ITC 3/47

Journal of Information Technology and Control
Vol. 47 / No. 3 / 2018
pp. 431-446
DOI 10.5755/j01.itc.47.3.17361
© Kaunas University of Technology

Cryptanalysis and Improvement of a Multi-Server Authenticated Key Agreement by Chen and Lee's Scheme

Received 2016/12/30 | Accepted after revision 2018/07/30

crossref **http://dx.doi.org/10.5755/j01.itc.47.3.17361**

Cryptanalysis and Improvement of a Multi-Server Authenticated Key Agreement by Chen and Lee's Scheme

Azeem Irshad, Husnain Naqvi, Shehzad Ashraf Chaudhry

Department of Computer Science & Software Engineering, International Islamic University, Islamabad
e-mail: irshadazeem2@gmail.com, husnain.naqvi@iiu.edu.pk, shahzad@iiu.edu.pk

Muhammad Usman

Department of Computer Science, Faculty of Natural Science, Quaid-I-Azam University, Islamabad, Pakistan
e-mail: musman@qau.edu.pk

Muhammad Shafiq

Department of Information Technology, University of Gujrat, Gujrat, Pakistan, e-mail: shafiq.pu@gmail.com

Omid Mir

The Institute of Networks and Security, Johannes Kepler University Linz, Austria, e-mail: mir@ins.jku.at

Ambrina Kanwal

Department of Computer Science, Bahria University, Islamabad, Pakistan, e-mail: ambrina_kanwal@yahoo.com

Corresponding author: shahzad@iiu.edu.pk

Multi-server authentication makes convenient to benefit from services of various service providers on the basis of one-time registration through a trusted third party. Since, the users are reluctant to register themselves separately from all servers due to the hassle of remembering many passwords and other cost constraints. The multi-server authentication enables the immediate provision of services by the real-time verification of users on an insecure channel. The literature for multi-server oriented authenticated key agreement could be traced back to Li et al. and Lee et al., in 2000. Since then, numerous multi-server authentication techniques have been put forth. Nonetheless, the research academia looks for more secure and efficient authentication protocols. Recently, Chen and Lee's scheme presented a two-factor multi-server key agreement protocol, which is found to be prone to impersonation, stolen smart card, key-compromise impersonation attack, and trace attacks. Besides, the scheme is also found to have the inefficient password modification procedure. We propose an improved protocol that counters the above limitations in almost an equivalent computation cost. Moreover, our protocol is supplemented with formal security analysis using BAN logic along with performance analysis and evaluation.

KEYWORDS: Multi-server authentication, cryptanalysis, biometrics, remote authentication, attack.

1. Introduction

In peer-to-peer environment, Multi-Server Authentication (MSA) permits the quick accessibility of numerous online multimedia-based services to users on the basis of a single registration. The architecture of MSA [39, 29] is favorable for both sides, i.e. service providers as well as users. This is because the users need not remember more than one password due to single registration of a trusted third party. Similarly, the MSA architecture eases the service providers of the maintenance of verifier database for each registered user, and the trouble of individualized registrations. The users count on a single registration of a trusted third party to benefit from services of different service providers. The MSA setting would comprise numerous users (Ui), servers (Sj), and a registration centre (RC). The trust flows from RC towards users and servers, as RC registers these entities in the initialization setup on confidential channel. Then onwards, the users could benefit themselves of the services offered by service providers.

Previously, numerous MSA-based schemes gearing towards augmentation in security and efficiency have been presented. Yet, it is believed on account of frequent threats and weaknesses that more resilient MSA protocols need to be demonstrated. Earlier in 2000, Lee and Chang [34] presented a key agreement protocol for MSA framework. The scheme was found vulnerable to masquerading attack and compromised anonymity [51]. Thereafter, Tsaur [47] presented a remote subscriber-based MSA scheme employing RSA crypto-primitives as well as Lagrange interpolating polynomials. The protocol was exposed to password-guessing threat [47]. Then, Li et al. [35] presented a password-based MSA protocol in an artificial neural network system, which requires high training time and a bit higher cost. Thereafter, Lin et al. [39] presented an ElGamal digital signature related MSA protocol. However, the scheme was found too costly for the memory requirements to be applied in smart card based applications. After that, Juang [29] presented a symmetric cryptosystem-based MSA protocol, however having scalability problems due to maintaining users' verifier-repository at server's end for all users. Next, Chang and Lee [8] also demonstrated a MSA protocol, which was discovered to be susceptible for privileged-insider and server masquerading threats [38, 18]. Liao and Wang [38], subsequently introduced another dynamic ID-based remote user authenticated key agreement for MSA architecture. Hsiang and Shih [18] discovered the protocol [38] as vulnerable to privileged insider and spoofing threats, and also put forward an improved protocol. Lee et al. [33] remarked that the scheme [18] is unable to accomplish mutual authentication agreement, and onwards demonstrated an enhanced protocol. Nonetheless, Chen and Lee [11] analyzed that the protocol [7] is incapable of providing the security feature of smart card security to comply with two-factor authentication. Besides, [7] also could not resist impersonation attack and bears an inefficient password modification steps due to RC's involvement. After a deep analysis of Chen and Lee's scheme [11], we came to know that this protocol sustains stolen smart card attack that leads to the disclosure of session key and password. This protocol is prone to spoofing and trace attack as well. In addition, the scheme bears a defective password-alteration phase. The current study work ascertains few weaknesses in Chen and Lee's scheme [11] and presents an enhanced protocol ensuring security with efficiency as supported with formal analysis. Moreover, the strength of session key establishment in our protocol is ratified under BAN-logic and random oracle-based formal analysis.

Section 2 relates to a review of Chen and Lee's protocol. Section 3 studies the cryptanalysis of Chen and Lee's protocol. Section 4 illustrates our proposed work. Section 5 would demonstrate the security and performance evaluation analysis. The last section wraps up the presented work.

2. Preliminaries

This section briefly illustrates some salient features of hash function, and bio-hashing process.

2.1. Hash Function

A hash function [9, 14, 26], defined as h:{0,1}* $\rightarrow \{0,1\}^{\tau}$ where τ denotes a safe length, generating γ string of pre-determined length as output from inputting a random string ω of any length, i.e., $\gamma = h(\omega)$, maintains the following characteristics:

- To define the first characteristic, a one-way hash function serves as a hard problem to alter the string ω without updating the hash digest $h(\omega)$.
- For the second characteristic, it is hard to form a string ω generating $h(\omega)$ as preimage resistance.
- For the third characteristic, it is hard to produce ω and ω' provided $\omega \neq \omega'$where as $h(\omega)= h(\omega')$ holds as well.

The advantage of attacker may be shown by the following formalization:

$$Adv_{\mathbb{A}}^{HASH}(t_e) = Pro[(\omega, \omega') \Leftarrow_R \mathbb{A}: \omega \neq \omega' and\ h(\omega) = h(\omega')], \qquad (1)$$

where $Pro[E_{te}]$ stands for the event E_{te}'s probability of conducting the random experiment, and $(\omega, \omega') \Leftarrow_R \mathbb{A}$ depicts the selected random pair (ω, ω') by the adversary. In this set-up, $\mathbb{A}$ is probabilistic, while the probability related to advantage $Adv_{\mathbb{A}}^{HASH}(t_e)$ can be calculated using the random choices as given by $\mathbb{A}$ in execution time t_e. The hashing function $h()$ is assumed to be resistant to collision, in case $Adv_{\mathbb{A}}^{HASH}(t_e) \leq \epsilon$ holds for adequately small $\epsilon > 0$.

2.2. Bio-Hashing

The bio-hashing, being one of the mechanisms to ensure three-factor authentication, complements the two-factor authentication framework with another biometric factor to boost the security. Many studies employing bio-hashing as a three-factor authentication mechanism can be witnessed lately [12, 41]. The sample from biometric scanning tends to behave differently each time it is collected. The bio-hashing function engenders a randomly generated, compressed set of codes by converting the finger-impression codes in so-called biocodes. The hamming distance assists in differentiating the set of various biocodes. Thus, the bio-hashing function is known for countering the de-synchronization problem that might result in capturing the biometric imprints [28].

3. A Review and Cryptanalysis of Chen and Lee's Scheme

We employed a few notations to make the protocol comprehensible, as given in Table 1.

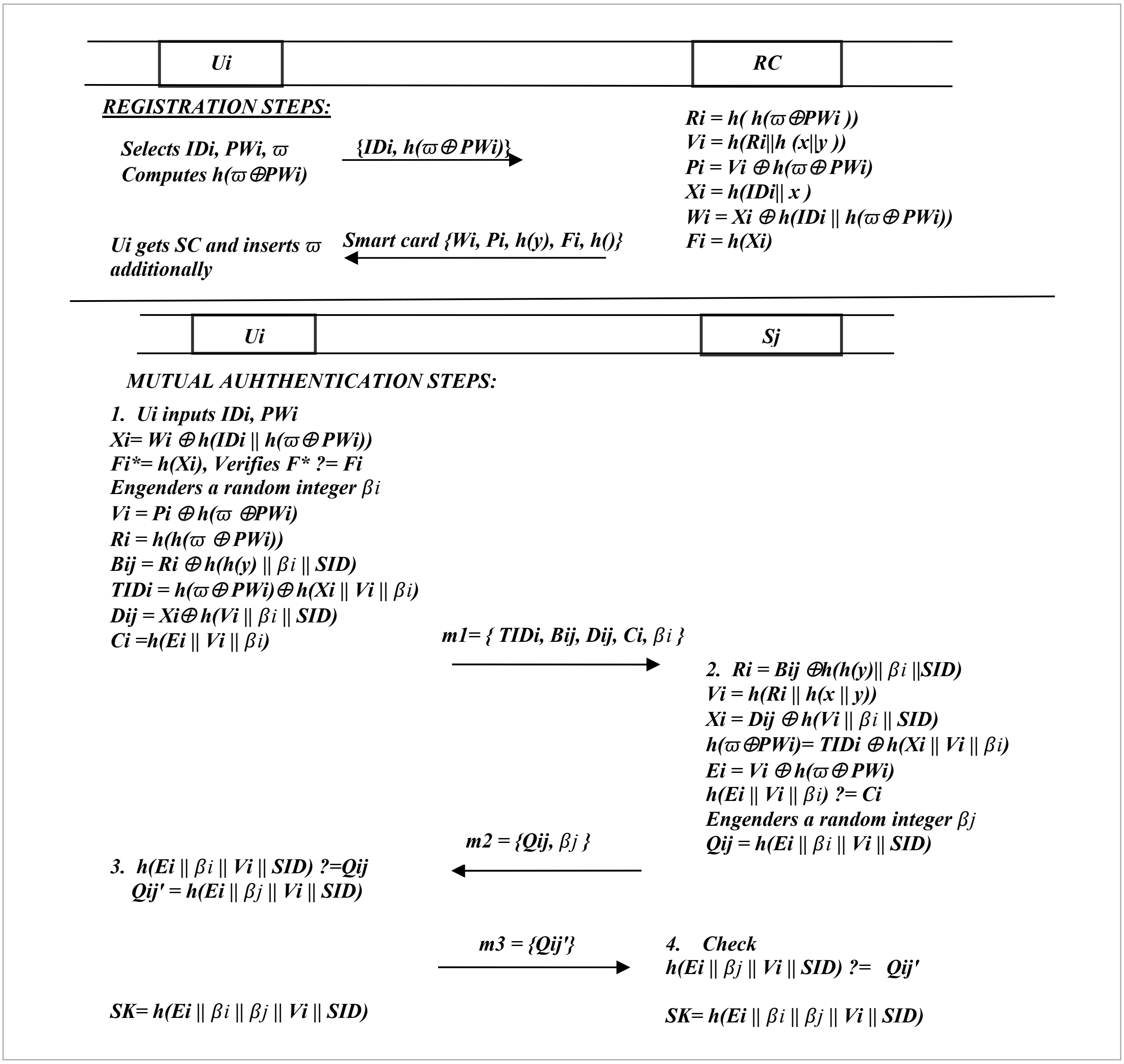
The Chen and Lee's protocol includes a few of participating entities, particularly a trusted RC, users Ui and numerous servers Sj. Both users and servers get registered before hand of mutual authentication phase. For this purpose, Sj shares the secret PID_r with on confidential channel. The working of Chen and Lee's protocol [11] is outlined next.

Table 1
Notation Guide

Notations	Narration
RC/Ui/Sj	Registration Centre/User/Service provider
IDi/ SID	Users' identity/ Service provider's identity
PWi:	User's password
PID_r:	One-time pre-shared secret between RC/Sj and Ui
x:	RC's master secret key
y:	RC's long term secret key
BIOi	Biometric Identity of Ui
H(.)	Bio-hash function
h(.):	A secure hash digest function
SC:	Smart Card
||/⊕	Concatenation/ XOR function

Figure 1

Chen and Lee's protocol's registration and mutual authentication phases


Ui
RC
REGISTRATION STEPS:
Selects IDi, PWi, ϖ
Computes h(ϖ⊕PWi)
{IDi, h(ϖ⊕ PWi)}
Ri = h(h(ϖ⊕PWi))
Vi = h(Ri||h (x||y))
Pi = Vi ⊕ h(ϖ⊕ PWi)
Xi = h(IDi|| x)
Wi = Xi ⊕ h(IDi || h(ϖ⊕ PWi))
Fi = h(Xi)
Ui gets SC and inserts ϖ additionally
Smart card {Wi, Pi, h(y), Fi, h()}
Ui
Sj
MUTUAL AUHTHENTICATION STEPS:
1. Ui inputs IDi, PWi
Xi= Wi ⊕ h(IDi || h(ϖ⊕ PWi))
Fi*= h(Xi), Verifies F* ?= Fi
Engenders a random integer βi
Vi = Pi ⊕ h(ϖ ⊕PWi)
Ri = h(h(ϖ ⊕ PWi))
Bij = Ri ⊕ h(h(y) || βi || SID)
TIDi = h(ϖ⊕ PWi)⊕ h(Xi || Vi || βi)
Dij = Xi⊕ h(Vi || βi || SID)
Ci =h(Ei || Vi || βi)
m1= { TIDi, Bij, Dij, Ci, βi }
2. Ri = Bij ⊕h(h(y)|| βi ||SID)
Vi = h(Ri || h(x || y))
Xi = Dij ⊕ h(Vi || βi || SID)
h(ϖ⊕PWi)= TIDi ⊕ h(Xi || Vi || βi)
Ei = Vi ⊕ h(ϖ⊕ PWi)
h(Ei || Vi || βi) ?= Ci
Engenders a random integer βj
Qij = h(Ei || βi || Vi || SID)
m2 = {Qij, βj }
3. h(Ei || βi || Vi || SID) ?=Qij
Qij' = h(Ei || βj || Vi || SID)
m3 = {Qij'}
4. Check
h(Ei || βj || Vi || SID) ?= Qij'
SK= h(Ei || βi || βj || Vi || SID)
SK= h(Ei || βi || βj || Vi || SID)

3.1. Design of Chen and Lee's Protocol

The Chen and Lee's protocol involves two procedures, i.e. 1) registration procedure and 2) login and authentication procedure as exhibited in Figure 1.

3.1.1. User Registration Process

The user completes its registration process by employing the succeeding steps with RC:

1 Initially, Ui selects its identity *IDi,* password *PWi,* and engenders a random number *ϖ.* Thereafter, it calculates *h(ϖ ⊕ PWi)* and sends *{IDi, h(ϖ ⊕ PWi)}* to registration centre.

2 Next, the registration centre calculates *Ri=h(h(ϖ ⊕ PWi)), Vi=h(Ri||h(x||y)), Pi=Vi⊕ h(ϖ⊕PWi), Xi=h(IDi||x), Wi = Xi⊕h(IDi||h(ϖ⊕PWi))* and *Fi=h(Xi).* Subsequently, *RC* stores these contents in SC *{Wi, Pi, Fi, h(), h(y)}* and submits to *Ui.*

3 Next, Ui receives smart card and adds the factor ϖ in it to finalize the registration

3.1.3. Login and Authentication Procedure

We illustrate login and authentication procedure in this sub-section.

1 In login process, Ui is approved from the smart card to initiate the authentication process. For the said objective, Ui inserts its identity and password, i.e. (*IDi* and *PWi*). This is followed by the smart card computation of $Xi= Wi \oplus h(IDi || h(\varpi \oplus PWi))$, $Fi^{*}= h(Xi)$ parameters. Then, the user compares the equation, i.e. $F^{*} ?= Fi$. If it holds valid, then the user engenders a random number βi, and calculates $Vi = Pi \oplus h(\varpi \oplus PWi)$, $Ri=h(h(\varpi \oplus PWi))$, $Bij = Ri \oplus h(h(y) || \beta i || SID)$, $TIDi=h(\varpi \oplus PWi) \oplus h(Xi || Vi || \beta i)$, $Dij = Xi \oplus h(Vi || \beta i || SID)$ and $Ci =h(Ei || Vi || \beta i)$. Thereafter, Ui submits the parameters $m_1= \{TIDi, Bij, Dij, Ci, \beta i\}$ to service provider.

2 The service provider receives $m_1= \{ TIDi, Bij, Dij, Ci, \beta i\}$ and calculates $Ri=Bij \oplus h(h(y) || \beta i ||SID)$, $Vi = h(Ri || h(x || y))$, $Xi = Dij \oplus h(Vi || \beta i || SID)$, $h(\varpi \oplus PWi)= TIDi \oplus h(Xi || Vi || \beta i)$ and $Pi = Vi \oplus h(\varpi \oplus PWi)$. Thereafter, it compares the equation, i.e. $h(Pi || Vi || \beta i) ?= Ci$. If valid, it creates a random number βi, calculates $Qij = h(Pi || \beta i || Vi || SID)$ and sends $m_2 = \{Qij, \beta j\}$ towards user for the purpose of verification.

3 Then, *Ui* calculates $h(Pi || \beta i || Vi || SID)$ and also verifies the equation, i.e. $h(Pi || \beta i || Vi || SID) ?=Qij$. If this equality is valid, *Ui* calculates $Qij' = h(Pi || \beta j || Vi || SID)$ and submits the message $m_3 = \{Qij'\}$ to service provider for further confirmation with βj challenge.

4 The service provider receives m_3 and computes $h(Pi || \beta j || Vi || SID)$. Next, the service provider verifies the equation, i.e. $h(Pi || \beta j || Vi || SID) ?= Qij'$. If this equality holds true, the service provider further computes the agreed session key with *Ui* as $SK= h(Pi || \beta i || \beta j || Vi || SID)$.

3.2. Pitfalls in Chen and Lee's Protocol

The Chen and Lee's protocol has been found prone to stolen smart card threat, user masquerading threat, trace threat, key compromise impersonation threat. At the same time, the protocol bears an expensive password alteration process. Before recounting those pitfalls, we describe an attack model.

3.2.1. Attack Model

In this study, an adversary $\mathbb{A}$ is assumed to be proficient [4, 40, 42] in the following skills:

1 $\mathbb{A}$ could apply reverse engineering procedures on the stolen smart card contents and attempt to guess low-entropy secrets, like password or identity.

2 $\mathbb{A}$ could intercept the messages on insecure channel and manipulate by modifying or replaying the same contents.

3 $\mathbb{A}$ could be any legal user (insider) behaving maliciously.

3.2.2. Cryptanalysis and Drawbacks

The details of reported attacks and other limitations in Chen and Lee's scheme are given below:

a Stolen smart card threat

An adversary $\mathbb{A}$ may trigger this attack if he/she could access the smart card contents which are not properly encrypted before storage. In our protocol, the smart card contains the parameters $\{Wi, Pi, Fi, \varpi, h(), h(y)\}$ while the messages that may be intercepted on public channel are $m_1= \{TIDi, Bij, Dij, Ci, \beta i \}$, $m2 = \{Qij, \beta j \}$ and $m_3 = \{Qij'\}$. Given that βi and *SID* could be accessed on public channel, and $h(y)$ could be approached from stolen card, the attacker may produce $h(h(y) || \beta i||SID)$ and approach *Ri'* factor by calculating $Ri' = Bij \oplus h(h(y) || \beta i || SID)$. Subsequently, owing to the accessibility of 'ϖ' random integer in smart card, $\mathbb{A}$ may initiate an offline-dictionary attack to guess the original password of *Ui*. Now, the adversary attempts all dictionary strings as password (PWi^{*}) in computing $Ri^{*}= h(h(\varpi \oplus PWi^{*})$ and verifying the equation, i.e. $Ri' ?= Ri^{*}$. Whenever the adversary finds the matching equation, the former will come to know the right password. After having the password *PWi* guessed, the adversary may compute $Vi'= h(\varpi \oplus PWi) \oplus Pi$. Onwards, $\mathbb{A}$ may comfortably establish the legal session key on executing the hash function as $h(Pi || \beta i || \beta j || Vi' || SID)$. In this manner, the attacker may easily guess the identical (valid) session key SK after stealing the smart card, as constructed by the legitimate members. Hence the protocol is prone to stolen smart card threat.

b User impersonation threat

The Chen and Lee's protocol is prone to user spoofing attack, provided the smart card contents are available to adversary. By employing these contents, $\mathbb{A}$ may compute the legitimate password *PWi* after following the steps as mentioned in sub-section 3.2.2(a).

The attacker may compute $Vi = Pi \oplus h(\varpi \oplus PWi)$ and $Ri=h(h(\varpi \oplus PWi))$. Subsequently, $\mathbb{A}$ makes a guess of the IDi string after checking the entire set of potential strings IDi^* by verifying the equations, i.e., $Xi^*= Wi \oplus h(IDi^* \,||\, h(\varpi \oplus PWi))$ and $Fi\ ?= h(Xi^*)$, frequently. On positive matching, the legal identity (IDi) and Xi^* are exposed. Thereafter, $\mathbb{A}$ engenders a random number βi and calculates $Bij = Ri \oplus h\ (h(y) \,||\, \beta i \,||\, SID)$, $TIDi = h(\varpi \oplus PWi)\ h(Xi \,||\, Vi \,||\, \beta i)$, $Dij = Xi \oplus h(Vi \,||\, \beta i \,||\, SID)$ and $Ci =h(Pi \,||\, Vi \,||\, \beta i)$. Ultimately, $\mathbb{A}$ designs authentication request as $m_1= \{TIDi, Bij, Dij, Ci, \beta i\}$ effectively.

c Trace attack

In this threat, the attacker could discover the session participants on the basis of distinguishing and comparing known parameters between different sessions of the same participants. In scheme [11], a privileged insider with known $h(y)$, could eavesdrop the request $m_1=\{ TIDi, Bij, Dij, Ci, \beta i\}$ acting maliciously and try to trace the similarity between different sessions through Ri after calculating $Ri = Bij \oplus h\ (h(y) \,||\, \beta i \,||SID)$. The Ri parameter is not changed among various sessions constructed between user and server, in case the user does not update his/her PWi or ϖ parameters in SC. Thus, the scheme [11] is vulnerable to trace threat.

d Key-compromise impersonation threat (KCI)

In KCI attack, the attacker may use the guessed or stolen factor of some user to spoof as a service provider.

The Chen and Lee's protocol is vulnerable to KCI threat, if the data contents in user's smart card are accessed by attacker. After accessing the password of Ui, as shown in Section 3.2.2(a), the attacker could impersonate as a service provider by designing a message $m_2 = \{Qij, \beta j\}$ after generating a random integer βj, and constructing Qij^* as $Qij^* = h(Pi \,||\, \beta i \,||\, Vi \,||\, SID)$. This is because Pi and Vi factors could be produced by maneuvering the smart card factors as depicted in Section 3.2.2(b). The message m_2 is submitted to user, and will be duly verified by user, though fake. In this manner, a successful spoofing attack could be launched towards user in scheme [11].

e No session key security

In case the parameters Pi and Vi are recovered by the attacker out of data stolen from smart card, the adversary might calculate past session keys through eavesdropping βi, βj and computing session key, i.e. $SK= h(Pi \,||\, \beta i \,||\, \beta j \,||\, Vi \,||\, SID)$.

f No direct password alteration

The Chen and Lee's scheme claims that user does not consult RC to modify the password; nonetheless, the scheme [11] does not provide any procedure for altering PWi without the involvement of RC. The alteration of the password needs updating $Pi=Vi \oplus h(\varpi \oplus PWi)$, whenever the password PWi is modified. Here, Ri is employed for computing Vi, as $Vi = h(Ri \,||\, h\ (x||y))$. Moreover, Ri is a parameter that cannot be constructed without password, i.e. $Ri = h(h(\varpi \oplus PWi))$. Consequently, Ui will need to consult Sj every instant to update Ri since it does not possess the parameter $h(x||y)$. The above proof negates the claim of Chen and Lee's scheme for the capability of password alteration without engaging RC.

4. The Proposed Model

The multi-server architecture involves three participating entities namely; registration centre (RC), user (Ui), and server or service provider (Sj). RC enables to register users and provide services from servers onwards. In initialization, the RC chooses its master secret key as x and another long term secret integer as y. These two parameters are utilized in registering all users. RC calculates $h(x \,||\, y)$ and $h(y)$ and then shares these parameters with all legal service providers Sj, using a confidential channel. The contributed model also includes three sub-procedures, i.e., user registration procedure, login and authentication procedure, and password alteration method as illustrated below:

4.1. User Registration Procedure

To become a legal subscriber of the network, the user performs the succeeding steps with RC:

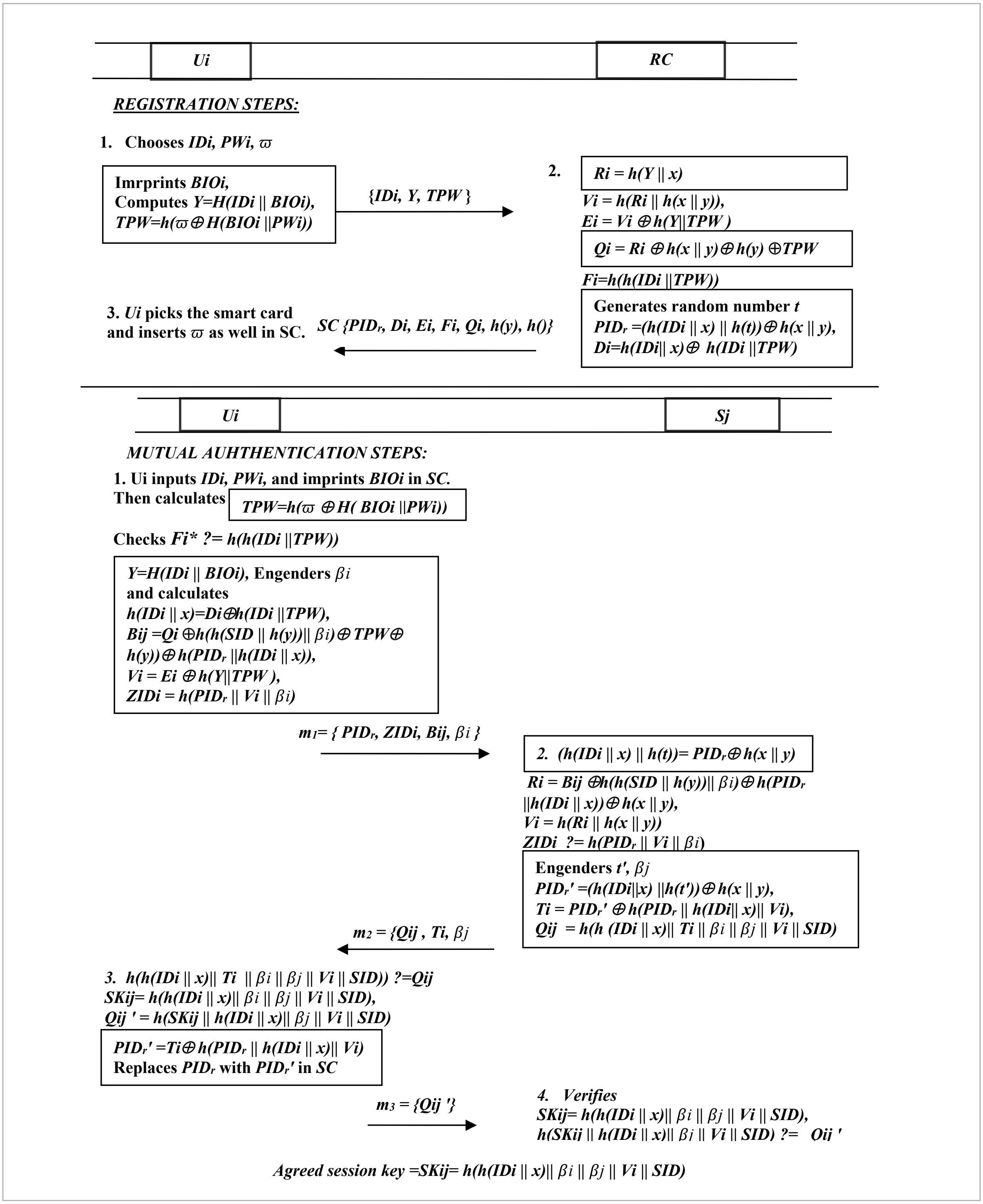
1 The user chooses the parameters as identity IDi, biometric $BIOi$, password PWi, and creates a random integer ϖ. Then, user further calculates $Y=H(IDi \,||\, BIOi)$, $TPW=h(\varpi \oplus H(BIOi \,||\, PWi))$, and sends $\{IDi, Y, TPW\}$ to RC to complete registration.

2 Next RC calculates $Ri = h(Y \,||\, x)$, $Vi = h(Ri \,||\, h(x \,||\, y))$, $Ei = Vi \oplus h(Y||TPW)$, $Qi = Ri \oplus h(x \,||\, y) \oplus h(y) \oplus TPW$ and $Fi= h(h(IDi \,||\, TPW))$. Subsequently, it creates random integer t, and calculates $PID_r =(h(IDi||x) \,||\, h(t)) \oplus h(x \,||\, y)$ and $Di = h(IDi \,||\, x) \oplus h(IDi||TPW)$. Later, the registration centre stores $\{PID_r, Di, Ei, Fi, Qi, h(s), h()\}$ in smart card and sends towards Ui.

3 Ui adds the parameter ϖ in smart card finally.

Figure 2

The proposed protocol (Registration and mutual authentication)



Ui RC

REGISTRATION STEPS:

1. Chooses IDi, PWi, ϖ

Imrprints $BIOi$,
Computes $Y=H(IDi \| BIOi)$,
$TPW=h(\varpi \oplus H(BIOi \| PWi))$

$\{IDi, Y, TPW\}$

2. $Ri = h(Y \| x)$
$Vi = h(Ri \| h(x \| y))$,
$Ei = Vi \oplus h(Y \| TPW)$
$Qi = Ri \oplus h(x \| y) \oplus h(y) \oplus TPW$
$Fi=h(h(IDi \| TPW))$
Generates random number t
$PID_r =(h(IDi \| x) \| h(t)) \oplus h(x \| y)$,
$Di=h(IDi \| x) \oplus h(IDi \| TPW)$

$SC\ \{PID_r, Di, Ei, Fi, Qi, h(y), h()\}$

3. Ui picks the smart card and inserts ϖ as well in SC.

Ui Sj

MUTUAL AUHTHENTICATION STEPS:

1. Ui inputs IDi, PWi, and imprints $BIOi$ in SC.
Then calculates $TPW=h(\varpi \oplus H(BIOi \| PWi))$

Checks $Fi^* ?= h(h(IDi \| TPW))$

$Y=H(IDi \| BIOi)$, Engenders βi
and calculates
$h(IDi \| x)=Di \oplus h(IDi \| TPW)$,
$Bij =Qi \oplus h(h(SID \| h(y)) \| \beta i) \oplus TPW \oplus h(y)) \oplus h(PID_r \| h(IDi \| x))$,
$Vi = Ei \oplus h(Y \| TPW)$,
$ZIDi = h(PID_r \| Vi \| \beta i)$

$m_1= \{ PID_r, ZIDi, Bij, \beta i \}$

2. $(h(IDi \| x) \| h(t))= PID_r \oplus h(x \| y)$
$Ri = Bij \oplus h(h(SID \| h(y)) \| \beta i) \oplus h(PID_r \| h(IDi \| x)) \oplus h(x \| y)$,
$Vi = h(Ri \| h(x \| y))$
$ZIDi\ ?= h(PID_r \| Vi \| \beta i)$
Engenders $t', \beta j$
$PID_r' =(h(IDi \| x) \| h(t')) \oplus h(x \| y)$,
$Ti = PID_r' \oplus h(PID_r \| h(IDi \| x) \| Vi)$,
$Qij = h(h(IDi \| x) \| Ti \| \beta i \| \beta j \| Vi \| SID)$

$m_2 = \{Qij , Ti, \beta j$

3. $h(h(IDi \| x) \| Ti \| \beta i \| \beta j \| Vi \| SID))\ ?=Qij$
$SKij= h(h(IDi \| x) \| \beta i \| \beta j \| Vi \| SID)$,
$Qij' = h(SKij \| h(IDi \| x) \| \beta j \| Vi \| SID)$
$PID_r' =Ti \oplus h(PID_r \| h(IDi \| x) \| Vi)$
Replaces PID_r with PID_r' in SC

$m_3 = \{Qij'\}$

4. Verifies
$SKij= h(h(IDi \| x) \| \beta i \| \beta j \| Vi \| SID)$,
$h(SKij \| h(IDi \| x) \| \beta i \| Vi \| SID)\ ?= Qij'$

Agreed session key $=SKij= h(h(IDi \| x) \| \beta i \| \beta j \| Vi \| SID)$

4.2. Login and Authentication Procedure

The mutual authentication phase between Ui and Sj is given below:

1 In this procedure, the user seeks authenticated access of services from server on account of RC. To serve the purpose, Ui inputs the identity IDi and password PWi into smart card while inputs biometric $BIOi$ into the scanner. Then smart card computes $TPW=h(\varpi \oplus H(BIOi || PWi))$ and checks whether $Fi^* ?= h(h(IDi || TPW))$. If true, then Ui creates a random integer βi, and calculates $Y= H(IDi || BIOi)$, $h(IDi || x) = Di \oplus h(IDi || TPW)$, $Bij = Qi \oplus h(h(SID || h(y)) || \beta i) \oplus TPW \oplus h(y)) \oplus h(PID_r || h(IDi || x))$, $Vi = Ei \oplus h(Y || TPW)$, and $TIDi = h(PID_r || Vi || \beta i)$. Next, Ui sends the message $m_1= \{PID_r, TIDi, Bij, \beta i\}$ to Sj for verification.

2 RC , after receiving $m_1= \{ PID_r, TIDi, Bij, \beta i\}$ computes $(h(IDi || x) || h(t))=PID_r \oplus h(x || y)$, $Ri = Bij \oplus h(h(SID || h(y)) || \beta i) \oplus h(PID_r || h(IDi || x)) \oplus h(x || y)$ and $Vi = h(Ri || h(x || y))$. Next, RC further computes $h(PID_r || Vi || \beta i)$ and compares $TIDi ?= h(PID_r || Vi || \beta i)$. If the equation is verified, RC will create a random integer t' and calculate $PID_r' =(h(IDi || x) || h(t')) \oplus h(x || y)$, $Ti = PID_r' \oplus h(PID_r || h(IDi || x) || Vi)$ and $Qij = h(h(IDi || x) || Ti || \beta i || \beta j || Vi || SID)$ after generating a random number βj. Ultimately, RC sends the message $m2 = \{Qij , Ti, \beta j \}$ to Ui.

3 After receiving $m2$, Ui computes $h(h(IDi || x) || \beta i || \beta j || Vi || SID))$ and compares the equation $h(h(IDi || x) || Ti || \beta i || \beta j || Vi || SID)) ?=Qij$.

4 If the equation is verified, Ui further calculates $SKij= h(h(IDi || x) || \beta i || \beta j || Vi || SID)$, $Qij ‘ = h(SKij || h(IDi || x) || \beta j || Vi || SID)$ and forwards $m_3 = \{Qij ‘\}$ towards server so that it may verify the βj-based challenge. At the same time, Ui calculates $PID_r'=Ti \oplus h(PID_r || h(IDi || x) || Vi)$ and replaces the parameter PID with PID_r' in SC.

5 The server (Sj), after receiving m_3, calculates $SKij= h(h(IDi || x)|| \beta i || \beta j || Vi || SID)$. Afterwards, it verifies the equation, i.e. $h(SKij || h(IDi || x) || \beta j || Vi || SID) ?= Qij ‘$. On successful verification, it constructs session key with user as $h(h(IDi || x) || \beta i || \beta j || Vi || SID)$, finally. The details of the contributed protocol can be witnessed from Figure 2.

4.3. Password Alteration Mechanism

Ui may alter his/her password through initiating the password alteration steps, into another password (PWi^{new}) without getting any assistance out of registration centre. These steps are illustrated below.

1 Initially, the user shall insert its SC into the reader for inputting identity (IDi^*), password (PWi^*) and imprinting its biometric factor $BIOi^*$ into the scanner device. Thereafter, the SC calculates $TPW=h(\varpi \oplus H(BIOi ||PWi))$ and checks $Fi^* ?=h(h(IDi ||TPW))$. If this equality holds, then user proceeds to the next step.

2 Afterwards, the smart card calculates $TPW=h(\varpi \oplus H(BIOi || PWi))$ and computes $Vi = Ei \oplus h(H(IDi || BIOi)||TPW)$, $Qi^* = Qi \oplus TPW$, $h(IDi || x) = Di \oplus h(IDi || TPW)$.

3 Subsequently, the user shall insert a new password (PWi^{new}). The smart card then calculates $TPW'=h(\varpi \oplus H(BIOi||PWi^{new}))$, $Ei^{new} = Vi \oplus h(H(IDi || BIOi) || TPW')$, $Qi^{new} = Qi^* \oplus TPW'$, $Di^{new}= h(IDi || x) \oplus h(IDi || TPW')$ and $Fi^{new} = h(h(IDi || TPW'))$.

4 Next, the values Di, Ei, Fi, and Qi are replaced by Di^{new}, Ei^{new}, Fi^{new}, and Qi^{new} in the smart card.

5. Security Analysis

A comprehensive discussion on the security analysis of proposed model is provided in the following sub-sections.

5.1. Replay Attacks

In replay attacks, the intercepted messages are replayed without undergoing modifications to betray any legal member [1, 3, 17, 19, 44].

An attacker $\mathbb{A}$, having access to factors $\{PID_r, ZIDi, Bij, \beta i, Qij , Ti, \beta j, Qij ‘\}$ could try for replaying these contents in order to forge the legitimate participant. Nonetheless, the use of temporary novel parameters, such as βi and βj, by the legitimate members, for every session, discourage the attacker for initiating an attack. In case the adversary attempts to replay $m_1= \{PID_r, ZIDi, Bij, \beta i \}$ towards server, the server could confirm the legitimacy of user in m_3, in response to the βj -based challenge. Simultaneously, the user authenticates Sj in m_2 to respond the m_1-based βi challenge. Thus, the above discussion indicates towards a defense capability of the proposed model against replay attack.

5.2. Modification Attacks

The attacker could alter the intercepted parameters to resubmit to the intended party, in case a protocol is designed with least focus on resisting the modification attack.

If any adversary tries to alter the public parameters $\{PID_r, ZIDi, Bij, \beta i, Qij , Ti, \beta j, Qij \}$, $\mathbb{A}$ will be unable to reconstruct these contents $\{ZIDi, Bij, Qij , Qij \}$ by creating fresh session variables, since the construction of these messages requires the knowledge of Vi and $h(IDi \,||\, x)$ which are only known to the legitimate participants. Hence, the legitimate participant will be able to detect any malicious participant. Therefore, the contributed scheme may easily thwart this threat.

5.3. Password or Secret Guessing Threat

The guessing attack is possible if the adversary tries to guess the password of user or some Sj's long term secret on account of intercepted parameters. In the proposed scheme, $\mathbb{A}$ can approach the factors $\{PID_r, ZIDi, Bij, \beta i, Qij , Ti, \beta j, Qij \}$ on little inspection of any public channel. Nevertheless, an attacker could not derive the password, since it is not utilized as a factor for the calculation of any parameter; hence it minimizes the chances of guessing the corresponding parameters.

5.4. Stolen-Verifier Threats

The adversary could embezzle with valuable data which are stored at server's end; and the database of Ui's secrets like passwords or other parameters, could be utilized to impersonate as the legitimate users. The proposed scheme provides mutual authentication without depending on database maintenance on Sj or RC's end. This suggests that the stolen verifier attack is defeated in our scheme.

5.5. Offline-Dictionary Attack Based on Stolen Smart Card Contents

In this attack, the attacker attempts various combinations of dictionary contents after having the stolen smart card information [23, 46].

Using SC, an attacker might try to manipulate with its available contents of smart card i.e., $\{PID_r, Di, Ei, Fi, Li, Qi, h()\}$. For guessing the password from Ei, Fi and Qi parameters, $\mathbb{A}$ needs to know IDi, r and $BIOi$ to guess PWi from TPW, where $TPW= h(r \oplus H(BIOi \,||PWi))$. Consequently, the offline-dictionary attack using SC cannot be launched in polynomial time.

5.6. Session Key Security

This security feature warrants the knowledge of session key only to the known legitimate parties, such as user and service provider.

In the contributed protocol, the established session key is designed as $SK= h(h(IDi \,||\, x)||\, \beta i \,||\, \beta j \,||\, Vi \,||\, SID)$. For constructing a valid session key, an attacker shall require $h(IDi \,||\, x)$ and Vi contents. If the user's identity is stolen or guessed by adversary, the latter may not be able to assemble $h(IDi \,||\, x)$ as the adversary does not possess the parameter x. This stops the adversary from establishing a valid SK, contrary to scheme [11]. Furthermore, $\mathbb{A}$ shall require Vi for creating a valid SK, nonetheless, an attacker is not able to recover Vi as $\mathbb{A}$ does not possess TPW, $BIOi$, and Ei factors. Therefore, there is much less of a chance for attacker to initiate this attack.

5.7. Known-Key Security

This feature ensures the confidentiality of private keys even if session key for a specific session gets revealed [2, 30].

Given that the agreed session key $SK= h(h(IDi|| \,x)||\beta i \,||\, \beta j \,||Vi \,||\, SID)$ does not include Ui's password PWi as a factor, though it bears $h(IDi \,||\, x)$, again the attacker may not derive x which is the high entropy master secret key of RC. Owing to this, the attacker might not recover the factors or parameters from an exposed session key. Thus, the contributed protocol is immune and fully complies with known-key security.

5.8. Mutual Authentication

The compliance to this feature lets the involved participants verify one another in the proposed scheme. In this scheme, both of the participants verify one another on account of $h(IDi \,||\, x)$ and Vi. These both parameters are only accessible to adversary if the secrets of both RC and Sj are exposed, and not otherwise. The attacker cannot recover $h(IDi \,||\, x)$ from PID_r by computing $(h(IDi \,||\, x)||h(t)) = PID_r \oplus h(x||y)$, since it does not possess $h(x||y)$. At the same time, the accessibility to Vi requires the information of either PWi and $BIOi$, or $h(x \,||\, y)$.

5.9. Anonymous Authentication

This feature lets the user communicate without exposing his/her identity [10, 32, 45]. The user submits the messages for authentication and gets verified without declaring its true identity.

In the proposed protocol, the user sends his/her identity in the form of $PID_r = (h(IDi \,||\, x) \,||\, h(t)) \oplus h(x \,||\, y)$, that is masked by using t, as assumed by server. The server recovers $h(IDi \,||\, x)$ by taking *XOR* of $h(x \,||\, y)$ with PID_r, and then computing $h(IDi \,||\, x)$ as a dynamic identity for additional calculation. This manner, our scheme fosters the element of anonymity to a particular user.

5.10. Immune from Key-Compromise Impersonation Threat

In such attack, an adversary could impersonate one participant of a particular session if it steals some key of another participant of the same session. The contributed protocol is immune of KCI threat in contrary to scheme [11], as the contents of stolen card will not help the attacker to get other constructive parameters, such as, *Vi* and $(IDi \,||\, x)$. Hence, the adversary cannot construct up-to-date *Qij* parameter, and ultimately no KCI attack may be initiated.

5.11. Alteration of Password Without RC Involvement

The password could be comfortably updated without engaging RC, as contrary to Lee et al. and Chen and Lee, by adopting the procedure described in Section 3.4. Both of the schemes [11, 33] do not modify the password without RC engagement. As in scheme [11], the design of *Ri* involves the password as a component, which is reused in the design of *Vi*, while *Vi* is again used in the construction of *Ei* for storing in SC [13, 49, 52]. The proposed protocol employs *BIOi* for the construction of *Ri* parameter, rather than *PWi*, which enables the proposed scheme to update the password without RC involvement.

6. Formal Security Analysis

We demonstrate the robustness of key agreement, session key's confidentiality and mutual authentication related features by using formal security analysis through Burrows-Abadi-Needham (BAN) logic [6] and random-oracle model (ROM). In this logic, we utilize few terms quite frequently, known as principals, keys and nonces which are described below.

The *principals* are the participating agents in an authentication protocol.

The *Keys* (symmetric) are utilized for encrypting the messages.

Nonces are the type of random secrets that are used only once.

Some notations related to BAN logic are defined as follows:

$\psi |\equiv \xi$: ψ believes the statement ξ.

$\psi \lhd \xi$: ψ sees ξ. ψ receives a message ξ and could either read or replay it.

$\psi \mid\sim \xi$: ψ once said ξ. Earlier the agent ψ had sent a message ξ and ψ also believed ξ when sent.

$\psi \Rightarrow \xi$: ψ has jurisdiction over ξ; or ψ enjoys authority over ξ or it could be trusted.

$\sharp(\xi)$: The message ξ is freshly created.

$(\xi)_{\Theta}$: The formulae ξ is used in combination with formulae Θ.

(ξ, Θ): ξ or Θ being the part of message (ξ, Θ).

$\{\xi, \Theta\}_K$: ξ or Θ is encrypted with key K.

$\psi \xleftrightarrow{K} \psi'$: ψ and ψ' can securely contact using he shared key K.

$\langle \xi, \Theta \rangle_K$: ξ or Θ *is hashed using the key K.*

Some rules particularly (Message meaning rule as Rule 1, nonce verification rule as Rule 2, jurisdiction rule as Rule 3, freshness conjuncatenation rule as Rule 4, belief rule as Rule 5, and session keys rule as Rule 6) employed in BAN logic are stated below:

Rule 1: $\dfrac{\psi|\equiv\psi \overset{K}{\leftrightarrow} \psi', \;\; \psi\lhd\langle\xi\rangle_{\Theta}}{\psi|\equiv\psi' \mid\sim \xi}$

Rule 2: $\dfrac{\psi|\equiv \quad (\xi), \;\; \psi|\equiv\psi' \mid\sim \xi}{\psi|\equiv\psi' |\equiv \xi}$

Rule 3: $\dfrac{\psi|\equiv\psi' \Rightarrow\xi, \;\; \psi|\equiv\psi' |\equiv \xi}{\psi|\equiv \xi}$

Rule 4: $\dfrac{\psi|\equiv \quad (\xi)}{\psi|\equiv \quad (\xi, \;\Theta)}$

Rule 5: $\dfrac{\psi|\equiv(\xi), \;\; \psi|\equiv(\Theta)}{\psi|\equiv(\xi, \;\Theta)}$

Rule 6: $\dfrac{\psi|\equiv \quad (\xi), \;\; \psi|\equiv\psi' |\equiv \xi}{\psi|\equiv\psi \overset{K}{\leftrightarrow} \psi'}.$

The contributed work should meet the following targets for ensuring the security using BAN logic, under the indicated postulates:

Target 1: $S \mid\equiv Ui \xleftrightarrow{SK} S$

Target 2: $S \mid\equiv Ui \mid\equiv Ui \xleftrightarrow{SK} S$

Target 3: $Ui \mid\equiv Ui \xleftrightarrow{SK} S$

Target 4: $Ui \mid\equiv SPj \mid\equiv Ui \xleftrightarrow{SK} S.$

To proceed, we first transform the communication messages into idealized form as given below:

IM_1: $Ui \rightarrow S$: $PID_r, ZIDi, Bij, \beta i: \{\langle h(IDi \| x) \| h(t) \rangle_{h(x \| y)}, \langle PID_r, \beta i \rangle_{Vi}, \langle Ri \rangle_{h(x \| y), h(y), h(IDi, x)}, \beta i\}$

IM_2: $S \rightarrow Ui$: $Qij, Ti, \beta j: \{\langle Ti, \beta i, \beta j, SID \rangle_{h(IDi, x), Vi}, Ti, \beta j\}$

IM_3: $Ui \rightarrow S$: $Qij': \{\langle SKij, \beta j, SID \rangle_{h(IDi, x), Vi}\}$.

Further, the following premises could be drafted to verify the strength of the proposed scheme:

$\hat{Z}1: Ui \mid\equiv \sharp \beta i$

$\hat{Z}2: S \mid\equiv \sharp \beta j$

$\hat{Z}3: Ui \mid\equiv S \xleftrightarrow{(h(y),\ h(IDi,\ x),\ Ri)} Ui$

$\hat{Z}4: S \mid\equiv S \xleftrightarrow{(h(y),\ h(IDi,\ x),\ Ri)} Ui$

$\hat{Z}5: Ui \mid\equiv S \mid\equiv Ui \xleftrightarrow{(h(y),\ h(IDi,\ x),\ Ri)} S$

$\hat{Z}6: S \mid\equiv Ui \mid\equiv Ui \xleftrightarrow{(h(y),\ h(IDi,\ x),\ Ri)} S$

$\hat{Z}7: Ui \mid\equiv S \Rightarrow Qij$

$\hat{Z}8: S \mid\equiv Ui \Rightarrow Qij'.$

Next, the established idealized forms of the contributed protocol could be evaluated and tested in view of postulates as listed above.

Employing these notations, idealizations and rules, we derive the following results:

Using the idealized forms, IM_1 and IM_3, we get:

IM_1: $Ui \rightarrow S$: $PID_r, ZIDi, Bij, \beta i: \{\langle h(IDi \| x) \| h(t) \rangle_{h(x \| y)}, \langle PID_r, \beta i \rangle_{Vi}, \langle Ri \rangle_{h(x \| y), h(y), h(IDi, x)}, \beta i\}$

IM_3: $Ui \rightarrow S$: $Qij': \{\langle SKij, \beta j, SID \rangle_{h(IDi, x), Vi}\}$

After implementing Seeing Rule [36], we have

$\mathbb{K}1$: $S \triangleleft PID_r, ZIDi, Bij, \beta i: \{\langle h(IDi \| x) \| h(t) \rangle_{h(x \| y)}, \langle PID_r, \beta i \rangle_{Vi}, \langle Ri \rangle_{h(x \| y), h(y), h(IDi, x)}, \beta i\}$

$\mathbb{K}2$: $S \triangleleft Qij': \{\langle SKij, \beta j, SID \rangle_{h(IDi, x), Vi}\}$

Using $\mathbb{K}1$, $\mathbb{K}2$, $\hat{Z}3$ and *Rule 1*, we get

$\mathbb{K}3$: $S \mid\equiv Ui \sim PID_r, ZIDi, Bij, \beta i: \{\langle h(IDi \| x) \| h(t) \rangle_{h(x \| y)}, \langle PID_r, \beta i \rangle_{Vi}, \langle Ri \rangle_{h(x \| y), h(y), h(IDi, x)}, \beta i\}$

$\mathbb{K}4$: $S \mid\equiv Ui \sim \{\langle SKij, \beta j, SID \rangle_{h(IDi, x), Vi}\}$

Using $\mathbb{K}3$, $\mathbb{K}4$, $\hat{Z}1$, *Rule 4* and *Rule 2*, we have

$\mathbb{K}5$: $S \mid\equiv Ui \mid\equiv \{\langle h(IDi \| x) \| h(t) \rangle_{h(x \| y)}, \langle PID_r, \beta i \rangle_{Vi}, \langle Ri \rangle_{h(x \| y), h(y), h(IDi, x)}, \beta i\}$

$\mathbb{K}6$: $S \mid\equiv Ui \mid\equiv \{\langle SKij, \beta j, SID \rangle_{h(IDi, x), Vi}\}$

Using $\mathbb{K}5$, $\mathbb{K}6$, $\hat{Z}4$, $\hat{Z}8$ and *Rule 3*, we have

$\mathbb{K}7$: $S \mid\equiv \{\langle h(IDi \| x) \| h(t) \rangle_{h(x \| y)}, \langle PID_r, \beta i \rangle_{Vi}, \langle Ri \rangle_{h(x \| y), h(y), h(IDi, x)}, \beta i\}$

$\mathbb{K}8$: $S \mid\equiv \{\langle SKij, \beta j, SID \rangle_{h(IDi, x), Vi}\}$

On applying $\mathbb{K}7$, $\mathbb{K}8$, $\hat{Z}4$, ($SK = h(h(IDi \| x) \| \beta i \| \beta j \| Vi \| SID)$) and *Rule 6*, we have

$\mathbb{K}9$: $S \mid\equiv Ui \ S$ **(Target 1)**

Considering $\mathbb{K}9$, $\hat{Z}6$, we implement *Rule 6* as

$\mathbb{K}10$: $S \mid\equiv Ui \mid\equiv Ui \xleftrightarrow{SK} S$ **(Target 2)**

Next using the idealized form IM_2, we get:

IM_2: $S \rightarrow Ui$: $Qij, Ti, \beta j: \{\langle Ti, \beta i, \beta j, SID \rangle_{h(IDi, x), Vi}, Ti, \beta j\}$

Again using the Seeing Rule, we have

$\mathbb{K}11$: $Ui \triangleleft Qij': \{\langle Ti, \beta i, \beta j, SID \rangle_{h(IDi, x), Vi}, Ti, \beta j\}$

On applying $\mathbb{K}11$, $\hat{Z}4$ and *Rule 1*, we have

$\mathbb{K}12$: $Ui \mid\equiv S \sim \{\langle Ti, \beta i, \beta j, SID \rangle_{h(IDi, x), Vi}, Ti, \beta j\}$

Using $\mathbb{K}12$, $\hat{Z}2$, *Rule 4* and *Rule 2*, we have

$\mathbb{K}13$: $Ui \mid\equiv S \mid\equiv \{\langle Ti, \beta i, \beta j, SID \rangle_{h(IDi, x), Vi}, Ti, \beta j\}$

Using $\mathbb{K}13$, $\hat{Z}3$, $\hat{Z}7$ and *Rule 3*, we have

$\mathbb{K}14$: $Ui \mid\equiv \{\langle Ti, \beta i, \beta j, SID \rangle_{h(IDi, x), Vi}, Ti, \beta j\}$

Using $\mathbb{K}14$, $\hat{Z}3$, ($SK = h(h(IDi \| x) \| \beta i \| \beta j \| Vi \| SID)$), and *Rule 6*, we have

$\mathbb{K}15$: $Ui \mid\equiv Ui \xleftrightarrow{SK} S$ **(Target 3)**

On applying $\mathbb{K}15$, $\hat{Z}5$, and *Rule 6*, we have

$\mathbb{K}16$: $Ui \mid\equiv S \mid\equiv Ui \xleftrightarrow{SK} S$ **(Target 4)**

We can witness from this analysis that the contributed protocol ensures mutual authentication and established mutually agreed session key (SK) between user and server.

By employing random oracle model [5], a formal security analysis is implemented to verify that the contributed protocol has been resilient to session key-related threats. To meet this purpose, we use an oracle *Reveal1* in the subsequent algorithms.

Reveal1: This oracle produces ∂ out of the resultant hash value $\sigma = h(\partial)$, unconditionally.

Algorithm 1. $ALG1_{\mathbf{SPMSAC}}^{HASH}$

```
1  Attacker recovers information from smart card using power analysis [31], i.e. $SC\{PID_r, Di, Ei, Fi, h(s), Qi, h()\}$.
2  Attacker intercepts $m2 = \{Qij, Ti, \beta j\}$ in the authentication phase, where $Qij = h(h(IDi \| x) \| \beta i \| \beta j \| Vi \| SID)$, $Ti = PID_r' \oplus h(PID_r \| IDi \| Vi)$.
```

```
Calls Reveal oracle on input $Qij$ to produce $(h(IDi || x), \beta i, \beta j, Vi, SID)$ as $(h(IDi || x) || \beta i || \beta j || Vi || SID) \leftarrow reveal1(Qij)$
Calls Reveal oracle on input $h(IDi || x)$ to produce $(IDi', x')$ as $(IDi' || x') \leftarrow reveal1(h(IDi || x))$
Calls Reveal oracle on input $Fi$ to produce $(IDi, TPW')$ as $(IDi || TPW') \leftarrow reveal1(reveal1(Fi))$
Computes $K' = Ri \oplus h(x || y) = Qi \oplus h(y) \oplus TPW'$
Eavesdrops the login request message $m1 = \{PID_r, ZIDi, Bij, \beta i$, where $PID_r = (h(IDi || x), t) \oplus h(x || y)$, $ZIDi = h(PID_r || Vi || \beta i)$, $Bij = Ri \oplus h(x || y) \oplus h(h(SID || h(y)) || \beta i) \oplus h(PID_r || h(IDi || x))$.
Computes $ZIDi' = K' \oplus h(h(SID || h(y)) || \beta i) \oplus h(PID_r || h(IDi' || x'))$
If $(ZIDi' == ZIDi)$ Then
    Accept $IDi$ as the true identity of the user $Ui$.
    Return 1 (True)
Else
    Return 0 (False)
End if
```

Theorem 1. If a one-sided hash function acts closely to some randomly behaving oracle, the contributed protocol shall remain protected of malicious adversary in case the latter attempts to capture the user's identity.

Proof. In this proof, any shrewd attacker $\mathbb{A}$, who approaches the publicly available message parameters as $\{PID_r, ZIDi, Bij, \beta i, Qij, Ti, \beta j, Qij'\}$, might use the oracle *Reveal1* to implement algorithm $ALG1_{\text{SPMSAC}}^{HASH}$. The probability for the success of $ALG1_{\text{SPMSAC}}^{HASH}$ amounts to Sussp1=Pr.2 $[ALG1_{\text{SPMSAC}}^{HASH}=1]-1$, where $\Pr[E_{vt1}]$ represents the probability of an event E_{vt1}. The advantage function for algorithm (experiment) $ALG1_{\text{SPMSAC}}^{HASH}$ is referred to as $Adv\_fun\_1_{\text{SPMSAC}}^{HASH}(t_{e1}, q_{Ry1}) = \max_{\mathbb{A}} [Sussp1_{\text{SPMSAC}}^{HASH}]$, with execution time t_{e1} and the corresponding random query q_{Ry1} as maximized on adversary ($\mathbb{A}$) [15-16, 27]. We could safely refer to the contributed protocol as secure against the attacker $\mathbb{A}$ so it may not recover the true identity IDi', provided $Adv\_fun\_1_{\text{SPMSAC}}^{HASH}(t_{e1}, q_{Ry1}) \leq \rho$ for any adequately small $\rho > 0$. According to the above testing algorithm, if the attacker $\mathbb{A}$ is capable enough of inverting a one-sided hash function $h(.)$, and deciphering the oracle, it might recover the valid legal IDi' and eventually wins the game. Nonetheless, keeping in view the above definition, this would be computationally impractical to reverse the hash function, as $Adv\_fun\_1_{\text{SPMSAC}}^{HASH}(t_{e1}) \leq \rho$ for any adequately small $\rho > 0$.

Algorithm 2. $ALG2_{\text{SPMSAC}}^{HASH}$

```
Attacker recovers information from smart card using power analysis as $SC\{PID_r, Di, Ei, Fi, Qi, h()\}$.
Attacker intercepts message $m2 = \{Qij, Ti, \beta j\}$ in the authentication phase, where $Qij = h(h(IDi || x) || \beta i || \beta j || Vi || SID)$, $Ti = PID_r' \oplus h(PID_r || IDi || Vi)$.
Calls Reveal oracle on input $Qij$ to produce $(h(IDi || x), \beta i, \beta j, Vi, SID)$ as $(h(IDi || x) || \beta i || \beta j || Vi || SID) \leftarrow reveal1(Qij)$
Calls Reveal oracle on input $h(IDi || x)$ to produce $(IDi', x')$ as $(IDi' || x') \leftarrow reveal1(h(IDi || x))$
Calls Reveal oracle on input $Fi$ to produce $(IDi, TPW')$ as $(IDi || TPW') \leftarrow (reveal1(Fi))$
Computes $K' = Ri \oplus h(x||y) = Qi \oplus h(y) \oplus TPW'$
Eavesdrops the message $m_1 = \{PID_r, ZIDi, Bij, \beta i\}$ in authentication phase, where $PID_r = (h(IDi || x), t) \oplus h(x || y)$, $ZIDi = h(PID_r || Vi || \beta i)$, $Bij = Ri \oplus h(x || y) \oplus h(h(SID || h(y)) || \beta i) \oplus h(PID_r || h(IDi || x))$.
Computes $Y = H(IDi || BIOi)$
Calls Reveal oracle on inputting $H(IDi || BIOi)$ to produce $(IDi, BIOi')$ as $(IDi || BIOi') \leftarrow reveal1(H(IDi || BIOi))$
Computes $Ri' = h(H(IDi' || BIOi') || x')$, $h(x || y) = Ri' \oplus K'$, $Vi' = h(Ri' || h(x || y))$
Calculates session key as $SKij^* = h(h(IDi' || x') || \beta i || \beta j || Vi' || SID)$
Compute $ZIDi'' = h(PID_r || Vi' || \beta i)$
If $(ZIDi' == ZIDi)$ Then
    Accept $SKij^*$ as the validated session key $SKij$ among participants $Ui$ and $Sj$.
    Return 1 (True)
Else
    Return 0 (False)
End if
```

Theorem 2. *If a one-sided hash function acts closely to some randomly behaving oracle, the contributed protocol shall remain protected of malicious adversary in case the latter attempts to intercept the parameters on insecure channel and compute a valid session key* SK_{ij}.

Table 2

A comparison of schemes on the basis of security features

	Liao and Wang [38]	Hsiang and Shih [18]	Lee et al. [33]	Chen and Lee [11]	Ours
Ensuring anonymity	✓	✓	✓	✓	✓
Supports mutual authentication	×	×	×	✓	✓
Immune to Insider Attack	×	✓	✓	✓	✓
Immune to Offline password-guessing threat	✓	✓	×	✓	✓
Immune to Stolen smart card threat	✓	✓	✓	×	✓
Immune to Impersonation threat	×	×	×	×	✓
Immune to KCI threat	✓	×	✓	×	✓
Supports session key security	✓	✓	✓	×	✓
Immune to trace attack	✓	✓	✓	×	✓
Reparability	✓	×	×	✓	✓
Efficient Password Modification	✓	✓	×	×	✓

Table 3

The computational cost of schemes

		Liao and Wang [38]	Hsiang and Shih [18]	Lee et al. [33]	Chen and Lee [11]	Ours
Login & Authentication phase	Server side	$7T_h$	$9T_h$	$8T_h$	$8T_h$	$8T_h$
	User side	$9T_h$	$10T_h$	$10T_h$	$11T_h$	$11T_h+3T_H$
	RC	$0T_h$	$5T_h$	$0T_h$	$0T_h$	$0T_h$
Total		$16\ T_h$	$24T_h$	$18T_h$	$19T_h$	$19T_h+3T_H$
Computation delay (s)		*0.008*	*0.012*	*0.009*	*0.0095*	*0.0395*
Energy (μJ)		*12.16*	*14.44*	*18.24*	*13.68*	*16.72*

Proof. In this proof, the attacker $\mathbb{A}$ having approached the publicly available parameters as *{PID*$_r$, *ZIDi, Bij, βi, Qij , Ti, βj, Qij }*, might use the oracle *Reveal1* to implement algorithm $ALG2^{HASH}_{\mathrm{SPMSAC}}$. The probability for the success of $ALG2^{HASH}_{\mathrm{SPMSAC}}$ amounts to Sussp2=Pr.2[$ALG2^{HASH}_{\mathrm{SPMSAC}}$ =1] - 1, where Pr[E_{vt2}] characterizes probability for an event E_{vt2}. The advantage function for algorithm $ALG2^{HASH}_{\mathrm{SPMSAC}}$ is referred to as $Adv\_fun\_2\ ^{HASH}_{\mathrm{SPMSAC}}$ (t_{e2}, q_{Ry2}) =max$_{\mathbb{A}}$ $Sussp2^{HASH}_{\mathrm{SPMSAC}}$], with the execution time t_{e2}, while the corresponding random query q_{Ry2} is maximized on adversary ($\mathbb{A}$) [15-16, 27]. We could safely refer to the contributed protocol as protected against the adversary $\mathbb{A}$ so it might not derive the convincing session key SK_{ij}, provided $Adv\_fun\_2\ ^{HASH}_{\mathrm{SPMSAC}}(t_{e2}, q_{Ry2}) \leq \rho$ for any adequately small $\rho > 0$ [24-25, 48]. According to this testing algorithm, if the adversary $\mathbb{A}$ is able enough to reverse the one-sided hash function *h(.)*, and decipher the oracle, it might recover the valid session key SK_{ij}, for that *IDi'*, and eventually wins the game. Nonetheless, keeping in view the above definition, this would be computationally impractical to invert hash function [20-22, 36-37, 50] $Adv\_fun\_2\ ^{HASH}_{\mathrm{SPMSAC}}(t_{e2}) \leq \rho$ for any adequately small $\rho > 0$.

7. Comparison and Performance Evaluation

In this section, we evaluate the strength for proposed protocol with other MSA-based protocols [11, 18, 33, 38]. Table 2 shows the security features and the analysis of resistance to various threats for various schemes, which signifies the contributed scheme as a resilient authenticated key agreement in contrary to previous schemes. For comparing the costs, we depict the hash-digest operation with T_h and bio-hashing with T_H and ignoring XOR function due to a quite negligible cost as shown in Table 3. The comparison in Table 2 is shown for Liao and Wang [38], Hsiang and Shih [18], Lee et al. [33], Chen and Lee [11], and our proposed scheme. Therefore, in view of the current performance evaluation, we infer that the proposed model is quite more secure than Liao and Wang, Hsiang and Shih, Lee et al., and Chen and Lee's schemes. All of these schemes are based on light weight hashed based symmetric cryptography. The contributed protocol bears a bit higher computation cost than Liao and Wang, and Lee et al., and Chen and Lee's schemes, but provides more security. Moreover, our scheme achieves the required security objectives in less cost than Hsiang and Shih's scheme. Adding a bit extra and negligible cost, the proposed protocol is immune to insider attack, password guessing attack, stolen smart card attack, impersonation and trace attacks as compared to previous schemes. Comparing on the same lines and taking the computation delay of hash function as 0.0005s and bio-hash operation as 0.01s, the cost of Liao and Wang, Lee et al., Chen and Lee, Hsiang and Shih, and proposed scheme amounts to 0.008s, 0.009s, 0.0095s, 0.012s, and 0.395s, respectively. Furthermore, the protocols may also be analyzed on account of energy consumptions by taking the energy cost of computation for SHA-1 as 0.76μJ against single byte [43]. Following this, the energy consumption for the Liao and Wang's, Lee et al.'s, Chen and Lee's, Hsiang and Shih's and contributed protocol amounts to 12.16, 13.68, 14.44, 18.24, and 16.72μJ, respectively. As obvious from Table 3, the proposed protocol has a bit more cost than other related schemes; this is for the reason that it makes a use of bio-hash function, which increases the cost of the proposed protocol from 0.01s to 0.395s. This paper makes the proper use of biometric input by employing bio-hash function, unlike previous schemes. Hence, in view of the current performance evaluation, we can safely deduce that our proposed protocol is secure enough as compared to other schemes being analyzed, and achieves this objective in almost an equivalent cost.

8. Conclusion

The multi-server authentication robustness is considered as a crucial requisite of the existing remote authentication paradigm. Much of the research efforts can be witnessed to strengthen multi-server authentication protocols, lately. This paper critically examines the Chen and Lee's multi-server authentication protocol. The Chen and Lee's protocol has been found recently susceptible to few attacks. Its cryptanalysis suggests the three ways where the Chen and Lee's protocol could be attacked or termed as inefficient. The Chen and Lee's scheme was found defenseless to impersonation attack, trace attack, stolen smart card attack exposing session key, key-compromise impersonation attack and inefficient password modification. The proposed study identified these attacks and also demonstrated an improved version countering the identified threats. This paper is complemented with formal security analysis and performance evaluation analysis among different schemes.

References

1. Amin, R., Biswas, G. P. Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-Server Environment. Wireless Personal Communications, 2015, 84(1), 439-462.
2. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Kumar, N. A Robust and anonymous Patient Monitoring System Using Wireless Medical Sensor Networks. Future Generation Computer Systems, 2018, 80, 483-495.
3. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., Kumar, N. Design of an Anonymity-Preserving Three-Factor Authenticated Key Exchange Protocol for Wireless Sensor Networks. Computer Networks, 2016, 101, 42-62.

4. Arshad, H., Nikooghadam, M. An Efficient and Secure Authentication and Key Agreement Scheme for Session Initiation Protocol Using ECC. Multimedia Tools and Applications, 2016, 75(1), 181-197.

5. Bellare, M., Rogaway, P. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. Proceeding of the ACM Conference on Computer and Communications Security, Fairfax, VA, USA, 1993, 62-73.

6. Burrows, M., Abadi, M. A Logic of Authentication. Proceedings of the Royal Society of London. Series A, 1989, 426(1871), 233-271.

7. Chang C. C., Lee C. Y. A Smart Card-Based Authentication Scheme Using User Identify Cryptography. International Journal of Network Security 2013, 15(2), 139-147.

8. Chang, C. C., Lee, J. S. An Efficient and Secure Multi-server Password Authentication Scheme Using Smart Cards. IEEE Proceedings of the International Conference on Cyberworlds, Tokyo, Japan, 2004, 417-422.

9. Chaudhry, S. A., Farash, M. S., Naqvi, H., Sher, M. A Secure and Efficient Authenticated Encryption for Electronic Payment Systems Using Elliptic Curve Cryptography. Electronic Commerce Research, 2016, 16(1), 113-139.

10. Chaudhry, S. A., Naqvi, H., Sher, M., Farash, M. S., Hassan, M. U. An Improved and Provably Secure Privacy Preserving Authentication Protocol for SIP. Peer-to-Peer Networking and Applications, 2017, 10(1), 1-15.

11. Chen, C. T., Lee, C. C. A Two-Factor Authentication Scheme with Anonymity for Multi-Server Environments. Security and Communication Networks, 2015, 8(8), 1608-1625.

12. Das, A. K., Goswami, A. A Secure and Efficient Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care. Journal of Medical Systems, 2013, 37(3), 1-16.

13. He, D. An Efficient Remote User Authentication and Key Agreement Protocol for Mobile Client–Server Environment from Pairings. Ad Hoc Networks, 2012, 10(6), 1009-1016.

14. He, D., Kumar, N., Chilamkurti, N. A Secure Temporal-Credential-Based Mutual Authentication and Key Agreement Scheme with Pseudo Identity for Wireless Sensor Networks. Information Sciences, 2015, 321, 263-277.

15. He, D., Wang, D. Robust Biometrics-Based Authentication Scheme for Multiserver Environment. IEEE Systems Journal, 2015, 9(3), 816-823.

16. He, D., Zeadally, S., Kumar, N., Wu, W. Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures. IEEE Transactions on Information Forensics and Security, 2016, 11(9), 2052-2064.

17. He, D., Zhao, W., Wu, S. Security Analysis of a Dynamic ID-Based Authentication Scheme for Multi-Server Environment Using Smart Cards. International Journal of Network Security 2013, 15(5), 350-356.

18. Hsiang, H. C., Shih, W. K. Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment. Computer Standards and Interfaces 2009, 31(6), 1118–1123.

19. Irshad, A., Chaudhry, S. A., Xie, Q., Li, X., Farash, M. S., Kumari, S., Wu, F. An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture. Arabian Journal for Science and Engineering, 2018, 43(2), 811-828.

20. Irshad, A., Sher, M., Ashraf, M. U., Alzahrani, B. A., Wu, F., Xie, Q., & Kumari, S. An Improved and Secure Chaotic-Map Based Multi-Server Authentication Protocol Based on Lu et al. and Tsai and Lo's Scheme. Wireless Personal Communications, 2017, 95(3), 3185-3208.

21. Irshad, A., Sher, M., Chaudhary, S. A., Naqvi, H., Farash, M. S. An Efficient and Anonymous Multi-Server Authenticated Key Agreement Based on Chaotic Map Without Engaging Registration Centre. The Journal of Supercomputing, 2016, 72(4), 1623-1644.

22. Irshad, A., Sher, M., Nawaz, O., Chaudhry, S. A., Khan, I., Kumari, S. A Secure and Provable Multi-Server Authenticated Key Agreement for TMIS Based on Amin et al. Scheme. Multimedia Tools and Applications, 2017, 76(15), 16463-16489.

23. Islam, S. K., Obaidat, M. S., Amin, R. An Anonymous and Provably Secure Authentication Scheme for Mobile User. International Journal of Communication Systems, 2016, 29(9), 1529-1544.

24. Jiang, Q., Khan, M. K., 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.

25. Jiang, Q., Ma, J., Li, G., Li, X. Improvement of Robust Smart-Card-Based Password Authentication Scheme. International Journal of Communication Systems, 2015, 28(2), 383-393.

26. 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.

27. Jiang, Q., Ma, J., Lu, X., Tian, Y. An Efficient Two-Factor User Authentication Scheme with Unlinkability for Wireless Sensor Networks. Peer-to-Peer Networking and Applications, 2015, 8(6), 1070-1081.

28. Jin, A. T. B., Ling, D. N. C., Goh, A. Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number. Pattern Recognition, 2004, 37(11), 2245-2255.

29. Juang, W. S. Efficient Multi-Server Password Authenticated Key Agreement Using Smart Cards. IEEE Transactions on Consumer Electronics 2004, 50(1), 251-255.

30. Kalra, S., Sood, S. K. Secure Authentication Scheme for IoT and Cloud Servers. Pervasive and Mobile Computing, 2015, 24, 210-223.

31. Kocher, P., Jaffe, J., Jun, B. Differential Power Analysis. In: Advances in Cryptology CRYPTO 99, Lecture Notes in Computer Science, 1999, 1666, 388-397.

32. Kumari, S., Chaudhry, S. A., Wu, F., Li, X., Farash, M. S., Khan, M. K. An Improved Smart Card Based Authentication Scheme for Session Initiation Protocol. Peer-to-Peer Networking and Applications, 2017, 10(1), 92-105.

33. Lee, C. C., Lin, T. H., Chang, R. X. A Secure Dynamic ID Based Remote User Authentication Scheme for Multiserver Environment Using Smart Cards. Expert Systems with Applications, 2011, 38(11), 13863-13870.

34. Lee, W. B., Chang, C. C. User Identification and Key Distribution Maintaining Anonymity for Distributed Computer Networks. Computer Systems Science and Engineering, 2000, 15(4), 211-214.

35. Li, L. H., Lin, L. C., Hwang, M. S. A Remote Password Authentication Scheme for Multiserver Architecture Using Neural Networks. IEEE Transactions on Neural Networks, 2001, 12(6), 1498-1504.

36. Li, X., Ma, J., Wang, W., Xiong, Y., Zhang, J. A Novel Smart Card and Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environments. Mathematical and Computer Modelling, 2013, 58(1), 85-95.

37. Li, X., Xiong, Y., Ma, J., Wang, W. An Efficient and Security Dynamic Identity Based Authentication Protocol for Multi-Server Architecture Using Smart Cards. Journal of Network and Computer Applications, 2012, 35(2), 763-769.

38. Liao, Y. P., Wang, S. S. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment. Computer Standards & Interfaces 2009, 31(1), 24-29.

39. Lin, I. C., Hwang, M. S., Li, L. H. A New Remote User Authentication Scheme for Multi-Server Architecture. Future Generation Computer Systems, 2003, 19(1), 13-22.

40. Mir, O., Nikooghadam, M. A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for e-Health Services. Wireless Personal Communications, 2015, 83(4), 2439-2461.

41. 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.

42. Nikooghadam, M., Jahantigh, R., Arshad, H. A Lightweight Authentication and Key Agreement Protocol Preserving User Anonymity. Multimedia Tools and Applications, 2017, 76(11), 13401-13423.

43. Potlapally, N. R., Ravi, S., Raghunathan, A., Jha N. K. A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols. IEEE Transactions on Mobile Computing, 2006, 5(2), 128-143.

44. Ravanbakhsh, N., Nazari, M. An Efficient Improvement Remote User Mutual Authentication and Session Key Agreement Scheme for E-Health Care Systems. Multimedia Tools and Applications, 2018, 77(1), 55-88.

45. Sharma, G., Kalra, S. Identity Based Secure Authentication Scheme Based on Quantum Key Distribution for Cloud Computing. Peer-to-Peer Networking and Applications, 2018, 11(2), 220-234.

46. Tsai, J. L. Efficient Multi-Server Authentication Scheme Based on One-Way Hash Function Without Verification Table. Computers & Security, 2008, 27(3-4), 115-121.

47. Tsaur, W. J. A Flexible User Authentication Scheme for Multi-Server Internet Services, In International Conference on Networking, LNCS 2093, Springer Verlag, Colmar, France, 2001, 174-183.

48. Wang, C., Zhang, X., Zheng, Z. Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme. Plos One, 2016, 11(2), e0149173.

49. Wang, D., Wang, P. On the Anonymity of Two-Factor Authentication Schemes for Wireless Sensor Networks: Attacks, Principle and Solutions. Computer Networks, 2014, 73, 41-57.

50. Wazid, M., Das, A. K., 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.

51. Wu, T. S., Hsu, C. L. Efficient User Identification Scheme with Key Distribution Preserving Anonymity for Distributed Computer Networks. Computers & Security, 2004, 23(2), 120-125.

52. 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.