PLOS ONE

RESEARCH ARTICLE

A secure heterogeneous mobile authentication and key agreement scheme for e-healthcare cloud systems

Han-Yu Lin *

Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung, Taiwan

* hanyu@mail.ntou.edu.tw

OPEN ACCESS

Citation: Lin H-Y (2018) A secure heterogeneous mobile authentication and key agreement scheme for e-healthcare cloud systems. PLoS ONE 13(12): e0208397. https://doi.org/10.1371/journal.pone.0208397

Editor: Muhammad Khurram Khan, King Saud University, SAUDI ARABIA

Received: September 30, 2018

Accepted: November 16, 2018

Published: December 12, 2018

Data Availability Statement: All relevant data are within the manuscript.

Funding: This work was supported by the Ministry of Science and Technology of Republic of China under the contract number MOST 107-2221-E-019-017. There was no additional external funding received for this study.

Competing interests: The authors have declared that no competing interests exist.

Abstract

Heterogeneous mobile authentication is a crucial technique to securely retrieve the resource of e-healthcare cloud servers which are commonly implemented in a public key Infrastructure (PKI). Conventionally, a mobile data user can utilize a self-chosen password along with a portable device to request the access privilege of clouds. However, to validate the membership of users, a cloud server usually has to make use of a password table, which not only increases the burden of management, but also raises the possibility of information leakage. In this paper, we propose a secure heterogeneous mobile authentication and key agreement scheme for e-healthcare cloud systems. In our system structure, an e-healthcare cloud server of traditional PKIs does not have to store a password table. A legitimate data user only possesses a security token hardware and keeps an offline updatable password without using any private key. Our scheme is classified into the category of dynamic ID authentication techniques, since a data user is able to preserve his/her anonymity during authentication processes. We formally prove that the proposed mechanism fulfills the essential authenticated key exchange (AKE) security and owns lower computational costs. To further ensure the practical application security, an automatic security validation tool called AVISPA is also adopted to analyze possible attacks and pitfalls of our designed protocol.

Introduction

In an open environment such as the Internet, the data communication security is considered as an important issue and has to be ensured to prevent exposure of confidential messages. Whenever a patient tries to request the service of a remote e-healthcare cloud server, the latter must confirm his/her identity before approving the request. We thus call such a protocol the user authentication scheme. Generally speaking, according to the used evidence, we can classify user authentication schemes into the following three techniques:

1. Something you know: It is a kind of intangible knowledge. That is, a user can be authenticated if he proves that he learns something, e.g., password or PIN.
2. Something you have: This approach depends on some tangible objects. A requested user has to reveal some physical objects, (e.g., key, security token or smart card) satisfying the authentication criteria.

3. Something you are: A potential user can only be authenticated if he demonstrates that he owns certain valid biometrical property such as fingerprint, iris pattern and hand geometry.

When a user authentication scheme is combined with two of the above techniques, we call such a protocol two-factor authentication. To protect subsequent data transmission, a shared session key between two parties is often generated after the authentication is achieved. In 1976, Diffie and Hellman [1] proposed the first public key exchange protocol using the hardness of Discrete Logarithm Problem (DLP). Yet, their scheme is easily subject to the man-in-the-middle attack and lacks of user anonymity. Lamport [2] further introduced a password-based user authentication scheme suitable for insecure communication in 1981. In his scheme, a remote server keeps a password table storing hashed passwords rather than plaintexts. However, several later literatures [3–6] still exhibit that his scheme has several security flaws.

To guarantee the characteristic of user anonymity during interactions, in 2004, Das *et al.* [7] addressed the notion of dynamic ID authentication schemes. In such a scheme, a pseudo identity (also known as dynamic ID) of the user is used for interactive authentication processes. It is feasible for a remote server to derive the real identity from a pseudo one, but is computationally infeasible for any adversary to do it. However, their scheme failed to withstand several active attacks pointed by [8–10].

By extending Wang *et al.*'s protocol [9], in 2011, Khan *et al.* [11] proposed an efficient variant which removes the necessity of maintaining a password table. Considering the authentication technique of something you have, Tsai *et al.* [12] incorporated smart cards into his designed protocol. A smart card is usually equipped with lightweight computing capability and limited storage space. Nevertheless, the information stored in the smart card must be carefully selected, or else a malicious adversary can easily obtain the confidential data from a stolen or lost smart card.

In 2011, Wen and Li [13] presented an improved dynamic ID-based remote user authentication with key agreement scheme fulfilling the requirement of user anonymity and supporting the feature of key-update. Unfortunately, in 2012, Tang and Liu [14] found out that their scheme are still vulnerable to known existential attacks. Utilizing the RSA cryptosystem, in 2013, Lin [15] proposed a dynamic ID-based authentication scheme designed for telecare medical information system. He also proved that a previous related work [16] cannot achieve the security requirement of user anonymity and is subject to both dictionary and smart card loss attacks.

In 2014, Chen *et al.* [17] separately demonstrated security flaws of Song's [18], Sood *et al.*'s [19] and Xu *et al.*'s [20] protocols and gave an enhanced one. Based on elliptic curve cryptosystems, in 2015, Yang *et al.* [21] addressed a two-party authentication key exchange protocol for mobile environments. Using biometric properties, in 2017, Kumari *et al.* [22] came up with a biometrics-based authenticated key agreement scheme for multi-servers. So far, there have been several related variants [4, 23–36] introduced.

Nevertheless, existing schemes are either vulnerable to known attacks, or unsuitable for heterogeneous application environments. This motivates us to design a theoretically and experimentally secure heterogeneous mobile authentication and key agreement protocol in this paper. Particularly, we consider commonly deployed e-healthcare cloud services where a central cloud server of public key infrastructures (PKIs) is responsible for handling requests from various data users of no pre-distributed keys. In our system architecture, we focus on the private cloud environment [37], as many existing hospitals already have their own data centers and essential firewall infrastructures. In this circumstance, hospitals usually bear the most responsibility of managing and securing patients' medical data. Since the user privacy is another critical point in private clouds, we must be aware of any improper administration that

could possibly result in privilege creep [38]. In addition, some general security principles and practices are also helpful for preserving user privacy, including separation of privilege principle, least privilege principle and defense in depth principle. In our protocol design, we adopt dynamic ID authentication techniques to ensure user privacy as well as anonymity. In case that a user's portable security token device is lost or tampered, it would cause no harm to the user's privacy, as no confidential data are stored in the form of plaintext.

Proposed scheme

We demonstrate the proposed heterogeneous mobile authentication and key agreement scheme for e-healthcare cloud systems in this section. Table 1 first defines some utilized symbols for roles, functions, numbers and operations. Without loss of generality, our scheme can be divided into three phases including User Registration, Authentication, and Password-Update. Let p and q be two large primes satisfying $q \mid (p-1)$ and g a generator of order q. There are two collision-resistant one-way hash functions, H_1 and H_2, which can accept a variable length input and return an output of fixed length. The notations ID_i and ID_{Sj} separately represent the identity of a patient U_i and a remote e-healthcare cloud server S_j. Detailed steps of each phase are described as follows:

User registration phase

Fig 1 illustrates the user registration phase of proposed scheme. Assume that each patient U_i owns a self-chosen password PW_i and a security token device SC_i. Before requesting the cloud services from the server S_j, U_i has to perform the user registration process for becoming a legitimate user. Initially, U_i will enter his (ID_i, PW_i) and the SC_i performs the following steps with S_j:

Step 1 SC_i first chooses a random integer k_i to compute $Q_i = H_2(PW_i)$ and

$$K_i = Q_i \oplus H_2(k_i, ID_{S_j}), \tag{1}$$

Table 1. Symbol notations.

Notation	Description
U_i	a patient
S_j	an e-healthcare server
p, q	large primes
g	a generator of order q
ID_i	the identity of U_i and $\|ID_i\| = n$
ID_{S_j}	the identity of S_j and $\|ID_{S_j}\| = n$
$(a)_n$	the first n bits of the value a
$H_1(\bullet)$	a secure one-way hash function and $\mid H_1(\bullet) \mid = n$
$H_2(\bullet)$	a secure one-way hash function and $\mid H_2(\bullet) \mid = 2n$
PW_i	U_i's password
SC_i	a security token hardware of U_i
x_j	S_j's private key
Y_j	S_j's public key such that $Y_j = g^{x_j} \bmod p$
k_i, a	random integers
t_1	a timestamp
SK	a session key
$\oplus$	the exclusive-OR operation
$\|\|$	the concatenation operation

https://doi.org/10.1371/journal.pone.0208397.t001

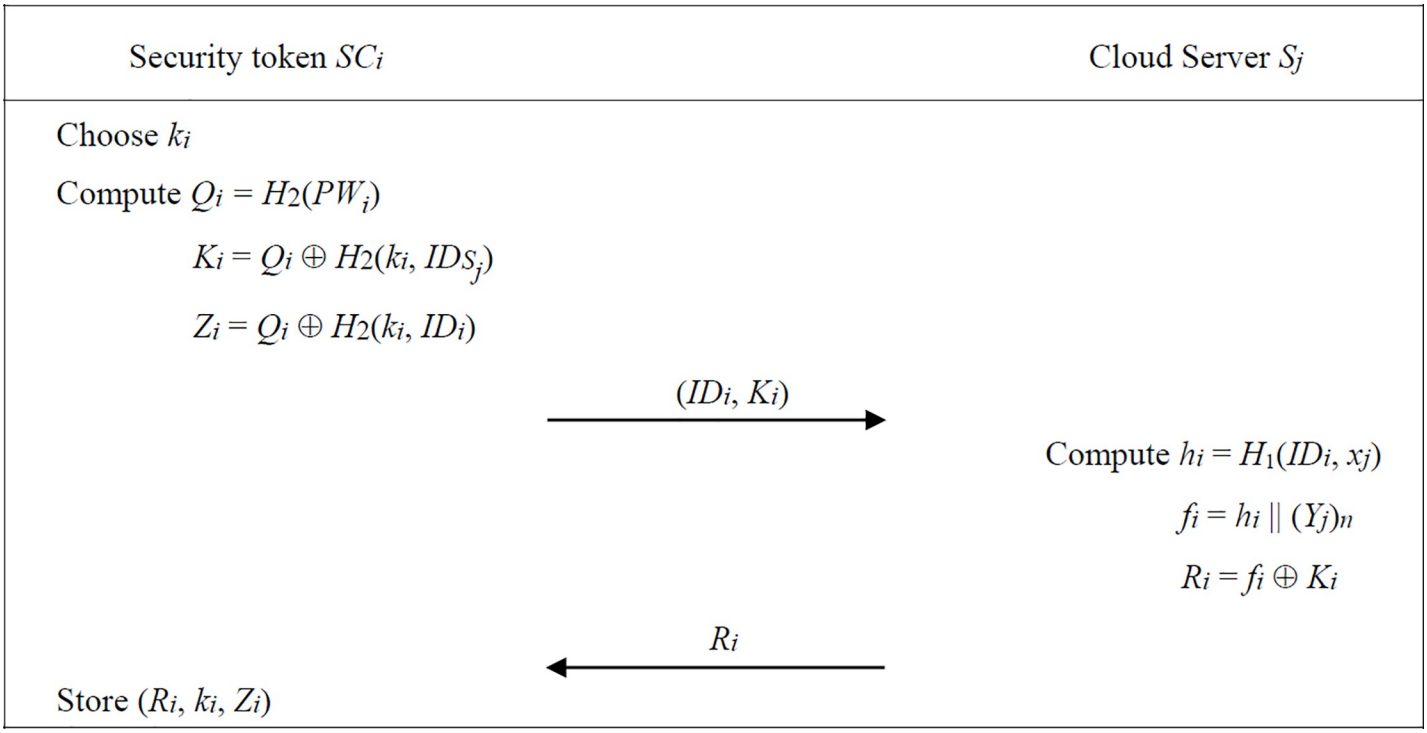

Fig 1. User registration phase of proposed scheme.

https://doi.org/10.1371/journal.pone.0208397.g001

$$Z_i = Q_i \oplus H_2(k_i, ID_i). \quad (2)$$

Then SC_i delivers (ID_i, K_i) to S_j via a secure channel. Since a random integer k_i is used in computing K_i and Z_i, it would be difficult for any malicious adversary to correlate one requested user with another.

Step 2 After receiving the registration request, S_j computes

$$h_i = H_1(ID_i, x_j), \quad (3)$$

$$f_i = h_i \| (Y_j)_n, \quad (4)$$

$$R_i = f_i \oplus K_i, \quad (5)$$

and returns R_i to SC_i via the same secure channel. SC_i will complete the registration process by storing (R_i, k_i, Z_i). Note that there is no identity related information kept in the SC_i. Thus, any attacker cannot have the knowledge of the owner of a lost security token device.

Authentication phase

We demonstrate the interactive authentication processes of our scheme in Fig 2. A registered patient U_i can login to remote cloud servers with the assistance of his password and a security token hardware. First, U_i enters his password PW_i and the identity ID_{Sj} of remote server, and

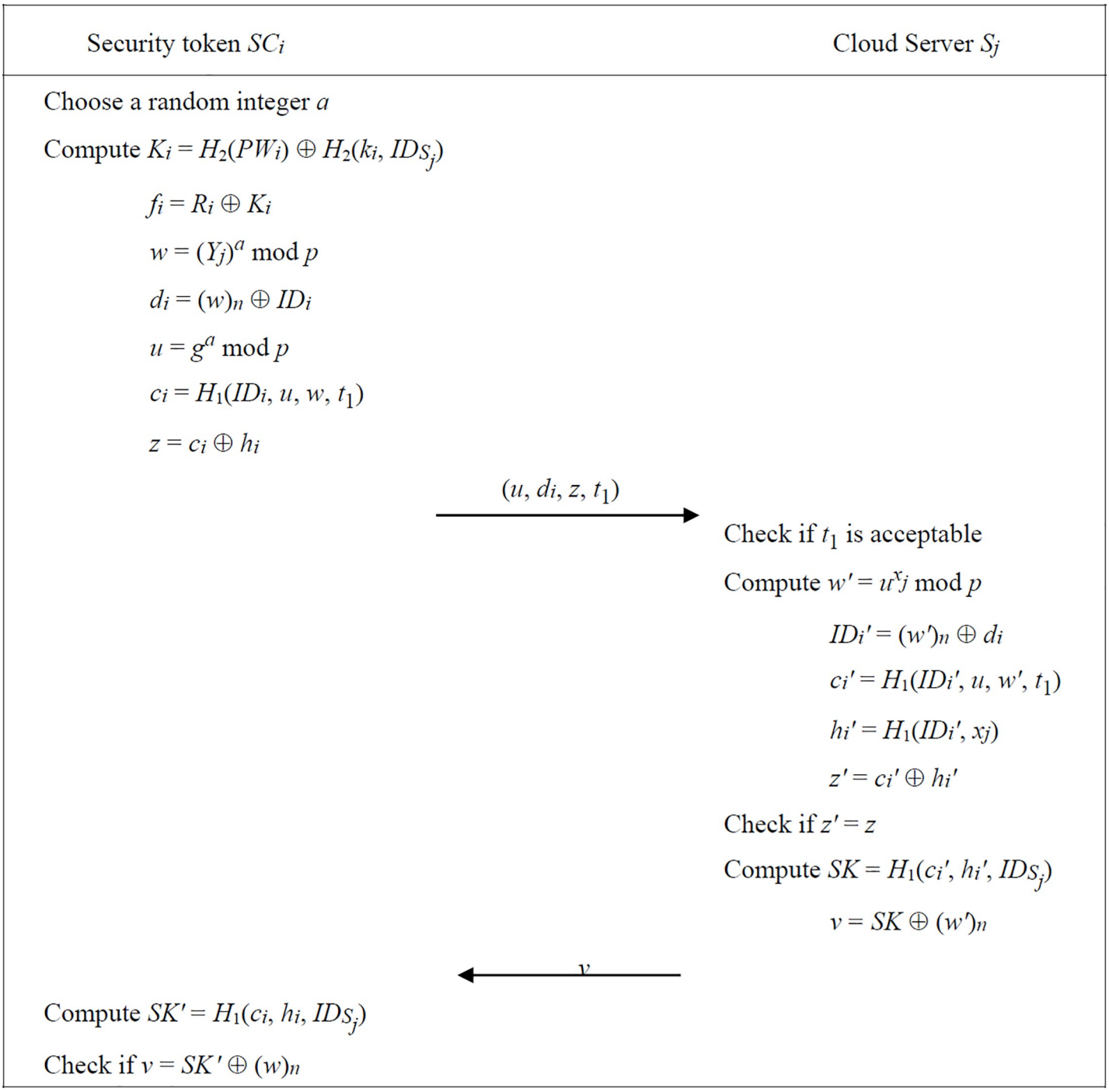

Fig 2. Authentication phase of proposed scheme.

https://doi.org/10.1371/journal.pone.0208397.g002

then the security token SC_i will select a random integer a and compute necessary parameters as follows:

$$K_i = H_2(PW_i) \oplus H_2(k_i, ID_{S_j}), \tag{6}$$

$$f_i = R_i \oplus K_i, \tag{7}$$

$$w = (Y_j)^a \bmod p, \tag{8}$$

$$d_i = (w)_n \oplus ID_i, \tag{9}$$

$$u = g^a \bmod p, \tag{10}$$

$$c_i = H_1(ID_i, u, w, t_1) \tag{11}$$

$$\text{where } t_1 \text{ is a timestamp,} \tag{12}$$

$$z = c_i \oplus h_i. \tag{13}$$

A valid login request is formed by (u, d_i, z, t_1) which is then sent to S_j. Upon receiving it, S_j first verifies the freshness of timestamp t_1. If it is not fresh, S_j will deny the service request; else, S_j further computes

$$w' = u^{x_j} \bmod p, \tag{14}$$

$$ID_i' = (w')_n \oplus d_i, \tag{15}$$

$$c_i' = H_1(ID_i', u, w', t_1), \tag{16}$$

$$h_i' = H_1(ID_i', x_j), \tag{17}$$

$$z' = c_i' \oplus h_i', \tag{18}$$

and then checks whether $z' = z$. If it holds, S_j derives

$$SK = H_1(c_i', h_i', ID_{S_j}), \tag{19}$$

$$v = SK \oplus (w')_n, \tag{20}$$

and sends the confirmation value v back to SC_i.

Upon receiving it, SC_i also computes

$$SK' = H_1(c_i, h_i, ID_{S_j}), \tag{21}$$

and confirms whether $v = SK' \oplus (w)_n$. If it holds, the user authentication process is successful and the session key SK is used for ensuring the confidentiality of this connection.

Password-update phase

We illustrate the password-update phase of proposed scheme in Fig 3. Each U_i can periodically update his password with his security token device. Note that we do not discuss the issue of password reset or recovery here. Specifically, U_i first enters ID_i along with his old and new passwords (PW_i, PW_i'). Then the security token SC_i computes $Q_i = H_2(PW_i)$,

$$N_i = Q_i \oplus H_2(PW_i'), \tag{22}$$

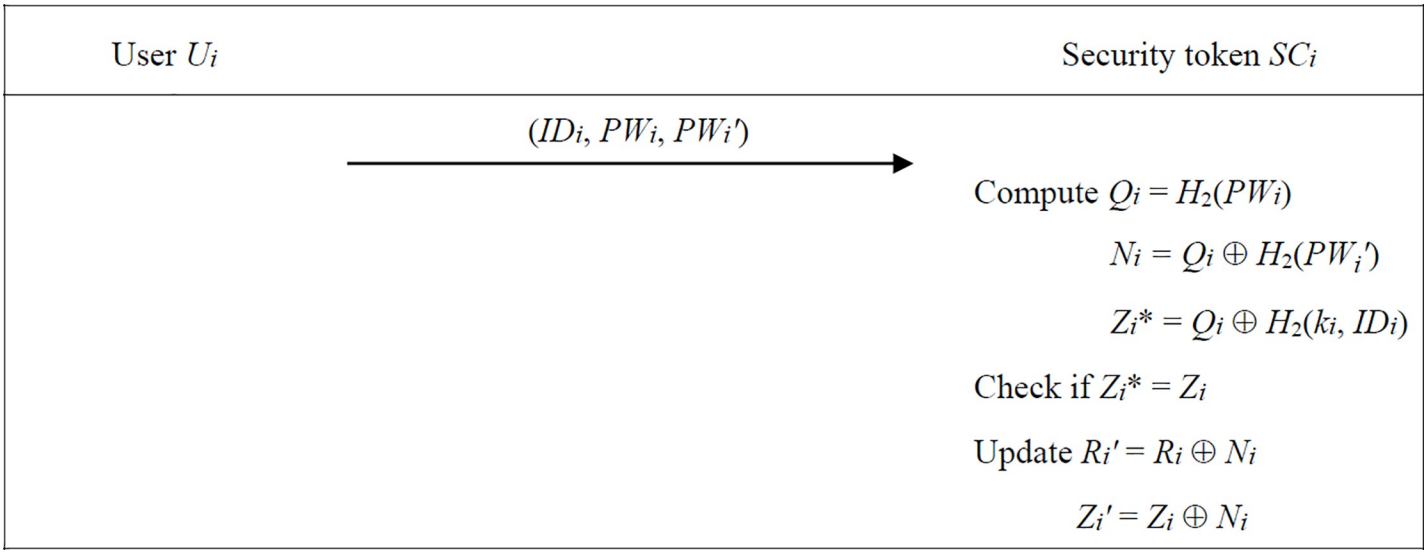

Fig 3. Password-update phase of proposed scheme.

https://doi.org/10.1371/journal.pone.0208397.g003

$$Z_i* = Q_i \oplus H_2(k_i, ID_i), \tag{23}$$

and checks whether $Z_i^* = Z_i$. If it holds, SC_i completes the password-update process by modifying the pre-stored R_i and Z_i as

$$R_i' = R_i \oplus N_i, \tag{24}$$

$$Z_i' = Z_i \oplus N_i, \tag{25}$$

Security proof

For facilitating the security proofs of our proposed heterogeneous mobile authentication and key agreement scheme for e-healthcare cloud systems, we first state the underlying computational problem and assumption as follows:

Decisional Diffie-Hellman (DDH) problem [39]

Let p and q be two large primes satisfying $q \mid p-1$, and g a generator of order q over GF(p). The DDH problem is, given (p, q, g^a, g^b) and g^c for some a, b, c randomly and independently chosen from Z_q, to decide whether $g^c = g^{ab} \bmod p$ or not.

Decisional Diffie-Hellman (DDH) assumption [39]

The advantage for any probabilistic polynomial-time (PPT) algorithm A to solve the DDH problem is negligible.

When it comes to user authentication protocols, we usually consider the crucial security requirement of authenticated key exchange (AKE). In this security notion, an adversary A can make **Test** queries to obtain either an invalid symbol $\perp$ or certain valid value. The former case happens when a protocol **P** rejects a user instance. In the latter case, the valid value could be a real session key if such a **Test** query is made in relation to partnered instances and only one of them is honest. If not, the query will return either the genuine session key or a random number

depending on the result of a flipped internal bit b. At last, the adversary A outputs a guessed bit b'. We say that A wins the indistinguishability game against the protocol **P** only if $b = b'$. The advantage of adversary A against the protocol **P** could be defined as $Adv_P^{ake}(\mathcal{A}) = |\Pr[b = b'] - \frac{1}{2}|$. When $Adv_P^{ake}(\mathcal{A})$ is negligible, we can claim that the protocol **P** is AKE-secure.

In practical application environments, a patient ID_i and an e-healthcare cloud server ID_{S_j} might be participated in various concurrent connections by using unique session keys, respectively. We therefore use the notation of $(\Pi_{U_i}^m, \Pi_{S_j}^n)$ to represent an instance (also known as oracle) of players (ID_i, ID_{S_j}) engaged in the (m, n)-th session, respectively. In general, a malicious adversary A is allowed to invoke the following queries:

- ***Send***$(\Pi_{U_i}^m, M)$: A ***Send*** query enables the adversary to take control of interactive communications of a protocol **P**. More precisely, a ***Send***$(\Pi_{U_i}^m, M)$ query gives A the computational results of the instance $\Pi_{U_i}^m$ with respect to the message M according to **P**'s protocol steps. Additionally, the ***Send***$(\Pi_{U_i}^m,$ "*start*") query indicates $\Pi_{U_i}^m$ to initialize the execution of protocol **P**.
- ***Corrupt***(U): By issuing this query, the adversary A can acquire the long-term private key of user U. In the proposed system, the session keys are viewed as short-term private keys while the passwords of users are thus regarded as long-term ones. This query can model the security requirement of perfect forward secrecy, i.e., a protocol **P** can still guarantee the confidentiality of previous short-term private keys even if the long-term ones have been exposed.
- ***Hash***(M): This query models the hash functions $H_1(\bullet)$ and $H_2(\bullet)$ of the proposed system. The adversary can make a ***Hash***(M) query and receive the generated result. If no matched entry can be found out in the target list, the oracle randomly selects a value a of proper length to return. The entry (M, a) is also preserved in the list.
- ***Reveal***$(\Pi_{U_i}^m)$: Once an instance $\Pi_{U_i}^m$ is accepted by a protocol **P**, A can invoke a ***Reveal***$(\Pi_{U_i}^m)$ query to learn its real session key. Otherwise, the oracle returns **Fail**. Such a query is used to evaluate the confidentiality of session keys when one of them is compromised, and is thus referred to as known key attacks.
- ***Test***$(\Pi_{U_i}^m)$: To simulate the security requirement for indistinguishability of session key SK, A can make use of ***Test*** queries. When a ***Test***$(\Pi_{U_i}^m)$ query is invoked and neither $\Pi_{U_i}^m$ nor its partner has been queried the ***Reveal*** oracle, it will return the real session key SK_i. Still, in another fresh case that both $\Pi_{U_i}^m$ and its partner are finally accepted by the protocol **P**, and on one had been issued the ***Reveal*** oracle, it will flip an internal coin b to decide a returned value. If $b = 1$, the real session key SK_i' is outputted; else if $b = 0$, a random number SK_i' of the same length is returned instead.

To prove the AKE-security of the proposed protocol, we first recall the definition of Difference Lemma [40] as follows:

Lemma 1. Difference lemma

Let A, B and F be events in some probability distribution. If the condition that $\Pr[A \wedge \neg F] = \Pr[B \wedge \neg F]$ holds, we can derive $|\Pr[A] - \Pr[B]| \leq \Pr[F]$.

From the perspective of theoretic security, we will formally prove that our protocol satisfies the AKE security in the random oracle model by employing the method of sequence of games along with the Difference Lemma as Theorem 1.

Theorem 1. *Let* Adv^{ddh} denote *the advantage of a DDH adversary who has the ability to break the DDH problem within the running time t. Then we could express the advantage for an adversary breaking the AKE security of proposed protocol* **P** *as*

$$Adv_P^{ake}(t', q_s, q_H) \leq \frac{q_s}{\omega} + \frac{{q_H}^2}{2^k} + Adv^{ddh}(t, q_s, q_H),$$

where q_s *and* q_H *separately represent the number of* ***Send*** *and* ***Hash*** *queries, and the symbol* ω *is the dictionary size of passwords.*

Proof: The proof idea is as follows. We first construct a sequence of games, named G_i's, for $i = 0$ to 4. In each game G_i, an adversary wins the game is defined as an event E_i. The transition between consecutive games, i.e., from G_i to G_{i+1} is made by adding slight modifications. We shall show that the difference between $\Pr[E_i]$ and $\Pr[E_{i+1}]$ is negligible. Let game G_0 be an adversary A attempting to defeat the AKE security of proposed protocol **P** in the real world. Since we have derived that $\Pr[E_i] = \Pr[E_{i+1}]$ for $i = 0$ to 3, it is sufficient to claim that $\Pr[E_0]$ approximates $\Pr[E_4]$ which is negligible. Consequently, we could complete this security proof with the final game G_4 showing that it is negligible for any probabilistic polynomial-time algorithm to defeat the AKE security of protocol **P**.

Game G_0: This game models a real situation that an adversary A tries to break the semantic security of session key *SK* in the proposed protocol **P**. More specifically, A will invoke a ***Test*** query and output a bit b'. When $b = b'$, which is defined as the event E_0, A wins the indistinguishability game against the protocol **P**. According to previous definition, we learn that

$$Adv_P^{ake}(\mathcal{A}) = \left|\Pr[E_0] - \frac{1}{2}\right|. \tag{26}$$

Game G_1: This game simulates the scenario that an adversary A aims at guessing a correct password, i.e., long-term private key of some user instance $\Pi_{U_i}^m$ by invoking ***Send*** queries. Nevertheless, a ***Send*** query of message M' composed of (u, d_i, z, t_1) will lead to different computational results during each execution of protocol **P**. Namely, it would be intractable for A to verify his/her guess. Hence, the success probability of this game could be expressed as the event that a ***Send*** query consisting of valid message $M' = (u, d_i, z, t_1)$ has been invoked, denoted by E_1. Then, we can compute

$$|\Pr[E_0] - \Pr[E_1]| \leq \frac{q_s}{\omega}. \tag{27}$$

Game G_2: In this game, we keep a list for correctly responding to all ***Hash*** queries. As long as no collision for each ***Hash*** query is found out by the adversary, the game is perfectly simulated just like previous game G_1. We therefore define E_2 to be the event of some hash collision happening in the simulation. Then, by employing the Difference Lemma and the birthday paradox, we know that

$$|\Pr[E_1] - \Pr[E_2]| \leq \frac{{q_H}^2}{2^k}. \tag{28}$$

Game G_3: We made a transition of game G_2 to game G_3 by adding a simulator S. The simulator S acts based on game G_2 to simulate all oracles except that the ***Send*** queries composed of a random DDH triple (u^*, Y_j^*, w^*) for honest players would be replaced by another indistinguishable triple (X, Y, Z). First, the simulator S randomly chooses $a^*, x_j^* \in Z_q$, sets S_j's private key as x_j^*, computes $X = g^{a^*} \bmod p$, $Y = g^{xj^*} \bmod p$ and $Z = (Y)^{a^*} \bmod p$, and then records the entries (a^*, X), (x_j^*, Y) and (X, Y, Z). By doing so, the simulator S is able to correctly respond to all the ***Send*** and ***Test*** queries in game G_3. It is evident that we utilize computationally

indistinguishable DDH triples to perfectly substitute for random DDH triples in game G_2. Consequently, the success probability of an adversary in game G_3 is determined by the event probability of E_3, i.e., distinguishing a random DDH triple and a simulated one computed by the simulator S, and we can observe that

$$\Pr[E_2] = \Pr[E_3]. \tag{29}$$

Game G_4: We start the final game and simulate all the oracles just like what we have done in game G_3. Yet, we add some little changes by using identically distributed random variables (X^*, Y^*, Z^*) to substitute for the computationally indistinguishable DDH triple (X, Y, Z) of related oracles. Assume that there is a polynomial-time adversary D trying to solve the above instance of DDH problems within the running time t. The adversary D flips an internal coin b to decide how it interacts with A. Whenever $b = 1$, the real session key SK is outputted to A. Otherwise, a random variable of the same length is returned to A instead. At last, A will generate a bit b' as its guess. Only when the equality $b' = b$ holds, we say that A wins the indistinguishability game. At the same time, D would finally output 1; else, D outputs 0. We express the event that D finally returns 1 as E_4 and we have

$$\Pr[E_4] = \frac{1}{2} \tag{30}$$

if the triple (X^*, Y^*, Z^*) is truly random variables and no information about the bit b is leaked. On the other hand, if the random triple (X^*, Y^*, Z^*) is also a DDH triple, $\Pr[E_4]$ would be equivalent to $\Pr[E_3]$ and we could derive that

$$|\Pr[E_3] - \Pr[E_4]| \leq Adv^{ddh}(\mathcal{D}), \tag{31}$$

Combining Eqs (26) to (31), we have that

$$Adv_P^{ake}(\mathcal{A}) = \left|\Pr[E_0] - \frac{1}{2}\right|$$

$$\leq \frac{q_s}{\omega} + \frac{q_H^{\,2}}{2^k} Adv^{ddh}(\mathcal{D}), \text{ which is negligible.} \qquad \text{Q.E.D.}$$

We further evaluate the security of our scheme by utilizing the well-developed tool of AVISPA (Automated Validation of Internet Security Protocols and Applications) [41]. Such a security analysis tool integrates several back-ends (analyzers) to realize automatic validation of security protocols as well as tracing possible attacks against the designed cryptographic schemes. Concretely speaking, the AVISPA has four modules including OFMC (On-the-Fly Model-Checker), CL-AtSe (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model-Checker) and TA4SP (Tree Automata tool based on Automatic Approximations for the Analysis of Security Protocols). Any security protocol to be analyzed must be specified in the format of HLPSL (High Level Protocols Specification Language) which will be transformed to IF specifications by a translator called hlpsl2if. Fig 4 illustrates the HLPSL specifications of our scheme. Then we employ the OFMC and the CL-AtSe modules to evaluate the security of our protocol. The analysis results shown in Fig 5 both reveal "SAFE" for our proposed protocol.

Comparison

In this section, we compare our authentication scheme with the Yang-Yang (YY for short) [32], the Khan-Kumari (KK for short) [42] and Chen *et al.*'s (CKW for short) [17] mechanisms

File

```
role patient(A,B:agent,Kab:symmetric_key,Yb:public_key,H:hash_func,G:text,SND, RCV: channel(dy))
played_by A def= local State : nat, PWa,Na,Ka,T1:text, Kaa, Zaa, Ha, W, U, Ca, SKab : message
          init State := 0
          transition 1. State  =0 /\ RCV(start) =|> State':=2 /\ Ka':=new() /\ PWa':=new() /\ Kaa':=xor(H(PWa'),H(Ka'.B))
                                  /\ Zaa':=xor(H(PWa'),H(Ka'.A)) /\ SND({A.Kaa'}_Kab)
                       2. State = 2 /\ RCV({{Ha'.Yb}_Kaa}_Kab) =|> State':= 4 /\ secret(Ha, ha, {A,B})
                                  /\ request(A, B, patient_server_kaa, Kaa) /\ T1':=new() /\ Na':=new() /\ W':= exp(Yb,Na')
                                  /\ U':= exp(G, Na') /\ Ca':= H(A.U'.W'.T1') /\ SND(U'.{A}_W'.{Ca'}_Ha.T1')
                                  /\ witness(A, B, patient_server_w, W') /\ SKab':= H(Ca'.Ha.B)
                       3. State  =4 /\ RCV({W'}_SKab) =|> State':=6 /\ request(A, B, patient_server_w, W) end role
role server(A,B:agent,Kab:symmetric_key,Yb:public_key,H:hash_func,G:text,SND, RCV: channel(dy))
played_by B def= local State : nat, PWa,Na,Ka,T1:text, Kaa, Zaa, Ha, W, U, Ca, SKab  : message
          init State := 1
          transition 1. State  =1 /\ RCV({A.Kaa'}_Kab) =|> State':=3 /\ Ha':= H(A.inv(Yb)) /\ SND({{Ha'.Yb}_Kaa'}_Kab)
                                  /\ witness(B, A, patient_server_kaa, Kaa')
                       2. State = 3 /\ RCV(U'.{A}_W'.{Ca'}_Ha.T1') =|> State':= 5 /\ W':= exp(U',inv(Yb)) /\ Ca':=H(A.U'.W'.T1')
                                  /\ Ha':=H(A.inv(Yb)) /\ SKab':= H(Ca'.Ha'.B) /\ SND({W'}_SKab') /\ secret(SKab', skab, {A,B})
end role
role session(A,B: agent,Kab: symmetric_key,Yb : public_key,H: hash_func,G : text)
def=  local SNDa,RCVa,SNDb,RCVb : channel(dy)
       composition patient(A, B, Kab, Yb, H, G, SNDa, RCVa) /\  server(A, B, Kab, Yb, H, G, SNDb, RCVb) end role
role environment()
def= const patient_server_kaa, patient_server_w, a,b: agent, skab,ha : protocol_id, kab,kai,kib : symmetric_key,
            yb: public_key, h:hash_func, g : text
      intruder_knowledge = {a,b,kai,kib,yb,h,g}
      composition session(a,b,kab,yb,h,g) /\ session(a,i,kai,yb,h,g)  /\ session(i,b,kib,yb,h,g)  end role
goal       secrecy_of skab, ha
           authentication_on patient_server_kaa, patient_server_w   end goal  environment()
```

Fig 4. HLPSL specifications of our scheme.

https://doi.org/10.1371/journal.pone.0208397.g004

in terms of security features and computational efforts. For facilitating the comparison, we first define some used symbols as Table 2. The approximate running time of each evaluated operation is also simulated according to [43, 44]. The detailed comparisons are listed in Table 3. From this table, one can observe that all compared protocols fail to provide user anonymity and provable AKE security. The YY scheme has to further assume a trusted third party (TTP). The KK scheme is the most time-consuming in the authentication processes. As for the CKW scheme, it not only incurs high computation overheads, but also cannot fulfill the requirements of offline password update, key contributory property and perfect forward secrecy. Here, we would like to discuss some aspects of the Man-At-The-End (MATE) attack [45] which is originated from the applications of digital assets' protection (DAP) and software protection. Fundamentally, such an attack is very difficult to evaluate and analyze than other security requirements due to its various forms and the complicated human nature. In a commonly seen scenario of MATE attacks, an adversary obtaining the access privilege to physical hardware might attempt to tamper it or inspect contained software. Consequently, we must be aware of the impact of MATE attacks and strengthen our current fortifications by resorting to anti-tamper techniques and software protection mechanisms. To sum up, the proposed scheme is still a better alternative from the perspective of functionalities, security and computational efficiency.

Conclusions

To provide a secure mechanism for accessing the resources of e-healthcare cloud systems implemented in a PKI, we propose a new heterogeneous mobile authentication and key

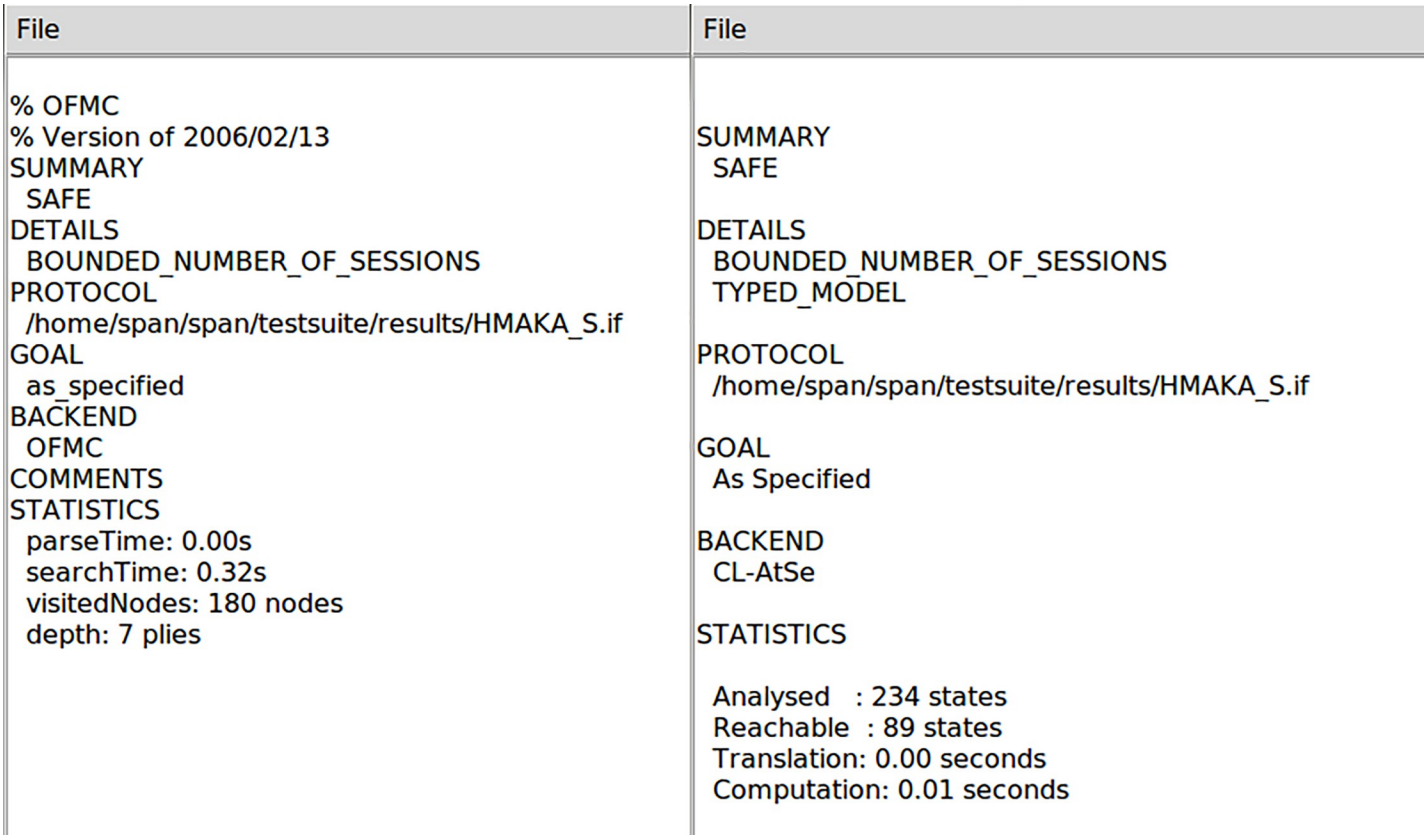

Fig 5. Analysis results of OFMC and CL-AtSe modules.

https://doi.org/10.1371/journal.pone.0208397.g005

Table 2. The used notations.

	Computation	Approximate running time
H	Collision-resistant hash function	0.2ms
M	Modular multiplication	0.2ms
E	Modular exponentiation	48ms

https://doi.org/10.1371/journal.pone.0208397.t002

Table 3. Computational comparisons of the proposed and previous schemes.

	YY	KK	CKW	Ours
Anonymity	No	No	No	Yes
Mutual authentication	Yes	Yes	Yes	Yes
Resist man-in-the-middle attack	Yes	Yes	Yes	Yes
Resist man-at-the-end attack	Unknown	Unknown	Unknown	Unknown
Offline password update	Yes	Yes	No	Yes
Key contributory property	Yes	Yes	No	Yes
Without trusted third party (TTP)	No	Yes	Yes	Yes
Perfect forward secrecy	Yes	Yes	No	Yes
Provable AKE security	No	No	No	Yes
Computational cost for registration	E + 3H (≈ 48.6ms)	E + 4H (≈ 48.8ms)	E + H (≈ 48.2ms)	4H (≈ 0.8ms)

(*Continued*)

Table 3. (Continued)

	YY	KK	CKW	Ours
Computational cost for authentication	4E + 8H (≈ 193.6ms)	5E + 9H (≈ 241.8ms)	3E + 3M + 8H (≈ 146.2ms)	3E + 7H (≈ 145.4ms)
Computational cost for password-update	3H (≈ 0.6ms)	6H (≈ 1.2ms)	2E + 2M + 2H (≈ 96.8ms)	3H (≈ 0.6ms)
Total computational cost	5E + 14H (≈ 242.8ms)	6E + 19H (≈ 291.8ms)	6E + 5M + 11H (≈ 291.2ms)	3E + 14H (≈ 146.8ms)

https://doi.org/10.1371/journal.pone.0208397.t003

agreement scheme using security token hardware. Our scheme preserves the property of user anonymity and allows users to change their passwords without the intervention of remote cloud servers. Each user can solely update his password with the help of his security token device. Besides, a remote e-healthcare cloud server is unnecessary to keep a password table for authenticating users, so as to prevent the risk of information leakage. Based on the security assumption of DDH which is believed to be polynomial-time intractable, we formally proved that our scheme achieves the AKE-security in the random oracle model. As for the practical application security, the well-developed AVISPA security protocol validation tool also found no possible attacks or pitfalls in the designed mechanism. Moreover, we demonstrate that the proposed scheme owns better security features and takes lower computational costs.

Author Contributions

Writing – original draft: Han-Yu Lin.

References

1. Diffie W, Hellman M, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, 1976, pp. 644–654.
2. Lamport L, Password authentication with insecure communication, *Communications of the ACM*, Vol. 24, No. 11, 1981, pp. 770–772.
3. Hwang MS, Li LH, A new remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electron*, Vol. 46, No. 1, 2000, pp. 28–30.
4. Lin CL, Sun HM, Hwang T, Attacks and solutions on strong-password authentication, *IEICE Transactions on Communications*, Vol. E84-B, No. 9, 2001, pp. 2622–2627.
5. Shimizu A A dynamic password authentication method by one-way function, *System and Computers in Japan*, Vol. 22, No. 7, 1991, pp. 32–40.
6. Shimizu A, Horioka T, Inagaki, H A password authentication method for contents communication on the Internet, *IEICE Transactions on Communications*, Vol. E81-B, No. 8, 1998, pp. 1666–1673.
7. Das ML, Saxana A, Gulati VP, A dynamic ID-based remote user authentication scheme, *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, 2004, pp. 629–631.
8. Liao I, Lee CC, Hwang MS, Security enhancement for a dynamic ID-based remote user authentication scheme, Proceedings of 2005 International Conference on Next Generation Web Services Practices, Seoul, Korea, 2005, pp. 437–440.
9. Wang YY, Liu JY, Xiao FX, Dan J, A more efficient and secure dynamic ID-based remote user authentication scheme, *Computer Communications*, Vol. 32, No. 4, 2009, pp. 583–585.
10. Yoon EJ, Yoo KY, Improving the dynamic ID-based remote mutual authentication scheme, *Proceedings of 2006 OTM Workshops*, Lecture Notes in Computer Science, Vol. 4277, Springer, Berlin, 2006, pp. 499–507.
11. Khan MK, Kim SK, Alghathbar A, Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme, *Computer Communications*, Vol. 34, No. 3, 2011, pp. 305–309.
12. Tsai JL, Wu TC, Tsai KY, New dynamic ID authentication scheme using smart cards, *International Journal of Communication Systems*, Vol. 23, No. 12, 2010, pp. 1449–1462.

13. Wen F, Li X, An improved dynamic ID-based remote user authentication with key agreement scheme, *Computers and Electrical Engineering*, Vol. 38, No. 2, 2011, pp. 381–387.
14. Tang HB, Liu XS, Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme, *International Journal of Communication Systems*, Vol. 25, No. 12, 2012, pp. 1639–1644.
15. Lin HY, On the security of a dynamic ID-based authentication scheme for telecare medical information systems, *Journal of Medical Systems*, Vol. 37, No. 2, 2013, pp. 1–5.
16. Chen HM, Lo JW, Yeh CK, An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems, *Journal of Medical System*, Vol. 36, No. 6, 2012, pp. 3907–3915.
17. Chen B, Kuo W, Wuu L, Robust smart-card-based remote user password authentication scheme, *International Journal of Communication Systems*, Vol. 27, No. 2, 2014, pp. 377–389.
18. Song R, Advanced smart card based password authentication protocol, *Computer Standards & Interfaces*, Vol. 32, No. 5, 2010, pp. 321–325.
19. Sood SK, Sarje AK, Singh K, An improvement of Xu et al.'s authentication scheme using smart cards, Proceedings of the 3rd Annual ACM Bangalore Conference, Bangalore, Karnataka, India, 2010, pp. 1–5.
20. Xu J, Zhu WT, Feng DG, An improved smart card based password authentication scheme with provable security, *Computer Standards & Interfaces*, Vol. 31, No. 4, 2009, pp. 723–728.
21. Yang H, Chen J, Zhang Y, An improved two-party authentication key exchange protocol for mobile environment, *Wireless Personal Communications*, Vol. 85, No. 3, 2015, pp. 1399–1409.
22. Kumari S, Das AK, Li X, Wu F, Khan MK, Jiang Q, et al, A provably secure biometrics-based authenticated key agreement scheme for multi-server environments, *Multimedia Tools Applications*, Vol. 77, No. 2, 2018, pp. 2359–2389.
23. Awasthi AK, Comment on a dynamic ID-based remote user authentication scheme. *Transaction on Cryptology*, Vol. 1, No. 2, 2004, pp. 15–16.
24. Chen C, He D, Chan S, Bu J, Gao Y, Fan R, Lightweight and provably secure user authentication with anonymity for the global mobility network, *International Journal of Communication Systems*, Vol. 24, No. 3, 2011, pp. 347–362.
25. He D, Chen J, Zhang R, A more secure authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, Vol. 36, No. 3, 2011, pp. 1989–1995. https://doi.org/10.1007/s10916-011-9658-5 PMID: 21360017
26. Juang WS, Wu JL, Two efficient two-factor authenticated key exchange protocols in public wireless lans, *Computers and Electrical Engineering*, Vol. 1, No. 35, 2009, pp. 33–40.
27. Ku WC, Chang ST, Impersonation attacks on a dynamic ID-based remote user authentication scheme using smart cards, *IEICE Transactions on Communications*, Vol. E88-B, No. 5, 2005, pp. 2165–2167.
28. Misbahuddin M, Bindu CS, Cryptanalysis of Liao-Lee-Hwang's dynamic ID scheme, *International Journal of Network Security*, Vol. 2, No. 6, 2008, pp. 211–213.
29. Su R, Cao ZF, An efficient anonymous authentication mechanism for delay tolerant networks, *Computers and Electrical Engineering*, Vol. 3, No. 36, 2010, pp. 435–441.
30. Wang RC, Juang WS, Lei CL, Robust authentication and key agreement scheme preserving the privacy of secret key, *Computer Communications*, Vol. 34, No. 3, 2011, pp. 274–280.
31. Wu S, Zhu T, Pu Q, Robust smart-cards-based user authentication scheme with user anonymity, *Security and Communication Networks*, Vol. 5, No. 2, 2011, pp. 236–248.
32. Yang D, Yang B, A biometric password-based multi-server authentication scheme with smart card, *Proceedings of IEEE International Conference on Computer Design and Applications (ICCDA)*, 2010, pp. 554–559.
33. Yoon EJ, Yoo KY, Ha KS, A user friendly authentication scheme with anonymity for wireless communications, *Computers and Electrical Engineering*, Vol. 3, No. 37, 2011, pp. 356–364.
34. Li X, Niu J, Kumari S, Wu F, Sangaiah AK, Choo KKR, A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, *Journal of Network and Computer Applications*, Vol. 103, No. 1, 2018, pp. 194–204.
35. Li X, Niu J, Bhuiyan MZA, Wu F, Karuppiah M, Kumari S, A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, 2018, pp. 3599–3609.
36. Li X, Peng J, Niu J, Wu F, Liao J, Choo KKR, A robust and energy efficient authentication protocol for industrial internet of things, *IEEE Internet of Things Journal*, Vol. 5, No. 3, 2018, pp. 1606–1615.
37. Siddiqui Z, Abdullah AH, KhanEmail MK, Alghamdi AS, Smart environment as a service: three factor cloud based user authentication for telecare medical information system, *Journal of Medical Systems*, Vol. 38, No. 9997, 2014, pp. 1–14.

38. Waqar A, Raza A, Abbas H, Khan MK, A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata, *Journal of Network and Computer Applications*, Vol. 36, No. 1, 2013, pp. 235–248.
39. Delfs H, Knebl H, *Introduction to Cryptography*: *Principles and Applications*, Springer, 2002.
40. Shoup V, Sequences of games: A tool for taming complexity in security proofs, 2006. http://www.shoup.net/papers/games.pdf
41. AVISPA (Automated Validation of Internet Security Protocols and Applications) http://www.avispa-project.org
42. Khan MK, Kumari S, An authentication scheme for secure access to healthcare services, *Journal of Medical Systems*, Vol. 37, No. 4, 2013, pp. 1–12.
43. Tan Z A chaotic maps-based authenticated key agreement protocol with strong anonymity, *Nonlinear Dynamics*, Vol. 72, No. 1–2, 2013, pp. 311–320.
44. Xue K, Hong P, Security improvement on an anonymous key agreement protocol based on chaotic maps, *Communications in Nonlinear Science and Numerical Simulation*, Vol. 17, No. 7, 2012, pp. 2969–2977.
45. Akhunzada A, Sookhak M, Anuar NB, Gani A, Ahmed E, Shiraz M, et al, Man-at-the-end attacks: analysis, taxonomy, human aspects, motivation and future directions, *Journal of Network and Computer Applications*, Vol. 48, 2015, pp. 44–57.