Privacy Preserving Authenticated Key Agreement based on Bilinear Pairing for uHealthcare

Sunghyun Cho[1] and Hyunsung Kim[2]
[1]College of Computing, Sungkyunkwan University, Korea
[2]School of Computer Science, Kyungil University, Korea

Abstract: *With the growth of wireless communication technologies and sensor technologies, ubiquitous Healthcare (uHealthcare) based on Internet of Things (IoT) is becoming a big research focus from various researchers. However, security and privacy issues are top most important focuses to be solved for the success of uHealthcare services. This paper shows that Mahmood et al.'s authentication and prescription safety protocol is prone to denial of service attack and stolen-verifier attack. Furthermore, we propose a privacy preserving authenticated key agreement protocol for IoT based uHealthcare, which is based on hash function, symmetric key cryptosystem and bilinear pairing. The proposed protocol efficiently solves the security and privacy problems in Mahmood et al.'s protocol and also provides computational efficiency compared to the related protocols.*

Keywords: *Authenticated key agreement, authentication, internet of things, prescription safety, ubiquitous healthcare.*

Received October 2, 2019; accepted October 25, 2020
https://doi.org/10.34028/18/4/4

1. Introduction

Information and communication technology for telecare health services and ubiquitous Healthcare (uHealthcare) allows medical staff and patients to perform services over Internet of Things (IoT) [4, 7, 10, 12, 16, 18, 20, 21]. Hospitals and medical institutions tend to adopt Telecare Medical Health Information Systems (TMIS) oruHealthcare. They can reduce healthcare operating costs by improving service quality and efficiency [5]. Despite these advantages, some challenges must be addressed before TMIS or uHealthcare can be adopted and deployed widely [3]. They are vulnerable to various security and privacy attacks built on public networks. The medical history and personal information of patients should be carefully managed by the TMIS or uHealthcare server and concealed in messages between network entities to prevent users' privacy from being disclosed.

For security and privacy issues, there are many types of studies conducted on TMIS or uHealthcare authentication and secure data transmission [1, 3, 5, 6, 7, 13, 14, 15, 17, 18, 19]. Wu *et al*. [19] have proposed a two-step authentication protocol for TMIS. Debiao *et al*. [3] discovered that Wu *et al*.'s [19] protocol was not resistant to insider and impersonal attacks and proposed an improved protocol. Wei *et al*. [17] showed that Wu *et al*.'s [19] protocol and Debiao *et al*.'s [3] protocol were both subjected to offline dictionary attack and proposed their own solution protocol. Zhu [21] showed that Wei *et al.'s* [17] protocol still suffer from offline dictionary attack. Recently, there are some three party password authenticated key exchange protocol, which provide mutual authentication between patients, doctors and Trusted Servers (TS) and hide their identities from their opponents [1, 6, 8, 11, 13, 14, 15]. IoT can be an appropriate approach to support TMIS [15]. Moosavi *et al*. [13, 14] proposed a user authentication and key agreement for fitness-IoT structures. Kim [6] proposed a non-interactive hierarchical key agreement protocol, which is based on bilinear pairing. However, his protocol only provide unilateral authentication. Recently, Mahmood *et al.* [11] argued that existing protocols are in sufficient to ensure reliable prescription safety with TMIS certification. Furthermore, they proposed an authentication and prescription safety protocol for TMIS.

First of all, this paper shows that Mahmood *et al*.'s [11] protocol is prone to denial of service attack and stolen-verifier attack. Then we propose a privacy preserving authenticated key agreement protocol for authentication and prescription safety for IoT based uHealthcare. The proposed protocol efficiently solves the security problems in Mahmood *et al*.'s [11] protocol.

2. Backgrounds

This section reviews system model and security preliminaries [9].

2.1. System Model

Our system model consists of patient with mobile phone, hospital server and doctor/nurse for uHealthcare. It is assumed that if a patient needs to be constantly monitored based on sensors, each patient visits the hospital in person and hands over the necessary details of him (or her) to hospital server. On successful registration, hospital server creates security credentials and sends them to mobile phone of the patient safely. Figure 1 illustrates the target system model used in this paper. In the architecture, patient is constantly monitored for some treatments by hospital server. Sensors are fixed in patients' body for sensing abnormal conditions and emergency situation. For this, sensors collect the data such as body temperature, blood pressure and electro cardio gram and send them to hospital server via patient's mobile phone through Zig bee or Bluetooth. When patient's biological data is in normal status, hospital server just stores the data in its database. If any emergency situation arises, hospital server forwards the data to doctor/nurse for the detailed condition check for the proper treatment of patient.

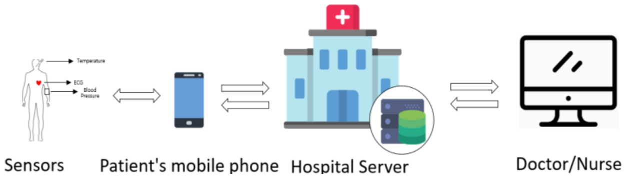

Figure 1. System model.

2.2. Security Preliminaries

This subsection provides basic overviews on hash function, Elliptic Curve Cryptosystem (ECC) and symmetric key cryptosystem [2].

- **Hash function**: A hash function is any function that can be used to map data of arbitrary size to data of a fixed size. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it by knowing the stored hash value.
- **ECC**: ECC is an approach to public key cryptography. ECC requires smaller length of key size compared to non-ECC to provide equivalent security. The properties of ECC allows for the assertion of security, which is Elliptic Curve Discrete Logarithm Problem (ECDLP). Assume that A and B are all points on the elliptic curve, and x is an integer. When A and B are known in $B=x\ A$, x is unknown, which is the difficulty of ECDLP.
- **Symmetric key cryptosystem**: Symmetric key cryptosystem is a system, which uses a cryptographic key for both encryption of plain text and decryption of cipher text. The key represents a shared secret between two or more parties that can be used to maintain a private information link. In the proposed scheme, we use Advanced Encryption Standard (AES) with 128 bits of key size for confidentiality.

3. Mahmood *et al.*'s [11] Protocol

This section shows that Mahmood *et al.*'s [11] protocol in is prone to denial of service attack and stolen-verifier attack. Table 1 shows the notations used in this paper.

3.1. Review of Mahmood et al.'s [11] Protocol

Mahmood *et al*. [11] proposed a new authentication and prescription safety protocol to protect patient's privacy and satisfy the security requirements of TMIS. There are four phases for the protocol between a new patient A to doctor/nurse B via trusted server TS.

1. Initialization by Patient

A chooses a random number R_p, and computes X_A by multiplying R_p by an ECC generator P of large order n.

Table 1. Notations.

Notation	Definition
TMIS	Telecare medical information system
E	A large-order finite field on elliptic curve
P	ECC generator of a large order n
A	Patient that is participant A
B	Doctor/nurse that is user B
TS	Trusted Server as a trusted third party
$ID_{A,\ B,\ TS}$	Masked identities of A, B and TS respectively
PW_p	TS shared password for patient
$PW_{D,N}$	Doctor/Nurse password shared with TS
$K_{A\text{-}TS}$	Pre-Shared key between TS and User A
$K_{B\text{-}TS}$	Pre-Shared key between TS and User B
$K_{TS\text{-}A/B}$	Temporary encryption key between TS& end entity
d	Private/public key of TS
XOR	The XOR operation
$\|\|$	The message concatenation operation
$MAC()$	Message authentication code
$H()$	Digestive hash function
$E_k()$, $D_k()$	Using key (k) to perform encryption/decryption
T_1, T_2, T_3	User (A, B, TS) time stamp
N_1, N_2, N_3	User (A, B, TS) nonce number
M_A, M_B	Message at user A and B
C_A, C_B	Cipher text at A and B

Similarly, A computes Y_A the resultant of R_p and TS's public key F that is equal to dP, where d is a random number from finite field selected by TS. For level 1 encryption of security credentials, a hash of Y_A is taken to prepare key H_{YA}. A prepares a message M_A that contains hash of IDs and PW_p as A's password and Message Authentication Code (MAC) is used for providing message integrity on TS side. A calculates $H(PW_p||ID_A||ID_B)$ and includes PW_p to keep it more secure. For transmission to the server, A computes cipher text P_A which is encrypted by A's generated secret key H_{YA}. After that, a cipher text C_A is generated using a pre-established key $K_{A\text{–}TS}$. A temporary ID as $ID_{A\sim T}$ of A is obtained by taking $H(X_A||P_A||N_1)$ and N_1 is used for the current session only. A new $ID_{A\sim T}$ is never transmitted and can be calculated at TS using $H(X_A||P_A||N_1)$ where N_1 can be extracted after decryption. It encrypts the parameters $\{X_A, P_A, T_1\}$ using $K_{A\text{–}TS}$ where, T_1 is timestamp. A transmits $\{ID_{A\sim T}, C_A\}$ to TS for authentication.

1. $X_A = R_pP$
2. $Y_A = R_pF$
3. $M_A = H(PW_p||ID_A||ID_B)$
4. $P_A = E_{HYA}(ID_A||M_A||N_1||\text{MAC}(M_A)||ID_B)$
5. $C_A = EKA\text{–}TS(X_A||P_A||T1)$
6. $ID_{A\sim T}= \{H(X_A||P_A||N_1)\}$

2. Verification at TS

Upon receiving $\{ID_{A\sim T}, C_A\}$ from A, TS decrypts the cipher text C_A to get $(X_A||P_A||T_1)$. It also checks the message freshness by taking the difference from T_1 to guard against replay attacks. After that, TS computes the temporary key of the patient by multiplying the received X_A with d which was pre-generated by TS as $Y_A' = dX_A$. To verify whether the message is original, TS computes A's masked identity as $R_pF = R_pdP = dX_A$. It also decrypts P_A to obtain security credentials, including ID_A, M_A, N_1, $MAC(M_A)$, and ID_B. The hash of these values is calculated as $M_A' = H(PW_p||ID_A||ID_B)$ and is then compared to verify the equality of M_A and M_A' to ensure message integrity. Otherwise, the message is discarded. $MAC(M_A)$ provides data integrity for M_A. TS computes the following steps.

1. Decrypts C_A using $K_{A\text{–}TS}$ to get $\{(X_A||P_A||T_1)\}$
2. Computes $Y_A' = dX_A$
3. Decrypts P_A using $K_{H(YA)}$ to get $\{ID_A, M_A, N_1, \text{MAC}(M_A), ID_B\}$
4. Computes $M_A' = H(PW_p||ID_A||ID_B)$
5. If verify $(MAC'(M_A) \mathrel{!}= MAC(M_A))$ then discards
6. If M_A NOT equals M_A' then discards message.

3. TS-based Mutual Authentication of B and A

After verification, TS picks a random number R_{Ts} and then computes $Z_{TS} = H(ID_{TS}||ID_B||R_{Ts})$ using identities of B and TS. It also generates a nonce N_2 to get its hash with identities of communicating parties A and B. After that, TS calculates XOR of hash value with Z_{TS} to get a new temporary ID for B. The value of C_{TS} is obtained by encrypting $(ID_A||Z_{TS}||T_2||N_2)$ using the pre-established key $K_{TS\text{–}B}$. TS transmits the temporary identity $ID_{B\sim T}$ and cipher text C_{TS} to B.

1. $Z_{TS} = H(ID_{TS}||ID_B||R_{Ts})$
2. $ID_{B\sim T} = Z_{TS} XOR\ H(ID_B||ID_A||N_2)$
3. $C_{TS} = E_{KTS\text{-}B}(ID_A||Z_{TS}||T_2||N_2||ID_{B\sim T})$

$$TS \rightarrow B: \{ID_{TS}, C_{TS}\}$$

B receives the message $\{ID_{TS}, C_{TS}\}$ and decrypts it to get the other party's prescription details and TS validates by computing the set time stamp threshold value, nonce number, received masked-ID values, and decrypted message using the pre-share key from TS. At each end, entity E_{KTS} is used as a key to encrypt secure credentials in addition to Message Authentication Code (MAC) and the hash function application to make them more secure.

1. Decrypts using $K_{TS\text{–}B}$ to get $\{(ID_A||Z_{TS}||T_2||N_2)\}$
2. If $\{Z_{TS}\ XOR\ \{H(ID_B||ID_A||N_2)\}\}$ NOT equals $ID_{B\sim T}$ then discards
3. $X_B = R_BP$, $Y_B = R_BF$
4. $M_B = H(PW_B||ID_{TS}||ID_B)$
5. $P_B = E_{HYB}(ID_B||M_B||N_3||\text{MAC}(M_B)||ID_{TS})$
6. $C_B = E_{KB\text{–}TS}(X_B||P_B||T_3)$

$B \rightarrow TS: \{ID_{B\sim T}, C_B\}$

TS receives the message $\{ID_{B\sim T}, C_B\}$ and decrypts it to get $(X_B||P_B||T_3)$. After that, TS computes $Y_B' = dX_B$ which is equal to $dR_BP = R_BdP = R_BF = Y_B$ calculated at B. It further decrypts P_B to get ID_B, M_B, N_3, $MAC(M_B)$ and ID_{TS}, as illustrated in steps below. After that, TS verifies the message's integrity by computing and comparing the hash of the message. Finally, it computes the common parameters CP_A and CP_B for both parties and forwards them to A and B for session key computation.

1. Decrypts C_B to get $[(X_B||P_B||T_3)]$
2. Computes $Y_B' = dX_B$
3. Decrypts P_B to get $[(ID_B||M_B||N_3||MAC(M_B)||ID_{TS})]$
4. Calculates $M_B' = H(PW_B||ID_{TS}||ID_B)$
5. If M_B' not equals M_B then drops message
6. $CP_A = \{E_{HYA'}(X_B||ID_A||ID_B||Y_A'||N_1)\}$
7. $CP_B = \{E_{HYB'}(X_A||ID_A||ID_B||Y_B'||N_1)\}$

$TS \rightarrow A: \{ID_{A\sim T}, CP_A\}$

$TS \rightarrow B: \{ID_{B\sim T}, CP_B\}$

4. Participant Validation and Common Session Key Generation

A decrypts CP_A, verified by its own nonce and MAC, which provide integrity and validity of TS and the message. The common parameters generated by TS are transmitted securely on each end. Upon receiving the secret credentials, the participating parties first verify message integrity and authority by verifying Y_A' and Y_B', respectively. After that, MAC, nonce, TS-ID, and the time stamp are also used for double-checking the source's integrity before processing secret credentials. After successful validation of both parties' identities and that of TS, participants start to compute the common key.

3.2. Security Weaknesses in Mahmood et al.'s Protocol

We show that Mahmood *et al.'s* [11] protocol is prone to denial of service attack and stolen-verifier attack.

1. Denial of Service Attack Feasibility

Mahmood *et al*.'s [11] protocol uses a temporary ID for the patient, which is to provide message freshness based on session dependent timestamp T_1. The usage of the temporary ID is to provide anonymity of patient, which claimed to be one of important factors in Mahmood *et al*.'s [11] protocol.

However, TS should have big overhead to compute any legal patient A's ID in the verification phase of Mahmood *et al*.'s [11] protocol, which results to be in denial of service. The reason is that TS requires to decrypt C_A to get $(X_A||P_A||T_1)$ with $K_{A\text{–}TS}$. However, for the operation, TS should choose a proper pre-shared key after identifying the patient with $ID_{A\sim T}$. Note that there are no ways that TS could know the patient ID, $ID_{A\sim T}$ in Mahmood *et al*.'s [11] protocol. The ID could be obtained only by taking hash operation of X_A, P_A and N_1. Thereby, there is only possibility that TS to retrieve

$ID_{A\sim T}$ is by performing hash operations of all patients, which results in denial of service. *TS* works the main role for the authentication in Mahmood *et al*.'s [11] protocol and there are not only one request for authentication in a certain period of time but should be many requests at the same time.

2. Stolen-Verifier Attack Feasibility

Mahmood *et al*.'s [11] protocol uses password to authenticate legal user and pre-shared secret key to provide secrecy of authentication and prescription safety. However, Mahmood *et al*.'s [11] protocol requires to use and keep the verifier because it requires computation of M_A', which needs to use ID_A and PW_p at the same time.

Stolen-verifier attack assumes that an adversary who steals the password-verifier from the server can use it directly to masquerade as a legitimate user in authentication [9]. As matter of fact, an adversary who achieves the verifier may further mount much complexed attacks in Mahmood *et al*.'s [11] protocol. Stolen-verifier attack is feasible in Mahmood *et al*.'s [11] protocol because it requires using the secret information in a verifier table for authentication.

4. Privacy Preserving Authenticated Key Agreement Protocol

This section proposes a privacy preserving authenticated key agreement protocol based on bilinear pairings for uHealthcare. It is consisted of four phases: setup phase, registration phase, login phase and authenticated key agreement phase.

4.1. Setup Phase

TS performs system setup for the proposed protocol. First of all, *TS* selects an elliptic curve *E* over E_q and a base point *P* of *E*, where *q* is a large order *n*. *TS* selects a bilinear map $\hat{e}: G_1\times G_1\rightarrow G_2$ and a secure one-way hash functions $h(\cdot)$: $\{0,1\}^* \rightarrow \{0,1\}^l$, where *l* is the length of output. *TS* selects a random number *d* as it's private key and computes the public key $F = \hat{e}(d, P)$. Finally, *TS* publishes $<E, P, F, h(\cdot), \hat{e}(\cdot)>$ as the system parameters.

4.2. Patient Registration Phase

When a patient *A* wants to register with *TS*, this phase is necessary to be performed through a secure channel. Figure 2 shows the steps of it and the detailed processes are as follows.

- *Step* 1: *A* selects his (or her) identity ID_A and sends it to *TS*.
- *Step* 2: *TS* computes $V_A = H(ID_{TS}||ID_A||d)$ and issues a Smart Card (SC) for *A* which stores { $E, P, F, H(\cdot), \hat{e}(\cdot), K_{A\text{-}TS}, ID_{TS}, ID_B, V_A$}.
- *Step* 3: *A* computes $W_A = ID_A\ XOR\ PW_A$, $V_1 = V_A\ XOR\ W_A$ and $V_2 = H(W_A)$ by using his (or her) identity ID_A and password PW_A. After that, *A* deletes V_A from the memory of the SC and writes $\{V_1, V_2\}$ on it.

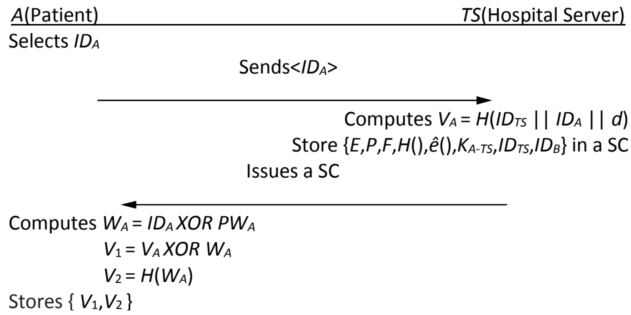

Figure 2. Patient registration phase.

4.3. Doctor/Nurse Registration Phase

Doctor/nurse *B* registration is the same as patient registration. Figure 3 shows the steps of it and the detailed processes are as follows.

- *Step* 1: *B* selects his (or her) identity ID_B and sends it to *TS*.
- *Step* 2: *TS* computes $V_B = H(ID_{TS}||ID_B||d)$ and issues a SC for *B* which stores { $E, P, F, H(\cdot), \hat{e}(\cdot), K_{B\text{-}TS}, ID_{TS}, ID_A, V_B$}.
- *Step* 3: *B* computes $W_B=ID_B\ XOR\ PW_B$, $V_3=V_B\ XOR\ W_B$ and $V_4=H(W_B)$ by using his (or her) identity ID_B and password PW_B. After that, *B* deletes V_B from the memory of the SC and writes $\{V_3, V_4\}$on it.

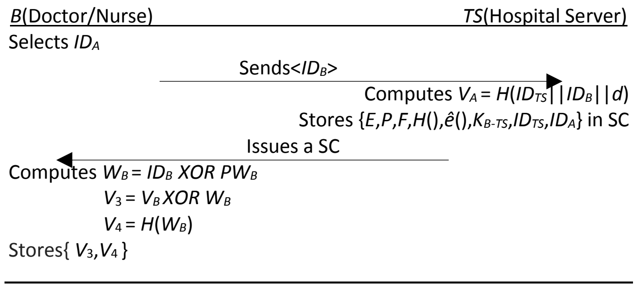

Figure 3. Doctor/Nurse registration phase.

4.4. Login Phase

When *A* wants to communicate to *B*, *A* performs this login phase with *B* via *TS*. Figure 4 shows the steps of it and the detailed processes are as follows.

- *Step* 1: *A* inputs ID_A and PW_A. *A*'s SC computes W_A' = $ID_A XOR\ PW_A$ and checks whether V_2equals to $H(W_A')$. If not, the SC stops the phase.
- *Step* 2: Otherwise, *A*'s SC chooses a random number R_A and computes $X_A = \hat{e}(R_A, P)$, $Y_A = \hat{e}(R_A, F) XOR\ ID_A$, $V_A' = V_1\ XOR\ W_A'$, $M_A = H(V_A'||ID_A||ID_B)$ and $C_{A\text{-}TS}= K_{A\text{-}TS}(M_A||ID_B)$. After that, *A* sends the message $<X_A, Y_A, C_{A\text{-}TS}>$ to *TS* through a public channel.

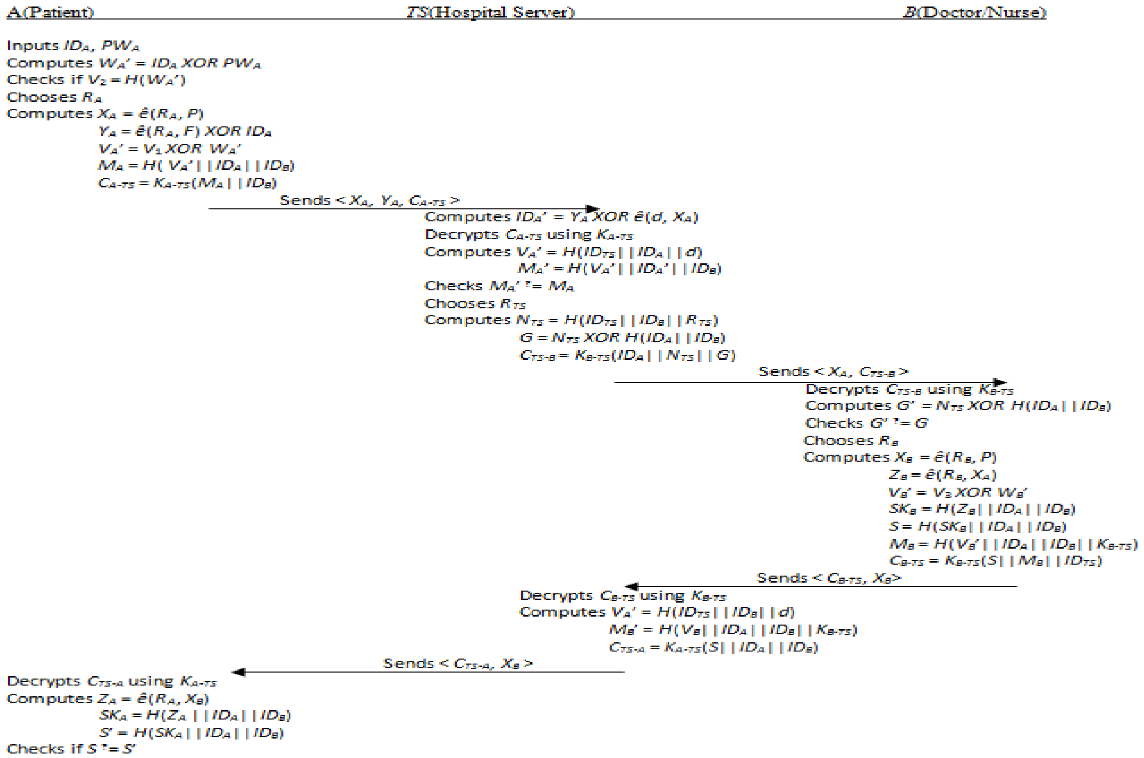

Figure 4. Privacy preserving authenticated key agreement.

4.5. Authenticated Key Agreement Phase

After the successful login with *TS*, all three participants communicate for the secure key agreement with privacy preserved. Figure 4 shows the steps of it and the detailed processes are as follows.

- *Step* 1: After *TS* receives the message $<X_A, Y_A, C_{A-TS}>$, it computes $ID_A' = Y_A XOR\ \hat{e}(d, X_A)$ and decrypts C_{A-TS} using K_{A-TS} to withdraw M_A and ID_B. Then, *TS* computes $V_A' = H(ID_{TS}||ID_A||d)$ and $M_A'=H(V_A'||ID_A'||ID_B)$ and checks whether M_A' equals to M_A. If not, *TS* stops the request. Otherwise, *TS* chooses a random number R_{TS} and computes $N_{TS} = H(ID_{TS}||ID_B||R_{TS})$, $G= N_{TS}XOR\ H(ID_A||ID_B)$ and $C_{TS-B}= K_{B-TS}(ID_A||N_{TS}||G)$. Then, *TS* sends the message $<X_A, C_{TS-B}>$ to *B*.
- *Step* 2: Upon receiving $<X_A, C_{TS-B}>$ from *TS*, *B* decrypts C_{TS-B} using K_{B-TS} to withdraw ID_A, N_{TS} and *G*. After that, *B* computes $G' = N_{TS}XOR\ H(ID_B||ID_A)$ and checks if *G'* equals to *G*. If not, this session is aborted.
- *Step* 3: Otherwise, *B* chooses a random number R_B and computes $X_B = \hat{e}(R_B, P)$, $Z_B = \hat{e}(R_B, X_A)$, $V_B' = V_3\ XOR\ W_B'$, $SK_B=H(Z_B||ID_A||ID_B)$, $S=H(SK_B||ID_A||ID_B)$,$M_B = H(V_B'||ID_A||ID_B||K_{B-TS})$, and $C_{B-TS}= K_{B-TS}(S||M_B||ID_{TS})$ and sends the message $<C_{B-TS},X_B>$ to *TS*.
- *Step* 4: After *TS* receives the message $<C_{B-TS},X_B>$, it decrypts C_{B-TS} using K_{B-TS} to withdraw *S*, M_B and ID_{TS}. Then, *TS* computes $M_B'=H(V_B||ID_B||ID_A||K_{B-TS})$ and checks whether M_B' equals to M_B. If not, *TS* stops the request. Otherwise, *TS* computes $C_{TS-A}= K_{A-TS}(S||ID_A||ID_B)$, and sends the message $< C_{TS-A}, X_B >$ to *A*.
- *Step* 5: Upon receiving $< C_{TS-A}, X_B >$ from *TS*, *A* decrypts C_{TS-A} using K_{A-TS} to withdraw *S*, ID_A and ID_B. After that, *A* computes $Z_A = \hat{e}(R_A, X_B)$, $SK_A = H(Z_A||ID_A||ID_B)$ and $S'=H(SK_A||ID_A||ID_B)$ and checks if *S'* equals to *S*. If not, the session is terminated.

After the successful authenticated key agreement phase, the agreed session key ($SK_A=SK_B$) could be used to provide confidentiality on the prescription. It means that *B* could send an encrypted prescription message based on the symmetric key cryptosystem using SK_B to *A* via *TS*. Then, *A* could decrypt the message using SK_A and perform necessary processes for health treatment.

5. Privacy and Security Analysis

This section provides privacy and security analysis on the proposed protocol. Table 2 shows comparisons of privacy and security features with Mahmood *et al.*'s [11] protocol.

Table 2. Privacy and security comparisons.

Protocols Features		Mahmood *et al.* [11]	The proposed
Privacy	P_1	Not Provide	Provide
	P_2	Not Provide	Provide
Security	S_1	Unsecure	Secure
	S_2	Unsecure	Secure
	S_3	Secure	Secure
	S_4	Secure	Secure
	S_5	Secure	Secure

P_1: *Anonymity*, P_2: *Untraceability*, S_1: Denial of service attack, S_2: Stolen-verifier attack, S_3: Password guessing attack, S_4: Replay attack, S_5: Stolen-smart card attack.

5.1. Privacy Analysis

Privacy could be preserved by supporting both terms of user anonymity and unlink ability.

1. User Anonymity
Based on the design of the proposed protocol, the excellent property of user anonymity can be guaranteed at every phase. The protocol used masking for the real identity via a public channel, and no attacker can compromise user's real identity by launching security attacks. In the login phase, patient's real identity is included in $Y_A = \hat{e}(R_A, F)\ XOR\ ID_A$. Thus, the attacker cannot reveal ID_A without having a power to perform ECDLP due to the bilinear pairing. Furthermore, all of the identities are transmitted in encrypted form instead of the message and these identities will be randomized at each session. As a result, the proposed protocol can provide user anonymity.

2. Untraceability
Untraceability means that nobody is capable to trace any related sessions from any patient. Normally, it is guaranteed together with anonymity. In the proposed protocol, any attacker could collect messages $<X_A, Y_A, C_{A-TS}>$,$<X_A, C_{TS-B}>$, $<C_{B-TS}, M_B>$ and $< C_{TS-A}, X_B >$ from any session. There are Y_A, C_{A-TS}, C_{TS-B}, and C_{TS-A}, which are related to track any patient with ID_A. However, it is difficulty the attacker to do that due to the one-way-ness of the hash function, symmetric key cryptosystem and ECDLP. Thereby, the proposed protocol could provide untraceability.

5.2. Security Analysis

This section provides security analysis in terms of password guessing attack, replay attack and stolen-smart card attack.

1. Password Guessing Attack
In the registration phase of the proposed protocol, patient's password PW_A is not transmitted to TS even if smart card stores PW_A in the form of W_A. Thereby, although the privileged-insider of TS can obtain the registration message, he (or she) is not feasible to know the registration entity's sensitive password related value. Moreover, there are no possibility that attacker knows the password even if the attacker steals a legitimated user's SC and reads the information on it. Thereby, the proposed protocol is strong against password guessing attack.

2. Replay Attack
The usage of random numbers is common solution for preventing replay attack in the authentication process. The messages $<X_A, Y_A, C_{A-TS}>$, $<C_{TS-B}>$, $<X_B, Z_B, C_{B-TS}>$ and $<C_{TS-A}>$ contain freshly generated random numbers in the proposed protocol. Furthermore, these random numbers are also embedded in the protected messages of $X_A = \hat{e}(R_A, P)$, $Y_A = \hat{e}(R_A, F) XOR\ ID_A$ and $C_{TS-B} = K_{B-TS}(ID_A||N_{TS}||G)$. Thus, each participant needs to check the freshness of the message to cope from the replay attack. Hence, the proposed protocol discards the possibility of replay attack.

3. Stolen-Smart Card Attack
Suppose that an attacker steals a legal smart care of a patient and could read the stored parameters $\{E, P, F, K_{A-TS}/K_{B-TS}, H(), \hat{e}()\}$. The attacker could try to impersonate A or B to successfully login to TS. However, in the proposed protocol, the attacker cannot guess any candidate's identity and password at the same time and compute V_1 and V_2. The way for the attacker to learn password is to find out the correct pair (ID_A, PW_A) such that $V_2 = H(W_A)$. In the proposed protocol, we assumed the probability of guessing ID_A composed of exact l characters and PW_A composed of exact m characters is approximately $1/(2^{6l+6m})$. This probability is negligible, and the attacker has no feasible way to derive ID_A and PW_A in polynomial time. Thereby, the proposed protocol is safe from the stolen-smart card attack.

6. Performance Analysis

This section provides performance analysis of the proposed protocol in terms of the computation complexity and the communication complexity focused on the login phase and the authenticated key agreement phase only. Performance evaluation is provided by comparing the proposed protocol with Mahmood *et al.*'s [11] protocol. The computational costs are measured by checking the execution time. They are generally conducted by focusing on operations performed by each party within the protocol. Therefore, for analysis of the computational costs, we concentrated on the operations that are conducted by the parties in the network: namely a patient, a server and doctor/nurse. In order to facilitate the analysis of the computational costs, we define the following three notations.

- T_h: time to execute a one-way hash operation
- T_s: time to execute a symmetric key encryption or decryption
- T_e: for the time to execute an ECC-160 encryption or decryption.

We performed an experiment using Crypto++ Library on a system using the 64-bits Windows 7, 3.2 GHz processor, 4 GB memory, Visual C++ 2013 Software, SHA-1 hash function, AES symmetric encryption/decryption and ECC-160 operation [2]. According to the experiment, T_h is nearly 0.0002 seconds on average, T_s is nearly 0.0087 seconds and T_e is nearly 0.6 seconds, respectively.

Table 3 shows a comparison of the computational cost between the related protocols. Mahmood et al.'s [11] protocol takes about 3.725 sec and the proposed protocol takes about 3.672 sec. As a result, the proposed protocol has lower computational overhead than Mahmood et al.'s [11] protocol.

Table 3. Computation cost comparisons.

Protocol \ Entity	Patient	*TS*	*Doctor/Nurse*	Total
Mahmood *et al.* [11]	$5T_h+3T_s+2T_e$	$6T_h+7T_s+2T_e$	$5T_h+4T_s+2T_e$	$16T_h+14T_s+6T_e$
The proposed	$4T_h+2T_s+3T_e$	$4T_h+4T_s+1T_e$	$4T_h+2T_s+2T_e$	$12T_h+8T_s+6T_e$

T_h: a one-way hash operation time, T_s: a symmetric key operation time, T_e: an ECC operation time.

The communication cost represents the number of communications, and the size of messages to be transmitted during the protocol run. The proposed protocol requires less number of communications and of bits compared to Mahmood *et al*.'s [11] protocol. The communication costs are presented in Table 4. The number of communication bits is based on various length of binary sequences such as: hash function-160 bits, identity-160 bits, symmetric encryption-128 bits and ECC element-160 bits. The number of communication bits required in the proposed protocol is given as: $<X_A, Y_A, C_{A\text{-}TS}>$-448 bits; $<X_A, C_{TS\text{-}B}>$-288 bits; $<C_{B\text{-}TS}, X_B>$-288 bits; $<C_{TS\text{-}A}, X_B>$-288 bits. Thus, the total number of communication bits required in the proposed protocol is 1,312 bits. Mahmood *et al.*'s [11] protocol requires $\{ID_{A\sim T}, C_A\}$-320 bits; $\{ID_{TS}, C_{TS}\}$-320 bits; $\{ID_{B\sim T}, C_B\}$-320 bits; $\{ID_{A\sim T}, CP_A\}$-320 bits; $\{ID_{B\sim T}, CP_B\}$-320 bits. So, Mahmood *et al*.'s [11] protocol requires 1,600 bits with 5 communications.

Table 4. Communicationcost comparisons.

Protocol \ Feature	Number of communications	Number of bits
Mahmood *et al.* [11]	5	1,600 bits
The proposed	4	1,312 bits

Thereby, the proposed protocol offers a better performance not only for the computation cost but also for the communication cost compared to Mahmood *et al*.'s [11] protocol. Furthermore, it assures higher security and privacy than Mahmood *et al*.'s [11] protocol.

7. Conclusions

This paper proposed a privacy preserving authenticated key agreement protocol for uHealthcare, which uses hash function, symmetric key cryptosystem and bilinear pairing. The proposed protocol is mainly focused on providing anonymity and untraceability, which are lack properties on Mahmood *et al*.'s [11] protocol. From the security analysis, we can argue that the proposed protocol efficiently solves security and privacy problems in Mahmood *et al*.'s [11] protocol. Furthermore, the proposed protocol is much efficient in the concern of computational cost compared to the counterpart protocol. Future works should be focused on pursuing more practical elaboration of the proposed protocol to the real uHealthcare application domain. Addition to this, some more researches should be done to reduce the computational overhead of patient side.

Acknowledgements

Corresponding author is Hyunsung Kim. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

References

[1] Cho S. and Kim H., "Hash Chain Based Authenticated Secure Communication for Healthcare System," *International Journal of Advances in Science Engineering and Technology*, vol. 7, no. 2, pp. 41-46, 2019.

[2] Dai W., http://www.cryptopp.com, Last Visited, 2021.

[3] Debiao H., Jianhua C., and Rui Z., "A More Secure Authentication Scheme for Telecare Medicine Information Systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989-1995, 2012.

[4] Houhamdi Z. and Athamena B., "Identity Identification and Management in the Internet of Things," *The International Arab Journal of Information Technology*, vol. 17, no. 4A, pp. 645-654, 2020.

[5] Kapito B., Nyirenda M., and Kim H., "Privacy-Preserving Machine Authenticated Key Agreement for Internet of Things," *International Journal of Computer Networks and Communications*, vol. 13, no. 2, pp. 99-120, 2021.

[6] Kim H., "Freshness-Preserving Non-Interactive Hierarchical Key Agreement Protocol over WHMS," *Sensors*, vol. 14, no. 12, pp. 23742-23757, 2014.

[7] Kim H., Ryu E., and Lee S., "Security Considerations on Cognitive Radio Based Body Area Networks for U-Healthcare," *Journal of Security Engineering*, vol. 10, no. 1, pp. 9-20, 2013.

[8] Ku D. and Kim H., "Enhanced User Authentication with Privacy for IoT-Based Medical Care System," *International Journal of Computer Theory and Engineering*, vol. 10, no. 4, pp. 125-129, 2018.

[9] Lee S., Kim H., and Yoo K., "Cryptanalysis of A User Authentication Scheme Using Hash Functions," *ACM SIGOPS Operating Systems Review*, vol. 38, no. 1, pp. 24-28, 2004.

[10] Liu H., Wu Z., Peng C., Tian F., and Lu L., "Privacy-Preserving Data Aggregation

Framework for Mobile Service Based Multiuser Collaboration," *The International Arab Journal of Information Technology*, vol. 17, no. 4, pp. 450-460, 2020.

[11] Mahmood Z., Ning H., Ullah A., and Yao X., "Secure Authentication and Prescription Safety Protocol for Telecare Health Services Using Ubiquitous IoT," *Applied Sciences*, vol. 7, no. 10, pp. 1-22, 2017.

[12] Mohamed M., Ghanem S., and Nagi M., "Privacy-Preserving for Distributed Data Streams: Towards I-Diversity," *The International Arab Journal of Information Technology*, vol. 17, no. 1, pp. 52-64, 2020.

[13] Moosavi S., Gia T., Nigussie E., Rahmani A., Virtanen S., Tenhunen H., and Isoaho J., "Session Resumption-Based End-to-End Security for Healthcare Internet-of-Things," *in Proceedings of the International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Liverpool, pp. 581-588, 2015.

[14] Moosavi S., Gia T., Rahmani A., Nigussie E., Virtanen S., Isaoaho J., and Tenhunen H., "SEA: A Secure and Efficient Authentication and Authorization Architecture for Iot-Based Healthcare Using Smart Gateways," *Procedia Computer Science*, vol. 52, 452-459, 2015.

[15] Nguyen H., Mirza F., Naeem M., and Nguyen M., "A Review on Iot Healthcare Monitoring Applications and A Vision for Transforming Sensor Data Into Real-Time Clinical Feedback," *in Proceedings of the 21st International Conference on Computer Supported Cooperative Work in Design*, Wellington, pp. 257-262, 2017.

[16] Rao R., https://theiotmagazine.com/internet-of-things-iot-healthcare-benefits-2aae663c5c79, Last Visited, 2018.

[17] Wei J., Hu X., and Liu W., "An Improved Authentication Scheme for Telecare Medicine Information Systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3597-3604, 2012.

[18] Wu S., Chiang R., Chang S., and Chang W., "An Interactive Telecare System Enhanced with IoT Technology," *IEEE Pervasive Computing*, vol. 16, no. 3, pp. 62-69, 2017.

[19] Wu Z., Lee Y., Lai F., Lee H., and Chung Y., "A Secure Authentication Scheme for Telecare Medicine Information Systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529-1535, 2012.

[20] Xiong H., Tao J., and Yuan C., "Enabling Telecare Medical Information Systems with Strong Authentication and Anonymity," *IEEE Access*, vol. 5, pp. 5648-5661, 2017.

[21] Zhu Z., "An Efficient Authentication Scheme for Telecare Medicine Information Systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3833-3838, 2012.

Sunghyun Cho received the M.Sc. degree in Cyber Security from Kyungil University, Korea, in 2021. He is a Master's Degree student at College of Computing, Sungkyunkwan University, Korea from 2021. His research interests include cryptography, authentication technologies, network security, ubiquitous computing security, and security protocol.

Hyunsung Kim received the M.Sc. and Ph.D. degrees in computer engineering from Kyungpook National University, Korea, in 1998 and 2002, respectively. He is a Professor at the School of Computer Science, Kyungil University, Korea from 2012. Furthermore, he is currently a visiting professor at the Department of Mathematical Sciences, Chancellor College, University of Malawi, Malawi from 2015. He also was a visiting researcher at Dublin City University in 2009. His research interests include cryptography, VLSI, authentication technologies, network security, ubiquitous computing security, and security protocol.