PLOS ONE

RESEARCH ARTICLE

An improved anonymous authentication scheme for roaming in ubiquitous networks

Hakjun Lee[1], Donghoon Lee[1], Jongho Moon[1], Jaewook Jung[1], Dongwoo Kang[1], Hyoungshick Kim[2], Dongho Won[2]*

1 Department of Electrical and Computer Engineering, Sungkyunkwan University, 2066 Seoburo, Suwon, Gyeonggido 16419, Korea, **2** Department of Computer Engineering, Sungkyunkwan University, 2066 Seoburo, Suwon, Gyeonggido 16419, Korea

* dhwon@security.re.kr

OPEN ACCESS

Citation: Lee H, Lee D, Moon J, Jung J, Kang D, Kim H, et al. (2018) An improved anonymous authentication scheme for roaming in ubiquitous networks. PLoS ONE 13(3): e0193366. https://doi.org/10.1371/journal.pone.0193366

Editor: Ozgu Can, Ege Universitesi Muhendislik Fakultesi, TURKEY

Received: June 7, 2017

Accepted: January 29, 2018

Published: March 5, 2018

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

Funding: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2010-0020210), http://www.nrf.re.kr/index.

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

Abstract

With the evolution of communication technology and the exponential increase of mobile devices, the ubiquitous networking allows people to use our data and computing resources anytime and everywhere. However, numerous security concerns and complicated requirements arise as these ubiquitous networks are deployed throughout people's lives. To meet the challenge, the user authentication schemes in ubiquitous networks should ensure the essential security properties for the preservation of the privacy with low computational cost. In 2017, Chaudhry et al. proposed a password-based authentication scheme for the roaming in ubiquitous networks to enhance the security. Unfortunately, we found that their scheme remains insecure in its protection of the user privacy. In this paper, we prove that Chaudhry et al.'s scheme is vulnerable to the stolen-mobile device and user impersonation attacks, and its drawbacks comprise the absence of the incorrect login-input detection, the incorrectness of the password change phase, and the absence of the revocation provision. Moreover, we suggest a possible way to fix the security flaw in Chaudhry et al's scheme by using the biometric-based authentication for which the bio-hash is applied in the implementation of a three-factor authentication. We prove the security of the proposed scheme with the random oracle model and formally verify its security properties using a tool named ProVerif, and analyze it in terms of the computational and communication cost. The analysis result shows that the proposed scheme is suitable for resource-constrained ubiquitous environments.

Introduction

The development of communication technology provides efficient services based on sustainable infrastructures that improve the human quality of life. As smart devices such as smartphones, smart watches, and tablets become widely available, it has become possible to access various services and to allow people to utilize information anytime and anywhere. Also, the ubiquitous smart society, in which the combining of the data from smart devices and various sensors enables intelligent communication, is being built in the form of the smart city [1, 2].

In this smart city, the ubiquitous network provides useful information and resources for remote operations such as human-resource management and enterprise-resource management by connecting to a home agent (HA) through the roaming of a foreign agent (FA) while a citizen is moving [3, 4].

For a user mobile device to be able to remotely access the authority of various services via the HA, remote user authentication is required. In the remote authentication scheme, the user identifier is required to verify that the user is legitimate. This identifier such as an ID and password is associated with user privacy, and it can seriously affect the user security when they are leaked; therefore, the login and authentication requests of the user that are transmitted to the public channel with the identifier can be easily targeted by an attacker. Due to this issue, the user anonymity and untraceability should be maintained in the remote authentication process [5].

In addition, after the user login and authentication requests are accepted, the participants on the ubiquitous network must share the same session key for secure future communications. At this time, to establish a secure session key from an attacker's spoofing attack that threatens the security of the participants, the key should not be directly distributed from one node to the other. The key agreement must be performed after a mutual authentication in which the participants identify each other's legitimacy [6].

In recent years, authentication techniques [7–13] have been frequently proposed. A two-factor authentication scheme using the user ID and password is widely used. However, the password-based authentication scheme has the security issue that it is vulnerable to password-guessing attacks. A key technology to overcome this security issue is a biometric-based three-factor authentication method. Since biometric keys (irises, fingerprints, hand geometry, palm prints, etc.) represent unique human characteristics, they have the following advantages [14]: (1) Biometric keys cannot be lost or forgotten; (2) it is extremely difficult to forge or distribute biometric keys; (3) biometric keys maintain uniqueness; and (4) it is difficult to guess biometric keys. Thus, it is obvious that the biometric-based user authentication methods are more secure and reliable than the traditional password-based user authentication methods.

Combining password and biometric key makes it difficult to guess the user credentials. Because of this, three-factor authentication schemes that use the uniqueness of users have recently been proposed [15, 16]. However, there are some caveats to be noted when practically applying biometric-based authentication techniques. First, as mentioned, biometrics is a human characteristic, so it cannot be changed, unlike a password. Consequently, if it is leaked, it will cause serious privacy problems [17]. Therefore, the original biometric template or the feature-vector value of users should not be directly exported. To enhance the security, many biometric-based authentication schemes have been proposed using techniques for extracting user's biometrics into a random value such as a bio-hash or a fuzzy-extractor [18–20].

Over the past few years, a number of authentication scheme have been proposed to support the roaming in ubiquitous networks. In 2004, Zhu and Ma [21] presented the first password-based authentication scheme for ubiquitous networks to protect the security of ubiquitous networks, but Lee et al. [22] then demonstrated that this scheme does not achieve a perfect backward secrecy and a mutual authentication, and also its failure to resist the forgery attack. To enhance the security of Zhu and Ma's scheme [21], Lee et al. [22] proposed an improved password-based authentication scheme. In 2008, however, Wu et al. [23] proved that the schemes of both Zhu and Ma [21] and Lee et al. [22] do not preserve the user anonymity, and the latter scheme does not achieve a perfect backward secrecy; additionally, Wu et al. [23] proposed simple solutions to fix the drawbacks of the two schemes. In 2012, however, Mun et al. [24]

showed that the scheme of Wu et al. [23] does not achieve the user anonymity and a perfect forward secrecy and they presented an enhanced password-based authentication scheme to overcome these weaknesses. Unfortunately, in 2014, Zhao et al. [25] then proved that the scheme of Mun et al. [24] is vulnerable to various attacks.

In 2011, He et al. [26] proposed a lightweight password-based authentication scheme, claiming that it satisfies the various security requirements for ubiquitous networks. In 2013, however, Jiang et al. [27] proved that He et al.'s scheme [26] does not prevent the off-line password guessing, server-spoofing, replay, and privileged-insider attacks, and they also presented an enhanced password-based authentication scheme to overcome these weaknesses. Wen et al. [28] subsequently showed that Jiang et al.'s scheme [27] is vulnerable to stolen-verifier, server-spoofing, replay, and denial-of-service attacks and its failure regarding the provision of the forward secrecy. In 2015, in a different study of Farash et al. [29], and Gope and Hwang [30], it was common that Wen et al.'s scheme [28] is insecure against the known attacks. Then, Farash et al. [29], and Gope and Hwang [30] independently introduced the improved password-based authentication schemes that prevent the various attacks. Nevertheless, Wu et al. [31] showed both schemes of Farash et al. [29], and Gope and Hwang [30] are vulnerable to various attacks. In addition, Chaudhry et al. [32] also found a number of security pitfalls in Farash et al.'s scheme [29] such as a user-anonymity violation and the disclosure of the secret parameters of the mobile node (MN) and the session key.

Contributions of the paper

Recently, Chaudhry et al. [32] proposed a privacy-preserving password-based authentication scheme for roaming in ubiquitous networks to solve the security issues of Farash et al.'s scheme [29]. They claimed that their scheme is secure against the various known attacks and is lightweight compared with the earlier scheme of Farash et al. [29]. However, We found that Chaudhry et al.'s scheme [32] is still vulnerable to several attacks; therefore, in this paper, we provide the proof that Chaudhry et al.'s scheme [32] is vulnerable to stolen-mobile devices and user impersonation attacks, and has drawbacks to the absence of the incorrect login-input detection, incorrect password change phase, and the absence of the revocation-process provision. To fix the security flaw of the scheme of Chaudhry et al. [32], we present an improved biometric-based authentication scheme for roaming in ubiquitous networks in this paper. In addition, to achieve the three-factor authentication that protects the user's biometrics, a bio-hash technique is applied in the proposed scheme whenever the user imprints his/her biometrics on a mobile device. Furthermore, we perform formal and informal analyses to prove that the proposed scheme meets the various security requirements, and conduct the comparisons in terms of the computational and communication cost to show the efficiency of the proposed scheme.

Organization of the paper

The remainder of this paper is organized as follows. In Section 2, a number of preliminaries are introduced. A brief review of the scheme of Chaudhry et al. [32] is presented in Section 3, and a cryptanalysis of Chaudhry et al. [32]'s scheme is presented in Section 4. The proposed scheme is presented in Section 5. The proposed scheme is analyzed in terms of formal and informal security in Section 6. Data from the comparisons of the performance of the proposed scheme with other related works are presented in Section 7. The conclusion of this paper is provided in Section 8.

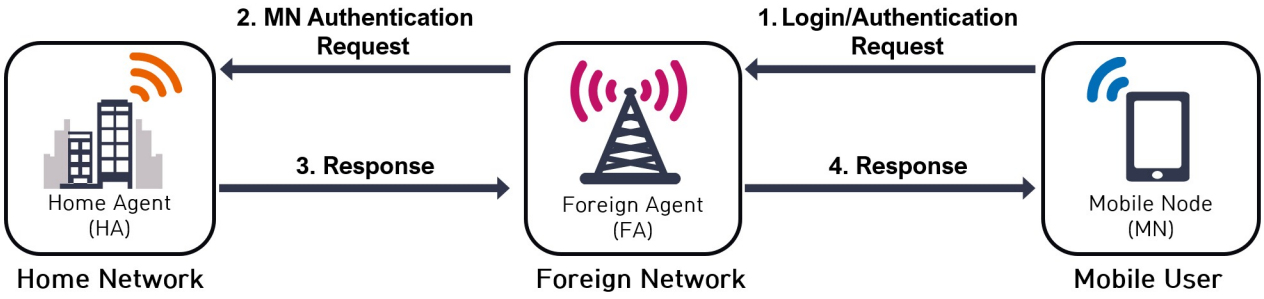

Fig 1. User authentication process in ubiquitous networks.

https://doi.org/10.1371/journal.pone.0193366.g001

Preliminary knowledge

This section introduces the requisite basic knowledge for the attainment of an understanding of the authentication process in ubiquitous networks, adversarial models, security requirements, and bio-hash functions.

User authentication in ubiquitous networks

To enable the roaming service in ubiquitous networks, *MN* and *FA* perform a mutual authentication and share the session key with the support of the *HA*. The brief description of the user authentication process that is depicted in Fig 1 is as follows:

1. *MN* sends a login and authentication request message to *FA* while it visits foreign networks.
2. After it receives the request message from *MN*, *FA* transmits it to *HA* for the authentication of *MN*.
3. *HA* authenticates *MN* by checking the received message from *FA*, and it responds accordingly to *FA*.
4. *FA* sends a response to *MN*, and then both *MN* and *FA* authenticate each other.

Adversarial model

For the analysis of the security of Chaudhry et al. and the proposed scheme in this paper, we consider the adversarial model with following the capacity of adversary:

1. The adversary $\mathcal{A}$ has full control over the public communication channel, which means that $\mathcal{A}$ can eavesdrop, insert, delete, alter, or intercept any of the transmitted messages of the public channel.
2. If $\mathcal{A}$ obtains a stolen or lost mobile device of a user in some way, he/she is able to extract the secret parameters from the device using side-channel attacks [33–36].
3. $\mathcal{A}$ is capable of enumerating off-line all of the possible items in the Cartesian product $\mathcal{D}_{id} * \mathcal{D}_{pw}$ within polynomial time, where $\mathcal{D}_{id}$ and $\mathcal{D}_{pw}$ denote the dictionary spaces of the identity and password, respectively [37, 38].

Security requirements

Based on recent research efforts [6, 39–41], a biometrics-based authentication scheme for roaming in ubiquitous networks should meet the following security requirements against the adversarial model and the functional requirements to provide user-friendliness:

1. **User anonymity**: The scheme must ensure the user anonymity to preserve the privacy of *MN*, i.e., $\mathcal{A}$ should not be able to discover the real identity of *MN*.
2. **Unlinkability**: To provide greater security for the user's privacy, the scheme should ensure unlinkability, i.e., $\mathcal{A}$ should not be able to trace the user's actions.
3. **Mutual authentication**: The schemes should support mutual authentication to ensure the legitimacy of each participant, i.e., *MN*, *FA*, and *HA* are capable of authenticating each other in the authentication phase.
4. **Session key agreement**: When the scheme permits the establishment of a session key between each of the participants, the session key that is used to encrypt and decrypt messages in the future communications should be fresh and provide the forward secrecy.
5. **Three-factor secrecy**: To ensure the secrecy of the user's private keys, the scheme should provide three-factor (e.g., identity, password, and biometrics) secrecy. The $\mathcal{A}$ should not be able to extract one secret value from the remaining two factors.
6. **Resilience to various attacks**: The scheme should provide all major security goals and should be resistant to different types of the known attacks.

Bio-hash function

The biometrics provides a unique identification method to solve the security vulnerabilities of passwords, pins, and tokens that are easy to forget or can be stolen. The imprint biometric characteristics may be slightly different each time due to a variety of reasons such as the user's dry or cracked skin, and the presence of dirt on the imprint sensor [42]. Therefore, high false rejection of genuine users that results in a denial of access often occur in the evaluation of biometric systems, and this consequently impacts on the usability of a system [43]. To resolve the problem of high false rejection instances, Jin et al. [44] proposed a two-factor authenticator in 2004 that is based on the iterated inner products between a tokenized pseudorandom number and the user-specific fingerprint features. To achieve this, a set of user-specific compact codes called the bio-hash code can be created. The bio-hash is a random mapping of biometric feature onto binary strings with user-specific tokenized pseudorandom numbers. In recent times, many authentication schemes using bio-hash have been proposed [45–47]. According to the recent bio-hash researches [48–51], the execution times of bio-hash are considered to be the same as the one-way hash function. In contrast, the execution time of the fuzzy extractor that is also generally used in biometric-system is considered to be the same as the elliptic-curve cryptography (ECC) [52]. Bio-hash is an effective technique for biometrics-based authentication schemes [53], and it is convenient mechanisms for small devices such as smart cards and mobile devices.

Review of Chaudhry et al.'s scheme

This section discusses Chaudhry et al.'s [32] user authentication scheme for roaming in ubiquitous networks. This scheme consists of the following three phases: (1) registration, (2) login

Table 1. Notations.

Values	Description
MN_i	Mobile node
FA_j	Foreign agent
HA_k	Home agent
ID_{mi}, ID_{fj}, ID_{hk}	Identities of MN_i, FA_j, HA_k
PW_{mi}	Password of MN_i
BIO_{mi}	Biometrics of MN_i
T_x	Timestamp of x
n_x	Random number of x
r_x	Random nonce for a specific purpose
SK_x	Session key of x
$E_k(\cdot)$, $D_k(\cdot)$	Symmetric encryption/decryption
$h(\cdot)$	Hash function
$H(\cdot)$	Bio-hash function
$\|\|$	Concatenation
$\oplus$	XOR operation
$K_{F,H}$	Pre-shared secret key between FA_j and HA_k
K_H	Private key of HA_k

https://doi.org/10.1371/journal.pone.0193366.t001

and authentication, and (3) password change. All of the notations that are used in this paper are presented in Table 1.

Registration phase

In the registration phase, MN_i registers with HA_k and the following operations are performed:

1. $MN_i \rightarrow HA_k$: ID_{mi}, $h(PW_{mi}||r_A||ID_{mi})$
   MN_i selects his/her identity ID_{mi} and password PW_{mi}, and generates r_A. MN_i then computes $h(PW_{mi}||r_A||ID_{mi})$ and sends a registration request message $\langle ID_{mi}, h(PW_{mi}||r_A||ID_{mi})\rangle$ to HA_k via a secure channel.

2. $HA_k \rightarrow MN_i$: PID_{mi}, A_{mi}
   HA_k verifies whether MN_i's ID_{mi} is valid. If it is valid, HA_k computes the following equations:

$$EID_{mi} = E_{h(K_H)}(ID_{mi}) \tag{1}$$

$$A_{mi} = h(K_H \oplus ID_{mi}) \oplus (PW_{mi}||r_A||ID_{mi}) \tag{2}$$

   HA_k then sends EID_{mi} and A_{mi} to MN_i via a secure channel.

3. MN_i retains the secret parameters EID_{mi}, A_{mi} and r_A in the mobile device.

Login and authentication phase

In this phase, MN_i and FA_j perform a mutual authentication to establish a session key with the support of MN_i's HA_k. It is assumed that each pair of FA_j and HA_k share pre-shared key $K_{F,H}$. The details of the login and authentication procedure, which are depicted in Fig 2 are as follows:

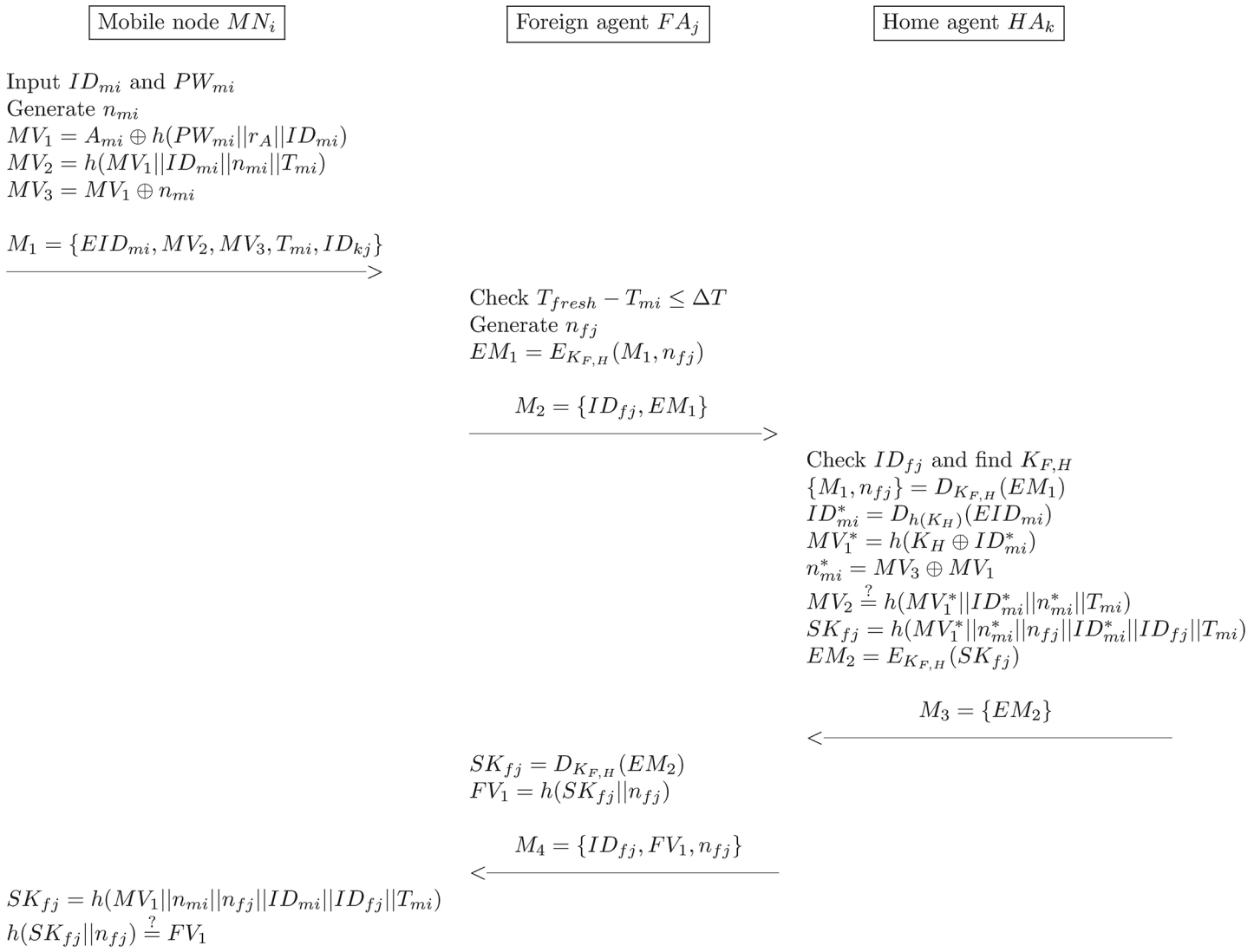

Fig 2. The login and authentication phase of Chaudhry et al.'scheme.

https://doi.org/10.1371/journal.pone.0193366.g002

1. $MN_i \rightarrow FA_j$: $M_1 = \langle PID_{mi}, MV_2, MV_3, T_{mi}, ID_{hk} \rangle$
   MN_i enters his/her ID_{mi} and PW_{mi}, generates the random number n_{mi}, and computes the following equations:

$$MV_1 = A_{mi} \oplus h(PW_{mi}||r_A||ID_{mi}) \tag{3}$$

$$MV_2 = h(MV_1||ID_{mi}||n_{mi}||T_{mi}) \tag{4}$$

$$MV_3 = MV_1 \oplus n_{mi} \tag{5}$$

   MN_i sends the login request message $M_1 = \langle EID_{mi}, MV_2, MV_3, T_{mi}, ID_{hk} \rangle$ to FA_j via a public channel.

2. $FA_j \rightarrow HA_k$: $M_2 = \langle ID_{fj}, EM_1) \rangle$
FA_j checks the freshness of T_{mi}. If it is fresh, FA_j generates the random number n_{fj} and computes as follows:

$$EM_1 = E_{K_{F,H}}(M_1, n_{fj}) \tag{6}$$

FA_j then sends the message $M_2 = \langle ID_{fj}, EM_1) \rangle$ to HA_k.

3. $HA_k \rightarrow FA_j$: $M_3 = \langle EM_2) \rangle$
HA_k checks ID_{fj} and finds its corresponding $K_{F,H}$. To obtain M_1 and n_{fj}, HA_k decrypts EM_1 and computes the following equations:

$$\{M_1, n_{fj}\} = D_{K_{F,H}}(EM_1) \tag{7}$$

$$ID^*_{mi} = D_{h(K_H)}(EID_{mi}) \tag{8}$$

$$MV^*_1 = h(K_H \oplus ID^*_{mi}) \tag{9}$$

$$n^*_{mi} = MV_3 \oplus MV^*_1 \tag{10}$$

Then, HA_k checks the validity of the following equation:

$$MV_2 \stackrel{?}{=} h(MV^*_1 || ID^*_{mi} || n^*_{mi} || T_{mi}) \tag{11}$$

If Eq (11) does not hold, this phase is terminated; otherwise, HA_k computes as follows:

$$SK_{fj} = h(MV^*_1 || n^*_{mi} || n_{fj} || ID^*_{mi} || ID_{fj} || T_{mi}) \tag{12}$$

$$EM_2 = E_{K_{F,H}}(SK_{fj}) \tag{13}$$

Lastly, HA_k sends the message $M_3 = \langle EM_2 \rangle$ to FA_j.

4. $FA_j \rightarrow MN_i$: $M_4 = \langle ID_{fj}, FV_1, n_{fj} \rangle$
To obtain SK_{fj}, FA_j decrypts the received message EM_2 and computes as follows:

$$SK_{fj} = D_{K_{F,H}}(EM_2) \tag{14}$$

$$FV_1 = h(SK_{fj} || n_{fj}) \tag{15}$$

Then, FA_j sends the message $M_4 = \langle ID_{fj}, FV_1, n_{fj} \rangle$ to MN_i.

5. To check validity of the session key, MN_i computes the following equations:

$$SK_{mi} = h(MV_1 || n_{mi} || n_{fj} || ID_{mi} || ID_{fj} || T_{mi}) \tag{16}$$

$$h(SK_{mi} || n_{fj}) \stackrel{?}{=} FV_1 \tag{17}$$

If Eq (17) does not hold, MN_i terminates connection; otherwise, MN_i accepts FA_j as legal and authenticated.

Password change phase

MN_i inputs ID_{mi}, a old password PW_{mi}^{old} and a new password PW_{mi}^{new} into his/her mobile device. The mobile device then computes the following equations:

$$MV_1 = A_{mi} \oplus h(PW_{mi}^{old}||r_A||ID_{mi}) \tag{18}$$

$$A_{mi}^{new} = MV_1 \oplus (PW_{mi}^{new}||r_A||ID_{mi}) \tag{19}$$

Lastly, the mobile device replaces A_{mi} with A_{mi}^{new}.

Cryptanalysis of Chaudhry et al.'s scheme

This section consists of the cryptanalysis of Chaudhry et al.'s scheme [32].

Stolen-mobile device attack

Under the previously explained adversarial model, it is assumed that $\mathcal{A}$ somehow acquires MN_i's mobile device, extracts the secret parameters, and captures the login request message M_1. Using the extracted parameters and the captured messages, $\mathcal{A}$ can attempt to guess MN_i's identity and password until the correct identity and password are found.

In [33, 34, 37, 38, 54], the identity and password can be guessed simultaneously after the user's device is stolen by $\mathcal{A}$; therefore, it is prudent to consider off-line identity and password guessing attacks.

Based on [37], $|\mathcal{D}_{id}| \leq |\mathcal{D}_{pw}| \approx 2^{20} \approx 10^6$. The time complexity to determine a identity and password is linear to $|\mathcal{D}_{id}|$ and $|\mathcal{D}_{pw}|$ because the more candidate data the attacker has, the more that matching operations are required to determine the desired value.

To demonstrate the vulnerability of Chaudhry et al.'s scheme [32] to the stolen-mobile device attack, the following scenario is used:

1. $\mathcal{A}$ eavesdrops the previous login messages $M_1 = \langle EID_{mi}, MV_2, MV_3, T_{mi}\rangle$, and compromises the secret parameters $\langle A_{mi}, EID_{mi}, r_A\rangle$ from the mobile device.
2. $\mathcal{A}$ selects any of the identity and password candidates ID_{mi}^* and PW_{mi}^*.
3. $\mathcal{A}$ computes $MV_2^* = h(A_{mi} \oplus h(PW_{mi}^*||r_A||ID_{mi}^*)||ID_{mi}^*||MV_3 \oplus A_{mi} \oplus h(PW_{mi}^*||r_A||ID_{mi}^*)||T_{mi})$.
4. $\mathcal{A}$ compares $MV_2^* \stackrel{?}{=} MV_2$.
5. If the comparison shows they are equal, $\mathcal{A}$ successfully guesses the correct ID_{mi} and PW_{mi}. Otherwise, $\mathcal{A}$ selects another identity and password, and repeats the steps 3 and 4 until he/she finds the correct identity and password.

In Chaudhry et al.'s scheme [32], the time complexity of the guessing attack process is $O(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * (2T_h + 3T_{XOR}))$, where T_h is the execution time of the hash operation and T_{XOR} is the execution time of the exclusive-or operation. Therefore, the time complexity of the guessing attack in Chaudhry et al.'s scheme is not negligible, and their scheme is consequently vulnerable to the stolen-mobile device attack.

User impersonation attack

This subsection presents a demonstration of the way that Chaudhry et al.'s scheme [32] allows $\mathcal{A}$ to impersonate a legal user if $\mathcal{A}$ obtains the MN_i's identity and password through a guessing attack, as presented in the previous subsection, as follows:

1. $\mathcal{A}$ obtains the secret parameters $\langle A_{mi}, EID_{mi}, r_A \rangle$, correctly guessing the identity ID^*_{mi} and password PW^*_{mi} of MN_i by completing the stolen-mobile device attack.
2. The mobile device of $\mathcal{A}$ generates the random number n_{ai}, and computes the following equation:

$$MV^*_1 = A_{mi} \oplus h(PW^*_{mi}||r_A||ID^*_{mi})$$
$$MV^*_2 = h(MV^*_1||ID^*_{mi}||n_{ai}||T_A)$$
$$MV^*_3 = MV^*_1 \oplus n_{ai}$$

   $\mathcal{A}$ sends the login request message $M^*_1 = \langle EID_{mi}, MV^*_2, MV^*_3, T_A \rangle$ to FA_j, where T_A is the current timestamp of $\mathcal{A}$.
3. Because of the validation of M^*_1, FA_j and HA_k successfully proceed the subsequent steps of the authentication phase. Lastly, FA_j sends the message $M_4 = \langle ID_{fj}, FV_1, n_{fj} \rangle$ to MN_i, but $\mathcal{A}$ receives M_4 and computes the following equations:

$$SK_A = h(MV^*_1||n_A||n_{fj}||ID^*_{mi}||ID^*_{fj}||T_A) \quad (20)$$

$$h(SK_A||n_{fj}) \stackrel{?}{=} FV_1 \quad (21)$$

   If Eq (21) holds, $\mathcal{A}$ has successfully established a session key with FA_j.

   Therefore, Chaudhry et al.'s scheme [32] is vulnerable to the user impersonation attack.

Absence of the incorrect login-input detection

The detection of the incorrect login inputs must be performed at the beginning of the login phase. However, Chaudhry et al.'s scheme [32] does not support the incorrect input detection during the login and authentication phase. In their scheme, the MN_i sends the message M_1 without verifying the correctness of the ID_{mi} and PW_{mi}. Even if MN_i mistakenly enters the wrong ID'_{mi} and PW'_{mi}, the mobile device can still compute $MV'_1 = A_{mi} \oplus h(PW'_{mi}||r_A||ID'_{mi})$, $MV'_2 = h(MV'_1||ID'_{mi}||n_{mi}||T_{mi})$ and $MV'_3 = MV'_1 \oplus n_{mi}$. As a result, an invalid form of the login request message, M_1, is transmitted to HA_k through FA_j, thereby resulting in unnecessary computations and communication costs.

Incorrectness of the password change phase

Chaudhry et al.'s scheme [32] allows the user to change his/her password easily without any server assistance. However, in the password change phase, the mobile device does not check the accuracy of the old password when MN_i enters the old and new passwords to replace the old password with a new password. If MN_i enters the old password incorrectly, an incorrect MV_1 is computed with Eq (18), and an incorrect A^{new}_{mi} is also computed with Eq (19). As a result, $h(K_H \oplus ID_{mi})$ will be damaged beyond the possibility of a restoration, thereby causing HA_k's rejection of MN_i in the future authentication phase.

No provision for revocation

The revocation of a stolen or lost mobile device is essential for the practical deployment of smart card-based authentication schemes [55]. If a legal MN_i's mobile device is lost or stolen, some kind of mechanism must be in place to prevent the misuse of the mobile device. To address this problem, the server needs to maintain the identity information that will serve as

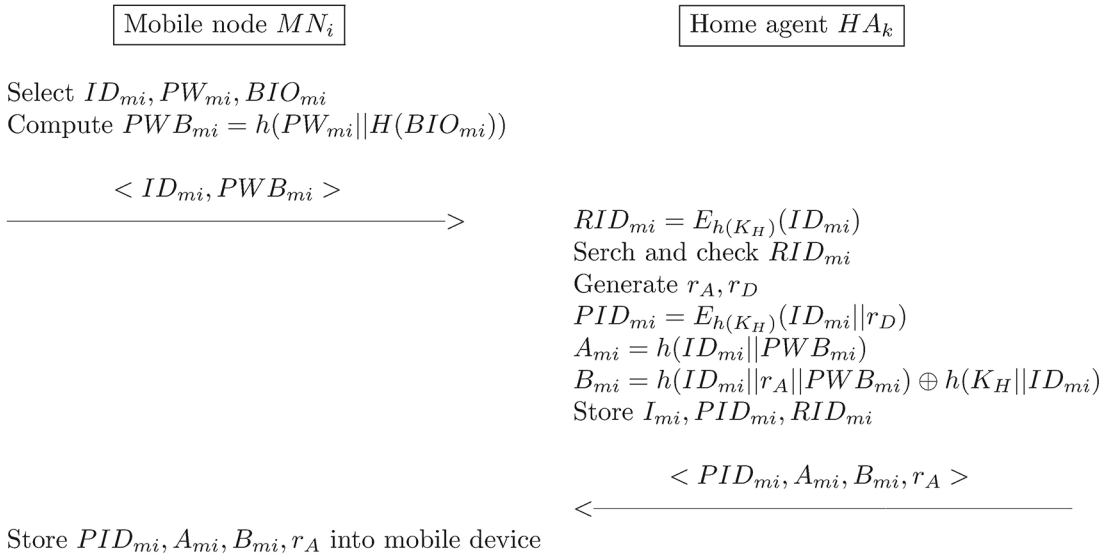

Fig 3. The registration phase of the proposed scheme.

https://doi.org/10.1371/journal.pone.0193366.g003

the basis for the detection of the invalid mobile device [56]. However, Chaudhry et al.'s scheme [32] scheme does not take this feature into consideration.

Proposed scheme

This section contains the proposal for the improved and anonymous biometrics-based authentication scheme for roaming in ubiquitous networks. The proposed scheme consists of the following three phases: (1) registration, (2) login and authentication, (3) password change, and (4) mobile-device revocation.

Registration phase

The registration phase for the mobile user MN_i that are illustrated in Fig 3 involves the following operations:

1. $MN_i \rightarrow HA_k$: ID_{mi}, PWB_{mi}
   MN_i selects his/her ID_{mi} and PW_{mi} and inputs BIO_{mi}. MN_i then computes the following equation:
   $$PWB_{mi} = h(PW_{mi}||H(BIO_{mi})) \quad (22)$$
   MN_i subsequently sends a registration request message $\langle ID_{mi}, PWB_{mi} \rangle$ to HA_k via a secure channel.
2. $HA_k \rightarrow MN_i$: PID_{mi}, A_{mi}, B_{mi}, r_A
   HA_k then verifies the identity of MN_i and computes the following equation:
   $$RID_{mi} = E_{h(K_H)}(ID_{mi}) \quad (23)$$
   HA_k searches RID_{mi} in the database to verify the presence of an already registered user with the same ID_{mi}; if this is verified, HA_k requests a new identity from MN_i. Otherwise HA_k

gernerates r_A and r_D, and computes the following equations:

$$PID_{mi} = E_{h(K_H)}(ID_{mi}||r_D) \tag{24}$$

$$A_{mi} = h(ID_{mi}||PWB_{mi}) \tag{25}$$

$$B_{mi} = h(ID_{mi}||r_A||PWB_{mi}) \oplus h(K_H||ID_{mi}) \tag{26}$$

If MN_i is a new user, HA_k sets I_{mi} to zero, otherwise, $I_{mi} = I_{mi} + 1$. HA_k then stores I_{mi}, PID_{mi}, and RID_{mi} as a tuple in the database, and it sends $\langle PID_{mi}, A_{mi}, B_{mi}, r_A \rangle$ to MN_i via a secure channel.

3. MN_i stores all of the received parameters into the mobile device.

Login and authentication phase

In this phase, MN_i and FA_j perform a mutual authentication to establish a session key with the support of MN_i's HA_k. It is assumed here that each pair of FA_j and HA_k share the pre-shared key $K_{F,H}$. The details of the login and authentication procedure that are illustrated in Fig 4 are as follows:

1. $MN_i \rightarrow FA_j$: $M_1 = \langle PID_{mi}, MV_2, MV_3, ID_{hk} \rangle$
   MN_i enters his/her ID_{mi}, PW_{mi}, and BIO_{mi}, and it then computes as follows:

$$PWB_{mi} = h(PW_{mi}||H(BIO_{mi})) \tag{27}$$

   HA_k then checks the validity of:

$$A_{mi} \stackrel{?}{=} h(ID_{mi}||PWB_{mi}) \tag{28}$$

   If Eq (28) does not hold, MN_i terminates the user's login request. Otherwise, MN_i generates n_{mi} and computes the following equations:

$$MV_1 = B_{mi} \oplus h(ID_{mi}||r_A||PWB_{mi}) \tag{29}$$

$$MV_2 = h(MV_2||ID_{mi}||n_{mi}) \tag{30}$$

$$MV_3 = MV_1 \oplus n_{mi} \tag{31}$$

   MN_i then sends the login request message $M_1 = \langle PID_{mi}, MV_2, MV_3, ID_{hk} \rangle$ to FA_j.

2. $FA_j \rightarrow HA_k$: $M_2 = \langle ID_{fj}, FV_2, FV_3, M_1 \rangle$
   FA_j generates the random number n_{fj} and computes the following equations:

$$FV_1 = h(K_{F,H}||MV_2||MV_3) \tag{32}$$

$$FV_2 = FV_1 \oplus n_{fj} \tag{33}$$

$$FV_3 = h(FV_1||FV_2||n_{fj}) \tag{34}$$

   FA_j sends the message $M_2 = \langle ID_{fj}, FV_2, FV_3, M_1 \rangle$ to HA_k.

Mobile node MN_i	Foreign agent FA_j	Home agent HA_k
Input $ID_{mi}, PW_{mi}, BIO_{mi}$ $PWB_{mi} = h(PW_{mi}\|\|H(BIO_{mi}))$ Check $A_{mi} \stackrel{?}{=} h(ID_{mi}\|\|PWB_{mi})$ Generate n_{mi} $MV_1 = B_{mi} \oplus h(ID_{mi}\|\|r_A\|\|PWB_{mi})$ $MV_2 = h(MV_1\|\|ID_{mi}\|\|n_{mi})$ $MV_3 = MV_1 \oplus n_{mi}$ $M_1 = \{PID_{mi}, MV_2, MV_3, ID_{hk}\}$ $\longrightarrow$		
	Generate n_{fj} $FV_1 = h(K_{F,H}\|\|MV_2\|\|MV_3)$ $FV_2 = FV_1 \oplus n_{fj}$ $FV_3 = h(FV_1\|\|FV_2\|\|n_{fj})$ $M_2 = \{ID_{fj}, FV_2, FV_3, M_1\}$ $\longrightarrow$	
		Check ID_{fj} and find $K_{F,H}$ $FV_1^* = h(K_{F,H}\|\|MV_2\|\|MV_3)$ $n_{fj}^* = FV_1^* \oplus FV_2$ $FV_3 \stackrel{?}{=} h(FV_1^*\|\|FV_2\|\|n_{fj}^*)$ $\{ID_{mi}^*, r_D\} = D_{h(K_H)}(PID_{mi})$ $MV_1^* = h(K_H\|\|ID_{mi}^*)$ $n_{mi}^* = MV_1^* \oplus MV_3$ $MV_2 \stackrel{?}{=} h(MV_1^*\|\|ID_{mi}^*\|\|n_{mi}^*)$ Generate r_D^{new} $PID_{mi}^{new} = E_{h(K_H)}(ID_{mi}^*\|\|r_D^{new})$ $SK_{fj} = h(MV_1^*\|\|ID_{mi}^*\|\|ID_{fj}\|\|n_{mi}^*)$ $HV_1 = SK_{fj} \oplus h(K_{F,H}\|\|n_{fj}^*)$ $HV_2 = h(K_{F,H}\|\|SK_{fj}\|\|ID_{hk})$ $M_3 = \{PID_{mi}^{new}, HV_1, HV_2\}$ $\longleftarrow$
	$SK_{fj} = HV_1 \oplus h(K_{F,H}\|\|n_{fj})$ $HV_2 \stackrel{?}{=} h(K_{F,H}\|\|SK_{fj}\|\|ID_{hk})$ $FV_4 = h(SK_{fj}\|\|ID_{fj})$ $M_4 = \{PID_{mi}^{new}, ID_{fj}, FV_4\}$ $\longleftarrow$	
$SK_{mi} = h(MV_1\|\|ID_{mi}\|\|ID_{fj}\|\|n_{mi})$ $FV_4^* = h(SK_{mi}\|\|ID_{fj})$ $FV_4^* \stackrel{?}{=} FV_4$		

Fig 4. The login and authentication phase of the proposed scheme.

https://doi.org/10.1371/journal.pone.0193366.g004

3. $HA_k \longrightarrow FA_j : M_3 = \langle PID_{mi}^{new}, HV_1, HV_2) \rangle$
HA_k checks ID_{fj} to find its corresponding $K_{F,H}$ and computes the following equations:

$$FV_1^* = h(K_{F,H}||MV_2||MV_3) \tag{35}$$

$$n_{fj}^* = FV_1^* \oplus FV_2 \tag{36}$$

$$FV_3 \stackrel{?}{=} h(FV_1^*||FV_2||n_{fj}^*) \tag{37}$$

If Eq (37) does not hold, this phase is terminated; otherwise, HA_k accepts FA_j as legitimate. HA_k then computes the following equations:

$$\{ID_{mi}^*, r_D\} = D_{h(K_H)}(PID_{mi}) \tag{38}$$

$$MV_1^* = h(K_H||ID_{mi}^*) \tag{39}$$

$$n_{mi}^* = MV_1^* \oplus MV_3 \tag{40}$$

$$MV_2 \stackrel{?}{=} h(MV_1^*||ID_{mi}||n_{mi}) \tag{41}$$

If Eq (41) does not hold, this phase is terminated; otherwise, HA_k accepts MN_i as legitimate. HA_k then generates r_D^{new} and computes the following equations:

$$PID_{mi}^{new} = E_{h(K_H)}(ID_{mi}^*||r_D^{new}) \tag{42}$$

$$SK_{fj} = h(MV_1^*||ID_{mi}^*||ID_{fj}||n_{mi}^*) \tag{43}$$

$$HV_1 = SK_{fj} \oplus h(K_{F,H}||n_{fj}^*) \tag{44}$$

$$HV_2 = h(K_{F,H}||SK_{fj}||ID_{hk}) \tag{45}$$

HA_k then replaces PID_{mi} with PID_{mi}^{new}, and it then sends the message $M_3 = \langle PID_{mi}^{new}, HV_1, HV_2 \rangle$ to FA_j.

4. $FA_j \longrightarrow MN_i : M_4 = \langle PID_{mi}^{new}, ID_{fj}, FV_4 \rangle$
FA_j computes the following equations:

$$SK_{fj} = HV_1 \oplus h(K_{F,H}||n_{fj}) \tag{46}$$

$$HV_2 \stackrel{?}{=} h(K_{F,H}||SK_{fj}||ID_{hk}) \tag{47}$$

If Eq (47) does not hold, FA_j terminates the connection; otherwise, FA_j computes the following equation:

$$FV_4 = h(SK_{fj}||ID_{fj}) \tag{48}$$

FA_j then sends the message $M_4 = \langle PID_{mi}^{new}, ID_{fj}, FV_4 \rangle$ to MN_i.

5. MN_i computes the following equations to check the validity of the session key:

$$SK_{mi} = h(MV_1||ID_{mi}||ID_{fj}||n_{mi}) \tag{49}$$

$$FV_4^* = h(SK_{mi}||ID_{fj}) \tag{50}$$

$$FV_4^* \stackrel{?}{=} FV_4 \tag{51}$$

If Eq (51) does not hold, MN_i terminates the connection; otherwise, MN_i accepts FA_j as legal and authenticated. That is, MN_i, FA_j and HA_j have all successfully established the same session key, SK. Lastly, MN_i replaces PID_{mi} with PID_{mi}^{new}.

Password change phase

In this phase, MN_i changes its password on the mobile device without the help of the HA. The details of the password change phase that are illustrated in Fig 5 are as follows:

1. MN_i inputs ID_{mi}, BIO_{mi}, a old password PW_{mi}^{old} and a new password PW_{mi}^{new} into his/her mobile device. MN_i then computes the following equations:

$$PWB_{mi}^{old} = h(PW_{mi}^{old}||H(BIO_{mi})) \tag{52}$$

$$A_{mi} \stackrel{?}{=} h(ID_{mi}||PWB_{mi}^{old}) \tag{53}$$

If Eq (57) does not hold, MN_i terminates this phase; otherwise, MN_i computes the following equations:

$$MV_1 = A_{mi} \oplus h(PWB_{mi}^{old}||r_A||ID_{mi}) \tag{54}$$

$$PWB_{mi}^{new} = h(PW_{mi}^{new}||H(BIO_{mi})) \tag{55}$$

$$B_{mi}^{new} = MV_1 \oplus h(PWB_{mi}^{new}||r_A||ID_{mi}) \tag{56}$$

$$A_{mi}^{new} = h(ID_{mi}||PWB_{mi}^{new}) \tag{57}$$

Finally, MN_i replaces A_{mi}^{old} and B_{mi}^{old} with A_{mi}^{new} and B_{mi}^{new}, respectively.

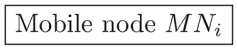

Fig 5. The password change phase of the proposed scheme.

https://doi.org/10.1371/journal.pone.0193366.g005

Mobile device revocation phase

To recover a stolen/lost mobile device or a long-term key of MN_i, the mobile device revocation mechanism that is illustrated in Fig 6 is activated as follows:

1. $MN_i \longrightarrow HA_k : ID_{mi}^{old}, ID_{mi}^{new}, PWB_{mi}^{new}$
   If MN_i wants to revoke and reissue a secret parameter, MN_i selects an old identity ID_{mi}^{old} and a new identity ID_{mi}^{new}, inputs a new password PW_{mi}^{new} and BIO_{mi} into his/her mobile device. MN_i then computes the following equation:

$$PWB_{mi}^{new} = h(PW_{mi}^{new}||H(BIO_{mi})) \tag{58}$$

   MN_i subsequently sends a revocation request message $\langle ID_{mi}^{old}, ID_{mi}^{new}, PWB_{mi}^{new} \rangle$ to HA_k via a secure channel.

2. $HA_k \rightarrow MN_i$: A_{mi}, B_{mi}
   HA_k then verifies the identity of MN_i and computes the following equation:

$$RID_{mi}^{old} = E_{h(K_H)}(ID_{mi}^{old}) \tag{59}$$

   HA_k searches RID_{mi}^{old} in the database to verify the presence of a registered user. If this is the case, HA_k generates the new random nonces r_A^{new} and r_D^{new}, and computes the following equations:

$$PID_{mi}^{new} = E_{h(K_H)}(ID_{mi}^{new}||r_D^{new}) \tag{60}$$

$$A_{mi}^{new} = h(ID_{mi}^{new}||PWB_{mi}^{new}) \tag{61}$$

$$B_{mi}^{new} = h(ID_{mi}^{new}||r_A^{new}||PWB_{mi}^{new}) \oplus h(K_H||ID_{mi}^{new}) \tag{62}$$

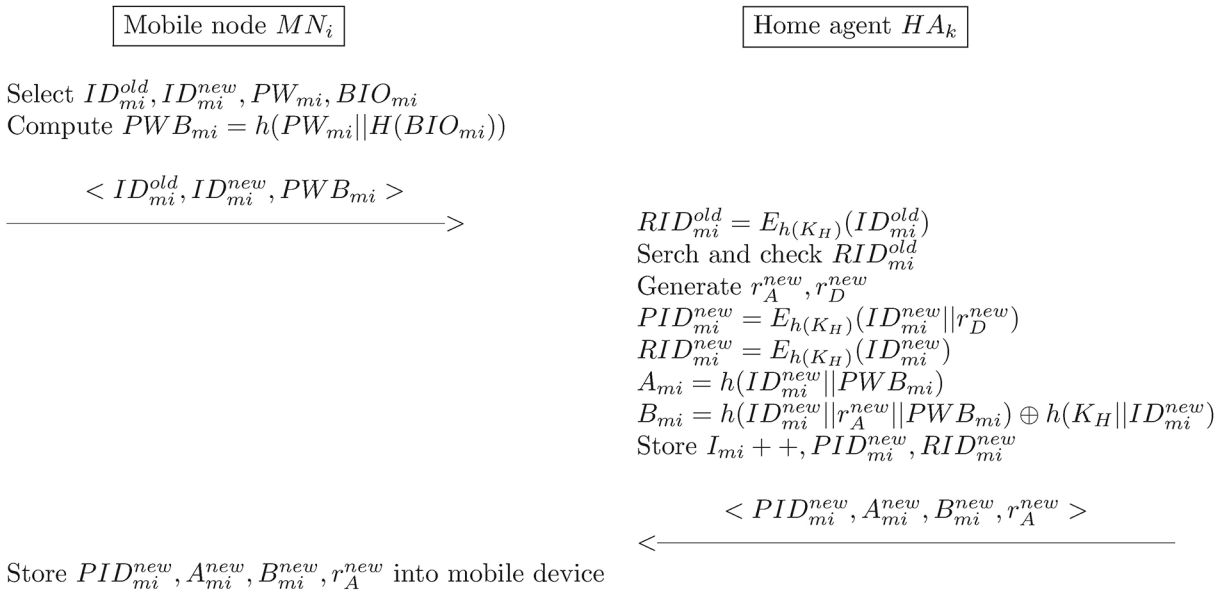

Fig 6. The revocation phase of the proposed scheme.

https://doi.org/10.1371/journal.pone.0193366.g006

HA_k updates I_{mi}, PID_{mi}, and RID_{mi} with $I_{mi} = I_{mi} + 1$, PID_{mi}^{new}, and RID_{mi}^{new}, respectively. It then sends $\langle PID_{mi}^{new}, A_{mi}^{new}, B_{mi}^{new}, r_A^{new} \rangle$ to MN_i via a secure channel.

3. Finally, MN_i stores all of the received parameters into the mobile device.

Security analysis

In this section, a security analysis of the proposed scheme is performed using formal and informal verification methods. The formal analysis is conducted using automatic analysis tool named ProVerif and a random oracle model.

Formal verification using ProVerif

ProVerif is an automatic tool for analyzing cryptographic protocols according to the formal model (the so-called Dolev–Yao model). It supports a wide range of cryptographic primitives that are defined by rewrite rules or equations, as follows: asymmetric and symmetric en/decryption, digital signatures, and hash functions. This tool can prove the various security properties as follows: secrecy, authentication, and process equivalences of the protocol with unlimited sessions and message space [57].

The verification structure of ProVerif is illustrated in Fig 7. First, ProVerif takes as its input a protocol description to perform a verification in a dialect of the applied pi calculus, which is an extension of the pi-calculus and is a language for describing and analyzing protocols.

It also takes an input the security properties that are being proven here. It then automatically translates this protocol description into Horn clauses and the security properties into derivability queries on these clauses, and it determines whether a fact can be proved from these clauses using an algorithm that is based on a resolution with a free selection. If the fact is

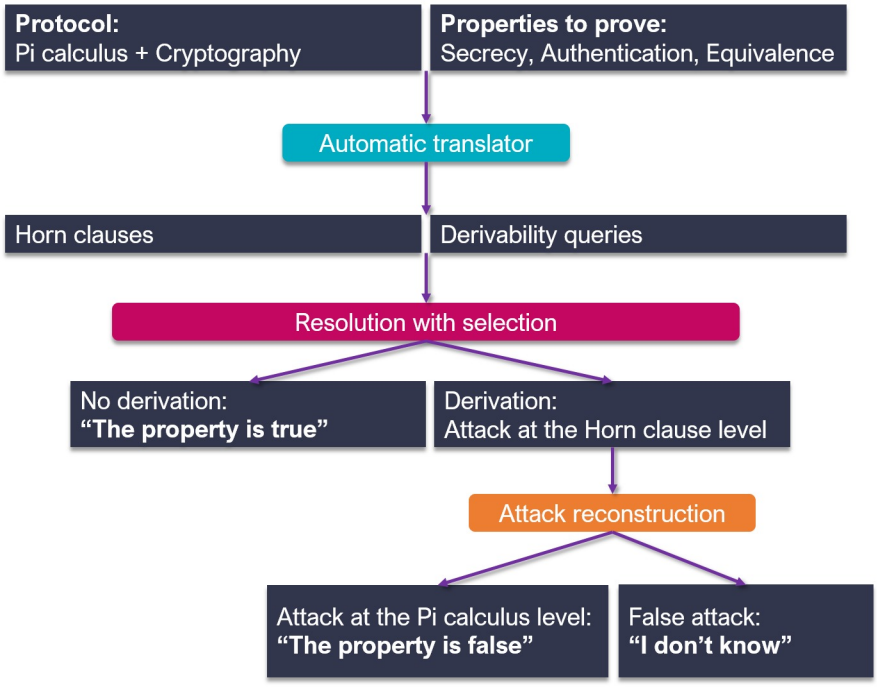

Fig 7. Structure of ProVerif.

https://doi.org/10.1371/journal.pone.0193366.g007

not derivable, the corresponding security properties are proved. If the fact is derivable, the protocol may be vulnerable to an attack against the corresponding security properties. Actually, the derivation either corresponds to a real attack or a false attack, since the problem of the protocol verifications for an unbounded number of sessions is not decidable.

Recently, many researchers [58–61] have used ProVerif to verify the security of the schemes for the key agreement and authentication. In this section, the security of the proposed scheme is proven using ProVerif, where the ProVerif code is introduced as a description of the proposed scheme, and the analysis results are then provided.

The definitions for the process of the proposed scheme are shown in Fig 8, wherein the following identifiers are used: "cha" denotes the private channel between the MN_i and HA_k; "chb" and "chc" denote the public channels between the MN_i and FA_j and the FA_j and HA_k, respectively; "IDmi", "PWmi", and "BIOmi" denote the private MN identity, password, and biometrics, respectively; "IDfj" and "IDhk" denote the public identity of FA_j and HA_k, respectively. "KH" denotes the HA_k's private key; "KFH" denotes the pre-shared key between the FA_j and HA_k; "SKfj" denotes a HA_k-generated session key that is transmitted to the FA_j; and "SKmi" denotes an MN_i-generated session key. The constructors for the operations of the concatenation, symmetric cryptography, exclusive-or, one-way hash, and bio-hash are defined from the lines 18 to 22. In addition, the destructors for the symmetric decryption and exclusive-or operations are defined in the lines 23 and 24. In the lines 26 to 31, six events that indicate the start and end of each node are defined to verify the correspondence relations for the messages of each node.

Fig 9 shows the code for the entire MN_i process. The MN_i process of the registration phase is modeled in the lines 34 to 36. The MN_i process of the login and authentication phase is modeled in the lines 37 to 50.

Fig 10 shows the code for the entire FA_j process. The FA_j process of the login and authentication phase is modeled in the lines 53 to 70.

Fig 11 shows the code for the entire HA_k process. The HA_k process of the registration phase is modeled in the lines 73 to 80. The HA_k process of the login and authentication phase is modeled in the lines 81 to 101.

The code for the modeling of the adversary capabilities and the verifying of the interprocess equivalences is shown in Fig 12. The lines 103 to 104 prove that the session keys SKfj and SKmi are secret and unknown to the adversary. The lines 105 to 107 verify the internodal relationships to determine the execution of the proposed scheme in the correct order.

When the code that defines the elements that are needed to configure the protocol is run, ProVerif prints the results in the following format:

1. RESULT inj–event[Event] ==> inj–event[Event] is true: The event is proved; for example, the authentication of A to B or the others hold.
2. RESULT inj–event[Event] ==> inj–event[Event] is false: The event is not proved; that is, the authentication of A to B or the others does not hold
3. RESULT [Query] is true: The query is proved, so there is no attack. In this case, ProVerif displays no attack derivation and no attack trace.
4. RESULT [Query] is false: The query is false, as ProVerif has discovered an attack against the desired security property. The attack traces with the attack derivations, which represent the real attack, are displayed.

The execution of the ProVerif code for the verification of the security and the authentication of the proposed scheme produces the simulation result, as shown in Fig 13, thereby

```
(*......chanels......*)
free cha:channel [private].
free chb:channel.
free chc:channel.
(*......constants......*)
free IDmi:bitstring [private].
free IDfj:bitstring.
free IDhk:bitstring.
free PWmi:bitstring [private].
free BIOmi:bitstring [private].
(*......secret key......*)
free KH:bitstring [private].
free KFH:bitstring [private].
(*......shared key......*)
free SKfj:bitstring [private].
free SKmi:bitstring [private].
(*......functions......*)
fun concat(bitstring,bitstring) : bitstring.
fun syme(bitstring,bitstring):bitstring.
fun xor(bitstring,bitstring):bitstring.
fun h(bitstring):bitstring.
fun H(bitstring):bitstring.
reduc forall ma:bitstring, key:bitstring; symd(syme(ma,key),key)=ma.
equation forall p:bitstring, q:bitstring; xor(xor(p,q), q)=p.
(*......events......*)
event beginHAgent(bitstring).
event endHAgent(bitstring).
event beginFAgent(bitstring).
event endFAgent(bitstring).
event beginMNode(bitstring).
event endMNode(bitstring).
```

Fig 8. ProVerif code for definitions.

https://doi.org/10.1371/journal.pone.0193366.g008

verifying the accuracy of the results for all of the events and queries. That is, the successful mutual authentication of the proposed scheme has been achieved as the mutual communication with all of the authentication factors among MN_i, FA_j, and HA_k, as defined by the previously mentioned events. Furthermore, the session keys of the proposed scheme are secure against the adversary; therefore, the proposed scheme can be considered as secure against simulated attacks.

```
(*.....MN's process.....*)
let pMNode=
let PWBmi = h(concat(PWmi,H(BIOmi))) in
out(cha,(IDmi,PWBmi));
in(cha,(XPIDmi:bitstring,XAmi:bitstring,XBmi:bitstring,XrA:bitstring));
event beginMNode(IDmi);
new nmi:bitstring;
let Ami=h(concat(IDmi,PWBmi)) in
if XAmi=Ami then
let MV1=xor(XBmi,h(concat(IDmi,concat(XrA,PWBmi)))) in
let MV2=h(concat(MV1,concat(IDmi, nmi))) in
let MV3=xor(MV1,nmi) in
let M1=concat(XPIDmi,concat(MV2,concat(MV3,IDhk))) in
out(chc,(M1));
in(chc,XM4:bitstring);
let(XXNPIDmi:bitstring, XXIDfj:bitstring, XFV4:bitstring) = XM4 in
let SKmi=h(concat(MV1, concat(IDmi,concat(XXIDfj,nmi)))) in
let FV4'=h(concat(SKmi,XXIDfj)) in
if(FV4' = XFV4) then event endMNode(IDmi).
```

Fig 9. ProVerif code for entire MN process.

https://doi.org/10.1371/journal.pone.0193366.g009

Formal verification using the random oracle model

In this section, the formal security analysis of the proposed scheme is demonstrated using the random oracle model. For this, we define a hash function and symmetric cryptography as follows:

Definition 1. A hash function h: $\{0, 1\}^* \rightarrow \{0, 1\}^n$ is a one-way function that takes an input $x \in \{0, 1\}^*$ of an arbitrary length and outputs a bit string with a fixed-length $h(x) \in \{0, 1\}^n$ and it satisfies the following three security requirements:

- It is computationally infeasible to find an input x such that $y = h(x)$.
- It is computationally infeasible to find another input $x' \neq x$ such that the $h(x') = h(x)$.
- It is computationally infeasible to find the inputs (x, x'), with $x' \neq x$, such that $h(x') = h(x)$.

Definition 2. A symmetric cryptography $\prod = (E, K, KSPC, MSPC)$ is a pair of algorithms that is associated with the finite sets, $KSPC(k)$ and $MSPC(k)$, $\{0, 1\}^*$, for $k \in N$.

- E, called the encryption algorithm, is a deterministic algorithm that takes a pair of the strings, a and x and produces $y = E_a(x)$.
- D, called the decryption algorithm, is a deterministic algorithm that takes a pair of the strings, a and y and outputs the string $x = D_a(y)$

It is required here, for any $k \in N$, if $a \in KSPC(k)$, $x \in MSPC$, any $y = E_a(x)$, then $D_a(y) = x$.

```
(*.....FA's process.....*)
let pFAgent=
in(chc, (XM1:bitstring));
event beginFAgent(IDfj);
new nfj:bitstring;
let (XXPIDmi:bitstring,XMV2:bitstring,XMV3:bitstring, XIDhk:bitstring) = XM1 in
let FV1=h(concat(KFH,concat(XMV2,XMV3))) in
let FV2=xor(FV1,nfj) in
let FV3=h(concat(FV1,concat(FV2,nfj))) in
let M2=concat(IDfj,concat(FV2,concat(FV3,XM1))) in
out(chb,(M2));
in(chb,(XM3:bitstring));
let (XNPIDmi:bitstring, XHV1:bitstring, XHV2:bitstring)=XM3 in
let XSKfj=xor(XHV1,h(concat(KFH,nfj))) in
let HV2'=h(concat(KFH,concat(XSKfj,XIDhk))) in
if HV2'=XHV2 then
let FV4=h(concat(XSKfj,IDfj)) in
let M4 = concat(XNPIDmi,concat(IDfj,FV4)) in
out(chc,(M4));
event endFAgent(IDfj).
```

Fig 10. ProVerif code for entire FA process.

https://doi.org/10.1371/journal.pone.0193366.g010

Theorem 1. Under the assumption that the one-way hash function and the symmetric cryptography closely behave like an oracle, then the proposed scheme is provably secure against $\mathcal{A}$ for the protection of the identity ID_{mi} of MN_i, and the private key K_H of HA_k.

Reveal: Given the hash result $y = h(x)$, this random oracle will unconditionally output the input x.

Extract: Given the cipher text $C = E_{K_x}(P)$, this random oracle will unconditionally output the plain text P.

Proof. A method for the formal security proof that is similar to that used in [62–64] is applied in the proposed scheme. For the proof, it is assumed that $\mathcal{A}$ is able to derive ID_{mi} and K_H. For this, $\mathcal{A}$ runs the experimental algorithm that is shown in Algorithm 1, $EXP1^{IAUAS,A}_{HASH,SYMM}$ for the proposed improved and anonymous user authentication scheme, called IAUAS. The success probability of $EXP1^{IAUAS,A}_{HASH,SYMM}$ is defined by the following equation:

$$Success1^{IAUAS,A}_{HASH,SYMM} = |Pr[EXP1^{IAUAS,A}_{HASH,SYMM} = 1] - 1| \tag{63}$$

The advantage function for this experiment becomes as following equation:

$$Adv1^{IAUAS,A}_{HASH,SYMM}(t, q_R, q_E) = max_A\{Success1^{IAUAS,A}_{HASH,SYMM}\} \tag{64}$$

in which the maximum is determined by all of $\mathcal{A}$ with the execution time t and the number of queries q_R and q_E that are made to the Reveal and Extract oracles, respectively. If $\mathcal{A}$ is able to

```
(*.....HA's process.....*)
let pHAgent=
in(cha,(XIDmi:bitstring, XPWBmi:bitstring));
new rA:bitstring;
new rD:bitstring;
let RIDmi=syme(XIDmi, h(KH)) in
let PIDmi=syme(concat(XIDmi, rD), h(KH)) in
let Ami=h(concat(XIDmi,XPWBmi)) in
let Bmi=xor(h(concat(XIDmi,concat(rA,XPWBmi))),h(concat(KH,XIDmi))) in
out(cha,(PIDmi,Ami,Bmi));
event beginHAgent(IDhk);
in(chb, XM2:bitstring);
let (XIDfj:bitstring, XFV2:bitstring, XFV3:bitstring, XXM1:bitstring) = XM2 in
let (XXXPIDmi:bitstring,XXMV2:bitstring,XXMV3:bitstring, XXrA:bitstring) = XXM1 in
let FV1'=h(concat(KFH,concat(XXMV2,XXMV3))) in
let nfj'=xor(FV1',XFV2) in
let FV3'=h(concat(FV1',concat(XFV2,nfj'))) in
if FV3'=XFV3 then
let (IDmi':bitstring, rD':bitstring) = symd(XXXPIDmi,h(KH)) in
let MV1'=h(concat(KH,IDmi)) in
let nmi'=xor(MV1',XXMV3) in
let MV2'=h(concat(MV1',concat(IDmi',nmi'))) in
if MV2'=XXMV2 then
new NrD:bitstring;
let NPIDmi=syme(concat(IDmi',NrD),h(KH)) in
let SKfj=h(concat(MV1', concat(IDmi', concat(XIDfj, nmi')))) in
let HV1=xor(SKfj,h(concat(KFH,nfj'))) in
let HV2=h(concat(KFH,concat(SKfj,IDhk))) in
let M3=concat(NPIDmi,concat(HV1,HV2)) in
out(chb, (M3));
event endHAgent(IDhk).
```

Fig 11. ProVerif code for entire HA process.

https://doi.org/10.1371/journal.pone.0193366.g011

invert the hash function and the symmetric cryptography that are provided in Definitions 1 and 2, $\mathcal{A}$ can directly derive ID_{mi} and K_H. Consider the attack experiment that is shown in Algorithm 1. In this case, $\mathcal{A}$ will discover the complete connections between all of the participants. However, it is computationally infeasible to invert the input from the given hash and encrypted values, i.e., $Adv1^{IAUAS,A}_{HASH,SYMM}(t) \leq \epsilon, \forall \epsilon > 0$. Then, $Adv1^{IAUAS,A}_{HASH,SYMM}(t, q_R, q_E) \leq \epsilon$ is obtained, because it depends on $Adv1^{IAUAS,A}_{HASH,SYMM}(t)$. Since $Adv1^{IAUAS,A}_{HASH,SYMM}(t) \leq \epsilon$ is negligible,

```
(*.....quries.....*)
query attacker(SKfj).
query attacker(SKmi).
query id:bitstring; inj-event(endFAgent(id)) ==> inj-event(beginFAgent(id)).
query id:bitstring; inj-event(endHAgent(id)) ==> inj-event(beginHAgent(id)).
query id:bitstring; inj-event(endMNode(id)) ==> inj-event(beginMNode(id)).

process
        ((!pMNode)|(!pFAgent)|(!pHAgent))
```

Fig 12. ProVerif code for adversary capabilities and verifying equivalences verification.

https://doi.org/10.1371/journal.pone.0193366.g012

```
RESULT inj-event(endMNode(id)) ==> inj-event(beginMNode(id)) is true.
RESULT inj-event(endHAgent(id_14906)) ==> inj-event(beginHAgent(id_14906)) is true.
RESULT inj-event(endFAgent(id_42859)) ==> inj-event(beginFAgent(id_42859)) is true.
RESULT not attacker(SKmi[]) is true.
RESULT not attacker(SKfj[]) is true.
```

Fig 13. ProVerif simulation result of the proposed scheme.

https://doi.org/10.1371/journal.pone.0193366.g013

$Adv1^{IAUAS,A}_{HASH,SYMM}(t, q_R, q_E) \leq \epsilon$ is also negligible. As a result, $\mathcal{A}$ cannot compute the ID_{mi} and K_H and the proposed scheme is provably secure against $\mathcal{A}$ for the deriving of them.

Algorithm 1: Algorithm $EXP1^{IAUAS,A}_{HASH,SYMM}$

1. Eavesdrop login request message $\langle PID_{mi}, MV_2, MV_3, ID_{hk} \rangle$ during the login and authentication phase.
2. Call the Reveal oracle. Let $(MV'_1, ID'_{mi}, n'_{mi}) \leftarrow Reveal(MV_2)$
3. Call the Extract oracle. Let $(ID''_{mi}, r'_D) \leftarrow Reveal(PID_{mi})$
4. Computes $MV'_3 = MV'_1 \oplus h(n'_{mi})$
5. **if** $(MV'_3 = MV_3$ && $ID''_{mi} = ID'_{mi})$ **then**
6. Call the Reveal oracle. Let $(K'_H, ID'''_{mi}, r''_D) \leftarrow Reveal(MV'_1)$
7. **if** $(ID'_{mi} = ID'''_{mi}$ && $r'_D = r''_D)$ **then**
8. Compute $PID'_{mi} = E_{h(K'_H)}(ID'''_{mi}, r''_D)$
9. **if** $(PID_{mi} = PID'_{mi})$ **then**
10. **Accept K'_H as the correct secret key K_H of HA_k**
11. **Accept ID'_{mi} as the correct secret key ID_{mi} of MN_i**
12. **return 1 (Success)**
13. **else**
14. **return 0**
15. **end if**
16. **else**
17. **return 0**
18. **end if**
19. **else**
20. **return 0**
21. **end if**

Theorem 2. Under the assumption that the one-way hash function and the symmetric cryptography closely behave like an oracle, then the proposed scheme is provably secure against $\mathcal{A}$ for the protection of ID_{mi}, PW_{mi}, and BIO_{mi} of MN_i, and the private key K_H of HA_k.

Proof. For this proof, it is assumed that $\mathcal{A}$ is able to derive ID_{mi}, PW_{mi}, BIO_{mi} and K_H after extracting the secret parameters A_{mi}, B_{mi}, and C_{mi} that are stored in the mobile device using side-channel attacks [33, 34, 65]. $\mathcal{A}$ runs the experimental algorithm $EXP2^{IAUAS,A}_{HASH,SYMM}$ that is shown in Algorithm 2. The success of the probability of $EXP2^{IAUAS,A}_{HASH,SYMM}$ is defined as the following equation:

$$Success2^{IAUAS,A}_{HASH,SYMM} = |Pr[EXP2^{IAUAS,A}_{HASH,SYMM} = 1] - 1| \tag{65}$$

The advantage function for this experiment becomes as following equation:

$$Adv2^{IAUAS,A}_{HASH,SYMM}(t_2, q_R, q_E) = max_A\{Success2^{IAUAS,A}_{HASH,SYMM}\} \tag{66}$$

in which the maximum is determined by all of $\mathcal{A}$ with the execution time t_2 and the number of queries q_R and q_E that are made to the Reveal and Extract oracles, respectively. If $\mathcal{A}$ is able to invert the hash function and the symmetric cryptography, $\mathcal{A}$ can directly derive ID_{mi}, PW_{mi}, BIO_{mi}, and K_H. Consider the attack experiment that is shown in Algorithm 2. It is computationally infeasible to invert the input from given hash and encrypted values, i.e., $Adv2^{IAUAS,A}_{HASH,SYMM}(t_2) \leq \epsilon, \forall \epsilon > 0)$. Then, $Adv2^{IAUAS,A}_{HASH,SYMM}(t_2, q_R, q_E) \leq \epsilon$ is obtained, because it depends on $Adv2^{IAUAS,A}_{HASH,SYMM}(t)$. Since $Adv2^{IAUAS,A}_{HASH,SYMM}(t) \leq \epsilon$ is negligible, $Adv2^{IAUAS,A}_{HASH,SYMM}(t_2, q_R, q_E) \leq \epsilon$ is also negligible. As a result, $\mathcal{A}$ cannot compute the ID_{mi}, PW_{mi}, BIO_{mi}, and K_H, and the proposed scheme is provably secure against $\mathcal{A}$ for deriving them even if the mobile device is stolen by $\mathcal{A}$.

Algorithm 2: Algorithm $EXP2^{IAUAS,A}_{HASH,SYMM}$

1. Extract the information $\{PID_{mi}, A_{mi}, B_{mi}, r_A, h(\cdot), H(\cdot)\}$ that is stored in the mobile device through a physical monitoring of its power consumption.
2. Call the Reveal oracle. Let $(ID'_{mi}, PWB'_{mi}) \leftarrow Reveal(A_{mi})$
3. Call the Reveal oracle. Let $(PW'_{mi}, BIO'_{mi}) \leftarrow Reveal(PWB'_{mi})$
4. Computes $A'_{mi} = h(ID'_{mi}||PWB''_{mi}) = h(ID'_{mi}||h(PW'_{mi}||H(BIO'_{mi})))$
5. **if** $(A'_{mi} = A_{mi})$ **then**
6. **Accepts** PW'_{mi} **and** BIO'_{mi} **as the correct** PW_{mi} **and** BIO_{mi} **of** MN_i
7. Call the Extract oracle. Let $(ID''_{mi}, r'_D) \leftarrow Reveal(PID_{mi})$
8. **if** $(ID''_{mi} = ID'_{mi})$ **then**
9. Compute $F_1 = h(ID'_{mi}||r_A||PWB''_{mi})$
10. Compute $F_2 = F_1 \oplus B'_{mi} = h(K_H||ID_{mi}||r_D)$
11. Call the Reveal oracle. Let $(K'_H||ID'''_{mi}||r''_D) \leftarrow Reveal(F_1)$
12. **if** $(ID'''_{mi} = ID'_{mi}$ && $r'_D = r''_D)$ **then**
13. **Accepts** ID'_i **as the correct** ID_i **of user** MN_i
14. Compute $PID_{mi} = E_{h(k'_H)}(ID'_{mi}, r'_D)$
15. **if** $(PID'_{mi} = PID_{mi})$ **then**
16. **Accept** K'_H **as the correct secret key** K_H **of** HA_k
17. **return 1 (Success)**
18. **else**
19. **return 0**
20. **end if**
21. **else**
22. **return 0**
23. **end if**

```
24.   else
25.     return 0
26.   end if
27. else
28.   return 0
29. end if
```

Informal verification

In this section, we perform an informal security analysis of the proposed scheme to prove that it is secure against the various security threats. According to the adversarial model that is described in the preliminary knowledge section, $\mathcal{A}$ can perform the following attacks to undermine the security of the proposed scheme.

i. $\mathcal{A}$ has full control over the public communication channel, eavesdropping on the messages M_1, M_2, M_3, and M_4, and then inserting new values or removing a value.

ii. If $\mathcal{A}$ obtains a stolen or lost mobile device of a user in some way, he/she is able to extract the PID_{mi}, A_{mi}, B_{mi}, and r_A from the device using side-channel attacks [33, 34].

iii. $\mathcal{A}$ has the ability to make an offline guessing attack within a polynomial time and can try to threaten the privacy of the user by enumerating the eavesdropped messages and the extracted parameters.

Table 2 shows the analysis summary of the comparison of the proposed scheme with the related schemes [26–29, 32].

Table 2. Comparative summary: Security requirements.

Property	Jiang et al. [27]	Wen et al. [28]	Farash et al. [29]	Gope and Hwang [30]	Wu et al. [31]	Chaudhry et al. [32]	Proposed scheme
SR_1	O	O	X	O	O	X	O
SR_2	O	O	O	O	O	O	O
SR_3	O	X	X	X	O	X	O
SR_4	O	X	X	O	O	O	O
SR_5	O	O	O	O	O	O	O
SR_6	O	O	X	O	O	X	O
SR_7	X	X	X	O	O	O	O
SR_8	X	O	X	O	X	X	O
SR_9	X	X	O	O	O	O	O
SR_{10}	O	O	O	O	O	O	O
SR_{11}	O	O	X	O	O	X	O
SR_{12}	O	X	X	X	O	O	O
SR_{13}	O	O	O	O	O	O	O
SR_{14}	X	X	X	X	O	X	O
SR_{15}	X	X	X	X	X	X	O

SR_1: user anonymity; SR_2: untraceability; SR_3: resistance to stolen-mobile device or smart card attack; SR_4: mutual authentication; SR_5: session key agreement; SR_6: resistance to impersonation attack; SR_7: resistance to replay attack; SR_8: local user verification process; SR_9: resistance to stolen-verifier attack; SR_{10}: resistance to privileged-insider attack; SR_{11}: user-friendly password change; SR_{12}: forward secrecy; SR_{13}: resistance to foreign bypass attack; SR_{14}: does not need time synchronization; SR_{15}: provision of the revocation phase;

https://doi.org/10.1371/journal.pone.0193366.t002

User anonymity

In the proposed scheme, the pseudo-identity $PID_{mi} = E_{h(K_H)}(ID_{mi}||r_D)$ that varies each session by r_D is used. After MN_i is authenticated by HA_k in Eq (41), HA_k replaces the existing PID_{mi} with a new PID_{mi}^{new} using a new r_D^{new}. Then, PID_{mi}^{new} is transmitted to MN_i that has been encrypted with HA_k's private key K_H in Eq (42). Therefore, even if $\mathcal{A}$ obtains PID_{mi} by eavesdropping the public messages or extracting the secret parameters stored in the mobile device, the proposed scheme guarantees the user anonymity because it is not possible for $\mathcal{A}$ to know the real identity ID_{mi} of MN_i.

User untraceability

In the login and authentication phase, MN_i sends PID_{mi}, MV_2 and MV_3 via a public channel. They contain n_{mi} and r_D, which are changed for each session. That is, $\mathcal{A}$ cannot trace MN_i's actions in the proposed scheme because these parameters are computed each time with a different value. Therefore, the proposed scheme ensures the user untraceability.

Stolen-mobile device attack

With the proposed scheme, $\mathcal{A}$ needs to know K_H to guess ID_{mi} and PW_{mi}; however, K_H is not stored in the mobile device directly, nor it is transmitted via the public channel as plaintext. Also, even if $\mathcal{A}$ finds this value somehow, he/she still cannot guess PW_{mi} without $H(BIO_{mi})$ that is unique to only MN_i. Therefore, the proposed scheme withstands the stolen-mobile device attack.

Mutual authentication

In the proposed scheme, MN_i and FA_j authenticate each other with the assistance of HA_k. Only a legitimate MN_i can compute MV_1 that $\mathcal{A}$ cannot compute because of PWB_{mi}. Accordingly, HA_k authenticates only the legitimate MN_i using Eq (41). Also, only the legitimate HA_k is authenticated by MN_i through the verification of $FV_4^* \stackrel{?}{=} FV_2$, as shown in Eq (51). Only FA_j and HA_k that share $K_{F,H}$ can verify each other using the same key to compute valid messages, and only they can compute and obtain a valid session key, SK. Therefore, the adversary or invalid participants cannot carry out the login and authentication phase. Furthermore, FA_j authenticates HA_k by performing Eq (47). After it receives M_4, MN_i can verify that $FV_4^* \stackrel{?}{=} FV_4$ using Eq (51) to authenticate FA_j and to establish the session key, SK. Therefore, the proposed scheme achieves the mutual authentication.

Session key agreement

After the login and authentication process, FA_j receives HV_1 and obtains the session key SK_{fj} from HA_k, and MN_i generates the session key SK_{mi}. As a result, only the legitimate MN_i and FA_j establish the same session key $SK_{mi} = h(MV_1||ID_{mi}||ID_{fj}||n_{mi}) = SK_{fj}$. Therefore, the proposed scheme provides a secure session key agreement.

User impersonation attack

With the proposed scheme, the user impersonation attack is prevented by the mutual authentication, local user-verification process, and prevention of the stolen-mobile-device attack. Furthermore, the proposed scheme provides a secure session key agreement. Therefore, the proposed scheme ensures the prevention of the user impersonation attack.

Replay attack

$\mathcal{A}$ might replay an old login request message M_1 to FA_j and receive the message M_4 from FA_j. However, $\mathcal{A}$ still cannot compute the correct session key SK as he/she is not capable of computing ID_{mi} and n_{mi} without K_H. Furthermore, $\mathcal{A}$ cannot derive the session key, SK, without $K_{F,H}$. Therefore, the proposed scheme is secure against the replay attack.

Local user verification process

With the proposed scheme, mobile devices verify the legality of the user. Only a user who enters the correct ID_{mi}, PW_{mi}, and BIO_{mi} can pass the user-verification process, as given by Eq (28). In addition, since BIO_{mi} of each individual user is unique, $\mathcal{A}$ cannot attempt an illegal access.

Stolen-verifier attack

In the login and authentication phase of the proposed scheme, HA_k does not store and receive any of the credentials of MN_i such as PW_{mi} and $H(BIO_{mi})$. Furthermore, HA_k retains RID_{mi} in the database; however, $\mathcal{A}$ cannot know the real identity of MN_i even if $\mathcal{A}$ steals the user registration information from HA_k's database. Therefore, the proposed scheme withstands the stolen-verifier attack.

Privileged-insider attack

In the registration phase of the proposed scheme, MN_i sends ID_{mi} and PWB_{mi} to HA_k. Here, PWB_{mi} contains $H(BIO_{mi})$. The insider of HA_k cannot derive MN_i's password PW_{mi}. Therefore, he/she cannot try to impersonate MN_i to access FA_j. Furthermore, MN_i can change his/her password, PWB_{mi}, without the assistance of HA_k in the password change phase. Since it is not possible for the insider to know the MN_i's password, PW_{mi}, the proposed scheme resists the privileged-insider attack.

User-friendly password change

Generally, it is recommended that the performance of the password change process is without any server involvement, thereby providing a user-friendliness and an improvement of the computational efficiency. In the password change phase of the proposed scheme, the existing user password is self-verified in the user's mobile device, and it is replaced by the new password only if it passes the verification process. Therefore, the proposed scheme supports an efficient password change phase.

Forward secrecy

In the proposed scheme, even though the generated session key between all of the participants can be compromised by $\mathcal{A}$, he/she cannot recover any earlier session keys because the session key $SK_{mi} = h(MV_1||ID_{mi}||ID_{fj}||n_{mi}) = SK_{fj}$ is different each time. Consequently, a significant correlation was not found between the past, current, and future session keys. Therefore, the proposed scheme ensures the forward secrecy.

Foreign bypass attack

During the authentication phase of the proposed scheme, $\mathcal{A}$ may try to construct the messages M_1 and M_2 using the parameters that are stored in a stolen mobile device and transmitted over a public channel to impersonate a legitimate FA_j. However, $\mathcal{A}$r cannot compute FV_1, because

$K_{F,H}$ is not public information. Thus, $\mathcal{A}$ cannot construct a sufficient message to cheat HA_k. Eventually, $\mathcal{A}$ is unable to impersonate a valid FA_j.

Does not need time synchronization

In many authentication schemes, timestamps are used to resist the replay attack. However, by using the timestamp in the authentication scheme, the clocks of MN_i and HA_k must be synchronized beforehand. In the synchronization process, there is the possibility that time synchronization error occurs; therefore, to prevent this problem, the proposed scheme only uses random-number-based authentication mechanism instead of timestamps.

Provision of the revocation phase

In the proposed scheme, if MN_i's mobile device is stolen/lost or a secret parameter/authentication factor is revealed, HA_k can issues new secret parameters to MN_i for the purpose of recovery. HA_k retains RID_{mi} that is encrypted with the real identity of MN_i, in the database. When HA_k receives a revocation request with ID_m *i* from MN_i, HA_k computes $RID_{mi}^{old} = E_{K_H}(ID_{mi})$ and compares it with the existing RID_{mi} that is stored in the database to verify that MN_i is registered and legitimate. Therefore, the proposed scheme can cope with unexpected problems by supporting the revocation phase.

Performance analysis

In this section, we perform the comparisons of the computational and communication cost of the proposed scheme with the related schemes [27–32].

Comparisons of the computational costs

We consider four cryptographic operations: hash function T_h, the symmetric en/decryption T_s, the ECC-based asymmetric en/decryption T_e, and the modular exponent operation T_m were considered. The authors [66] measured the approximate execution time of each cryptographic operation on the following central processing unit (CPU): Intel(R) Core(TM)2T6570 2.1GHz, 4G memory, OS:Win7 32-bit, and Visual C++ 2008 software using the MIRACL C/C++ library. The authors considered the 1024-bit Rivest–Shamir–Adleman (RSA) algorithm, the 320-bit ECC algorithm, the 128-bit Advanced Encryption Standard (AES) algorithm, and the 160-bit Secure Hash Algorithm 1 (SHA-1) hash function, and the experiment the results are $T_m \approx 1.8269$ms, $T_e \approx 1.6003$ms, $T_s \approx 0.1303$ms, and $T_h \approx 0.0004$ms, respectively. The registration and password change phases were excluded from the comparison because the registration phase of the mobile node occurs only once and the password change phase can be executed only within *MN*. Therefore, only the login and authentication phase was considered in the comparison, because this phase frequently occurs during the intercommunication between participants when the mobile node accesses the ubiquitous networks and the roaming occurs.

Table 3 shows the comparative summary in terms of the computational costs of *MN*, *FA*, and *HA*, as well as the total cost of the different participants. The result of the proposed scheme is 0.2614ms, while the results of the schemes of Jiang et al., Wen et al., Farash et al., Gope and Hwang, Wu et al., and Chaudhry et al. are 3.6543ms, 7.3081ms, 0.5217ms, 3.6543ms, 6.9232ms, and 0.6519ms, respectively. The Table 3 highlights that the computational cost of the proposed scheme is lowest in comparison with the related schemes.

Table 3. Comparative summary: Computational cost.

	Jiang et al. [27]	Wen et al. [28]	Farash et al. [29]	Gope and Hwang [30]	Wu et al. [31]	Chaudhry et al. [32]	Proposed scheme
MN	$3T_h + 1T_m$	$4T_h + 1T_m$	$6T_h$	$4T_h + 1T_m$	$8T_h + 2T_e$	$5T_h$	$7T_h$
FA	$4T_h$	$4T_h + 1T_m$	$1T_h + 2T_s$	$4T_h$	$4T_h + 1T_s + 2T_e$	$1T_h + 2T_s$	$4T_h$
HA	$5T_h + 1T_m$	$5T_h + 2T_m$	$5T_h + 2T_s$	$4T_h + 1T_m$	$8T_h + 3T_s$	$4T_h + 3T_s$	$9T_h + 2T_s$
Total	$12T_h + 2T_m$	$13T_h + 4T_m$	$12T_h + 4T_s$	$12T_h + 2T_m$	$20T_h + 4T_s + 4T_e$	$10T_h + 5T_s$	$20T_h + 2T_s$
Time(ms)	3.6543	7.3081	0.5217	3.6543	6.9232	0.6519	0.2614

https://doi.org/10.1371/journal.pone.0193366.t003

Table 4. Comparative summary: Communication cost.

Mssage	Jiang et al. [27]	Wen et al. [28]	Farash et al. [29]	Gope and Hwang [30]	Wu et al. [31]	Chaudhry et al. [32]	Proposed scheme
M_1	1152	1152	608	1152	864	736	704
M_2	1504	1440	384	1440	1280	384	1152
M_3	320	320	256	320	736	256	576
M_4	224	160	448	160	1056	448	544
Total (bits)	3200	3072	1696	3072	3936	1824	2976

https://doi.org/10.1371/journal.pone.0193366.t004

Comparisons of the communication costs

For the communication costs, a comparison of the login and authentication phases that referred to [67, 68] was performed, and it is assumed that the lengths of the identity, random number, and timestamp are 128 bits, 64 bits, and 32 bits, respectively. The hash function and the symmetric-key encryption produce 160 bits and 256 bits, respectively. For the asymmetric-key encryption, the modular prime operation and the scalar multiplication operation on the elliptic curve produces 1024 bits and 320bits, respectively.

Table 4 provides the data of the comparisons of the communication costs of the login and authentication phases of the proposed scheme with the other existing schemes. The total communication cost of proposed scheme is 2976 bits, while the schemes of Jiang et al., Wen et al., Farash et al., Gope and Hwang, Wu et al., and Chaudhry et al. are 3200 bits, 3072 bits, 1696 bits, 3072 bits, 3936 bits, and 1824 bits, respectively. Although the total communication costs of the scheme of Farash et al. and Chaudhry et al. are less than that of the proposed scheme, their schemes are insecure, as previously mentioned. Therefore, the proposed scheme is a more practical option for the ubiquitous network environment.

Conclusion

In this paper, Chaudhry et al.'s authentication scheme for roaming in ubiquitous networks is reviewed, and the scheme's ongoing vulnerability to several attacks is proven; furthermore, the improved proposed scheme resolves the security issues of Chaudhry et al.'s scheme. To demonstrate the security of the proposed scheme, informal and formal analyses were performed using the random oracle model and the automated verification tool, ProVerif. Also, the performance evaluation that was conducted with related works shows that the proposed scheme is suitable for resource-constrained ubiquitous environments.

Author Contributions

Software: Hakjun Lee, Donghoon Lee, Jongho Moon, Jaewook Jung, Dongwoo Kang, Dongho Won.

Validation: Hyoungshick Kim.

Writing – original draft: Hakjun Lee.

Writing – review & editing: Hakjun Lee, Hyoungshick Kim.

References

1. Lambrechts J, Sinha S. Microsensing networks for sustainable cities. Smart sensors, measurement and instrumentation (ISSN 2194-8402). 2016; 18.
2. Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS. The internet of things for health care: a comprehensive survey. IEEE Access. 2015; 3:678–708. https://doi.org/10.1109/ACCESS.2015.2437951
3. Rabari C, Storper M. The digital skin of cities: urban theory and research in the age of the sensored and metered city, ubiquitous computing and big data. Cambridge Journal of Regions, Economy and Society. 2014; 8(1):27–42. https://doi.org/10.1093/cjres/rsu021
4. Yeh CK, Lee WB. An Overall Cost-effective Authentication Technique for the Global Mobility Network. IJ Network Security. 2009; 9(3):227–232.
5. Chaudhry SA, Farash MS, Naqvi H, Kumari S, Khan MK. An enhanced privacy preserving remote user authentication scheme with provable security. Security and Communication Networks. 2015; 8 (18):3782–3795. https://doi.org/10.1002/sec.1299
6. Mishra D. Efficient and secure two-factor dynamic ID-based password authentication scheme with provable security. Cryptologia. 2017; p. 1–30.
7. Choi Y, Lee Y, Moon J, Won D. Security enhanced multi-factor biometric authentication scheme using bio-hash function. PLoS ONE. 2017; 12(5):e0176250. https://doi.org/10.1371/journal.pone.0176250 PMID: 28459867
8. Lee Y, Kim S, Won D. Enhancement of two-factor authenticated key exchange protocols in public wireless LANs. Computers & electrical engineering. 2010; 36(1):213–223. https://doi.org/10.1016/j.compeleceng.2009.08.007
9. Choo KKR, Nam J, Won D. A mechanical approach to derive identity-based protocols from Diffie–Hellman-based protocols. Information Sciences. 2014; 281:182–200. https://doi.org/10.1016/j.ins.2014.05.041
10. Moon J, Choi Y, Jung J, Won D. An improvement of robust biometrics-based authentication and key agreement scheme for multi-server environments using smart cards. PLoS ONE. 2015; 10(12): e0145263. https://doi.org/10.1371/journal.pone.0145263 PMID: 26709702
11. Nam J, Choo KKR, Han S, Kim M, Paik J, Won D. Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation. PLoS ONE. 2015; 10(4):e0116709. https://doi.org/10.1371/journal.pone.0116709 PMID: 25849359
12. Kang D, Jung J, Mun J, Lee D, Choi Y, Won D. Efficient and robust user authentication scheme that achieve user anonymity with a Markov chain. Security and Communication Networks. 2016; 9 (11):1462–1476. https://doi.org/10.1002/sec.1432
13. Chaudhry SA, Naqvi H, Mahmood K, Ahmad HF, Khan MK. An improved remote user authentication scheme using elliptic curve cryptography. Wireless Personal Communications. 2017; 96(4):5355–5373. https://doi.org/10.1007/s11277-016-3745-3
14. Chaturvedi A, Mishra D, Jangirala S, Mukhopadhyay S. A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme. Journal of Information Security and Applications. 2017; 32:15–26. https://doi.org/10.1016/j.jisa.2016.11.002
15. Mishra D, Mukhopadhyay S, Kumari S, Khan MK, Chaturvedi A. Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. Journal of medical systems. 2014; 38(5):41. https://doi.org/10.1007/s10916-014-0041-1 PMID: 24771484
16. Srinivas J, Mishra D, Mukhopadhyay S, Kumari S. Provably secure biometric based authentication and key agreement protocol for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing. 2017; p. 1–21.
17. Ignatenko T, Willems FM. Biometric systems: Privacy and secrecy aspects. IEEE Transactions on Information Forensics and Security. 2009; 4(4):956–973. https://doi.org/10.1109/TIFS.2009.2033228
18. Wazid M, Das AK, Kumari S, Li X, Wu F. Provably secure biometric-based user authentication and key agreement scheme in cloud computing. Security and Communication Networks. 2016; 9(17):4103–4119. https://doi.org/10.1002/sec.1591

19. Jung J, Kang D, Lee D, Won D. An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated EPR information system. PLoS ONE. 2017; 12(1): e0169414. https://doi.org/10.1371/journal.pone.0169414 PMID: 28046075
20. Odelu V, Das AK, Kumari S, Huang X, Wazid M. Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. Future Generation Computer Systems. 2017; 68:74–88. https://doi.org/10.1016/j.future.2016.09.009
21. Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. IEEE Transactions on Consumer Electronics. 2004; 50(1):231–235. https://doi.org/10.1109/TCE.2004.1277867
22. Lee CC, Hwang MS, Liao IE. Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Transactions on Industrial Electronics. 2006; 53(5):1683–1687. https://doi.org/10.1109/TIE.2006.881998
23. Wu CC, Lee WB, Tsaur WJ. A secure authentication scheme with anonymity for wireless communications. IEEE Communications Letters. 2008; 12(10).
24. Mun H, Han K, Lee YS, Yeun CY, Choi HH. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Mathematical and Computer Modelling. 2012; 55(1):214–222. https://doi.org/10.1016/j.mcm.2011.04.036
25. Zhao D, Peng H, Li L, Yang Y. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. Wireless Personal Communications. 2014; 78(1):247–269. https://doi.org/10.1007/s11277-014-1750-y
26. He D, Chan S, Chen C, Bu J, Fan R. Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. Wireless Personal Communications. 2011; 61(2):465–476. https://doi.org/10.1007/s11277-010-0033-5
27. Jiang Q, Ma J, Li G, Yang L. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wireless Personal Communications. 2013; 68(4):1477–1491. https://doi.org/10.1007/s11277-012-0535-4
28. Wen F, Susilo W, Yang G. A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. Wireless personal communications. 2013; 73(3):993–1004. https://doi.org/10.1007/s11277-013-1243-4
29. Farash MS, Chaudhry SA, Heydari M, Sadough S, Mohammad S, Kumari S, et al. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. International Journal of Communication Systems. 2017; 30(4). https://doi.org/10.1002/dac.3019
30. Gope P, Hwang T. Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks. Wireless Personal Communications. 2015; 82(4):2231–2245. https://doi.org/10.1007/s11277-015-2344-z
31. Wu F, Xu L, Kumari S, Li X, Khan MK, Das AK. An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks. Annals of Telecommunications. 2017; 72(3-4):131–144. https://doi.org/10.1007/s12243-016-0547-2
32. Chaudhry SA, Albeshri A, Xiong N, Lee C, Shon T. A privacy preserving authentication scheme for roaming in ubiquitous networks. Cluster Computing. 2017; 20(2):1223–1236. https://doi.org/10.1007/s10586-017-0783-x
33. Jiang Q, Ma J, Yang C, Ma X, Shen J, Chaudhry SA. Efficient end-to-end authentication protocol for wearable health monitoring systems. Computers & Electrical Engineering. 2017; 63:182–195. https://doi.org/10.1016/j.compeleceng.2017.03.016
34. Wu F, Xu L, Kumari S, Li X, Khan MK, Das AK. An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks. Annals of Telecommunications. 2016; p. 1–14.
35. Kumari S. Design flaws of an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. Multimedia Tools and Applications. 2017; 76 (11):13581–13583. https://doi.org/10.1007/s11042-016-3771-x
36. Kumari S, Khan MK, Li X. A more secure digital rights management authentication scheme based on smart card. Multimedia Tools and Applications. 2016; 75(2):1135–1158. https://doi.org/10.1007/s11042-014-2361-z
37. Wang D, Gu Q, Cheng H, Wang P. The request for better measurement: A comparative evaluation of two-factor authentication schemes. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM; 2016. p. 475–486.
38. Jiang Q, Zeadally S, Ma J, He D. Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks. IEEE Access. 2017; 5:3376–3392. https://doi.org/10.1109/ACCESS.2017.2673239

39. Feng Q, He D, Zeadally S, Wang H. Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. Future Generation Computer Systems. 2017;.
40. Odelu V, Banerjee S, Das AK, Chattopadhyay S, Kumari S, Li X, et al. A secure anonymity preserving authentication scheme for roaming service in global mobility networks. Wireless Personal Communications. 2017; 96(2):2351–2387. https://doi.org/10.1007/s11277-017-4302-4
41. Srinivas J, Mukhopadhyay S, Mishra D. A self-verifiable password based authentication scheme for multi-server architecture using smart card. Wireless Personal Communications. 2017; 96(4):6273–6297. https://doi.org/10.1007/s11277-017-4476-9
42. Mishra D, Das AK, Mukhopadhyay S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Systems with Applications. 2014; 41 (18):8129–8143. https://doi.org/10.1016/j.eswa.2014.07.004
43. Srinivas J, Mukhopadhyay S, Mishra D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Networks. 2017; 54:147–169. https://doi.org/10.1016/j.adhoc.2016.11.002
44. Jin ATB, Ling DNC, Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition. 2004; 37(11):2245–2255. https://doi.org/10.1016/j.patcog.2004.04.011
45. Chaudhry SA, Naqvi H, Farash MS, Shon T, Sher M. An improved and robust biometrics-based three factor authentication scheme for multiserver environments. The Journal of Supercomputing. 2015; p. 1–17.
46. Khan I, Chaudhry SA, Sher M, Khan JI, Khan MK. An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data. The Journal of Supercomputing. 2016; p. 1–19.
47. Chaudhry SA, Naqvi H, Khan MK. An enhanced lightweight anonymous biometric based authentication scheme for TMIS. Multimedia Tools and Applications. 2017; p. 1–22.
48. Mishra D, Vijayakumar P, Sureshkumar V, Amin R, Islam SH, Gope P. Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimedia Tools and Applications. 2017; p. 1–31.
49. Amin R, Biswas G. A novel user authentication and key agreement protocol for accessing multi-medical server usable in tmis. Journal of medical systems. 2015; 39(3):33. https://doi.org/10.1007/s10916-015-0217-3 PMID: 25681100
50. Amin R, Biswas G. A secure three-factor user authentication and key agreement protocol for tmis with user anonymity. Journal of medical systems. 2015; 39(8):78. https://doi.org/10.1007/s10916-015-0258-7 PMID: 26112322
51. Moon J, Choi Y, Kim J, Won D. An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. Journal of medical systems. 2016; 40(3):70. https://doi.org/10.1007/s10916-015-0422-0 PMID: 26743628
52. Jung J, Moon J, Lee D, Won D. Efficient and Security Enhanced Anonymous Authentication with Key Agreement Scheme in Wireless Sensor Networks. Sensors. 2017; 17(3):644. https://doi.org/10.3390/s17030644
53. Kumari S, Li X, Wu F, Das AK, Choo KKR, Shen J. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Generation Computer Systems. 2017; 68:320–330. https://doi.org/10.1016/j.future.2016.10.004
54. Jiang Q, Khan MK, Lu X, Ma J, He D. A privacy preserving three-factor authentication protocol for e-Health clouds. The Journal of Supercomputing. 2016; 72(10):3826–3849. https://doi.org/10.1007/s11227-015-1610-x
55. Mishra D, Chaturvedi A, Mukhopadhyay S. Design of a lightweight two-factor authentication scheme with smart card revocation. Journal of Information Security and Applications. 2015; 23:44–53. https://doi.org/10.1016/j.jisa.2015.06.001
56. Jiang Q, Ma J, Wei F. On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Systems Journal. 2016;. https://doi.org/10.1109/JSYST.2016.2574719
57. Blanchet B, et al. Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif. Foundations and Trends® in Privacy and Security. 2016; 1(1-2):1–135. https://doi.org/10.1561/3300000004
58. Karuppiah M, Kumari S, Li X, Wu F, Das AK, Khan MK, et al. A Dynamic ID-Based Generic Framework for Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks. Wireless Personal Communications. 2016; p. 1–25.

59. Wu F, Xu L, Kumari S, Li X, Shen J, Choo KKR, et al. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications. 2016;.

60. Kumari S, Chaudhry SA, Wu F, Li X, Farash MS, Khan MK. An improved smart card based authentication scheme for session initiation protocol. Peer-to-Peer Networking and Applications. 2017; 10(1):92–105. https://doi.org/10.1007/s12083-015-0409-0

61. Chaudhry SA, Khan I, Irshad A, Ashraf MU, Khan MK, Ahmad HF. A provably secure anonymous authentication scheme for Session Initiation Protocol. Security and Communication Networks. 2016;. https://doi.org/10.1002/sec.1672

62. Lu Y, Li L, Yang X, Yang Y. Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. PLoS ONE. 2015; 10(5):e0126323. https://doi.org/10.1371/journal.pone.0126323 PMID: 25978373

63. Das AK. A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. Networking Science. 2013; 2(1-2):12–27. https://doi.org/10.1007/s13119-012-0009-8

64. Das AK, Paul NR, Tripathy L. Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem. Information Sciences. 2012; 209:80–92. https://doi.org/10.1016/j.ins.2012.04.036

65. Kumari S, Khan MK, Li X, Wu F. Design of a user anonymous password authentication scheme without smart card. International Journal of Communication Systems. 2016; 29(3):441–458. https://doi.org/10.1002/dac.2853

66. Xu L, Wu F. Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. Journal of medical systems. 2015; 39(2):10. https://doi.org/10.1007/s10916-014-0179-x PMID: 25631840

67. Reddy AG, Das AK, Odelu V, Yoo KY. An enhanced biometric based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography. PLoS ONE. 2016; 11(5):e0154308. https://doi.org/10.1371/journal.pone.0154308 PMID: 27163786

68. Kumari S, Khan MK, Atiquzzaman M. User authentication schemes for wireless sensor networks: A review. Ad Hoc Networks. 2015; 27:159–194. https://doi.org/10.1016/j.adhoc.2014.11.018