,S\}}^{j}$ flips an unbiased coin b. If $b = 1$, it returns a session key. Otherwise, it returns a random string. Note that this query models the semantic security of session key.

6.2. Mutual Authentication between U_i and TA

Theorem 1. *In the random oracle model, assume that there exists an adversary $\mathcal{A}$ with a non-negligible advantage ϵ_0 that can impersonate U_i to communicate with TA. Then, there is a challenger $\mathcal{C}$, which can solve the elliptic curve Diffie–Hellman problem (ECDHP) with advantage $q \cdot \epsilon_0 < \epsilon \leq \frac{q_H}{2^k}$, where q_S denotes the maximum number of send queries issued by $\mathcal{A}$, q_H denotes the maximum number of hash queries issued by $\mathcal{A}$ and k denotes the length of the hash value.*

Proof. Note that we say that $\mathcal{A}$ successfully impersonates U_i to communicate with TA. This means that TA accepts (M_i, Q_i, T_L), but it has not been produced by U_i. In this case, it could be that $\mathcal{A}$ guessed (M_i, Q_i, T_L). Then, this leads to:

$$\epsilon_0 < \tfrac{q_S}{q} \times \Pr[O_i = h(ID_i||V_i||TL)|ID_i||O_i = Q_i \oplus h(N_i'); V_i = h(ID_i||S_0||a)] \times \tfrac{1}{q_S} \leq \tfrac{q_S}{q} \times \tfrac{q_H}{2^k} \times \tfrac{1}{q_S}. \quad (1)$$

Given that $M_i = a \cdot P$ and $P_{pub} = b \cdot P$ to $\mathcal{A}$ for $a, b \in \mathbb{Z}_q^*$ are unknown, then, $\mathcal{A}$ can compute $N_i' = abP$. Thus, given $(P, M_i, P_{pub}) = (P, aP, bP)$, $\mathcal{C}$ can use $\mathcal{A}$ as a subroutine to compute abP. In other words, $\mathcal{C}$ can solve ECDLP with the advantage $q \cdot \epsilon_0 < \epsilon \leq \frac{q_H}{2^k}$. □

Theorem 2. *In the random oracle model, assume that there exists an adversary $\mathcal{A}$ with a non-negligible advantage ϵ_1 that can impersonate TA to communicate with U_i. Then, there is a challenger $\mathcal{C}$, which can solve the elliptic curve Diffie–Hellman problem (ECDHP) with advantage $\epsilon \geq \epsilon_0 - \frac{1}{2^k} - \frac{q_S^2 \cdot q_H^2}{q \cdot 2^k}$, where q_S denotes the maximum number of send query issued by $\mathcal{A}$, q_H denotes the maximum number of hash query issued by $\mathcal{A}$ and k denotes the length of the hash value.*

Proof. Without of loss generality, we assume that the event that violates U_i-to-TA authentication denoted by $Event^{U_i 2TA}$ does not occur. Similarly, we use the symbol $Event^{TA2U_i}$ to define the event that violates TA-to-U_i authentication. We say that $\mathcal{A}$ successfully impersonates TA to communicate with U_i. This means that at some point, U_i accepts RM after sending (M_i, Q_i). However, RM has not been produced by TA. In this case, it could be the following three cases:

1. $\mathcal{A}$ guessed RM. The probability of this case is $\frac{1}{2^k}$.
2. M_i and Q_i were obtained in other session. The probability of this case is $\frac{q_S \cdot (q_S - 1)}{q} \times \frac{q_H \cdot (q_H - 1)}{2^k}$ less than $\frac{q_S^2 \cdot q_H^2}{q \cdot 2^k}$.
3. $\mathcal{A}$ had issued the hash query for N_i'.

Thus, we have:

$$\Pr[Event^{TA2U_i} | \neg Event^{U_i 2TA}] \leq \Pr[RM = h(N_i') \oplus (ID_i || TID_i || T_u || E)] + \frac{1}{2^k} + \frac{q_S^2 \cdot q_H^2}{q \cdot 2^k}. \quad (2)$$

Given $M_i = a \cdot P$ and $P_{pub} = b \cdot P$ to $\mathcal{A}$ for $a, b \in \mathbb{Z}_q^*$ are unknown, then, $\mathcal{A}$ can compute $N_i' = abP$. Thus, given $(P, M_i, P_{pub}) = (P, aP, bP)$, $\mathcal{C}$ can use $\mathcal{A}$ as a subroutine to compute abP. In other words, $\mathcal{C}$ can solve ECDLP with the advantage $\epsilon \geq \epsilon_0 - \frac{1}{2^k} - \frac{q_S^2 \cdot q_H^2}{q \cdot 2^k}$. □

6.3. S Authenticates U_i and Key Agreement

Theorem 3. *Under the elliptic curve computational Diffie–Hellman problem (ECDHP), no adversary can impersonate user U_i to communicate with sensor node S after U_i is authenticated as a legal user by TA.*

Proof. No one can forge $C = h(a || TID_i || T') \oplus E$ except legal user U_i because a is a secret value stored in U_i's smart card, and E is obtained from the procedures of U_i authenticating TA. By Theorem 2, we have proved that no one can impersonate TA to communicate with U_i under the ECDHP. Even if the U_i's smart card is broken, the adversary is still unable to forge E. □

Theorem 4. *Under the elliptic curve computational Diffie–Hellman problem (ECDHP), only user U_i and sensor node S can establish a session key SK after U_i is authenticated as a legal user by TA. In other words, no adversary can compute SK except U_i and S.*

Proof. According to the proofs of Theorems 2 and 3, no one can compute $SK = h(E \oplus a \oplus T_u)$ except U_i, an authenticated legal user. In another aspect, only S can compute SK because TA sends a and (T_u, b, TID_i) to S via a secure channel, and E is computed by $h(b \oplus TID_i)$. □

7. Performance Analyses and Comparisons

In this section, we provide a performance comparisons among our scheme and two existing ECC-based authentication schemes [5,21] for wireless healthcare sensor networks in terms of computation costs in the authentication process (which includes the login, verification, and access control and encryption phases). According to the experimental results of He [31], the execution times are given in Table 1, where the hardware platform is a Pentium IV 3-GHz processor with library MIRACL [32]. As shown in Table 1, it is clear that the elliptic curve scalar point multiplication and the

bilinear pairing operation are more complicated than other operations, and the running time of the addition operation of points, the map-to-point hash function and the one-way hash function could be ignored. Therefore, we only need to count the execution time of the elliptic curve scalar point multiplication and the bilinear pairing operation.

Table 1. Execution time (in milliseconds; ms) of various cryptographic operations.

Notations	Descriptions
T_{EM}	The time of executing an elliptic curve scalar point multiplication, $1T_{EM} \approx 1.17$ ms
T_{BP}	The time of executing a bilinear pairing operation, $1T_{BP} \approx 3.16$ ms
T_{EA}	The time of executing an addition operation of points, $1T_{EA} < 0.1$ ms, which is negligible
T_{MH}	The time of executing a map-to-point hash function, $1T_{MH} < 1$ ms, which is negligible
T_H	The time of executing a one-way hash function, $1T_H < 0.01$ ms, which is negligible

In Table 2, we summarize the efficiency comparisons among our proposed scheme and other previous WSN-based authentication schemes in terms of computational complexity and the execution time, where the total execution times are measured using Table 1. From Table 2, we can see that the computation cost of our scheme is lower than that of Yeh et al.'s and Liu–Chung's schemes on both the user, the trusted authority and the sensor node side. Therefore, our proposed scheme is the most efficient compared to the other two related schemes in terms of overall computation costs, and it can be claimed that the execution time of the proposed scheme is suitable for different real-life applications, including medical care systems.

Table 2. Performance comparisons among the proposed scheme and other related schemes.

	Yeh et al. [5] (2011)	Liu–Chung [21] (2016)	The Proposed Scheme
Computation cost (U_i)	$2T_{EM} + 1T_{EA} + 1T_{MH} + 3T_H$	$1T_{EM} + 1T_{BP} + 1T_{MH} + 2T_H$	$2T_{EM} + 8T_H$
Computation cost (TA)	$5T_{EM} + 3T_{EA} + 4T_{MH}$	$2T_{BP} + 1T_H$	$1T_{EM} + 4T_H$
Computation cost (S)	$2T_{EM} + 2T_{EA} + 3T_{MH}$	$1T_{BP} + 1T_{MH} + 2T_H$	$4T_H$
Total execution time	10.53 ms	13.81 ms	3.51 ms

Lastly, the security criteria and functional properties of three ECC-based authentication schemes are summarized in Table 3. It is visible from Table 3 that Yeh et al.'s scheme [5] is vulnerable to password disclosure attack in the registration phase and also does not provide the user anonymity property, where Liu–Chung's scheme [21] does not support this property. The proposed scheme can prevent all of the security weaknesses of the former scheme and provide mutual authentication and user anonymity to protect data integrity and user privacy. From Tables 2 and 3, the proposed scheme not only keeps lower computational cost, but also possesses more security requirements along with strong security protection on the relevant security attacks for IoT-based medical care systems.

Table 3. Functionality comparisons among the proposed scheme and other related schemes.

	Yeh et al. [5] (2011)	Liu–Chung [21] (2016)	The Proposed Scheme
F1	χ	χ	$\surd$
F2	$\surd$	χ	$\surd$
F3	$\surd$	$\surd$	$\surd$
F4	$\surd$	χ	$\surd$
F5	χ	χ	$\surd$
F6	$\surd$	χ	$\surd$
F7	−	χ	$\surd$
F8	−	χ	$\surd$
F9	$\surd$	χ	$\surd$
F10	$\surd$	χ	$\surd$

F1: Provision of user anonymity; F2: provision of efficient login phase; F3: provision of mutual authentication; F4: provision of session key security; F5: prevention of password disclosure attack; F6: prevention of replay attack; F7: prevention of sensed data disclosure attack; F8: prevention of sensed data forgery attack; F9: prevention of stolen smart card attack; F10: prevention of off-line password guessing attack; $\surd$: yes; χ: no; −: not mentioned.

8. Conclusions

In this paper, we first give a brief review of Liu–Chung's authentication scheme combined with its basic security analysis and find that their scheme is vulnerable to password disclosure, off-line password guessing, sensed data disclosure, sensed data forgery, replay attacks and the stolen smart card problem. Furthermore, their scheme cannot achieve user anonymity and session key security, and it has unnecessary redundancy in protocol design. In order to repair their security flaws and improve the system performance, an improved efficient scheme is proposed. The security analysis indicates that the proposed authentication scheme is able to withstand those attacks mentioned and satisfies all desirable security attributes, such as user anonymity, mutual authentication, session key security and an efficient verification mechanism during the login phase. Comparing the efficiency with other ECC-based authentication schemes, the proposed scheme is comparable in terms of the computational overheads and practical as the secure authentication mechanism for the IoT-based medical care system.

Acknowledgments: The authors would like to thank the anonymous reviewers and the Editor for their constructive and generous feedback on this paper. In addition, this research was partially supported and funded by the Ministry of Science and Technology, Taiwan, R.O.C., under Contract No. MOST 105-2221-E-165-005.

Author Contributions: Chun-Ta Li proposed the ideas and wrote the paper; Tsu-Yang Wu and Chin-Ling Chen are corresponding authors who contributed to prove, analyze the data and supervise the paper; Cheng-Chi Lee and Chien-Ming Chen also supported the writing, and supervised parts of the scheme.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chiou, S.Y.; Ying, Z.; Liu, J. Improvement of a privacy authentication scheme Based on cloud for medical environment. *J. Med. Syst.* **2016**, *40*, 101.
2. He, D.; Kumar, N.; Chen, J. Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks. *Multimed. Syst.* **2015**, *21*, 49–60.
3. Li, C.T.; Weng, C.Y.; Lee, C.C. An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. *Sensors* **2013**, *13*, 9589–9603.
4. Li, C.T.; Lee, C.C.; Weng, C.Y. A secure cloud-assisted wireless body area network in mobile emergency medical care system. *J. Med. Syst.* **2016**, *40*, 117.
5. Yeh, H.L.; Chen, T.H.; Liu, P.C.; Kim, T.H.; Wei, H.W. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors* **2011**, *11*, 4767–4779.
6. Zhou, J.; Cao, Z.; Dong, X.; Xiong, N.; Vasilakos, A.V. 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Inf. Sci.* **2015**, *314*, 255–276.

7. Choi, J.; In, Y.; Park, C.; Seok, S.; Seo, H.; Kim, H. Secure IoT framework and 2D architecture for end-to-end security. *J. Supercomput.* **2016**, doi:10.1007/s11227-016-1684-0.
8. Kumari, S.; Khan, M.K.; Atiquzzaman, M. User authentication schemes for wireless sensor networks: A review. *Ad Hoc Netw.* **2015**, *27*, 159–194.
9. Li, C.T. A secure chaotic maps based privacy-protection scheme for multi-server environments. *Secur. Commun. Netw.* **2016**, *9*, 2276–2290.
10. Maitra, T.; Amin, R.; Giri, D.; Srivastava, P.D. An efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card. *Int. J. Netw. Secur.* **2016**, *18*, 553–564.
11. Messai, M.L.; Seba, H.; Aliouat, M. A lightweight key management scheme for wireless sensor networks. *J. Supercomput.* **2015**, *71*, 4400–4422.
12. Rawat, P.; Singh, K.D.; Chaouchi, H.; Bonnin, J.M. Wireless sensor networks: A survey on recent developments and potential synergies. *J. Supercomput.* **2014**, *68*, 1–48.
13. Wong, K.; Zheng, Y.; Cao, J.; Wang, S. A dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), Taichung, Taiwan, 5–7 June 2006; pp. 244–251.
14. Tseng, H.R.; Jan, R.H.; Yang, W. An improved dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE Globecom, Washington, DC, USA, 26–30 November 2007; pp. 986–990.
15. Lee, T.H. Simple dynamic user authentication protocols for wireless sensor networks. In Proceedings of the 2nd International Conference on Sensor Technologies and Applications, Cap Esterel, France, 25–31 August 2008; pp. 657–660.
16. Das, M.L. Two-factor user authentication in wireless sensor Networks. *IEEE Trans. Wirel. Commun.* 2009, *8*, 1086–1090.
17. Huang, H.F.; Chang, Y.F.; Liu, C.H. Enhancement of two-factor user authentication in wireless sensor networks. In Proceedings of the 2010 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Darmstadt, Germany, 15–17 October 2010; pp. 27–30.
18. Li, C.T.; Lee, C.C.; Wang, L.J.; Liu, C.J. A secure billing service with two-factor user authentication in wireless sensor networks. *Int. J. Innov. Comput. Inf. Control* **2011**, *7*, 4821–4831.
19. Yoo, S.G.; Park, K.Y.; Kim, J. A security-performance-balanced user authentication scheme for wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2012**, 2012, 382810.
20. Xue, K.; Ma, C.; Hong, P.; Ding, R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *J. Netw. Comput. Appl.* **2013**, *36*, 316–323.
21. Liu, C.H.; Chung, Y.F. Secure user authentication scheme for wireless healthcare sensor networks. *Comput. Electr. Eng.* **2016**, *59*, 250–261, doi: 10.1016/j.compeleceng.2016.01.002.
22. Joux, A. The weil and tate pairings as building blocks for public key cryptosystems. *Lect. Notes Comput. Sci.* **2002**, *2369*, 20–32.
23. He, D.; Zhao, W.; Wu, S. Security analysis of a dynamic ID-based authentication scheme for multi-server environment using smart cards. *Int. J. Netw. Secur.* **2013**, *15*, 350–356.
24. He, D.; Zeadally, S.; Kumar, N.; Lee, J.H. Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.* **2016**, doi:10.1109/JSYST.2016.2544805.
25. Wang, Y.; Zhong, H.; Xu, Y.; Cui, J. ECPB: Efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs. *Int. J. Netw. Secur.* **2016**, *18*, 374–382.
26. Messerges, T.S.; Dabbish, E.A.; Sloan, R.H. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* **2002**, *51*, 541–552.
27. Bellare, M.; Rogaway, P. Random oracles are practical: A paradigm designing efficient protocols. In Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, VA, USA, 3–5 November 1993; pp. 62–73.
28. Canetti, R.; Goldreich, O.; Halevi, S. The random oracle metholodology, revisited. *J. ACM* **2004**, *51*, 557–594.
29. Chen, C.M.; Li, C.T.; Liu, S.; Wu, T.Y.; Pan, J.S. A provable secure private data delegation scheme for mountaineering events in emergency system. *IEEE Access* **2017**, *5*, 3410–3422.
30. Wu, T.Y.; Tseng, Y.M. An efficient user authentication and key exchange protocol for mobile client-server environments. *Comput. Netw.* **2010**, *54*, 1520–1530.

31. He, D. An efficient remote user authentication and key agreement protocol for mobile client-Vserver environment from pairings. *Ad Hoc Netw.* **2012**, *10*, 1009–1016.
32. Shamus Software. Available online: https://github.com/miracl/MIRACL (accessed on 22 June 2017).