An improved Multi-server Authentication Scheme for Distributed Mobile Cloud Computing Services

Azeem Irshad[1], Muhammad Sher[1], Hafiz Farooq Ahmad[2], Bander A. Alzahrani[3], Shehzad Ashraf Chaudhry[1], Rahul Kumar[4]

[1]Department of Computer Science & Software Engineering, International Islamic University, Islamabad
[e-mail: irshadazeem2@gmail.com, m.sher@iiu.edu.pk, shahzad@iiu.edu.pk]
[2]College of Computer Sciences and Information Technology (CCSIT), King Faisal University,Alahssa, Saudi Arabia
[e-mail: hfahmad@kfu.edu.sa]
[3]Faculty of Computing & Information Technology, King Abdulaziz University, Saudi Arabia
[e-mail: baalzahrani@kau.edu.sa]
[4]S. S. V. (P.G.) college Hapur, Uttar Pradesh, India
[e-mail: ujjwalrahul@gmail.com]
*Corresponding author: Azeem Irshad

Received July 24, 2016; revised October 18, 2016; accepted October 31, 2016; published December 31, 2016

Abstract

Mobile cloud computing (MCC) has revolutionized the way in which the services can be obtained from the cloud service providers. Manifold increase in the number of mobile devices and subscribers in MCC has further enhanced the need of an efficient and robust authentication solution. Earlier, the subscribers could get cloud-computing services from the cloud service providers only after having consulted the trusted third party. Recently, Tsai and Lo has proposed a multi-server authenticated key agreement solution for MCC based on bilinear pairing, to eliminate the trusted third party for mutual authentication. The scheme has been novel as far as the minimization of trusted party involvement in authenticating the user and service provider, is concerned. However, the Tsai and Lo scheme has been found vulnerable to server spoofing attack (misrepresentation attack), de-synchronization attack and denial-of-service attack, which renders the scheme unsuitable for practical deployment in different wireless mobile access networks. Therefore, we have proposed an improved model based on bilinear pairing, countering the identified threats posed to Tsai and Lo scheme. Besides, the proposed work also demonstrates performance evaluation and formal security analysis.

Keywords: Multi-server authentication, mobile cloud computing, trusted third party, attacks, cryptanalysis

http://dx.doi.org/10.3837/tiis.2016.12.021 **ISSN : 1976-7277**

1. Introduction

This is because of mobile cloud computing, that the number of wireless devices is going to surpass the wired ones for about 50 percent of the total IP based internet traffic, by the year 2016. The mobile cloud computing is gaining ground with the subscribers' ever increasing reliance on mobility to meet their service requirements on the move. According to the Association of British Insurers (ABI) study report [1], the mobile broadband subscribers will get to almost 5 billion by the start of 2016, and the advancement can be rightly attributed to MCC [1-5, 6]. In mobile cloud computing, all of the cloud-based services may be acquired by the use of mobile devices employing Wireless Local Area Network (WLAN) or 3G/4G/5G based telecommunication networks. A user has to activate service by using a Web browser or any kind of cloud service application installed on one's mobile device for availing the mobile cloud computing service. Then, the user application and mobile cloud computing service application could mutually authenticate each other, positively. In this regard, we can witness many authentication protocols as introduced for various cloud applications [7-10]. These protocols need to be designed with a special focus on devices with low computing end, along with meeting the minimum security requirements [2, 11-14]. The security is of crucial concern, since the messages need to traverse out of insecure WLAN or telecommunication networks, and the adversaries can easily intercept the messages to launch various kind of attacks. These protocols also need to consider the privacy and identity tracing concerns.

It is quite difficult to register all service providers and keep more than one password or keys for various services when there are a variety of cloud computing service providers. That may cause severe management issues for individual users, registered with each service providing servers, handling tens and hundreds of server passwords, in a distributed mobile cloud environment. In this regard, conventional single sign-on (SSO) schemes like Passport and OpenID are one of the possible key management techniques [15-23]. The users can avail many services, in such systems, by utilizing a single secret key or password. Nonetheless, majority of SSO based techniques involve a trusted third party to establish an authenticated communing session. While, OpenID, being a decentralized SSO technique, has been adopted by some major ISPs (Internet service providers) like Yahoo and Google, with a roughly estimate of more than 50000 websites utilizing the same OpenID for authentication purpose. The three entities, user, relaying partner i.e., service provider (SP) and identity providers (IdP) participate in the mutual authentication between a user and a service provider. The IdP and service provider can alternately act as IdP and SP to serve the user, in OpenID. A user who registers with IdP for OpenID identifier, might login to various websites that are based on OpenID, and will have to use the (Secure Socket Layer) (SSL) protocol on a secure channel [24]. The user, while performing mutual authentication phase with SP, needs to resort to IdP for authenticating a service provider. As a matter of fact, a user initially sends login request towards SP. The SP, after verifying the OpenID identifier, forwards the authentication request to IdP for verification. The IdP responds positive to both, user and SP, if the identity is found valid in its database. Then, the SP and user mutually authenticate one another. This might lead to an extra delay, if there is already burden on IdP for responding to many other users' pending authentication requests, and could become a bottleneck. The use of SSO requires another secure message transmission protocol to function in a secure and reliable manner. Besides, it is based on public key cryptography, i.e., SSL relies on Rivest, Shamir and Adleman (RSA) for authenticity verification, which is costly computation technique. Likewise, it serves as a costly

technique for distributed mobile cloud environments.

1.1 Objectives

Hence, in the light of above comments, the objectives for the current scheme can be refined as stated below:

1. There is a need for an efficient cryptographic technique that is less computation intensive than SSL.
2. Secondly, the trusted third party would be required to register the users and potential service providers before these entities can participate in the system. It would be beneficial to engage registration center in the beginning for registration that leads to establish a direct mutual authentication between **a** user and service providers, onwards, whenever a service is required.
3. The third objective emphasizes the use of a single private key or low-entropy password on part of a user, and is enough to avail multiplicity of services as offered in any system, synonymous with the assumption as taken in multi-service authentication paradigm. This eases the management of secrets, manifolds, on the part of a user, in comparison with the hassle of maintaining more passwords.
4. Our fourth objective is to avoid the management of either verifier database at the server's or Registration Centre (RC)'s end.
5. Lastly, fifth objective is to avoid hassle of management of digital certificates bearing public keys.

The multi-server authentication (MSA) environment consists of users, servers, and registration centre (RC). The RC acts as a trusted third party, which in the initialization phase, registers all users and servers using secure channels. Then afterwards, users could avail services directly from the servers.

1.2 Related Work

The authentication serves is the crucial requirement for acquiring network based services to avert any unauthorized access from malicious users. In the last two decades, a lot of public key cryptography based solutions have been proposed, that involves RSA, DLP (Discrete Logarithm Problem) for the techniques. However, these were costly solutions and not efficient in terms of key sizes. The ECC (Elliptic Curve Cryptography) provides an equivalent level of security in far less key sizes than its other counterparts. For instance, a public key of 3072-bit RSA provides an equivalent level of security as 256-bit based ECC public key does. The mobile cloud computing devices require battery and energy efficient solutions, while ECC is to suitable for scenarios having smart wireless devices with low end processor and batteries.
Hence, so far, not a single ECC, DLP or Chebyshev map based solution has been sufficient to meet the above defined objectives. Alternatively, a solution is required that involves RC only in the registration phase and not in the mutual authentication phase, onwards. At the same time, no password verifier table or database should be maintained at RC's end, or any kind of certificate issued by the RC, since the management of certificates issuance, revocation and re-issuance would be costly. Recently, in the wake of current analysis, an ID-based cryptosystem, based on bilinear pairing, has been realized by the research community to meet the said objectives. In ID-based cryptosystem, the identity of the user serves as its public key, while its private key is generated by a centralized authority using the corresponding user identity and is delivered to the user during registration phase. The ID-based cryptography obviates the need to verify the public key of the requesting participant through any public key

certificate or seeking help of any external authority or storing the certificates in database for a long time. We can see, recently, many ID-based cryptosystem applications in Grid computing and cloud computing environments, sensor and ad hoc networks, internet of things and group-based signatures etc. In Grid computing security, first application of ID-based cryptosystem was introduced by Lim and Robshaw [22] [23], in 2004. Afterwards, Mao [25] also contributed in ID-based cryptosystems in Grid. Li et al. [26] presented a novel ID-based authentication technique for cloud computing paradigm, although criticized for not providing user anonymity and untraceability [27], [28].

Most of the authentication techniques focused on single server authentication in the literature, and those techniques are not compatible with the architectures based on MSA, where each of the servers competes for providing its services. These MSA architectures are beneficial so that a user does not have to remember so many passwords of the servers. A single password is sufficient to avail the services of multiple service providers. In most of the previous schemes, a user needs to resort the registration centre every time services are required or mutual authentication with server is sought. Moreover, a few schemes have been observed where a single master key is shared among all service providers in the system, which could lead to impersonation attack on part of malicious servers. Hence, the earlier schemes could not meet the required objectives, however, recently, Tsai and Lo [29] presented a mobile cloud computing based authentication scheme that employs bilinear pairing technique. However, after careful study**,** Tsai and Lo scheme has been found vulnerable to server impersonation attack, de-synchronization attack, and Denial-of-Service attack, which renders the scheme inapplicable to be deployed in any practical scenario. The current study reviews the Tsai and Lo scheme along with the cryptanalysis. We propose an improved protocol which is adapted to multi-server, and assumed the trusted party as RC instead of IdP (Identity provider in Tsai and Lo) and SPj instead of SP (Service provider in Tsai and Lo), in our scheme, where SPj is the j^{th} service provider in proposed scheme. Since, due to multi-server scenario, architectures of both of these protocols remain the same. Hence, we propose a MSA scheme by improving Tsai and Lo authentication scheme based on mobile cloud computing employing the bilinear pairing technique. The proposed work also comprises performance evaluation and formal security analysis based on BAN logic.

1.3 Threat Model

We assume the following assumptions regarding an attacker $\mathcal{A}$ under threat model [30-34]:

1. An attacker is capable of intercepting and examining the messages over an insecure channel, exchanged during the communication between the legal participants.
2. An attacker may repeat, delete, or modify the parameters during exchange of messages.
3. An attacker may be a malicious legitimate insider within the organization.
4. An attacker may guess low entropy identity and passwords; however, it will not be able to guess the high entropy random secrets in polynomial time.
5. Lastly, an attacker may steal smart card and its contents to manipulate for its malicious intentions.

1.4 Organization of the paper

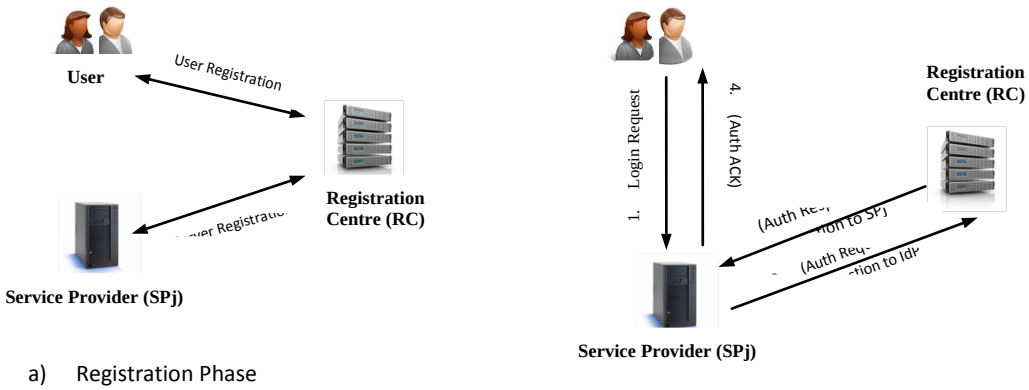
As far the organization of this study work, section 2 describes preliminary concepts as used in the paper. Section 3 relates to review and cryptanalysis of Tsai and Lo scheme. Section 4 describes the proposed model. Section 5 exhibits security analysis, formal security analysis of the proposed scheme. Section 6 demonstrates performance analysis and the last section concludes the findings.

2. Preliminaries

The preliminaries section takes a review of MSA, bilinear pairing, bio-hashing, and one-way hash function.

2.1 Multi-Server Authentication

Fig. 3 depicts multi-server environment, where each user, in the beginning, registers with the Registration Centre (RC). Then, it avails the required services from various servers, by login and authentication procedure using the similar account as established with RC. In old MSA procedure, users could mutually authenticate with the service provider SPj, however, with the mandatory participation of RC, during each mutually authentication session, as shown in **Fig. 1**.



a) Registration Phase

b) Authentication Phase

Fig. 1. Multi-server authentication procedure between user and SPj using OpenID

2.2 Bilinear Pairing

In bilinear pairing [19, 35], two of the pairings namely, the Weil pairings or Tate pairings are the mostly used types in cryptographic applications, particularly in identity (ID)-based cryptography. We assume $<G_1, +>$ as the additive cyclic group, and $<G_2, \times>$ as the multiplicative cyclic group, while P be the generator for group G_1. A mapping $e: G_1 \times G_1 \rightarrow G_2$ is regarded as bilinear mapping if it holds the following features:

1. Bilinear: For all $X, Y, Z \epsilon G_1$, $e(X+Y, Z) = e(X, Z) \times e(Y, Z)$ and $e(X, Y+Z)=e(X, Y) \times e(X, Z)$.
2. Non-degeneracy: Given, 1 is the identity element of a multiplicative cyclic group G_2, there exist $X, Y \epsilon G_1$, such that $e(X, Y) \neq 1$.
3. Computability: An efficient algorithm exists for computing $e(X, Y)$ for all X, Y belonging to G_1.

2.3 Bio-hashing

According to [36], the Bio-hashing technique maps the patient's biometric traits onto random vectors which are responsible for generating the user-specific code, termed as the Bio-code. This helps in discretization of the projection coefficients into one or zero. The Bio-hashing is a

one-way function, and serves the purpose of hashed password security. The Bio-hashing term was coined when Jina et al., proposed a two-factor authenticator that is based on iterated inner products among the tokenized pseudo-random numbers and user-specific finger impression that lead towards the development of such compact codes. Onwards, the concept was improved and enhanced to Bio-hashing, by Lumini and Nanni in [37].

2.4 One-way hash function

A secure one-way hash operation h: ($u \rightarrow v$) comprises the following four features:

1. The hash function h inputs a message of arbitrary length and generates a message digest of fixed-length.
2. Given $h(u)=v$, it is not possible to compute $h^{-1}(v)=u$ in polynomial time;
3. Given u, it is intractable to find u', such that $u' \neq u$, nonetheless $h(u') = h(u)$;
4. It is computationally intractable to find any pair u, u' such that $u' \neq u$, and $h(u') = h(u)$.

An adversary $\mathbb{A}$'s advantage can be represented with the following formalization.

$$Adv_{\mathbb{A}}^{HASH}(t) = Pr[(u,u') \Leftarrow_R \mathbb{A}: u \neq u' and\ h(u) = h(u')]$$

Where $Pr[E_t]$ indicates the probability for an event E_t for performing a random experiment, and $(u,u') \Leftarrow_R \mathbb{A}$ represents the randomly selected pair (u,u') by $\mathbb{A}$. Given the above status, an adversary $\mathbb{A}$ can be probabilistic and the probability for the advantage $Adv_{\mathbb{A}}^{HASH}(t)$ is computed over the random choices input by the adversary $\mathbb{A}$ in execution time t. The hash function $h(.)$ is supposed to be resistant to collision if $Adv_{\mathbb{A}}^{HASH}(t) <= \epsilon$ for any sufficiently small $\epsilon > 0$.

3. REVIEW AND CRYPTANALYSIS OF TSAI AND LO SCHEME

The Tsai and Lo's scheme [29] comprises three entities that participate in a system setup; these are user Ui, service providers or servers SPj, and IdP or RC as trusted third party. The Ui and SPj get registered before joining the system, and afterwards, both of these instances can get mutually authenticated without consulting the RC. This section describes the system setup, working and review analysis for the Tsai and Lo scheme [29].

3.1 System Setup

We assume $\boldsymbol{G_1}$ to be a cyclic additive group as constructed on P generator, and $\boldsymbol{G_2}$ be a cyclic multiplicative group, while p defines the prime order for $\boldsymbol{G_1}$ and $\boldsymbol{G_2}$. Initially, the RC selects s as its master secret key and computes its public key as $P_{pub} = sP$. Then, it computes $e(P, P)$ and also the pairing functions as $e: G_1 \times G_1 \rightarrow G_2$, along with five collision-resistant hash functions as $H_1: Z_p \rightarrow Z_p$, $H_2: G_2 \rightarrow Z_p$, $H_3: Z_p \rightarrow Z_p$, $H_4: Z_p \rightarrow Z_p$, $h: Z_p \rightarrow G_1$. Finally, the RC publishes these parameters as public, i.e., $\{e, h, P, P_{pub}, H_1, H_2, H_3, H_4, e(P,P)\}$.

3.2 Working of Tsai and Lo scheme

The Tsai and Lo authentication protocol comprises registration, login and authentication phases, as shown in **Fig. 2**. Some of the used notations in the scheme are given in **Table 1**.

Table 1. Notations description

Notations	*Description*
Ui, SPj, RC	i^{th} User, j^{th} Service provider , Registration Centre
IDi, IDj	Ui's identity, SPj's identity
PWi, fi	Ui's password and finger impression
$e:G_1 \times G_1 \rightarrow G_2$	A bilinear mapping, while G_1 and G_2 being additive and multiplicative cyclic groups
K_i, K_j:	Ui's private key , SPj's private key
$H_1(IDi)$, $H_1(IDj)$	Ui's public key, SPj's public key
s,P_{pub}	RC private secret, RC's public key
x, y	SPj secrets (*x*), Ui secrets (*y*)
H()	Private hash function
$H_b()$	A Biohash function
h(.)	a secure hash digest function
+	Point Addition
⊕, ||	XOR, Concatenation

3.2.1 The Registration Phase

In registration phase, each user Ui or service provider SPj sends registration request to RC. After receiving the request, the RC generates a private key for Ui or SPj, by employing its master key *s* in the following manner.

$$K_i = \frac{1}{s + H_1(IDi)} P$$

Next, the RC sends the K_i parameter to Ui or SPj using a secure channel. After receiving the private key from RC, the Ui computes $Ei = K_i \oplus h(PWi \,||\, fi)$. Next, it stores *Ei* on the card or device, where *PWi* is the password, and *fi* being the fingerprint of user. Likewise, the SPj, after obtaining the private key from RC, stores it in a secure memory for future access.

3.2.2 The Login and Authentication Phase

1. In this phase, initially, *Ui* sends login request to service provider SPj.
2. Then, SPj computes $A = e(P, P)^x$ and sends towards Ui.
3. Next, Ui computes the following parameters:

$$Mij = H_2(A^y) = H_2(e(P,P)^{xy}) \quad (1)$$

$$R_2 = yP_{pub} + H_1(IDj)yP, \quad (2)$$

$$w = yP_{pub} + H_1(IDi)yP, \quad (3)$$

$$R_i = \frac{1}{y + H_3(IDi \,||\, A \,||\, IDj \,||\, w \,||\, Mij)} K_i \quad (4)$$

$$U_1 = Mij \oplus (IDi \,||\, R_i \,||\, w) \quad (5)$$

Where *y* is a random number, the Ui generates the above parameters and sends the message $<R_2,U_1>$. Here the parameter *y* can be already selected, while the parameters yP_{pub}, yP, and $yH_1(IDi)P$ are already computed before mutual authentication process, this reduces the computation cost of scheme.

4. After receiving $<R_2, U_1>$ from Ui, SPj computes the key Mij in beginning as follows.

$$Mij = H_2 (e (R_2, K_j)^x)=H_2(e(P, P)^{xy}) \quad (6)$$

Then, SPj recovers $(IDi \,||\, R_i \,||\, w)$ by computing $(IDi \,||\, R_i \,||\, w) = Mij \oplus(U_1)$. The SPj, afterwards, computes $e(R_i, w + H_3 (IDi \,||\, A \,||\, IDj \,||\, w \,||\, Mij) Vi)$ and compares against pre-calculated $e(P, P)$, e.g,

$$e(R_i, w + H_3 (IDi \,||A||IDj \,||w \,||Mij)V_i) \stackrel{?}{=} e(P, P) \quad (7)$$

Whereas the V_i is computed as $V_i = (P_{pub}+H_1 (IDi)P)$. Next, SPj computes $F_i = H_4 (Mij \,||\, A \,||\, IDi \,||\, IDj)$ and sends F_i towards Ui.

5. The Ui receives F_i and computes F_i' as

$$F_i' = H_4 (Mij \,||\, A \,||\, IDi \,||\, IDj) \quad (8)$$

Then, it compares the equality for F_i' against F_i. If true, the Ui validates SPj as a valid server.

3.3 Weaknesses in Tsai and Lo scheme.

The Tsai and Lo scheme is a multi-server authentication protocol relying on bilinear pairing based operations. However, the scheme has been found vulnerable to the following attacks.

3.3.1 Impersonation /Server Spoofing Attack

An adversary $\mathbb{A}$ may launch an impersonation attack towards user by spoofing as a server SPj, using the following steps.

1. Initially, after intercepting the login request from a genuine user, an adversary generates the parameter A by computing the bilinear map as shown in the following Eq (9) and sends towards user Ui.

$$A = e(P_{pub}+H_1(IDj)P, P)^x \quad (9)$$

2. Next, the user receives A from adversary under the guise of SPj, and computes Mij, R_2, w, R_i and U_1.

$$Mij = H_2 (A^y) = H_2 (e(P, P)^{xy}), \quad (10)$$
$$R_2 = yP_{pub} + H_1 (IDj)yP, \quad (11)$$
$$w = yP_{pub} + H_1 (IDi)yP, \quad (12)$$
$$R_i = \frac{1}{y+H_3 (IDi \,||A \,||IDj \,||\, w \,||\, Mij)} K_i \quad (13)$$
$$U_1 = Mij \oplus (IDi \,||\, R_i \,||\, w), \quad (14)$$

Then, the user sends the computed message $<R_2, U_1>$ to SPj for verification, as intercepted by $\mathbb{A}$.

Next, $\mathbb{A}$ receives $<R_2, U_1>$ and computes the bilinear pairing map Mij^* of the inputs R_2, x and P as shown in Eq (15).

$$Mij^* = H2(e(R_2, P)^x) \quad (15)$$

3. The adversary, then recovers the user's identity IDi by computing

$$(IDi \,||\, R_i \,||\, w) = Mij^* \oplus U_1 \quad (16)$$

Next, the adversary computes F_i* and sends to user as a response to user's presented challenge as shown in (17).

$$F_i^* = H_4 (Mij^* \| A \| IDi \| IDj) \quad (17)$$

4. Next, the user receives F_i* from Ⱥ, and computes $F_i = H_4 (Mij \| A \| IDi \| IDj)$. Then, the user compares the equality for F_i* and F_i. On positive verification, the user perceives Ⱥ as a valid service provider SPj.

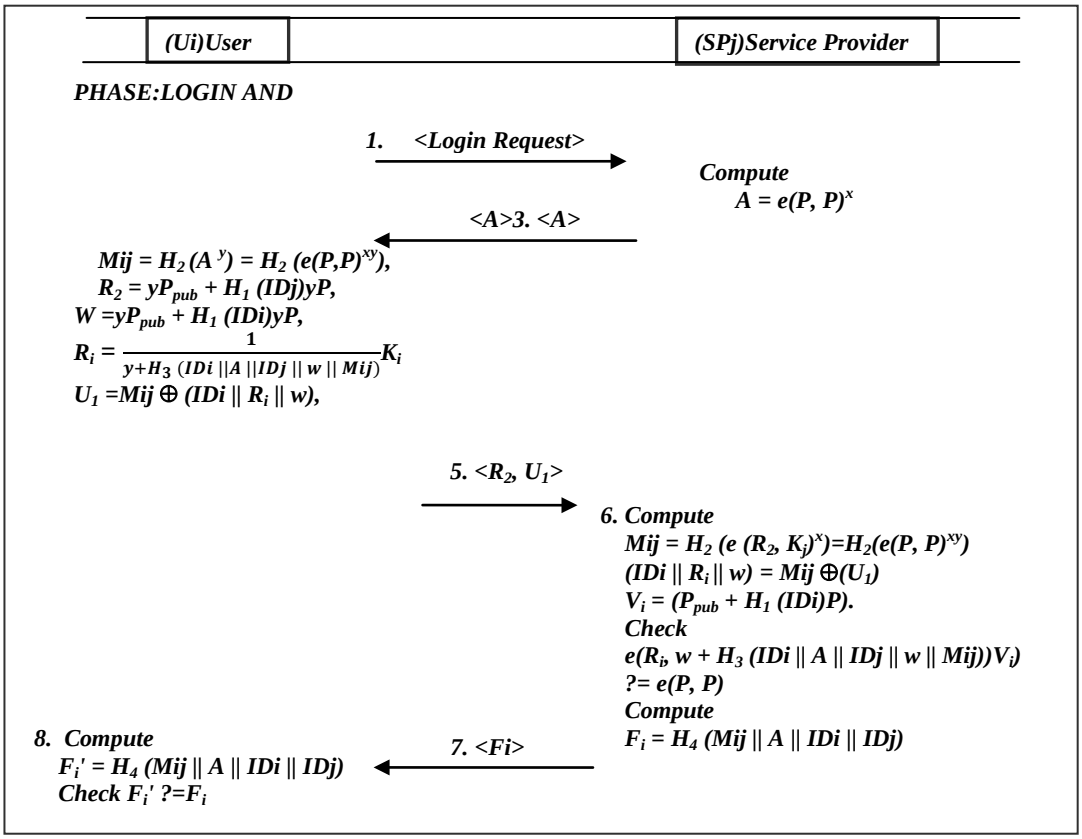


Fig. 2. Tsai and Lo's login and authentication phase

3.3.2 De-synchronisation attack

The registration phase of Tsai and Lo treats the biometric input in smart card for user's verification, without engaging any pre-dealing tool like fuzzy extractor [45] or bio-hashing [36, 37] i.e., Tsai scheme computes $Ei = K_i \oplus h(PWi \| fi)$ by treating the biometric imprint *fi* directly into the hash function without applying any pre-dealing tool. This might lead to de-synchronization attack [45], due to the non-matching biometric input with the pre-stored biometric template, if the pre-dealing tools are not employed. Hence, for being a noisy biometric input, it is preferable to use pre-dealing tools, while taking biometric imprints (for both, registration phase and login phase), to avoid de-synchronization attacks.

3.3.3 No smart card verification leading to Denial-of-service attack

In Tsai and Lo scheme, a smart card does not verify the authenticity of a user before forwarding the request message towards service provider. Owing to this, the server may come

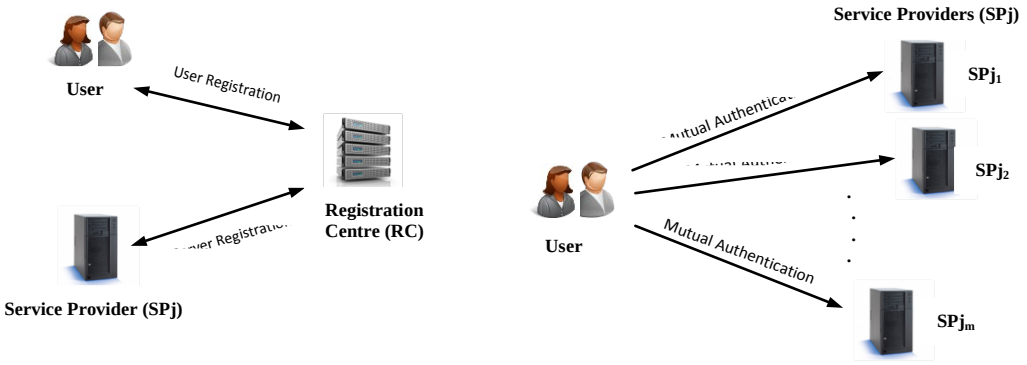
under Denial-of-Service (DoS) attack with the input of fake password *PWi** and biometric input *fi**, if an adversary gets hold over smart card. The smart card produces K_i* on the input of fake parameters, which further may be used to produce *Ri**, and ultimately the message <R_2*, U_1*> could be produced. Although, a server may decline authentication request on the comparison of Eq (7), still it consumes the server's computational power. Even, many legitimate users (insiders) may also act maliciously by inputting fake parameters to burden the server.

3.3.4 Technical flaw/omission in the scheme

In the login and authentication phase of Tsai and Lo scheme, the smart card uses the private key K_i in other computations without deriving it from *Ei* i.e., $K_i = Ei \oplus h(PWi \,||\, fi)$.

4. Proposed Model

The proposed model has been presented in the wake of indicated vulnerabilities in Tsai and Lo protocol. In our scheme, Ui and SPj get registered before joining the system, and afterwards, both of these instances can get mutually authenticated without consulting RC as shown in **Fig. 3.** Our proposed protocol consists of three phases, i.e., registration, login and authentication phase, and password update phase as shown in **Fig. 4**. While, our scheme assumes the same system setup as described in Section 3.1.



a) Registration Phase

b) Authentication Phase

Fig. 3. Proposed mutual authentication between user and SPj without RC engagement

4.1 The Registration Phase

This section deals with all the users and service providers in a single registration phase as shown in **Fig. 4**. In registration phase, each user Ui or service provider SPj sends registration request to registration centre RC. After receiving the request, RC generates private key for Ui or SPj, by using its master key *s* in the following manner.

$$K_i = \frac{1}{s+H_1(IDi)} P \qquad (18)$$

Next, the RC sends K_i or K_j parameter to Ui or SPj using a secure channel. After having received the private key from RC, Ui calculates $Di=h(IDi \,||\, PWi \,||\, H_b(fi))$, $Ei = K_i \oplus h(PWi \,||\, H_b(fi))$. Next, the user stores *Ei*, *Di* on smart card, where *PWi* is the password, and *fi* being the fingerprint of user. Likewise, the SPj, after obtaining the private key from RC, also stores it in a secure memory for future access.

4.2 The Login and Authentication Phase

When a user wants to login into the server for mutual authentication, it takes the following steps.

1. In this phase, initially, the user inputs identity *IDi*, password *PWi*, imprints *fi** and computes $Di' = h(IDi \,||PWi\, ||\, H_b\,(fi))$, and verifies $Di' \,?= Di$. If does not hold true, it aborts. Otherwise, Ui sends the login request to SPj.
2. Then, SPj computes $A = e(P, P)^x$ and sends towards Ui.
3. Ui computes Mij, R_2, w, R_i and U_1 as follows:

$$Mij = H_2\,(A^{\,y}) = H_2\,(e(P,P)^{xy}) \tag{19}$$

$$R_2 = yP_{pub} + H_1\,(IDj)yP, \tag{20}$$

$$w = yP_{pub} + H_1\,(IDi)yP, \tag{21}$$

$$R_i = \frac{1}{y + H_3\,(IDi\,||A\,||\,IDj\,||\,w\,||\,Mij)}\,K_i \tag{22}$$

$$U_1 = Mij \oplus (IDi\,||\,R_i\,||\,w) \tag{23}$$

Ui generates the above parameters and sends the message $<R_2, U_1>$, where y is a random number, which can be already selected, and the parameters yP_{pub}, yP, and $H_1(IDi)yP$ can already be computed before mutual authentication process, this reduces the computation cost for the scheme. Here, the Eq (19) and Eq (23) are equivalent to Eq (10) and Eq (14), since these two steps are alike in both schemes.

4. After receiving $< R_2, U_1>$ from Ui, the server computes the session key Mij in the beginning, as follows.

$$Mij = H_2\,(e\,(R_2, K_j)^x) = H_2(e(P, P)^{xy}) \tag{24}$$

Then, SPj recovers $(IDi\,||\,R_i\,||\,w)$ by computing $(IDi\,||\,R_i\,||\,w) = Mij \oplus U_1$. SPj, afterwards, computes $e(R_i, w + H_3\,(IDi\,|\,A||IDj||w||\,Mij)\,Vi)$ and compares against pre-calculated $e(P, P)$, *i.e.*

$$e(R_i, w + H_3\,(IDi\,||A\,||IDj\,||w\,||Mij)\,V_i) \,?= e(P, P) \tag{25}$$

Whereas the parameter V_i is computed as $V_i = (P_{pub} + H_1\,(IDi)P)$. In this way, the SPj validates the user after positive verification in Eq (25). Next, the server computes R_3 and Z_i as in Eq (26) and Eq (27), and sends the message $< R_3, Z_i>$ to Ui, so that the server can be validated by the user as well.

$$R_3 = xP_{pub} + H_1\,(IDi)xP \tag{26}$$

$$Z_i = H_4(Mij\,||\,A\,||\,IDi\,||\,IDj) \tag{27}$$

5. Next, Ui receives $<R_3, Z_i>$ and computes Mij' and compares Z_i with the computation as shown in Eq (29)

$$Mij' = H_2(e\,(R_3, K_i)^y) \tag{28}$$

$$Z_i \,?= H_4(Mij'\,||\,A\,||\,IDi\,||\,IDj) \tag{29}$$

If Eq (29) verifies to be true, the user validates the SPj as a valid service provider, otherwise aborts the session. Hence, both of the participants, user and SPj mutually authenticate each other and establish the shared session key as $Sk = Mij$.

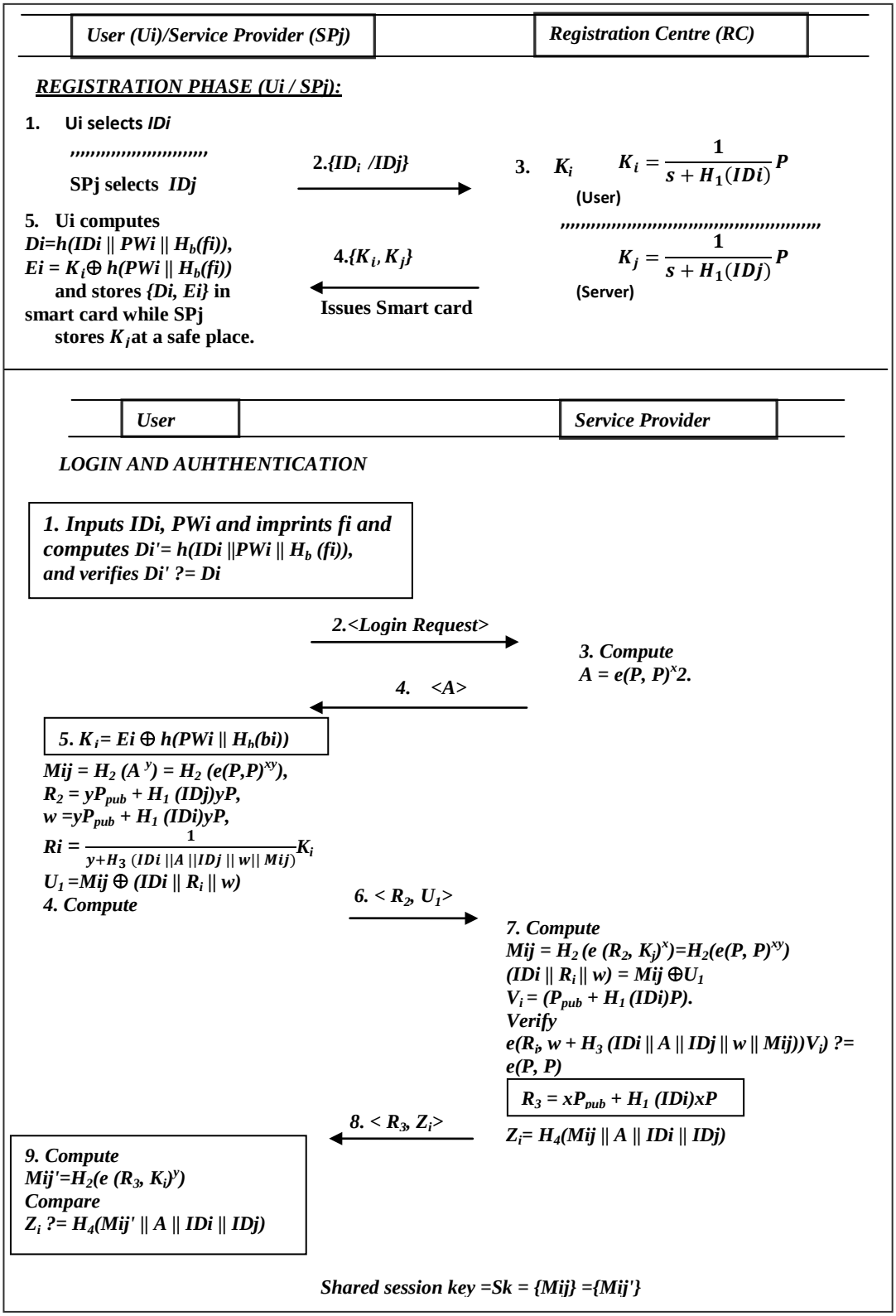


Fig. 4. Proposed Authentication Protocol

4.3 Password Modification Phase

Ui modifies its old password *PWi* into a new password PWi^{new} without any interaction with RC by invoking the following procedure.

1. The Ui inputs its identity *IDi*, password *PWi* into the smart card and also imprints its biometric finger prints *fi* into the sensor device and opts for modifying the password.

1) Next, the smart card (SC) computes $Di^* = h(IDi \,||PWi \,||\, H_b(fi)$ and checks the equality for $Di^* \;?= Di$. If it is false, the SC declines the request, otherwise permits the user to continue with modifying the password.
2) Then, SC computes $K_i = Ei \oplus h(PWi \,||\, H_b(\, fi))$ and prompts user for a new password PWi^{new}.
3) Next, it computes $Di^{new} = h(IDi \,||PWi^{new} \,||\, H_b(fi)$ and $Ei^{new} = K_i \oplus h\,(PWi^{new}||H_b\,(fi))$.
4) Finally, the SC replaces the *Di*, *Ei* with the updated Di^{new} and Ei^{new} values.

5. SECURITY ANALYSIS

This section describes informal and formal security analysis as follows:

5.1 SECURITY DISCUSSION

The informal security analysis has been illustrated as below.

5.1.1 Resistance to Replay Attack

The replay attacks can be launched while an attacker replays the original message parameters at some other time to betray or impersonate any legal participant. An adversary $\mathbb{A}$ intercepts publicly available messages $<A>$, $<R_2, U_1>$, $<R_3, Z_i>$ and may try to replay these messages to either of the legal participants. If the adversary replays either $<A>$ or $<R_3, Z_i>$ messages towards Ui, the Ui could discern in the fourth step of mutual authentication phase by comparing the equality check $Z_i \;?= H_4(Mij'||A \,||IDi||IDj)$ as shown in *Eq* (29). If this does not hold true, Ui may treat this as a replay attack. Likewise, on the replay of message $<R_2, U_1>$, SPj determines the equality check for *Eq* (25)by comparing $e(R_i, w+H_3(IDi||\, A||IDj||w||\, Mij))\, V_i) \;?= e(P, P)$. If the equation does not match, it would be treated as a replay attack by SPj. Hence, the proposed scheme can successfully foil a replay attack.

5.1.2 Resistance to Modification /Man In The Middle Attack (MiTM)

This attack could be initiated if an adversary modifies and reconstruct the message contents in an unauthorized manner to present it to any legitimate user or server, to let the original participants wrongly perceive those as the actual parties; however these are not the right participants, though.

If an adversary tries to modify any of these messages $<A>$,$<R_2, U_1>$ or $<R_3\,, Z_i>$, then Ui or SPj may easily thwart the attack by verifying the equality checks $e(R_i, w + H_3(IDi||A||IDj||w||\, Mij)\, V_i) \;?= e(P, P)$ and $Z_i \;?= H_4\,(Mij' \,||\, A \,||\, IDi \,||\, IDj)$ for the server and user respectively,as shown in *Eq* (25) and(29). Hence, we can say the proposed scheme is resistant to MiTM from both ends.

5.1.3 Resistance to Password Guessing Attack

An adversary $\mathbb{A}$ may try to guess password *PWi* from the stolen smart card contents or from the messages intercepted publicly. The SC contains $Di = h(IDi \,||\, PWi \,||\, H_b\,(fi)$ and $Ei = K_i \oplus h(PWi \,||\, H_b\,(fi))$ parameters, however, $\mathbb{A}$ will not be able to derive the *PWi* from *Di* or *Ei*, since,

the adversary being unaware of the *fi*, a high entropy secret. Hence, the computation of *PWi* with the combination of *IDi* and *fi* will not be able to be recovered in polynomial time by the adversary. Hence, the proposed scheme is resistant from any password guessing attack.

5.1.4 Session key security

An attacker $\mathcal{A}$ may steal smart card or intercept all communication messages between the legitimate participants and try to compute the session key $Sk = \{Mij\} = \{Mij'\}$ from those contents. However, $\mathcal{A}$ is not able to compute session key, since it requires access to either *x* or *y* parameters, while an attacker is restricted to the access to those parameters by the hardness of ECDLP problem [16]. Hence, the stolen smart contents or the messages interception from an insecure channel cannot lead to the disclosure of mutual participants' legitimate session keys.

5.1.5 Resists Impersonation attack / Server spoofing attack

An adversary $\mathcal{A}$ may try to initiate an impersonation attack towards user by spoofing attempts as a malicious server. However, unlike Tsai and Lo, if $\mathcal{A}$ attempts to send the manufactured parameter *A* i.e., $A = e(P_{pub}+H_1(IDj)P, P)^x$ towards the user, the latter will be able to discover the attack in the fourth phase of mutual authentication of the proposed protocol while comparing bilinear maps in *Eq* (29). If $\mathcal{A}$ tries to launch such an attack, the equality check $Z_i \; ?= H_4(Mij' \,||\, A \,||\, IDi \,||\, IDj)$ would fail, and the user will have to abort the session. Hence, in the proposed protocol, both entities Ui and SPj mutually authenticate each other in a serial manner that restricts the adversaries to initiate any kind of impersonation attack or server spoofing attack.

5.1.6 Known-Key Security

The known-key security signifies towards guessing the other session keys provided the current session key has been compromised. In proposed scheme, even if an adversary, by some means, comes to know the session key $Sk = \{Mij\}$ of a session, then it may not help the adversary, by any means, in finding the other session keys between the same participants, as every session key is based on the novel session secrets which are randomly generated for a particular session. While, for attacker it would be a hard problem to access corresponding secret parameters, nearly equivalent to solving the ECDLP problem. Hence, for the known-key security, the proposed scheme has proved to be quite secure.

5.1.7 Perfect Forward secrecy

The perfect forward secrecy describes the property of security against session keys disclosure, in case the adversary gets access to master private keys related to central authorities, for instance, RC in our scenario.
In the proposed scheme, if an attacker accesses the private key *s* of RC, it might compute the private keys of the corresponding user and service provider, as K_i and K_j , after approaching the Ui's or SPj's identity *IDi*, *IDj* as shown in Eq (37) and (38).

$$K_i = \frac{1}{s+H_1(IDi)}P \qquad (30)$$

$$K_j = \frac{1}{s+H_1(IDj)}P \qquad (31)$$

However, it will not be able to compute the session key $Sk = \{Mij\}$ since the computation of Mij parameters, despite the knowledge of K_i and K_j, requires the knowledge of either of the secrets for a particular session, i.e., x or y to compute the Mij session key. Besides, $\mathcal{A}$ cannot derive these parameters from U_1 i.e., $U_1 = Mij \oplus (IDi \,||\, R_i \,||\, w)$ for not having the knowledge of R_i and w parameters. Hence, for the perfect forward secrecy, the proposed scheme has been quite secure.

5.1.8 Mutual Authentication

The mutual authentication defines that both entities authenticate each other in the same authentication protocol.

In the proposed protocol, the SPj authenticates the user on the basis of challenge $<A>$ sent by it and the received challenge response from the user. The SPj computes the bilinear map and compares against $e(P, P)$ as shown in Eq (25), and verifies the user's authenticity. In the same protocol, the user verifies the SPj's authenticity by computing the bilinear map and comparing Z_i against $H_4(Mij' \,||\, A \,||\, IDi \,||\, IDj)$ as shown in Eq. (29). In this way, both entities authenticate one another mutually in the same protocol.

5.1.9 Anonymous Authentication

The anonymous authentication provides anonymity to Ui along with its authentication from SPj, and attacker cannot tell the identity of the communicating participants by utilizing publicly open message parameters.

In proposed model, an attacker cannot derive the user's identity from the intercepted messages of the established sessions, since the IDi is contained in a secret parameter U_1, i.e., $U_1 = Mij \oplus (IDi \,||\, R_i \,||\, w)$, which is not possible to guess until the random secrets x, y and in return, session key is guessed, computed or accessed in polynomial time**.** Hence, our scheme provides anonymous authentication to user Ui.

5.1.10 Resists de-synchronisation Attack

The de-synchronization attack might happen when an attacker modifies the messages in such a manner that the legal participants fail to authenticate one another and are forced to abort the session during authentication phase. However, in the proposed protocol, if an adversary tries to modify the message $<A>$, $<R_2, U_1>$, $<R_3, Z_i>$, then the user may easily foil the de-synchronization attack by computing $Mij' = H_2(e(R_3, K_i)^y)$ and verifying the inequality $Z_i \stackrel{?}{=} H_4(Mij' \,||\, A \,||\, IDi \,||\, IDj)$ as shown in Eq. (29). Since, the calculated parameter Mij' will not lead to the matching of Zi against $H_4(Mij' \,||\, A \,||\, IDi \,||\, IDj)$, which keeps the adversaries from initiating any modification or MiTM attack. In this manner, the de-synchronization attack may be detected and foiled successfully. At the same time, the proposed scheme also resists de-synchronization attack, unlike Tsai and Lo, since it employed bio-hashing tool while imprinting biometrics fi.

5.1.11 Resistance to Denial-of-Service attacks (DoS)

The proposed scheme resists DoS attack, as in the propsoed scheme, we employ smart card-based local verification to resist any kind of DoS attack, in case the smart card gets stolen. Hence, the proposed scheme is resistant to DoS attack.

5.2 Formal Security Analysis

This section covers the formal security analysis of our proposed protocol under Burrows-Abadi-Needham logic (BAN) logic [38, 39] and random oracle model (ROM), while, the former is a model that analyzes the security based on mutual authentication, key distribution, and the strength against session key disclosure. Some notations, as used in the BAN logic are described as follows:

Principals are such agents that are involved in a protocol.
Keys are to be used for symmetric message encryption.

Few notations that have been used in the BAN security analysis are given as follows:

P $\models$ **X**: The principal P believes X, or alternatively, P believes the statement X.
P $\lhd$ **X**: P sees X. P receives some message X and may read or repeat it in any message.
P$\mid\sim$ **X**: P once said X. In the past, P had sent some message X which P believed.
P $\Rightarrow$ **X**: P has got jurisdiction over X; or P has authority over X and could be trusted.
$\sharp$ **(X)**: The message X may be treated as fresh.
(X, Y): X or Y being the part of message (X, Y).
$\langle$**X**$\rangle_{\mathbf{Y}}$: The formulae X is combined with formulae Y.
$\{$**X, Y**$\}_{\mathbf{K}}$: X or Y is encrypted with the key K.
(X, Y)$_{\mathbf{K}}$: X or Y is hashed with the key K.
P $\overset{\mathbf{K}}{\longleftrightarrow}$ **Q**: P and Q can communicate with the shared key K.

Some rules or logical postulates used in the BAN Logic are given as follows:

Rule 1. Message meaning rule: $\frac{P\mid\equiv P \overset{K}{\leftrightarrow} Q,\ \ P\lhd\langle X\rangle_Y}{P\mid\equiv Q\mid\sim X}$
If P believes the shared key K with Q, and sees message $\langle X\rangle_Y$, then P believes that Q once said X.

Rule 2. Nonce verification rule: $\frac{P\mid\equiv \#(X),\ \ P\mid\equiv Q\mid\sim\ X}{P\mid\equiv Q\mid\equiv\ X}$
If P believes message X as fresh, and that Q once sent X, then P believes that Q also believes X.

Rule 3. Jurisdiction rule: $\frac{P\mid\equiv Q\Rightarrow X,\ \ P\mid\equiv Q\mid\equiv\ X}{P\mid\equiv X}$
If P believes that Q has jurisdiction over X, and that Q believes X, then P also believes X.

Rule 4. Freshness conjuncatenation rule: $\frac{\mathrm{P}\mid\equiv\#\,(\mathrm{X})}{\mathrm{P}\mid\equiv\#\,(\mathrm{X},\ \mathrm{Y})}$
If P believes that X is fresh, then it also believes the freshness of (X, Y).

Rule 5. Belief rule: $\frac{P\mid\equiv(X),\ \ P\mid\equiv(Y)}{P\mid\equiv(X,\ Y)}$
If P believes X and Y individually, then the statement P $\mid\equiv$ (X, Y) gives the same meaning.

Rule 6. Session keys rule: $\frac{\mathrm{P}\mid\equiv\#(\mathrm{X}),\ \ \mathrm{P}\mid\equiv\mathrm{Q}\mid\equiv\ \mathrm{X}}{\mathrm{P}\mid\equiv\mathrm{P}\overset{\mathrm{K}}{\leftrightarrow}\mathrm{Q}}$
If P believes fresh X, and also that Q believes X, then P believes that K is shared between P and Q.

The proposed protocol needs to satisfy the following goals to ensure its security under BAN logic, using the above assumptions and postulates.

Goal1 : SPj $\mid\equiv$ SPj $\overset{Sk}{\longleftrightarrow}$ Ui

Goal2 : SPj $\mid\equiv$ Ui $\mid\equiv$ SPj $\overset{Sk}{\longleftrightarrow}$ Ui

Goal3 : Ui $|\equiv$ SPj$\overset{Sk}{\longleftrightarrow}$ Ui

Goal4 : Ui $|\equiv$ SPj $|\equiv$ SPj$\overset{Sk}{\longleftrightarrow}$ Ui

Initially, the messages exchanged in the proposed protocol can be transformed into idealized form in the following manner.
M_1: Ui $\rightarrow$ SPj: R_2, U_1: $\langle IDi, R_i, yP_{pub} + H_1(IDj).yP \rangle_{Mij}$
M_2: SPj $\rightarrow$ Ui: R_3, Z_i: $\langle IDj, xP_{pub} + H_1(IDi).xP \rangle_{Mij'}$

Secondly, the following assumptions are supposed to prove the security of proposed protocol.
A1 : Ui $|\equiv \sharp\, y$

A2 : SPj $|\equiv \sharp\,(x, A)$

A3 : Ui $|\equiv$ SPj $\overset{Mij}{\longleftrightarrow}$ Ui

A4 : SPj $|\equiv$ SPj$\overset{Mij'}{\longleftrightarrow}$ Ui

A5 : Ui $|\equiv$ SPj $\Rightarrow$ ($xP_{pub} + H_1(IDi).xP$)

A6 : SPj $|\equiv$ Ui $\Rightarrow$ ($R_i, yP_{pub} + H_1(IDj).yP$)

Thirdly, the idealized form i.e., M_1 and M_2 of the proposed protocol can be examined and verified in the light of above mentioned postulates and assumptions.

Considering the first message of the idealized form:
M_1: Ui $\rightarrow$ SPj: R_2, U_1: $\langle IDi, R_i, yP_{pub} + H_1(IDj).yP \rangle_{Mij}$
By applying seeing rule, we get
S1: SPj $\lhd$ R_2, U_1: $\langle IDi, R_i, yP_{pub} + H_1(IDj).yP \rangle_{Mij}$

According to S1, A3 and message meaning rule,
S2: SPj $|\equiv$ Ui ~ ($R_i, yP_{pub} + H_1(IDj).yP$)

According to A2, S2, freshness conjucatenation, and nonce verification rules, we get

S3: SPj $|\equiv$ Ui $|\equiv$ ($R_i, yP_{pub} + H_1(IDj).yP$)
While, ($IDi, R_i, yP_{pub}+H_1(IDj).yP$) are necessary parameters for the mutual authentication and verification of parameter *Mij*, which is used in session key *Sk = {Mij}*.
According to A6, S3, and Jurisdiction rule
S4: SPj $|\equiv$ ($R_i, yP_{pub} + H_1(IDj).yP$)
According to A3, S4, and session key rule, we get
S5: SPj $|\equiv$ Ui $|\equiv$ SPj$\overset{SK}{\leftrightarrow}$ Ui **(Goal 2)**
According to A6, S5, and Jurisdiction rule
S6: SPj $|\equiv$ SPj$\overset{SK}{\leftrightarrow}$ Ui **(Goal 1)**
Considering the second message of the idealized form as:

M_2: SPj $\rightarrow$ Ui: R_3, Z_i: $\langle IDj, xP_{pub} + H_1(IDi).xP \rangle_{Mij'}$
By applying seeing rule, we get
S7: Ui $\lhd$ SPj $\rightarrow$ Ui: R_3, Z_i: $\langle IDj, xP_{pub} + H_1(IDi).xP \rangle_{Mij'}$
According to S7, A4 and message meaning rule,
S8: Ui $|\equiv$ SPj ~ ($xP_{pub} + H_1(IDi).xP$)
According to A1, S8, freshness conjucatenation, and nonce verification rules we get,

S9: Ui $|\equiv$ SPj $|\equiv$ ($xP_{pub} + H_1(IDi).xP$)

Where, (xP_{pub} + H_1 *(IDi).xP*) are necessary parameters for the mutual authentication and verification of parameter *Mij'* which is used in session key *Sk = {Mij} = { Mij'}*.

According to A5, S9, and Jurisdiction rule

S10: Ui $\mid\equiv$ (xP_{pub} + H_1 *(IDi).xP*)
According to A4, S10, and session key rule, we get
S11: Ui $\mid\equiv$ SPj $\mid\equiv$ SPj$\overset{SK}{\leftrightarrow}$ Ui **(Goal 4)**
According to A5, S11, and Jurisdiction rule
S12: Ui $\mid\equiv$ SPj$\overset{Sk}{\longleftrightarrow}$ Ui **(Goal 3)**

The above BAN logic analysis formally proves that the proposed protocol achieves mutual authentication and the session key *Sk* is mutually established between Ui and SPj.

Using another random oracle model (ROM) as a generic contradiction model of cryptography [48], we may conduct a formal security analysis to prove that the proposed scheme is secure. For this purpose, we used an oracle *Reveal1* and *Reveal2* as defined under:

$Reveal_1$: The $Reveal_1$ oracle outputs *a* from the corresponding bilinear map $Z = e(P,P)^a$, unconditionally.
$Reveal_2$: The $Reveal_2$ oracle outputs *t* from the corresponding hash value *u=h(t)*,unconditionally.

The oracle $Reveal_1$ has been used for Algorithm 1. $EXP1^{Key}_{IMSADMCCS}$, indicating towards the disclosure of *Sk* in case the $Reveal_1$ is applied by inverting the hash function.

Algorithm 1. $\boldsymbol{EXP1^{Key}_{IMSADMCCS}}$

1. Eavesdrop the Login request message <*A*>in the login phase, where $A = e(P, P)^x$.
2. Call $Reveal_1$ oracle on input $A = e(P, P)^x$ to retrieve $x' \leftarrow reveal1(e(P, P)^x)$.
3. Eavesdrop the Authentication messages <R_2, U_1>and<R_3, Z_i> in the verification phase, where $R_2 = yP_{pub} + H_1(IDj)yP$, $R_3 = xP_{pub} + H_1(IDi)xP$, $U_1 = Mij \oplus (IDi \mid\mid R_i \mid\mid w_i)$ and $Z_i = H_4(Mij \mid\mid A \mid\mid IDi \mid\mid IDj)$.
4. Call $Reveal_2$ oracle on input Z_i to retrieve (Mij^*, A', IDi', IDj) as $(Mij \mid\mid A' \mid\mid IDi \mid\mid IDj) \leftarrow reveal_1(Z_i)$.
5. Next, it computes $Mij^* \oplus U_1$ and recovers the parameters as $(IDi'' \mid\mid R_i' \mid\mid w')$.
6. Further, it computes $V_i' = (P_{pub} + H_1(IDi)P)$.
7. If $[(IDi' == IDi'') \; AND \; e(R_i', w_i' + H_3(IDi' \mid\mid A' \mid\mid IDj' \mid\mid w_i' \mid\mid Mij^*)V_i') == e(P,P)]$
   Accept *IDi'* as the correct identity of the user Ui, and accept *Sk =Mij** as the correct session key between the Ui and SPj,
   Return 1 (success)
8. Else
9. Return 0 (failure)
10. End if

Theorem1
The proposed scheme stands secure, in case an attacker tries to derive the shared session key Sk between Ui and SPj, if one-way hash function H(.) behaves closely like a random oracle,.

Proof. In this proof, an attacker $\mathbb{A}$, capable of deriving the shared session key *Sk* between Ui and SPj, makes a use of the random oracle *Reveal1* and *Reveal2* for the implementation of algorithm $EXP1^{Key}_{IMSADMCCS}$. The success probability for $EXP1^{Key}_{IMSADMCCS}$ is

Suc1=Pr[$EXP1^{Key}_{IMSADMCCS}$=1]-1, whereas, Pr[E] shows the probability of an event E. The advantage function for this experiment becomes as $Adv^{Key}_{IMSADMCCS}$ (t_1, q_1, q_2) = $\max_{\mathbb{A}}$ [$Suc1^{Key}_{IMSADMCCS}$], with the execution time t_1 and random Reveal query q_1 and q_2 maximized on $\mathbb{A}$. We call our proposed technique as provably secure against an attacker $\mathbb{A}$ for deriving the shared session key *Sk* between Ui and SPj, if $Adv^{Key}_{IMSADMCCS}(t_1, q_1, q_2) \leq \varepsilon'$ for any sufficiently small $\varepsilon' > 0$. According to this experiment, if an attacker $\mathbb{A}$ has the ability of revealing private keys of participants, and discerning the bilinear map constituent components, then it can easily derive the original session key *Sk* as used between the legitimate participants Ui and SPj, and finally $\mathbb{A}$ wins the game. However, according to [16], this is computationally infeasible to break the bilinear map since $Adv^{Key}_{IMSADMCCS}(t_1) \leq \varepsilon'$ for any sufficiently small $\varepsilon' > 0$. Hence, the proposed scheme can be regarded as immune as the security properties for hash operation are hard to break.

6. COMPARISON AND PERFORMANCE ANALYSIS

In this section, the comparison for the security of the proposed model against Tsai and Lo and other authentication protocols has been shown. **Table 2** demonstrates the resistance of various schemes i.e., [26], [40], [41]-[43], [44], [29] and the proposed scheme, against a few renowned attacks. The proposed model is an improved and extended model of Tsai and Lo, while the former proves to be a robust authentication technique as indicated in the above formal and informal security analysis. We may notice that three of these schemes provide anonymity [44], [29], and the proposed protocol. Most of these schemes are traceable except [29] and the proposed protocol. The modification attack, stolen smart card attack, and time synchronization problems have been found in [40], and [41]-[43], as identified in subsequent papers of the attacked scheme. The schemes [40] and [41] are also vulnerable to replay attacks, while, [43] could not resist password guessing attack. In these previous studies, most of the schemes suffer impersonation attacks except [26]. Lastly, the schemes that provide multi-server authentication environment as well, to the clients using ID-based cryptography are [26], [29], amid the proposed scheme.

The actual cost for schemes, Tsai and Lo, and the proposed scheme have been compared in **Table 3**, since the current study reviewed only Tsai and Lo protocol with elaboration. We assume T_{BP} as the time required for the bilinear pair to complete its operation, and T_{PM} as the time for performing point multiplication. Some of the calculations on the users' end are taken as pre-computed and not included in the computational cost, while making comparison, e.g., *yPub*, *yP*, and $yH_1(IDi)P$. The registration procedure for Tsai and Lo and the proposed scheme takes $1T_{PM}$ of time delay responsible for generating the Ui and SPj's private keys. For the login and authentication phase, a user takes total time $4T_{PM}$ in Tsai and Lo protocol, while in the proposed model, it takes $4\ T_{PM} + 1T_{BP}$ for the same phase. The service provider takes $2\ T_{PM} + 3T_{BP}$ time delay for Tsai and Lo, while for the proposed protocol, it takes $4\ T_{PM} + 3T_{BP}$ time delay. Although the proposed scheme takes an extra operation of $1T_{BP}$ on the user's end, and $2T_{PM}$ on the service provider's end, however, the proposed scheme is not vulnerable to impersonation attack, as Tsai and Lo scheme does. The cost of the proposed scheme is almost 30% above of Tsai and Lo scheme due to additional point multiplications and bilinear pairing, however, the former is secure against probable impersonation attacks. In our proposed scheme, bilinear map operation provides the basis of ID-based cryptography, and enables the service provider and user the way to authenticate one another without seeking help from registration centre for establishing multiple subsequent mutual authentication sessions.

Table 2. Security comparison for various ID-based cryptographic schemes

	[40]	[41]	[42]	[43]	[44]	[26]	[29]	Ours
Provides Anonymity	No	No	No	No	Yes	No	Yes	Yes
Mutual Authentication	No	No	No	Yes	No	Yes	No	Yes
Known key secrecy	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Untraceable	No	No	No	No	No	No	Yes	Yes
Resist Modification Attack	No	No	No	No	Yes	Yes	Yes	Yes
Resist offline-password guessing attack	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Resist Stolen smart card attack	No	No	No	No	Yes	Yes	Yes	Yes
Resist Impersonation attack	No	No	No	No	No	Yes	No	Yes
Resist Replay attack	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Resist DoS attack	No	No	Yes	Yes	Yes	Yes	No	Yes
Resist De-synchronization attack	No	No	Yes	Yes	Yes	Yes	No	Yes
Multi-server Paradigm	No	No	No	No	No	Yes	Yes	Yes
Resistance to Time Synchronization issues	No	No	No	No	Yes	Yes	Yes	Yes

Table 3. Number of operations inTsai and Lo and Proposed protocol

	Tsai and Lo [29]	**Proposed protocol**
Registration messages	$1T_{PM}$	$1T_{PM}$
User	$4\ T_{PM}$	$4\ T_{PM} + 1T_{BP}$
Service provider	$2\ T_{PM} + 3T_{BP}$	$4\ T_{PM} + 3T_{BP}$

Since, the proposed scheme covers impersonation attacks that Tsai and Lo was unable to cover in that scheme, hence, in the light of above performance analysis, we can say that the proposed scheme is more secure than Tsai and Lo scheme with a bit additional cost, though necessary. At the same time, the security of the cryptographic protocol is more important, and to enhance the security, somehow an additional cost computation can be afforded.

7. CONCLUSION

The mobile cloud computing (MCC) has been paving its way towards being embraced in future services as keenly sought by the mobile subscribers. Recently, Tsai and Lo has proposed a multi-server authenticated key agreement solution based on bilinear pairing, to eliminate the trusted third party involvement in mutual authentication between user and service provider. However, the Tsai and Lo scheme has been found prone to server spoofing attack (misrepresentation attack), de-synchronization and DoS attacks, which renders the scheme inapt for being deployed in access networks. Thus, we have presented an improved and secure model based on bilinear pairing, countering the identified threats as posed to Tsai and Lo scheme. The proposed scheme also presents the formal and informal security analysis, which proves that the scheme has been resistant to the renowned threats so far, as posed to the earlier schemes.

References

[1] ABI Research Report, Mobile Cloud Applications. [Online]. Available: http://www.abiresearch.com/research/1003385-Mobile+Cloud+Computing

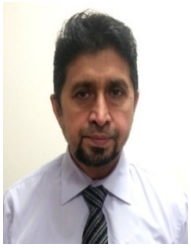
[2] X. F. Qiu, J.W. Liu, and P. C. Zhao, "Secure cloud computing architecture on mobile Internet," in *Proc. of 2nd Int. Conf. AIMSEC*, pp. 619–622, 2011. Article (CrossRef Link)
[3] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Gen. Comput. Sys.*, vol. 29, no. 1, pp. 84–106, Jan. 2013. Article (CrossRef Link)
[4] G. Le, K. Xu, M. Song, and J. Song, "A survey on research on mobile cloud computing," in *Proc. of10th IEEE/ACIS/Int. Conf. Comput. Inf. Sci*., pp. 387–392, 2011. Article (CrossRef Link)
[5] W. G. Song and X. L. Su, "Review of mobile cloud computing," in *Proc. of IEEE ICCSN*, pp. 1–4, 2011. Article (CrossRef Link)
[6] Han, N. D., Han, L., Tuan, D. M., In, H. P., & Jo, M., "A scheme for data confidentiality in cloud-assisted wireless body area networks," *Information sciences*, 284, 157-166, 2014. Article (CrossRef Link)
[7] H. Ahn, H. Chang, C. Jang, and E. Choi, "User authentication platform using provisioning in cloud computing environment," in *Proc. of ACN CCIS*, vol. 199, pp. 132–138, 2011. Article (CrossRef Link)
[8] P. Urien, E. Marie, and C. Kiennert, "An innovative solution for cloud computing authentication: Grids of EAP-TLS smart cards," in *Proc. of 5th Int. Conf. Digit. Telecommun*., pp. 22–27, 2010. Article (CrossRef Link)
[9] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure delegation-based authentication protocol for wireless roaming service," *IEEE Commun. Lett*., vol. 16, no. 7, pp. 1100–1102, Jul. 2012. Article (CrossRef Link)
[10] H. Chang and E. Choi, "User authentication in cloud computing," in *Proc. of UCMA CCIS*, vol. 151, pp. 338–342, 2011. Article (CrossRef Link)
[11] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures," in *Proc. of IEEE Int. Conf. Dependable Auton. Secure Comput*., pp. 711–716, 2009. Article (CrossRef Link)
[12] S. Pearson, "Taking account of privacy when designing cloud computing services," in *Proc. of CLOUD ICSEWorkshop Softw. Eng. Challenges Cloud Comput*., pp. 44–52, 2009. Article (CrossRef Link)
[13] H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security Privacy*, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010. Article (CrossRef Link)
[14] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys Tuts*., vol. 15, no. 2, pp. 843–859, Jul. 2012. Article (CrossRef Link)
[15] OpenID Foundation, OpenID Authentication 2.0, 2007. [Online]. Available: http://openid.net/specs/openid-authentication-2_0.html
[16] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209, 1987. Article (CrossRef Link)
[17] V. Miller, "Use of elliptic curves in cryptography," in *Proc. of CRYPTO*, pp. 417–426, 1986. Article (CrossRef Link)
[18] "Recommendation for key management—Part 1: General," Gaithersburg, MD, USA, Aug. 2005, Special Publication 800-57.
[19] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. of Advances in Cryptology-CRYPTO*, vol. 2139, LNCS. Berlin, Germany: Springer-Verlag, pp. 213–229, 2001. Article (CrossRef Link)
[20] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie–Hellman groups," in *Proc. of Public Key Cryptography PKC*, vol. 2139, LNCS. Berlin, Germany: Springer-Verlag, pp. 18–30, 2003. Article (CrossRef Link)
[21] H. Z. Du and Q. Y. Wen, "An efficient identity-based short signature scheme from bilinear pairings," in *Proc. of Int. Conf. CIS*, pp. 725–729, 2007. Article (CrossRef Link)
[22] H. W. Lim and M. Robshaw, "On identity-based cryptography and grid computing," in *Proc. of ICCS*, pp. 474–477, 2004. Article (CrossRef Link)
[23] H.W. Lim and M. Robshaw, "A dynamic key infrastructure for GRID," in *Proc. of EGC*, pp. 255–264, 2005. Article (CrossRef Link)

[24] A. Armando et al., "An authentication flaw in browser-based single sign-on protocols: Impact and remediations," *Comput. Security*, vol. 33, pp. 41–58, Mar. 2013. Article (CrossRef Link)
[25] W. Mao, "An identity-based non-interactive authentication framework for computational grids," *HP Labs, Palo Alto, CA, USA, Tech. Rep*. HPL-2004-96, Jun. 2004.
[26] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *Proc. of CloudCom*, pp. 157–166, 2009. Article (CrossRef Link)
[27] V. S. Hughes, "Information hiding, anonymity and privacy a modular approach," *J. Comput. Security*, vol. 12, no. 1, pp. 3–36, Jan. 2004. Article (CrossRef Link)
[28] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Trans. Ind. Informat*., vol. 9, no. 4, pp. 2004–2013, Nov. 2013. Article (CrossRef Link)
[29] J. L. Tsai and N. W. Lo, "A privacy-aware authentication scheme fordistributed mobile cloud computing services,"*IEEE Syst*. J.,vol.9, no. 3, pp. 805–815, Sep. 2015. Article (CrossRef Link)
[30] Wu, F., Xu, L., Kumari, S., & Li, X., "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Computers & Electrical Engineering*, *45*, 274-285, 2015. Article (CrossRef Link)
[31] Khan, M. K., & Kumari, S., "An improved biometrics-based remote user authentication scheme with user anonymity," *BioMed research international*, 2013. Article (CrossRef Link)
[32] Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M., "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, 36, 152-176, 2016. Article (CrossRef Link)
[33] 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*, 80(1), 175-192, 2015. Article (CrossRef Link)
[34] 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*, 1-14, 2015. Article (CrossRef Link)
[35] Boneh, D., Lynn, B., & Shacham, H., "Short signatures from the Weil pairing," in *Proc. of Advances in Cryptology—ASIACRYPT* 2001 (pp. 514-532). Springer Berlin Heidelberg, 2015. Article (CrossRef Link)
[36] Jin, A. T. B., Ling, D. N. C., & Goh, A., "Biohashing: Two factor authentication featuringfingerprint data and tokenised random number," *Pattern Recognition*, 37(11), 2245–2255, 2014. Article (CrossRef Link)
[37] Lumini, A., & Nanni, L., "An improved biohashing for human authentication," *Pattern Recognition*, 40(3), 1057–1065, 2007. Article (CrossRef Link)
[38] M. Burrows, Abadi, M., & Needham, R., "A logic of authentication," *ACM Transactions on Computer Systems*, 8(1), 18–36, 1990. Article (CrossRef Link)
[39] M. Burrows, Abadi, M., & Needham, R. M., "A logic of authentication," in *Proc. of the Royal Society of London A-Mathematical and Physical Sciences*, 233–271, 1989. Article (CrossRef Link)
[40] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phafstak, "A novel remote user authentication scheme using bilinear pairings," *Comput. Security*, vol. 25, no. 3, pp. 184–189, May 2006. Article (CrossRef Link)
[41] T. Goriparthia, M. L. Das, and A. Saxena, "An improved bilinear pairing based remote user authentication scheme," *Comput. Std. Interfaces*, vol. 31, no. 1, pp. 181–185, Jan. 2009. Article (CrossRef Link)
[42] A. S. Khan Pathan, C. S. Hong, and K. Hee, "Bilinear-pairing-based remote user authentication schemes using smart cards," in *Proc. of 3rd Int. Conf. Ubiquitous Inf. Manage. Commun*., pp. 356–361, 2009. Article (CrossRef Link)
[43] T. H. Chen, H. L. Yeh, and W. K. Shih, "An advanced ECC dynamic ID based remote mutual authentication scheme for cloud computing," in *Proc. of 5th FTRA Int. Confe. Multimedia Ubiquitous Eng*., pp. 155–159, 2011. Article (CrossRef Link)
[44] H. Sun, Q.Wen, H. Zhang, and Z. Jin, "A novel remote user authentication and key agreement scheme for mobile client–server environment," *Appl. Math. Inf. Sci*., vol. 7, no. 4, pp. 1365–1374, 2013. Article (CrossRef Link)

[45] Li, X., Niu, J., Wang, Z., & Chen, C., "Applying biometrics to design three-factor remote user authentication scheme with key agreement," *Security and Communication Networks*, 7(10), 1488-1497, 2014. Article (CrossRef Link)
[46] Jiang, Q., Ma, J., Li, G., & Ma, Z., "An improved password-based remote user authentication protocol without smart cards," *Information technology And control*, 42(2), 113-123, 2013. Article (CrossRef Link)
[47] D. Wang, Y. Mei, C. G. Ma, and Z. S. Cui, "Comments on an advanced dynamic ID-basedauthentication scheme for cloud computing," in *Proc. of Web Information Systems and Mining*, vol. 752, LNCS. Berlin, Germany: Springer-Verlag, pp. 246–253, 2012. Article (CrossRef Link)
[48] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key agreement secure against dictionary attacks," in *Proc. of EUROCRYPT*, pp. 139–155, 2000.
[49] M. Jakpbsson and D. Pointcheval, "Mutual authentication for low-power mobile devices," in *Proc. of FC*, Feb. 19–22, pp. 178–195, 2001. Article (CrossRef Link)
[50] F. Bao, R. H. Deng, and H. Zhu, "Variations of Diffie–Hellman problem," in *Proc. of 5th ICICS*, pp. 301–312, 2003. Article (CrossRef Link)
[51] He, D., & Wang, D., "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, 9(3), 816-823, 2015. Article (CrossRef Link)
[52] Wang, D., He, D., Wang, P., & Chu, C. H., "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, 12(4), 428-442, 2015. Article (CrossRef Link)
[53] Jiang, Q., Ma, J., Ma, Z., & Li, G., "A privacy enhanced authentication scheme for telecare medical information systems," *Journal of medical systems*, 37(1), 1-8, 2013. Article (CrossRef Link)
[54] Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., & Sakurai, K., "Authentication in mobile cloud computing: A survey," *Journal of Network and Computer Applications*, 61, 59-80, 2016. Article (CrossRef Link)

Azeem Irshad received Master's degree from Arid Agriculture University, Rawalpindi, Pakistan. Currently, he is persuing his PhD in security for multi-server architectures, from International Islamic University, Islamabad, Pakistan. His research interests include strengthening of authenticated key agreements in SIP multimedia, IoT, WBAN, TMIS, WSN, Ad hoc Networks, e-health clouds and multi-server architectures.

Muhammad Sher is a Professor having more than 120 scientific publications. He is chairman of the Department of Computer Science & Software Engineering, International Islamic University. He is also Dean of the Faculty of Basic & Applied Sciences. He did his Ph.D. Computer Science from TU Berlin, Germany and M. Sc. From Quaid-e-Azam University, Islamabad. His research interests include Next Generation Networks and Network Security.



Hafiz Farooq Ahmad completed his MSc and MPhill in the field of Electronics from Quaid-i-Azam University, Islamabad in 1990 and 1993 respectively. He holds PhD from Tokyo Institute of Technology (Tokyo Japan in Distributed Computing). He is Associate Professor at College of Computer Sciences and Information Technology. Dr. Farooq has been working on semantics systems, health informatics and application security projects. He has been participating in standardization of agent systems at international level through FIPA (Foundation for Intelligent Physical Agents). He contributed in agent cites project, a European funded research and development project for agent systems. Dr. Farooq initiated SAGE (Scalable fault tolerant Agent Grooming Environment) project and proposed the concept of developing decentralized Multi agent system SAGE back in 2002. He has more than 100 international publications including a book on security in sensors. He has been awarded a number of national and international awards such as PSF/COMSTECH best researcher of the year 2005 and Star Laureate awards 2004. In recognition of his research excellence, he was awarded the Best Researcher Award of the year 2011 by NUST.

Bander A Alzahrani is an assistance professor at King Abdulaziz University, Saudi Arabia. He completed his M.Sc. in Computer Security (2010), and his Ph.D. in Computer Science (2015), both from Essex University, United Kingdom. His research interests include Network security, Information centric networks, Bloom filter data structure and its applications, secure content routing, Big data privacy (IoT). Bander has published more than 17 research papers in International Journals and conferences.

Shehzad Ashraf Chaudhry received distinction in his Masters and PhD from International Islamic University Islamabad, Pakistan in 2009 and 2016 respectively. He was awarded Gold Medal for achieving 4.0/4.0 CGPA in his Masters. Currently, he is working as an Assistant Professor at the Department of Computer Science & Software Engineering, International Islamic University, Islamabad. He authored more than 40 scientific publications appeared in different international journals and proceedings including 29 in SCI/E journals. His research interests include Lightweight Cryptography, Elliptic/Hyper Elliptic Curve Cryptography, Multimedia Security, E- Payment systems, MANETs, SIP authentication, Smart Grid Security, IP Multimedia sub-system and Next Generation Networks.

Ruhul Kumar has received his PhD from Ch. Charan Singh University Meerut Uttar Pradesh India in 2016. Currently, he is an assistant professor with Department of Mathematics, SSV Degree college, Hapur, India. He has published 10 papers in reputed journals and conferences. His research interest are Robotics and Cryptography.