ITC 2/48
Journal of Information Technology and Control
Vol. 48 / No. 2 / 2019
pp. 211-224
DOI 10.5755/j01.itc.48.2.17417

An Improved Biometric Multi-Server Authentication Scheme for Chang et al.'s Protocol

Received 2017/01/15 | Accepted after revision 2019/05/06

http://dx.doi.org/10.5755/j01.itc.48.2.17417

An Improved Biometric Multi-Server Authentication Scheme for Chang et al.'s Protocol

Azeem Irshad
Department of Computer Science & Software Engineering, International Islamic University, Islamabad,
e-mail: irshadazeem2@gmail.com

Shehzad Ashraf Chaudhry
Department of Computer Science & Software Engineering, International Islamic University, Islamabad
Faculty of Computing & Information Technology, University of Sialkot, Pakistan,
e-mail: ashraf.shehzad.ch@gmail.com

Muhammad Shafiq
Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, South Korea,
e-mail: shafiq.pu@gmail.com

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

Muhammad Asif
Department of Computer Science, National Textile University, Faisalabad, Pakistan, e-mail: asif@ntu.edu.pk

Sajid Ali
Department of information sciences, University of Education, Lahore, Pakistan, e-mail: sajid.ali@ue.edu.pk

Saru Kumari
Department of Mathematics, Chaudhary Charan Singh University, Meerut, Uttar Pradesh 250004, India,
e-mail: saryusiirohi@gmail.com

Corresponding author: ashraf.shehzad.ch@gmail.com

The remote authentication has been advancing with the growth of online services being offered on remote basis. This calls for an optimal authentication framework other than single-server authentication. In this connection, the multi-server authentication architecture has been introduced in the literature that enables the users to avail variety of services of various service providers, using a single pair of identity and password. Lately, we have witnessed a few multi-server authentication protocols in the literature that had several limitations. One of those multi-server authentication protocols has been put forward by Chang et al. recently. Our analysis shows that the Chang et al.'s scheme is susceptible to impersonation threat, stolen smart card threat. In this study, we have reviewed the protocol thoroughly, and proposed an improved model, that is resistant to all known and identified threats. The formal security analysis along with discussion of informal analysis for contributed model is also presented in this study, besides performance and its evaluation analysis.

KEYWORDS: Multiserver authentication, cryptanalysis, biometrics, remote authentication, attacks.

1. Introduction

The growth of internet has facilitated the day-to-day introduction of new services on remote basis. In this regard, an efficient Multi-Server Authentication (MSA) serves as an integral component of this growth, which lets the users avail remote services from different servers, by utilizing a single pair of identity and password for all servers [10, 21, 29, 33]. MSA not only relieves the user of the hassle of memorizing so many passwords, but also relaxes the servers of individualized registration procedures with each user, prior to the authentication phase [17]. In the last five years, many multi-server authentication schemes were presented. Nevertheless, there is still a need of more secure and efficient techniques [35]. In MSA literature, for neural networks, Li et al. [23], Lin et al. [30], Juang [18], Chang and Lee [3] contributed few techniques that were based on symmetric cryptography and discrete logarithms. However, these schemes did not protect the identity of user, and were also computationally inefficient for their operations cost. Afterwards, Liao and Wang [28] presented a dynamic identity- based MSA protocol. However, the scheme was found vulnerable by Hsiang and Shih [9], for lacking mutual authentication, and improved scheme was presented by Hsiang and Shih. Then, Yeh et al. [36] found that the previous scheme is exposed to session key disclosure, replay threat, and forgery threat. Thereafter, Lee et al. [22] indicated that Yeh et al.'s scheme is prone to masquerading attack and also lacks mutual authentication. At the same time, Sood et al. [34] specifies that the same Yeh et al. protocol suffers stolen smart card, impersonation threat, and a flawed password changing procedure. Sood et al. and Lee et al. also demonstrated their enhanced models. Then, Li et al. [24, 27] discovered a mutual authentication weakness in Sood et al. protocol, and server spoofing, faulty authentication procedure in Lee et al.'s scheme [22], with contribution of improved schemes, respectively. Afterwards, Chang et al. [5] proposed a dynamic identity based authentication scheme, which was found to be vulnerable in impersonation threat, stolen smart card threat, insider threat, and password-guessing threat by Li et al. [26]. The Li et al. [24] protocol was found to be vulnerable against forgery attack by Chang et al. [4] and an inherent design weakness was discovered by Chang et al. that was providing the attacker a chance to perform illegal activities without being caught. Thereafter, Chang et al. put forward an enhanced model for protocol [24]. After careful study of Chang et al. [4], we found that the Chang et al.'s model is prone to impersonation threat, and session key disclosure attacks, once smart card gets stolen. We have contributed an enhanced biometric authentication model that covers all of the indicated limitations in the Chang et al. scheme. This study work demonstrates formal analysis of security and performance evaluation as well.

Our protocol is arranged in the following order: The section "Preliminaries" defines the preliminaries related to our scheme and section "A review of the Chang et al.'s protocol" presents a review and cryptanalysis of Chang et al.'s protocol. The section "Proposed model" demonstrates our contributed protocol. The section "Security discussion" and section "Formal security analysis" illustrate informal and formal security analysis, respectively. The "Comparison and performance analysis" section depicts the related performance analysis. The last section summarizes this paper.

2. Preliminaries

The properties of hash digest and bio-hashing function are illustrated in preliminaries section.

2.1. Hash Function

To act as a secure authentication protocol, one of the constituent lightweight crypto-operations, i.e. a one-way hash function $h: \{0, 1\}^* \rightarrow Z_q^*$, must hold the understated features.

1. The function h generates a fixed length hash digest after taking a variable sized input.
2. In case $h(\mu)=\delta$, it is hard in polynomial time for computing $h^{-1}(\delta)= \mu$;
3. If μ is given, it is improbable to compute μ' in polynomial time, such that $\mu' \neq \mu$ holds as well as $h(\mu') = h(\mu)$;
4. In addition, it is hard to get a pair (μ, μ') given that $\mu' \neq \mu$ and $h(\mu')$=h(μ) holds at the same time.

2.2. Bio-hashing

The bio-hashing function [19] is employed for capturing the inherent biometric features of a person, such as fingerprint to be used for authentication purpose, while these features remains permanent over a period of time. Jin et al. [16], in 2004 came up with a two-factor authenticator protocol which bears iterated inner products, as kept between tokenized pseudorandom number and user-oriented finger impression-based features. This procedure computes a particular compact code which provides the basis for the current bio-hashing concept. Thereafter, this bio-hashing function was improved further by Lumini and Loris [32]. The bio-hashing function produces a unique random vector as a function of specific user's biometric features, which is named as a Biocode. This, in addition, helps in discretizing the projection-coefficients and is computed as secure hashed password in general.

3. A Review of the Chang et al.'s Scheme

The protocol's working of Chang et al. [4] is described as under.

3.1. Revisiting Chang et al.'s Model

The Chang et al.'s model [4] is comprised of three procedures, such as the registration procedure, mutual authentication procedure which is also shown in Figure 1. We present a few notations that may be helpful to readers to comprehend the scheme as given in Table 1.

Table 1
Symbols guide

Notations	Meaning
Ui:	ith Subscriber or User
IDi, PWi	Subscriber's identity and password
H():	Private hash function
$H_B()$:	Bio-hashing function
SPj:	The jth service provider
RC:	Registration centre
h(.):	a secure hash digest function
Bi:	Biometric impression
K, b:	RC's master secret, RC's random secret
ni, nj:	Nonce
SC:	Smart Card
$\|\|, \oplus$	Concatenation and XOR functions

3.1.1. Server Registration Procedure

The Chang et al.'s model comprises a reliable registration centre (***RC***) along with n number of servers (***SPj***), while the range of $\boldsymbol{j}$ implies $\boldsymbol{1 \leq j \leq n}$. The *SPj* completes its registration procedure with RC before the user's registration. The ***SPj*** is registered from ***RC*** with the sharing of two secrets $\boldsymbol{K_1}$ and $\boldsymbol{K_2}$ between ***SPj*** and ***RC*** over a confidential channel. Earlier, RC selects a master secret key k and a random integer b. Afterwards, SPj submits the identity ***SIDj*** towards registration centre. Then, RC calculates $\boldsymbol{K_1 = h(k \,||\, b)}$ and $\boldsymbol{K_2 = h(SIDj \,||\, H(b))}$. Here, H(.) is a private hash digest, while h(.) represents public hash-digest function. Onwards, the registration centre forwards these keys to ***SPj*** employing a confidential channel.

Figure 1

Chang et al.'s registration and mutual authentication procedure

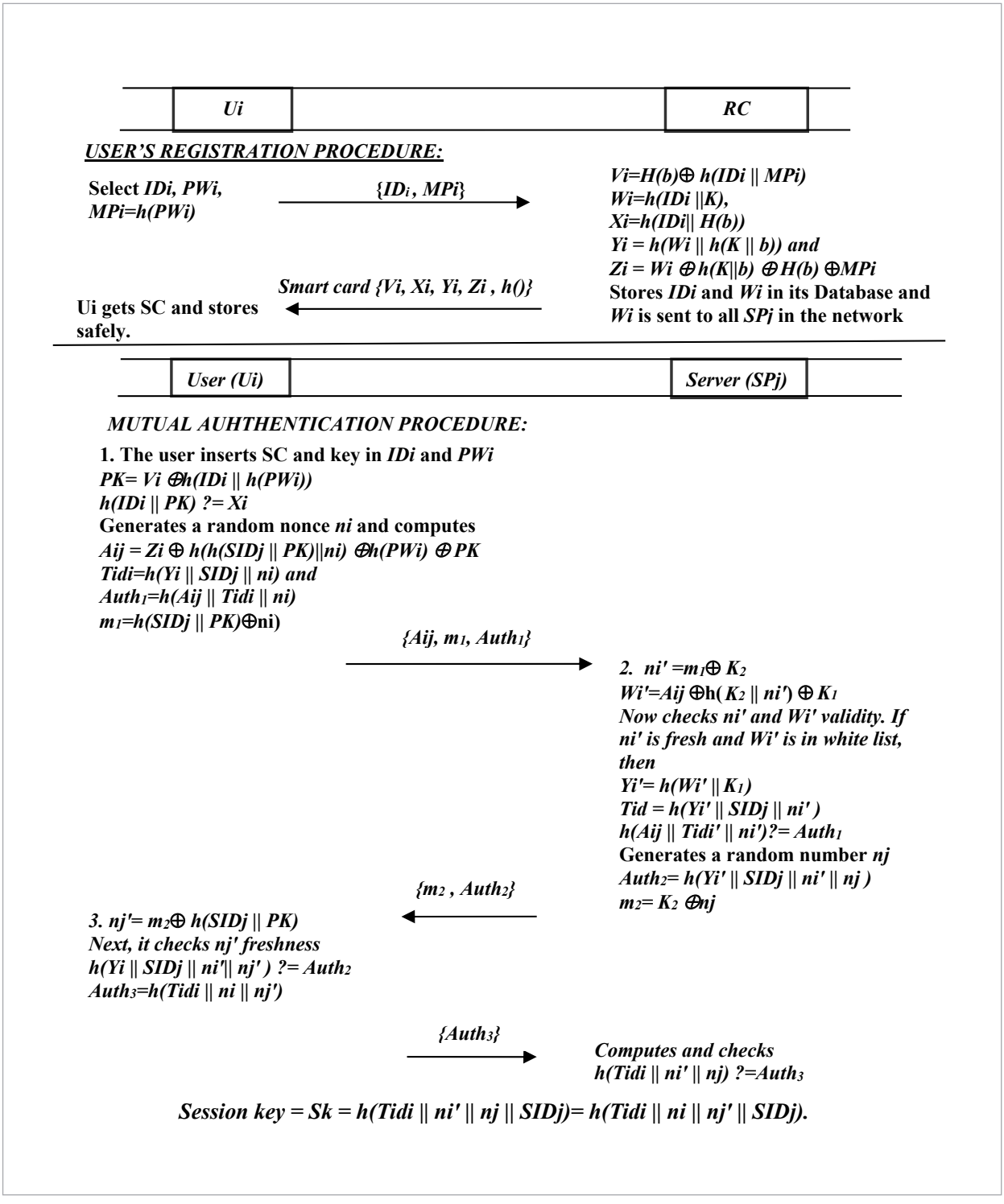
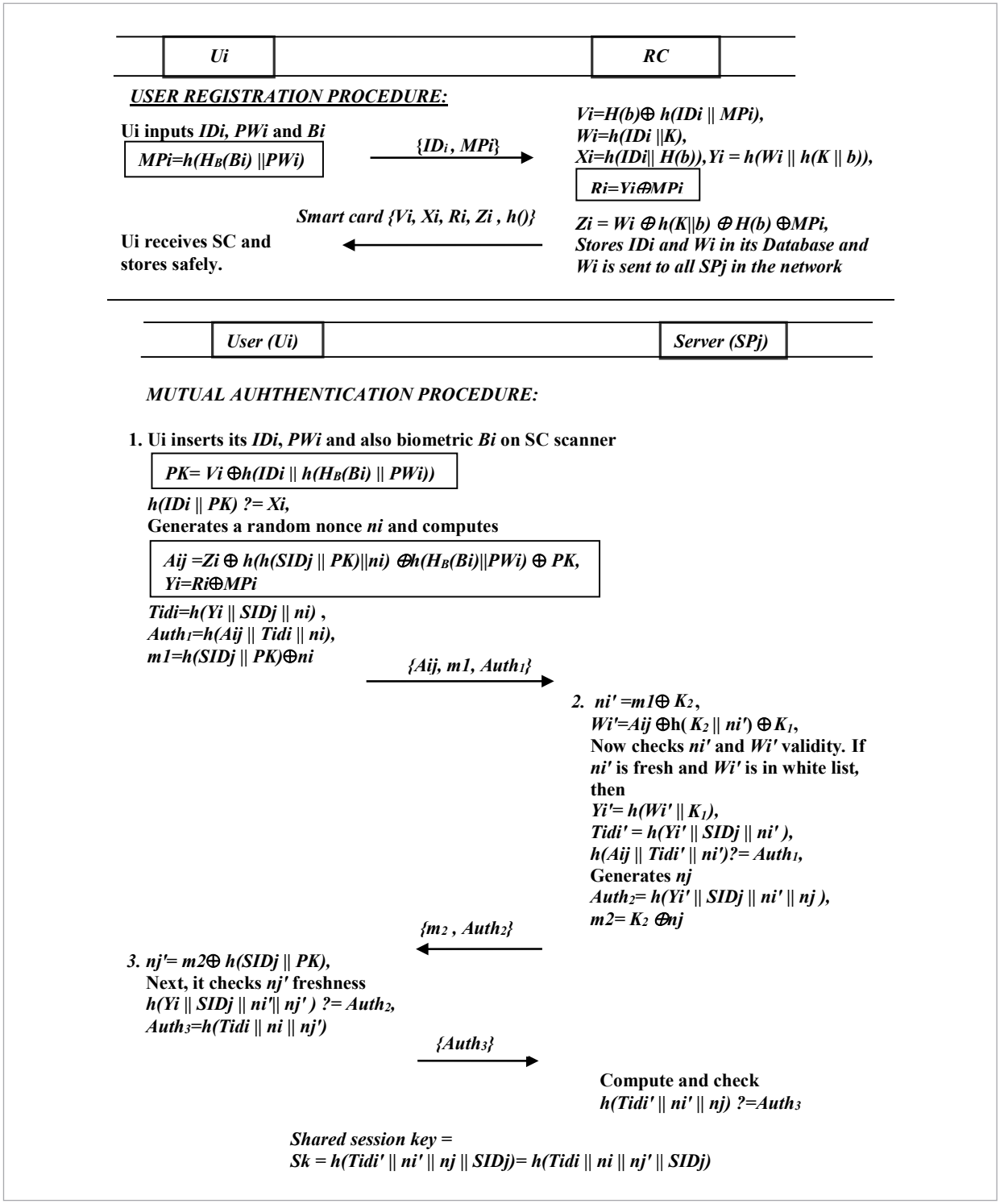


Figure 2
Proposed model



3.1.2. User Registration Procedure

In the registration procedure, Ui performs few registration steps with the RC. Afterwards Ui may access all service providers SPj. The RC performs the undermentioned steps with the user to implement the registration procedure.

1 Primarily, Ui chooses its identity ***(IDi)*** and a password ***(PWi)***. Then, it computes ***MPi by*** calculating ***MPi=h(PWi)*** and it sends ***{ID$_i$, MPi}*** to ***SPj*** as shown in Figure 1**.**

2 ***SPj,*** then, calculates ***Vi=H(b)*** $\oplus$ ***h(IDi || MPi), Wi=h(IDi || k), Xi=h(IDi || H(b)), Yi = h(Wi || h(k || b))*** and ***Zi = Wi*** $\oplus$ ***h(k||b)*** $\oplus$ ***H(b)*** $\oplus$ ***MPi.*** Afterwards, ***SPj*** stores ***IDi*** and ***Wi*** in its database, while ***Wi*** is sent to all servers in the network**.** ***RC*** now issues smart card to ***Ui*** with these parameters ***{Vi, Xi, Yi, Zi*** and ***h()}.***

3.1.3. Mutual Authentication Procedure

1 In this procedure, ***Ui*** employs its smart card to avail the ***SPj's*** services. For this reason, the user inserts SC and gives ***IDi*** and ***PWi*** as input. Next, it computes ***PK= Vi*** $\oplus$ ***h(IDi || h(PWi))*** and checks the equality ***h(IDi || PK) ?= Xi.*** On successful check, it produces a random nonce ***ni*** and calculate ***Aij = Zi*** $\oplus$ ***h(h(SIDj || PK)||ni)*** $\oplus$ ***h(PWi)*** $\oplus$ ***PK, Tidi=h(Yi || SIDj || ni), Auth$_1$=h(Aij || Tidi || ni)*** and ***m$_2$=h(SIDj || PK)*** $\oplus$ ***ni)***. Next, it submits the message ***{Aij, m$_2$, Auth$_1$}*** to ***SPj*** for verification**.**

2 The ***SPj*** receives ***{Aij, m$_2$, Auth$_1$}*** and computes ***ni' =m$_2$*** $\oplus$ ***K$_2$*** and ***Wi'=Aij*** $\oplus$ ***h(K$_2$ || ni')*** $\oplus$ ***K$_1$***. ***SPj*** now checks validity and freshness of ***ni'*** and ***Wi'.*** If ***ni'*** is fresh and ***Wi'*** is in its white list, it computes ***Yi'= h(Wi'||*** $_{K1}$***)*** and ***Tidi = h(Yi'||SIDj||ni').*** Next, it checks the equality ***h(Aij||Tidi'||ni')?= Auth$_1$.*** If true, it engenders a random integer ***nj*** and further calculates ***Auth$_2$= h(Yi'||SIDj||ni'||nj), m$_2$= K$_2$*** $\oplus$ ***nj.*** Next**,** it sends ***{m$_2$, Auth$_2$}*** to ***Ui***.

3 After receiving ***{m$_2$, Auth$_2$}***, ***Ui,*** calculates ***nj'= m$_2$*** $\oplus$ ***h(SIDj || PK***). He/She checks the validity or freshness for ***nj'*** and computes ***h(Yi || SIDj || ni'||nj')*** for checking the validity ***h(Yi || SIDj || ni'||nj') ?= Auth$_2$.*** If true, then calculates ***Auth$_3$= h(Tidi||ni||nj'),*** and sends the message ***{Auth$_3$}*** to ***SPj*** as acknowledgement.

4 ***SPj*** receives ***Auth$_3$*** message and computes ***h(Tidi || ni' || nj)*** for checking ***h(Tidi || ni' || nj) ?=Auth$_3$.*** If it proves to be valid, a session key is computed between the participants, as ***Sk=h(Tidi||ni'||nj||SIDj)=h(Tidi||ni||nj'||SIDj).***

3.2. Cryptanalysis of Chang et al.'s Protocol

The Chang et al.'s protocol is a multi-server authentication-based scheme relying on simple hash and XOR operations. Before presenting the limitations in Chang et al.'s model, we assume that adversary is proficient in the following capabilities.

- The adversary may intercept, modify or manipulate the message contents communicated on insecure public channel.
- The adversary may access the smart card and its parameters by stealth.
- The adversary might not get any of the contents communicated on secure channel, for instance, in registration phase.

The Chang et al.'s protocol is susceptible to the following attacks.

3.2.1. Impersonation Attack

The Chang et al.'s protocol is prone to impersonation attack if the user's smart card contents are revealed to adversary. Suppose, Eve, a valid but malicious user happens to steal the user's smart card contents in some manner. In this context, Eve seize all SC parameters ***{Vi, Xi, Yi, Zi}*** and intercepts public messages ***{Aij, m$_2$, Auth$_1$, m$_2$, Auth$_2$, Auth$_3$}***. Next, Eve may adopt the following steps to launch an impersonation attack.

1 Initially, Eve computes ***PK*** such as ***PK = Vi*** $\oplus$ ***h(ID$_{Eve}$||MPi),*** where ***PK*** and ***H(b)*** represent the same parameters.

2 Then, Eve computes ***ni=h(SIDj || PK)*** $\oplus$ ***m$_2$***.

3 Next, the ***PWi***, being a low entropy password, can easily be guessed by applying and testing various combinations ***PWi**** in the equation ***Aij ?= Zi*** $\oplus$ ***h(h(SIDj || PK)||ni)*** $\oplus$ ***h(PWi*)*** $\oplus$ ***PK.*** Wherever the match is found, the valid ***PWi*** becomes known**.**

4 After the seizure of SC contents and guessing the password ***PWi***, Eve may launch impersonation attacks on both sides (user and server). *On user's end*, having the knowledge of ***Yi*** and ***Zi,*** Eve generates a nonce ***ni*** and constructs the login message ***{Aij, m$_2$, Auth$_1$}*** comfortably by computing

$Tidi=h(Yi \| SIDj \| ni)$, $Auth_1=h(Aij \| Tidi \| ni)$, and $m_2=h(SIDj \| PK) \oplus ni$) towards server. *On server's end,* while impersonating as a server, Eve sends the message $\{m_2, Auth_2\}$ towards user by generating fresh nonce nj and computing $Auth_2= h(Yi \| SIDj \| ni' \| nj)$ and $m_2= h(SIDj \| PK) \oplus nj$.

3.2.2. No Session Key Security

In Chang et al.'s protocol, the attacker could deduce the session key comfortably, once the smart card is accessed by it. Since the session key is composed as $Sk = h(Tidi \| ni \| nj \| SIDj)$, Eve may try to reproduce Sk on the basis of computed elements. For this purpose, Eve, having the knowledge of $\{Vi, Xi, Yi, Zi, m_2\}$ parameters, computes $PK = Vi \oplus h(ID_{Eve} \| MPi)$, $ni=h(SIDj \| PK) \oplus m_2$, $nj = h(SIDj \| PK) \oplus m_2$, and $Tidi=h(Yi \| SIDj \| ni)$. Finally, Eve can generate the session key by concatenating as $Sk = h(Tidi \| ni \| nj \| SIDj)$. In this manner, Eve may generate all previous session keys by approaching the publicly available messages as communicated between the legal participants.

4. Proposed Scheme

Our proposed model is based on countering the limitations in Chang et al.'s model. The contributed model comprises service provider (server's) registration procedure, user's registration procedure, mutual authentication procedure, and password upgrading procedure.

4.1. Server Registration Procedure

The proposed model comprises a trustworthy RC and n number of servers (SPj), while the range of j implies $1 \le j \le n$. The SPj performs the registration with RC prior to user's registration procedure, using a secret channel. During initialization process, RC selects a master secret key k, and also chooses a random secret b. Then, SPj forwards its identity SIDj towards registration centre. Next, RC computes the two keys as $K_1=h(k \| b)$ and $K_2= h(SIDj \| H(b))$, and sends both keys (K_1 and K_2) to SPj employing a confidential channel. In this manner, the SPj gets registered through RC.

4.2. User Registration Procedure

In registration phase, Ui registers with registration centre (RC) and follows the under-mentioned steps:

1. The user initially selects its identity as IDi, password as PWi, and the biometric as Bi [17]. Subsequently, Ui calculates $MPi=h(H_B(Bi) \| PWi)$ and submits $\{ID_i, MPi\}$ to SPj.
2. Next, SPj calculates $Vi=H(b) \oplus h(IDi \| MPi)$, $Wi=h(IDi \| \| k)$, $Xi=h(IDi \| H(b))$, $Yi = h(Wi \| h(k \| b))$ $Ri=Yi \oplus MPi$, and $Zi = Wi \oplus h(k \| b) \oplus H(b) \oplus MPi$, and stores IDi and Wi in its database, while Wi is sent to all SPj in the network. Next, RC issues smart card to Ui with these parameters $\{Vi, Xi, Ri, Zi$ and $h()\}$.

4.3. Mutual Authentication Procedure

In this stage, the user is mutually authenticated with server SPj and uses smart card to avail services. The related procedure is shown in Figure 2.

1. Initially, Ui inserts its smart card in scanner and also inputs its ID and PWi. Then, it captures the biometric imprint Bi. Afterwards, Ui calculates $PK= Vi \oplus h(IDi \| h(H_B(Bi) \| PWi))$ and verifies the equality for $h(IDi \| PK) ?= Xi$. If true, then Ui engenders a random integer ni and further calculates $Aij = Zi \oplus h(h(SIDj \| PK) \| ni) \oplus h(H_B(Bi) \| PWi) \oplus PK$, $Yi = Ri \oplus MPi$, $Tidi=h(Yi \| SIDj \| ni)$, $Auth_1=h(Aij \| Tidi \| ni)$ and $m_2=h(SIDj \| PK) \oplus ni$). Then, Ui sends the message $\{Aij, m_2, Auth_1\}$ to SPj for verification.
2. Next, the SPj receives the message $\{Aij, m_2, Auth_1\}$ and computes $ni' =m_2 \oplus K_2$ and $Wi'=Aij \oplus h(K_2 \| ni') \oplus K_1$. The SPj confirms the validity and freshness of ni' and Wi'. If ni' is fresh and Wi' is in the white list, then it further computes $Yi'= h(Wi' \| K_1)$ and $Tidi = h(Yi' \| SIDj \| ni')$. Now, it verifies the equation $h(Aij \| Tidi' \| ni')?= Auth_1$. If this proves to be true, it engenders a random number nj, and computes $Auth_2= h(Yi' \| SIDj \| ni' \| nj)$ and $m2= K_2 \oplus nj$. Then, it sends $\{m_2, Auth_2\}$ to Ui for further verifications.
3. Upon receiving $\{m_2, Auth_2\}$ from SPj, Ui calculates $nj'= m_2 \oplus h(SIDj \| PK)$. Ui checks the validity for nj' and computes $h(Yi \| SIDj \| ni' \| nj')$ for verifying the validity for $h(Yi \| SIDj \| ni' \| nj') ?= Auth_2$. If this equation is found to be valid, it calculates $Auth_3=h(Tidi \| ni \| nj')$, and sends the message $\{Auth_3\}$ to SPj as an acknowledgement finally.
4. Upon having the message $Auth_3$, the SPj calculates $h(Tidi \| ni' \| nj)$ for verifying $h(Tidi \| ni' \| nj)$

?=Auth$_3$. If true, then develops the ultimate session key as ***Sk = h(Tidi || ni' || nj || SIDj)= h(Tidi || ni || nj' || SIDj).***

4.4. Password Updating Procedure

Ui modifies his/her old password (*PWi*) with a fresh password (PWi^{fr}) without involving RC, by adopting the under-mentioned steps:

1. To modify the password, the user would input his/her identity as ***IDi***, old password as ***PWi*** into the smart card. Next, the user imprints biometric identity ***Bi*** into a device scanner.
2. Subsequently, SC computes ***PK= Vi ⊕ h(IDi || h(H$_B$(Bi) || PWi))*** and validates the equality ***h(IDi || PK) ?= Xi.*** If it does not match, the smart card aborts the session, otherwise allows the user to proceed on the next step.
3. After that, the user would insert a new password as ***PWi^{fr}*** in SC, which calculates ***Vi^{new} = PK ⊕ h(IDi || h(H$_B$(Bi) || PWi^{fr})), Ri^{new} = Ri ⊕ h(H$_B$(Bi) || PWi) ⊕ h(H$_B$(Bi) || PWi^{fr}),*** and ***Zi^{new} = Zi ⊕ h(H$_B$(Bi)||PWi) ⊕ h(H$_B$(Bi) || PWi ^{fr})***. Then, the user replaces the ***Vi, Ri*** and ***Zi*** parameters in smart card with the new values ***Vi^{new}, Ri^{new}*** and ***Zi^{new}***.

5. Security Discussion

This segment illustrates the informal security discussion for contributed model in comparison with Chang et al.'s model.

5.1. Replay Attacks

These attacks may be attempted by an attacker after replaying the seized message contents at opportune time to deceive any legal entity of the protocol.

An attacker 𝔸 could seize the communication contents after examining a public channel as ***{Aij, m$_2$, Auth$_1$, m$_2$, Auth$_2$, Auth$_3$}*** and attempt to replay at some opportune time in future towards a valid participant. Nonetheless, 𝔸 cannot construct the parameter ***Auth$_1$,*** as it also comprises ***Aij*** which includes ***Ei*** and ***h(H$_B$(Bi) ||PWi)*** in its construction, such as ***Aij = Zi ⊕ h(h(SIDj || PK)||ni) ⊕ h(H$_B$(Bi) || PWi) ⊕ PK.*** An attacker 𝔸 neither knows the password nor biometric ***Bi***, which prevents the attacker for launching the replay attack. If 𝔸 replays the message ***{Aij, m$_2$, Auth$_1$}*** to ***SPj***, it may not be able to construct the upgraded challenge ***Auth$_3$,*** which requires the computation of ***Tidi***, which further needs ***Yi*** to be constructed that is inaccessible to 𝔸 even if the *SC* gets stolen. At the same time, if 𝔸 replays the message ***{m$_2$, Auth$_2$}*** towards Ui, the latter may easily detect the attack, since Ui knows that ***Auth$_2$*** cannot be constructed by the adversary due to the non-availability of ***Yi*** parameter. Hence, our proposed protocol may counter any replay threat.

5.2. Man-In-The-Middle-Attack

In this threat, the attacker intrudes between the legal participants by acting as an intermediary through replaying or modifying the message contents. A successful attack may let the legitimate members communicate with the adversary perceiving it as a right participant [6].

An adversary cannot construct the message ***{Auth$_2$, m$_3$}*** in request of ***{Aij, m$_2$, Auth$_1$}***, since the construction of ***Auth$_2$*** requires ***Yi***, which is inaccessible to 𝔸 from either intercepted messages or SC contents. Then, 𝔸 constructs a valid ***Auth$_3$*** against SPj's challenge ***{Auth$_2$, m$_2$},*** as ***Tidi*** is inaccessible to 𝔸 due to unknown ***Yi.*** Therefore, the contributed scheme is protected from MiTM threat.

5.3. Modification Threats

Such threats could be initiated by an attacker if it transforms the communication message illegally for submitting it to any valid participant [19].

An adversary may attempt to construct the message ***{Aij, m$_2$, Auth$_1$},*** however it may not be able to do so, since it needs the parameter ***Aij***, that further requires the knowledge of ***PWi*** and ***Bi*** as ***Aij = Zi ⊕ h(h(SIDj || PK) || ni) ⊕ h(H$_B$(Bi) || PWi) ⊕ PK.*** Likewise, it requires ***Tidi*** to construct ***Auth$_1$,*** which requires the knowledge of ***Yi,*** which is also inaccessible to 𝔸 due to the unreachable ***MPi***. Similarly, an adversary is not able to construct the message ***{Auth$_2$, m$_2$}*** in request of ***{Aij, m$_2$, Auth$_1$}***, given that the production of ***Auth$_2$*** requires the information of ***Yi***, which is not accessible to 𝔸 either from intercepted messages or stolen SC contents.

5.4. Password or Secret Guessing Threat

An attacker 𝔸 might try to recover password ***PWi*** either from messages intercepted or from stolen smart card contents. The password guessing requires the attacker

to be familiar with biometric information ***Bi*** of the user. If ***Bi*** is not available, then the password ***PWi*** may not be inferred or guessed from ***Vi , Zi*** and ***Ri*** parameters.

5.5. Session Key Disclosure Using Stolen Card

An attacker $\mathbb{A}$ might steal smart card contents and try to generate a session key (***Sk***) from its contents. Nonetheless, $\mathbb{A}$ ***cannot*** calculate the session key ***Sk = h(Tidi || ni || nj || SIDj)*** due to the inaccessible ***Tidi*** parameter in ***Sk***. While, the Tidi is constructed as ***Tidi=h(Yi || SIDj || ni)*** and the attacker cannot guess ***Yi*** either from stolen card contents or intercepted messages.

5.6. Impersonation Attack Using Smart Card Contents

An attacker $\mathbb{A}$ might steal smart card and try to impersonate the legitimate users or service provider by constructing the identical message ***{Aij, m_2, $Auth_1$}***. Nonetheless, it may not be able to do so [24], since it needs the parameter ***Aij***. Which further requires ***PWi*** and ***Bi*** to be guessed, as ***Aij = Zi ⊕ h(h(SIDj || PK) || ni) ⊕ h(H_B(Bi) || PWi) ⊕ PK.*** Besides, it needs ***Tidi*** to build ***$Auth_1$,*** which requires the value ***Yi,*** which is also inaccessible to $\mathbb{A}$ due to the unknown ***MPi***. Similarly, an adversary cannot construct the message ***{$Auth_2$, m_2}*** in response to a valid user request ***{Aij, m_2, $Auth_1$}***, since, the construction of ***$Auth_2$*** requires the information of ***Yi***, which is not accessible to $\mathbb{A}$ either from intercepted messages or stolen SC contents.

5.7. Session Key Security

This trait makes certain that the established session key is merely known to lawful members of a session, i.e. client and service provider.

In proposed model, the agreed session key, i.e. ***Sk = h(Tidi || ni || nj || SIDj)*** is secure, since, the ***Tidi*** calculation requires the access of ***Yi***, i.e., ***Tidi=h(Yi || SIDj || ni),*** while ***Yi*** requires the value ***MPi*** for guessing it, as ***Yi=Ri ⊕ MPi***. Hence, the session key ***Sk*** has been safe, in case the SC contents are accessed or $\mathbb{A}$ intercepts the public parameters.

5.8. Known Key Security

This attribute makes certain the protection of private keys of participants in case the current session key is exposed.

In contributed protocol, even if the adversary accesses the values ***Sk***, ***Ri***, an attacker cannot recover user password ***PWi***, since the ***PWi*** recovery from ***Sk=h(Tidi || ni || nj || SIDj)*** requires calculation of ***Yi=Ri ⊕ MPi*** and ***Tidi=h(Yi || SIDj || ni).*** This is not possible due to the inaccessibility of ***Bi*** in ***MPi=h(H_B(Bi) || PWi).*** At the same time, the server secret ***K*** is also secure as it is existent in a function i.e ***h(K || b)*** and is hard be guessed in polynomial amount of time. Therefore, the proposed protocol keeps the feature of known key security.

5.9. Mutual Authentication

This attribute assures that the concerned members authenticate one another in the protocol session and construct a mutual session key ultimately [7].

In our scheme, both of the participants authenticate each other mutually on account of ***Tidi*** and ***Yi'*** parameters. The server authenticates the user only if ***Tidi*** is valid in ***$Auth_3$,*** and this ***Tidi*** cannot be constructed by an attacker. Similarly, ***Ui*** authenticates ***SPj*** on account ***Yi'*** parameter used by server in the construction of ***$Auth_2$= h(Yi' || SIDj || ni' || nj).*** The ***Yi*** parameter cannot be accessed by an attacker even through ***Ri*** if the card gets stolen. Therefore, our protocol assures mutual authentication feature to the legitimate participants.

5.10. Anonymous Protocol

In an anonymous protocol [11, 12, 15], a legal user interacts with service provider without exposing its identity and an adversary may not recover the user's identity or secret credentials from intercepted contents on public channel.

In proposed scheme, the adversary cannot extract Ui's identity or other secret credentials out of intercepted contents on public channel or stolen smart card contents. This is because of the fact that the identity ***IDi*** is protected in a secret function ***Wi =h(IDi ||K),*** which is not possible to guess until the server secret ***K*** is exposed. Therefore, the contributed scheme confers anonymity to the user.

6. Formal Security Analysis

In this section, we exhibit the security strength of our protocol using formal analysis based on Burrows Aba-

di Needham-logic (BAN) [2] and random oracle model-based analysis.

The BAN logic proves the authenticated key agreement based on key distribution and mutual key agreement, and protocol robustness against the revelation of session key. We utilized few notations in this BAN logic proof as follows:

The agents interacting in a protocol are termed as *principals*

The symmetric encryption is performed using *keys* in a protocol.

Nonces in the protocol assist to distinguish various sessions.

We employed the following notations in proving the authenticity of our protocol using BAN logic:
$\beta \mid\equiv \varrho$: The principal β believes ϱ,
$\beta \lhd \varrho$: β sees ϱ.
$\beta \mid\sim \varrho$: β once said ϱ.
$\beta \Rightarrow \varrho$: β has got jurisdiction over ϱ.
$\sharp(\varrho)$: The message ϱ is fresh.
(ϱ, ϱ'): ϱ or ϱ' are parts of message (ϱ, ϱ').
$\langle \varrho \rangle_{\varrho'}$: The message ϱ is combined with ϱ'.
$\{\varrho, \varrho'\}_k$: ϱ or ϱ' is encrypted using key k.
$(\varrho, \varrho')_k$: ϱ or ϱ' is hashed with k.
$\varrho(\xleftrightarrow{k})\varrho'$: ϱ and ϱ' exchange message employing the shared key k.

Some related postulates utilized in BAN logic are shown below:

P_1. Message meaning postulate $\approx \dfrac{\beta \mid\equiv \beta \overset{k}{\leftrightarrow} \beta',\ \beta \lhd \langle \varrho \rangle_{\varrho'}}{\beta \mid\equiv \beta' \mid\sim \varrho}$

P_2. Nonce verification postulate $\approx \dfrac{\beta \mid\equiv (\varrho),\ \beta \mid\equiv \beta' \mid\sim \varrho}{\beta \mid\equiv \beta' \mid\equiv \varrho}$

P_3. Jurisdiction postulate $\approx \dfrac{\beta \mid\equiv \beta' \Rightarrow \varrho,\ \beta \mid\equiv \beta' \mid\equiv \varrho}{\beta \mid\equiv \varrho}$

P_4. Freshness conjuncatenation postulate $\approx \dfrac{\beta \mid\equiv (\varrho)}{\beta \mid\equiv (\varrho, \varrho')}$

P_5. Belief postulate $\approx \dfrac{\beta \mid\equiv (\varrho),\ \beta \mid\equiv (\varrho')}{\beta \mid\equiv (\varrho, \varrho')}$

P_6. Session keys postulate $\approx \dfrac{\beta \mid\equiv (\varrho),\ \beta \mid\equiv \beta' \mid\equiv \varrho'}{\beta \mid\equiv \beta \overset{k}{\leftrightarrow} \beta'}$

The contributed scheme must meet the under-mentioned goals to prove its session key's security under BAN logic on the basis of above postulates:

Goal-1 : $S_r \mid\equiv S_r \xleftrightarrow{SK} U_r$

Goal-2 : $S_r \mid\equiv U_r \mid\equiv S_r \xleftrightarrow{SK} U_r$

Goal-3 : $U_r \mid\equiv S_r \xleftrightarrow{SK} U_r$

Goal-4 : $U_r \mid\equiv S_r \mid\equiv S_r \xleftrightarrow{SK} U_r$

To proceed, we convert the exchanged messages in our scheme into idealized form as given below:

M_2: $U_r \rightarrow S_r$: $Aij, m_2, Auth_1$: $\langle Wi, ni, Tidi \rangle_{K1, K2, Yi}$

M_2: $S_r \rightarrow U_r$: $m2, Auth_2$: $\langle nj \rangle_{K2, Yi'}$

M_3: $U_r \rightarrow S_r$: $Auth_3$: $\langle ni, nj' \rangle_{Tidi}$

Besides, the understated assumptions are established for proving security of our scheme:

$\Upsilon 1: U_r \mid\equiv \sharp ni$

$\Upsilon 2: S_r \mid\equiv \sharp nj$

$\Upsilon 3: U_r \mid\equiv S_r \xleftrightarrow{Yi} U_r$

$\Upsilon 4: S_r \mid\equiv S_r \xleftrightarrow{Yi'} U_r$

$\Upsilon 5: U_r \mid\equiv S_r \Rightarrow nj$

$\Upsilon 6: S_r \mid\equiv U_r \Rightarrow ni$

Currently, the idealized forms such as M_2, M_2 and M_3 of our scheme may be analyzed and seen in the light of stated assumptions and postulates.

Taking the first one of the idealized forms:

M_2: $U_r \rightarrow S_r$: $Aij, m_2, Auth_1$: $\langle Wi, ni, Tidi \rangle_{K1, K2, Yi}$

By Applying seeing postulate, we have

$v1$: $S_r \lhd Aij, m_2, Auth_1$: $\langle Wi, ni, Tidi \rangle_{K1, K2, Yi}$

According to $v1$, $\Upsilon 3$ and message meaning postulate,

$v2$: $S_r \mid\equiv U_r \sim (Wi, ni, Tidi)$

According to $v1$, $\Upsilon 2$, freshness-conjucatenation, and nonce-verification postulates, we get

$v3$: $S_r \mid\equiv U_r \mid\equiv (Wi, ni, Tidi)$

The $(Wi, ni, Tidi)$ are essential parameters for mutual authentication and session key agreement.

According to $\Upsilon 6$, $v3$, and Jurisdiction rule

$v4$: $S_r \mid\equiv (Wi, ni, Tidi)$

Referring to $\Upsilon 3$, $v4$, and session key postulate, we have

$v5$: $S_r \mid\equiv U_r \mid\equiv S_r \xleftrightarrow{SK} U_r$ **(Goal-2)**

Referring to $\Upsilon 6$, $v5$, and Jurisdiction postulate

$v6$: $S_r \mid\equiv S_r \xleftrightarrow{SK} U_r$ **(Goal-1)**

Regarding the second idealized form, we have

M_2: $S_r \rightarrow$ Ui: $m_2, Auth_2$: $\langle nj \rangle_{K2, Yi'}$

Using the seeing rule, we have

$v7$: $U_r \lhd S_r \rightarrow U_r$: $m2, Auth_2$: $\langle nj \rangle_{K2, Yi'}$

Referring to $v7$, $\Upsilon 4$ and message-meaning postulate,

$v8$: $U_r \mid\equiv S_r \sim (nj)$

Regarding $\Upsilon 2$, $v8$, freshness-conjucatenation, and nonce-verification postulates, we have

$v\ 9$: $U_r \mid\equiv S_r \mid\equiv (nj)$

where (nj) is an essential parameter for the mutual authentication and session key establishment.

Regarding Υ5, *v*9, and Jurisdiction postulate, we have

*v*10: $U_r \mid\equiv (nj)$

Referring Υ4, *v*10, and session-key postulate, we get

*v*11: $U_r \mid\equiv S_r \mid\equiv S_r \xleftrightarrow{SK} U_r$ **(Goal-4)**

Regarding Υ5, *v*11, and Jurisdiction postulate, we have

*v*12: $U_r \mid\equiv S_r \xleftrightarrow{SK} U_r$ **(Goal-3)**

The stated BAN logic-based protocol examination establishes the fact that our model confers mutual authentication and the constructed session key (*SK)* is mutually established among the user U_r and server S_r.

Employing the random oracle model, we implement a formal security analysis for proving that our protocol is quite secure [29]. For the said objective, we employed the oracle *Reveal_oracle* as described below:

Reveal_oracle: This oracle would output x from the related hash digest y=h(x), for sure.

The *Reveal_oracle* has been employed in Algorithm 1, $EXP1_{IBMSACP}^{HASH}$, as shown above, signifying towards the session key's disclosure if the *Reveal_oracle* is executed by inverting hash digest.

Algorithm 1. $EXP1_{IBMSACP}^{HASH}$

1. Eavesdrop the login-request ***{Aij, m2, Auth1}*** where ***Auth1=h(Aij || Tidi || ni), m2=h(SIDj || PK)⊕ni), and Aij = Zi ⊕ h(h(SIDj || PK)||ni)⊕h(HB(Bi) ||PWi) ⊕ PK.***
2. Call *Reveal_oracle* oracle on the input of ***Auth1*** to get {***Aij', Tidi, ni}*** as ***(Aij'||Tidi ||ni)***← *Reveal_oracle* (***Auth1***)
3. Eavesdrop the Authentication message ***{Auth3}*** in verification phase, where ***Auth3=h(Tidi || ni || nj')***
4. Call *Reveal_oracle* on the input of ***Auth3*** to get {***Tidi', ni, nj'}*** as (***Tidi'*** || ***ni*** || ***nj')***← *Reveal_oracle* (***Auth3***)
5. Call *Reveal_oracle* on the input of ***Tidi*** to get {***Yi , SIDj , ni}*** as ***(Yi || SIDj || ni)*** ← *Reveal_oracle* (***Tidi'***)
6. Call *Reveal_oracle* on the input of ***Yi*** to retrieve ***{Wi , h(K || b}*** as ***(Wi || h(K || b)***← *Reveal_oracle* (***Yi***)
7. Call *Reveal_oracle* on inputting ***Wi*** to retrieve {***IDi' , K}*** as ***(IDi' ||K)*** ← *Reveal_oracle* (***Wi***)
8. Compute session key as ***SK***= ***h(Tidi || ni' || nj || SIDj)***
9. **If** (***Aij*** '= ***Aij***) AND (***Tidi*** '= ***Tidi***) **Then**
   Take ***SK*** as a legitimate session key for identity (***IDi'***) of Ui, against login request ***{Aij, m2, Auth1}***

Theorem 1. *The contributed scheme is secure, if an attacker attempts to determine the mutually agreed session key (SK) among legitimate participants SPj and Ui, provided one-way hash digest function acts nearly as a random oracle.*

Proof. In this proof [6, 8, 13-14], an adversary Ѧ, competent enough to derive the agreed session key (SK) among the participants particularly Ui and SPj, makes a use of this *Reveal_oracle* oracle to implement $EXP1_{IBMSACP}^{HASH}$. The probability of success corresponding to $EXP1_{IBMSACP}^{HASH}$ is $Sucs1=Prb.2[EXP1_{IBMSACP}^{HASH}=1]-1$, Here *Prb[E]* depicts the event probability for an event (E). The advantage function for the above experiment can be established as $Adv_{IBMSACP}^{HASH}(tm_2, q_{Ry1})=\max_A [Sucs1_{IBMSACP}^{HASH}]$, having execution delay time tm_2 and Reveal-query q_{Ry1} maximized on the adversary Ѧ [1]. We regard our contributed scheme as quite safe against an adversary Ѧ in recovering the agreed session key (*SK)* between Ui and SPj, if $Adv_{IBMSACP}^{HASH}(tm_2, q_{Ry1}) \le \varepsilon$ for a negligibly small $\varepsilon > 0$. In relation to this experiment, if the adversary is competent to invert a one-way hash digest function h(), it might comfortably recover the real session key (SK) shared between SPj and Ui, and at last Ѧ wins the game. Nonetheless, in accordance with *Reveal_oracle* definition, this is polynomially unfeasible to invert hash function since $Adv_{IBMSACP}^{HASH}$ and $Adv_{IBMSACP}^{HASH}(t_1) \le \varepsilon$ for a negligibly small value, i.e. $\varepsilon > 0$. Therefore, the contributed protocol may be safely considered as resistant as the security features for hash functions are tough to break in polynomial amount of time.

7. Comparison and Performance Analysis

The Chang et al. model presents a multi-server authenticated key agreement protocol and is based on light-weight symmetric key operations which are suitable for power deficient mobile devices. In this performance section, we evaluate performance efficiency of authentication protocol by Chang et al. with proposed protocol. Table 2 lists the limitations of Chang et al.'s model, while the proposed scheme acts as a vigorous authentication protocol as proven in the preceding sections. Table 2 demonstrates that Chang et al.'s model does not offer protection from stolen card threat, impersonation attack and lacks session

Table 2
Comparison for Multi-server schemes

	Chang et al. [4]	Proposed protocol
Anonymity	✓	✓
Mutual authentication	✓	✓
Known key secrecy	✓	✓
Resists MiTM threat	✓	✓
Resists modification threat	✓	✓
Resists password guessing threat	✓	✓
Resists stolen smart card threat	×	✓
Resists impersonation threat	×	✓
Resists replay threat	✓	✓
Session key security	×	✓

Table 3
Number of operations in Chang et al.'s model and contributed model

	Chang et al. [4]	Ours
Registration messages	$9\ T_H$	$8\ T_H$
User side	$9T_H$	$11\ T_H$
Server side	$6T_H$	$6T_H$
Password update messages	$4\ T_H$	$7\ T_H$

key security, while the proposed scheme is immune to those identified threats as verified in the formal security models. The actual cost for both schemes is shown in Table 3, where different hash operations are represented with T_H, and bypassing exclusive-OR operation for its insignificant computational cost.

Consequently, in consideration of above performance evaluation and analysis, we may infer that our protocol is more secure than Chang et al.'s protocol while bearing an equivalent cost. The proposed scheme provides immunity against impersonation and session key attacks in contrary to Chang et al.'s model. Table 3 compares the number of operations for Chang et al. protocol and contributed model and depicts that the phases of both schemes take an equivalent computational cost with a little variation in the cost of password modification phase.

8. Conclusion

The multi-server authentication serves as one of the main requirements of the current internet-based authentication framework. This manuscript studies the multi-server based Chang et al.'s remote authentication model which demonstrates that the Chang et al. scheme is prone to impersonation and session key attacks, subject to the stolen contents of smart card. The review and cryptanalysis of Chang et al.'s model has been demonstrated comprehensively. Thereafter, a proposed model is presented that foils those particular attacks with the contribution of an enhanced model. Moreover, this paper presents the formal security analysis using BAN logic and random oracle model, and evaluates the performance against the Chang et al.'s protocol.

Acknowledgement

This work was supported by the Brain Korea 21 Plus Program (No. 22A20130012814) funded by the National Research Foundation of Korea (NRF).

References

1. Bellare, M., Rogaway, P. Entity Authentication and Key Distribution. Proceedings of the 13th Annual International Cryptology Conference, LNCS 773, Santa Barbara, CA, August, 1993, 232-249. https://doi.org/10.1007/3-540-48329-2_21
2. Burrows, M., Abadi, M., Needham, R. M. A Logic of Authentication. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 1989, 426, 233-271. https://doi.org/10.1098/rspa.1989.0125
3. Chang, C. C., Lee, J. S. An Efficient and Secure Multi-Server Password Authentication Scheme Using Smart Cards. Proceedings of the 3rd International Conference on Cyberworlds, Tokyo, Japan, November, 2004, 417-22.

4. Chang, C.-C., Cheng, T.-F., Hsueh, W.-Y. A Robust and Efficient Dynamic Identity-Based Multi-Server Authentication Scheme Using Smart Cards. International Journal of Communication Systems, 2016, 29(2), 290-306. https://doi.org/10.1002/dac.2830

5. Chang, Y. F., Tai, W. L., Chang, H. C. Untraceable Dynamic-Identity-Based Remote User Authentication Scheme with Verifiable Password Update. International Journal of Communication Systems, 2013 (Article in press). https://doi.org/10.1002/dac.2552

6. Chaudhry, S. A., Khan, I., Irshad, A., Ashraf, M. U., Khan, M. K., Ahmad, H. F. A Provably Secure Anonymous Authentication Scheme for Session Initiation Protocol. Security and Communication Networks, 2016, 9(18), 5016-5027. https://doi.org/10.1002/sec.1672

7. Chaudhry, S. A., Naqvi, H., Farash, M. S., Shon, T., Sher, M. An Improved and Robust Biometrics-Based Three Factor Authentication Scheme for Multiserver Environments. The Journal of Supercomputing, 2018, 74(8), 3504-3520. https://doi.org/10.1007/s11227-015-1601-y

8. Chaudhry, S. A., Sher, M., Ghani, A., Naqvi, H., Irshad, A. An Efficient Signcryption Scheme with Forward Secrecy and Public Verifiability Based on Hyper Elliptic Curve Cryptography. Multimedia Tools and Applications, 2015, 74(5), 1711-1723. https://doi.org/10.1007/s11042-014-2283-9

9. Hsiang, H. C., Shih, W. K. Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multiserver Environment. Computer Standards and Interfaces, 2009, 31(6), 1118-1123. https://doi.org/10.1016/j.csi.2008.11.002

10. Hwang, M. S., Lee, C. C., Tang, Y. L. A Simple Remote User Authentication Scheme. Mathematical and Computer Modelling, 2002, 36(1-2), 103-107. https://doi.org/10.1016/S0895-7177(02)00106-1

11. 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. https://doi.org/10.1007/s13369-017-2764-z

12. Irshad, A., Naqvi, H., Chaudhry, S. A., Raheem, S., Kumari, S., Kanwal, A., Usman, M. An Efficient and Secure Design of Multi-Server Authenticated Key Agreement Protocol. The Journal of Supercomputing, 2018, 74(9), 4771-4797. https://doi.org/10.1007/s11227-018-2467-6

13. Irshad, A., Sher, M., Alzahrani, B. A., Albeshri, A., Chaudhry, S. A., Kumari, S. Cryptanalysis and Improvement of a Multi-server Authentication Protocol by Lu et al. KSII Transactions on Internet & Information Systems, 2018, 12(1). https://doi.org/10.3837/tiis.2018.01.025

14. 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. https://doi.org/10.1007/s11227-016-1688-9

15. Irshad, A., Sher, M., Chaudhry, S. A., Kumari, S., Sangaiah, A. K., Li, X., Wu, F. A Secure Mutual Authenticated Key Agreement of User with Multiple Servers for Critical Systems. Multimedia Tools and Applications, 2018, 77(9), 11067-11099. https://doi.org/10.1007/s11042-017-5078-y

16. Jin, A. T. B., Ling, D. N. C., Goh, A. Bio-hashing: 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

17. Juang, W. S. Efficient Multi-Server Password Authenticated Key Agreement Using Smart Cards. IEEE Transactions on Consumer Electronics, 2004, 50(1), 251-255. https://doi.org/10.1109/TCE.2004.1277870

18. Juang, W. S. Efficient Password Authenticated Key Agreement Using Smart Cards. Computers and Security, 2004, 23(2), 167-173. https://doi.org/10.1016/j.cose.2003.11.005

19. Kumari, S., Li, X., Wu, F., Das, A. K., Arshad, H., Khan, M. K. A User Friendly Mutual Authentication and Key Agreement Scheme for Wireless Sensor Networks Using Chaotic Maps. Future Generation Computer Systems, 2016, 63, 56-75. https://doi.org/10.1016/j.future.2016.04.016

20. Kumari, S., Li, X., Wu, F., Das, A. K., Choo, K. K. R., 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

21. Lamport, L. Password Authentication with Insecure Communication. Communications of the ACM, 1981, 24(11),770-772.https://doi.org/10.1145/358790.358797

22. Lee, C. C., Lin, T. H., Chang, R. X. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment Using Smart Cards. Expert Systems with Applications, 2011, 38(11), 13863-13870. https://doi.org/10.1016/j.eswa.2011.04.190

23. Li, L. H., Lin, I. 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. https://doi.org/10.1109/72.963786

24. 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(1-2), 85-95. https://doi.org/10.1016/j.mcm.2012.06.033

25. Li, X., Niu, J., Kumari, S., Liao, J., Liang, W. An Enhancement of a Smart Card Authentication Scheme for Multi-Server Architecture. Wireless Personal Communications, 2015, 80(1), 175-192. https://doi.org/10.1007/s11277-014-2002-x

26. Li, X., Niu, J., Liao, J., Liang, W. Cryptanalysis of a Dynamic Identity-Based Remote User Authentication Scheme with Verifiable Password Update. International Journal of Communication Systems, 2013 (Article in press). DOI: 10.1002/dac.2676. https://doi.org/10.1002/dac.2676

27. 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. https://doi.org/10.1016/j.jnca.2011.11.009

28. Liao, Y. P., Wang, S. S. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment. Computer Standards and Interfaces, 2009, 31(1), 24-29. https://doi.org/10.1016/j.csi.2007.10.007

29. Liao, Y.-P., Hsiao, C.-M. A Novel Multi-Server Remote User Authentication Scheme Using Self-Certified Public Keys for Mobile Clients. Future Generation Computer Systems, 2013, 29(3), 886-900. https://doi.org/10.1016/j.future.2012.03.017

30. Lin, C. W., Shen, J. J., Hwang, M. S. Security Enhancement for Optimal Strong-Password Authentication Protocol. ACM SIGOPS Operating Systems Review, 2003, 37(2), 12-16. https://doi.org/10.1145/881783.881785

31. Lin, I. C., Hwang, M. S., Li, L. H. A New Remote User Authentication Scheme for Multi-Server Architecture. Future Generation Computer System, 2003, 19(1), 13-22. https://doi.org/10.1016/S0167-739X(02)00093-6

32. Lumini, A., Loris, N. An Improved Bio-hashing for Human Authentication. Pattern recognition, 2007, 40(3), 1057-1065. https://doi.org/10.1016/j.patcog.2006.05.030

33. Shieh, W. G., Wang, J. M. Efficient Remote Mutual Authentication and Key Agreement. Computers and Security, 2006, 25(1), 72-77. https://doi.org/10.1016/j.cose.2005.09.008

34. Sood, S. K., Sarje, A. K., Singh, K. A Secure Dynamic Identity Based Authentication Protocol for Multi-Server Architecture. Journal of Network and Computer Applications, 2011, 34(2), 609-618. https://doi.org/10.1016/j.jnca.2010.11.011

35. Yang, W. H, Shieh, S. P. Password Authentication Schemes with Smart Cards. Computers and Security, 1999, 18(8), 727-733. https://doi.org/10.1016/S0167-4048(99)80136-9

36. Yeh, K. H., Lo, N. W, Li, Y. Cryptanalysis of Hsiang-Shih's Authentication Scheme for Multi-Server Architecture. International Journal of Communication Systems, 2011, 24(7), 829-836. https://doi.org/10.1002/dac.1184