Secure Dynamic ID-based user authentication scheme using symmetric encryption and smart cards*[1]

[Esquema seguro de autenticación de usuario basado en identificador dinámico utilizando cifrado simétrico y tarjetas inteligentes]

[Esquema de autenticação segura do usuário com base no identificador dinâmico usando criptografia simétrica e cartões inteligentes]

Rafael MARTÍNEZ PELÁEZ[2], Yésica Imelda SAAVEDRA BENÍTEZ[3], Pablo VELARDE ALVARADO[4], Joel RUIZ IBARRA[5], Homero TORAL CRUZ[6], Enrique AGUILAR VARGAS[7]

Recibo: 20.02.2016 – Aprobación: 12.10.2016

* **Modelo para la citación de este artículo:**
MARTÍNEZ PELÁEZ, Rafael; SAAVEDRA BENÍTEZ, Yésica Imelda; VELARDE ALVARADO, Pablo; RUIZ IBARRA, Joel; TORAL CRUZ, Homero & AGUILAR VARGAS, Enrique (2016). Secure Dynamic ID-based user authentication scheme using symmetric encryption and smart cards. En: Ventana Informática No. 35 (jul-dic). Manizales (Colombia): Facultad de Ciencias e Ingeniería, Universidad de Manizales. p. 31-46. ISSN: 0123-9678

1 Artículo de investigación proveniente del proyecto *Protocolo de Autenticación Dinámico, Robusto y Eficiente para Redes de Sensores Inalámbricas*, ejecutado en 2014, e inscrito en la *Facultad de Tecnologías de Información* de la *Universidad de la Salle Bajío*.

2 PhD. en Ingeniería Telemática, Ingeniero en Sistemas Computacionales. Profesor investigador, Facultad de Tecnologías de Información, Universidad de la Salle Bajío (León, Guanajuato, México). Correo electrónico: rmartinezp@delasalle.edu.mx.

3 PhD. en Informática, BSc. en Ingeniera Computacional Profesora, Instituto Tecnológico de Toluca (Metepec, México, México). Correo electrónico: ysaavedrab@toluca.tecnm.mx. ORCID ID: http://orcid.org/0000-0002-1125-5047

4 Doctor. Profesor, Universidad Autónoma de Nayarit (Tepic, Nayarit, México). Correo electrónico: pvelarde@uan.edu.mx. ORCID ID: http://orcid.org/0000-0002-1211-1061

5 PhD. en Ingeniería Eléctrica, Electrónica y de Comunicaciones por el Centro de Investigación Científica y de Educación Superior de Ensenada, MSc. en Ingeniería Eléctrica, Electrónica y de Comunicaciones. Bach. en Ingeniería Eléctrica, Electrónica y de Comunicaciones. Profesor, Universidad Estatal de Sonora (Hermosillo, Sonora, México). Correo electrónico: joel.ruiz@ues.mx.

6 PhD. en Ingeniería Eléctrica énfasis en Telecomunicaciones, MSC. en Ingeniería Eléctrica énfasis en Telecomunicaciones, BSc. en Ingeniería Electrónica. Profesor, Universidad de Quintana Roo (Chetumal, Quintana Roo, México). Correo electrónico: htoral@uqroo.edu.mx. ORCID ID: http://orcid.org/0000-0002-2068-8389

7 MSc. en Tecnologías de Información Empresarial, Esp. en Teleinformática y Redes, Lic. en Informática. Director, Facultad de Tecnologías de Información, Universidad de La Salle Bajío (León, Guanajuato, México). Correo electrónico: eaguilar@delasalle.edu.mx.

Resumen: *En 2004, Das, Saxena & Gulati propusieron un nuevo esquema de autenticación basado en un identificador dinámico cuyo principal propósito fue evitar el ataque de robo de identidad. Desde ese momento, se han propuesto varios esquemas con la intención de mejorar la seguridad de esquemas previos. Sood et al., propusieron un nuevo esquema y claman que es más seguro que el esquema propuesto por Liou, Lin & Wang. Sin embargo, un estudio de criptoanálisis ha demostrado que su esquema continúa siendo vulnerable a los siguientes ataques: encontrar la clave secreta, suplantación de identidad, y robo de información de la base de datos, haciendo al esquema inseguro para su uso en servicios electrónicos. En este artículo se propone un nuevo esquema que resuelve las fallas de seguridad encontradas en el esquema de Sood y cumple con todas las características de seguridad que un esquema de autenticación de usuario remoto de ofrecer.*

Palabras clave: *Criptoanálisis, autenticación mutua, seguridad en redes, tarjetas inteligentes.*

Abstract: *In 2004, Das, Saxena & Gulati introduced a new scheme called dynamic ID-based with the purpose of avoiding identity theft attack. Since then, many schemes have been proposed with the intention to improve security in different ways. Then, Sood et al. proposed a new scheme and claimed that it is more secure than Liou, Lin & Wang's scheme. However, cryptanalysis study demonstrates that it is still vulnerable to guessing secret key attack, impersonation attack and steal information from a database attack, making it unsecure for electronic services. This paper proposes a new scheme that resolves the security flaws found in Sood et al.'s scheme and achieves all the security goals which a secure remote user authentication scheme should provide.*

Keywords*: cryptanalysis, mutual authentication, network security, smart cards.*

Resumo: *Em 2004, Das, Saxena & Gulati propôs um novo esquema de autenticação baseado em um identificador dinâmico cujo objetivo principal era evitar ataque roubo de identidade. Desde então, vários esquemas foram propostos com a intenção de melhorar a segurança dos regimes anteriores. Sood et al., propôs um novo regime e afirmam que é mais seguro do que o esquema proposto por Liou, Lin & Wang No entanto, um estudo da criptoanálise mostrou que o esquema continua vulnerável aos seguintes ataques : encontrar a chave secreta, phishing, e roubo de informações do banco de dados, tornando o sistema inseguro para uso em serviços electrónicos. Este artigo descreve um novo esquema que resolve as falhas de segurança encontradas no*

esquema proposto Sood e cumpre todos os recursos de segurança que um esquema de autenticação para oferecer usuário remoto.

Palavras-chave: *criptoanálise, autenticação mútua, segurança de rede, cartões inteligentes.*

Introduction

The number of login request message through the Internet is growing day by day. One of the problems of this situation is that eavesdroppers can record the login request message and obtain valuable information about the users' activities. Therefore, more number of login request message which contain a static login ID, can be used to know the users' behaviour. Under this scenario, it is convenient used a dynamic login ID[8] of Das, Saxena & Gulati (2004, 629).

Since then, many dynamic ID-based remote user authentication schemes have been designed and proposed (Chen, Hsiang & Shih, 2011; Chung*, et al.*, 2009; Khan, Kim & Alghathbar, 2011; Lee*, et al.*, 2008; Liao, Lee & Hwang, 2005; Martinez-Peláez*, et al.* 2011; Martinez-Peláez*, et al.*, 2013; Wang*, et al.*, 2009; Wen & Li, 2012; Yeh*, et al.*, 2010; Yoon & Yoo, 2006), throughout the years, to provide stronger security. However, cryptanalysis study of each new scheme reveals security flaws, providing new knowledge. In this way, Sood, Sarje & Singh (2010, 17) carried out cryptanalysis study of the scheme proposed by Liou, Lin & Wang (2006, 200) and they discovered security weaknesses. In order to resolve the security flaws found in Liou, Lin & Wang (2006, 200), Sood, Sarje & Singh (2010, 19) proposed a new scheme, however, cryptanalysis study of this scheme found that it is still vulnerable to the following attacks: 1) guessing secret key; 2) impersonation; and 3) steal information from a database.

In this paper, a new dynamic ID-based remote user authentication scheme is proposed. Its design takes in consideration the security goals, proposed by Li (2011) and Madhusudhan & Mittal (2012, 1237), which an ideal authentication scheme should achieve. Moreover, cryptographic operations executed by smart cards and servers are one-way hash function and symmetric encryption/decryption due to its low computational cost. Cryptanalysis study demonstrates that it is more secure than the scheme proposed by Sood, Sarje & Singh (2010, 19).

8 The concept of dynamic login ID was introduced in 2004 by Sood, Sarje and Singh and its main purpose is keeping the ID of each user anonymous, by means of, the creation of one-time login request message.

The structure of the paper is as follows. In section 1 a brief review of the scheme proposed by Sood, Sarje & Singh (2010, 19) is explained. Section 2 presents a cryptanalysis study of this scheme. In section 3 a new dynamic ID-based remote user authentication scheme is proposed. Section 4 demonstrates that the new scheme overcomes the security weaknesses found in the scheme. Finally section 5 concludes the paper.

1. Review of Sood-Sarje-Singh's scheme

This section briefly reviews the scheme proposed by Sood, Sarje & Singh (2010, 19). The notations used in this paper are summarized in Table 1. Figure 1 shows the authentication process – step by step.

Table 1. Notations

Nomenclature	Meaning	Nomenclature	Meaning
U	The user	h( )	One-way hash function
ID	The identity of U	SK_{US}	The session key between U and S
PW	The password of U	$E_{SK}\{\}$	Symmetric encryption function using SK
SC	The smart card of U	$D_{SK}\{\}$	Symmetric decryption function using SK
S	The server	Å	Exclusive-OR operation
x, z	The secret keys of S	||	String concatenation operation
N_U	Nonce generated by U	➔	Secure channel
N_S	Nonce generated by S	→	Common channel

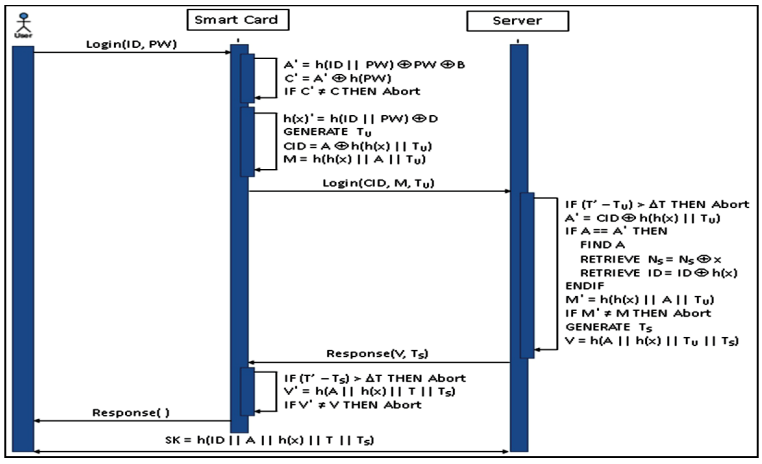

***Figure 1**. Authentication phase of Sood et al.'s scheme (Sood, Sarje & Singh, 2010, 20)*

1.1 Registration phase

In this phase, the user and the server carry out the registration process as follows:

$U \rightarrow S$: ID, PW

S: $A = h(x||N_S)$

S: $B = h(ID||PW) \oplus PW \oplus A$

S: $C = A \oplus h(PW)$

S: $D = h(ID||PW) \oplus h(x)$

S: STORE $N_S \oplus x$ and $ID \oplus h(x)$ corresponding to A INTO Database

$S \rightarrow U$: SC containing B, C, D, $h(\cdot)$

1.2 Login phase

In this phase, the user's smart card computes the login request message by means of the following process:

$U \rightarrow SC$: ID, PW

SC: $A^* = h(ID||PW) \oplus PW \oplus B$

SC: $C^* = A^* \oplus h(PW)$

SC: IF $C^* \neq C$ THEN Abort

SC: $h(x)^* = h(ID||PW) \oplus D$

SC: GENERATE T_U

SC: $CID = A \oplus h(h(x)^*||T_U)$

SC: $M = h(h(x)^*||A||T_U)$

$SC \rightarrow S$: CID, M, T_U

1.3 Authentication phase

In this phase, the server and the user verify the identity of each other as follows:

S: IF $(T' - T_U) > \Delta T$ THEN Abort
S: $A^* = CID \oplus h(h(x)||T_U)$
S: IF A == A^* THEN
FIND A
RETRIEVE $N_S = N_S \oplus x$
RETRIEVE $ID = ID \oplus h(x)$
ENDIF
S: $M^* = h(h(x)||A||T_U)$
S: IF $M^* \neq M$ THEN Abort
S: GENERATE T_S
S: $V = h(A||h(x)||T_U||T_S)$
S → SC: V, T_S
SC: IF $(T' - T_S) > \Delta T$ THEN Abort
SC: $V^* = h(A||h(x)||T||T_S)$
SC: IF $V^* \neq V$ THEN Abort
U: $SK = h(ID||A||h(x)||T||T_S)$
S: $SK = h(ID||A||h(x)||T||T_S)$

1.4 Password change phase

In this phase, the user and the server perform the update password process as follows:

U → SC: ID, PW, PW_{new}
SC: $A^* = h(ID||PW) \oplus PW \oplus B$
SC: $C^* = A^* \oplus h(PW)$
SC: IF $C' \neq C$ THEN Abort
$B_{new} = h(ID||PW_{new}) \oplus PW_{new} \oplus A$
$C_{new} = A \oplus h(PW_{new})$
$D_{new} = h(ID||PW_{new}) \oplus h(x)$
SC: UPDATE B, C and D by B_{new}, C_{new} and D_{new}

2. Weaknesses of Sood *et al.*'s Scheme

This section presents a cryptanalysis study of the scheme proposed by Sood, Sarje & Singh (2010, 19), demonstrating that it is still vulnerable to impersonation attack, guessing secret key attack and steal information from a database attack.

2.1 Guessing secret key attack

This attack is based on the studies presented in Kocher, Jaffe & Jun (1999, 2) and Messerges, Dabbish & Sloan (2002, 543). In this scenario, a malicious user can extract the secret information stored in its smart card (*B*, *C* and *D*) and computes:

$$\text{Attacker: } h(x)^{*} = h(ID||PW) \oplus D$$
$$\text{Attacker: WHILE } h(z) \neq h(x)^{*}$$
$$z = z + 1$$
$$h(z)$$

In this case, the security of the entire scheme is based on the security of the one-way hash function because an attacker can find a collision $h(z) == h(x)$. If the scheme is based on SHA-1, the attacker can find a collision within 2^61 operations (Stevens, 2013, 4). Thus, Sood *et al.*'s scheme cannot resist the guessing secret key attack.

2.2 Impersonation attack

If the eavesdropper has recorded one of the user's previous login request message (*CID*, *M*, *T*) and knows $h(x)$, the attacker can perform the impersonation attack as follows:

$$\text{Attacker: } A^{*} = CID \oplus h(h(x)||T)$$
$$\text{Attacker: } CID_{adversary} = A^{*} \oplus h(h(x)||T_{adversary})$$
$$\text{Attacker: } M_{adversary} = h(h(x)||A||T_{adversary})$$
$$\text{Attacker} \rightarrow \text{S: } CID, M, T_{adversary}$$

Upon receiving the login request message from the adversary, the server and the eavesdropper perform the authentication process. In this case, the server will accept the login request message from the attacker because the security parameters are correct. Although the session key computed by the server is unknown by the eavesdropper, the attack reveals a weakness by Sood, Sarje & Singh (2010, 19).

2.3 Steal information from a database attack

Sood, Sarje & Singh (2010, 19) the server maintains a verification table where sensitive information ($N_S \oplus x$ and $ID \oplus h(x)$) is stored. If the adversary can obtain the database and x^{*}, it can recover N_S from N_S

$\oplus$ *x* and *ID* from *ID* $\oplus$ *h*(*x*). Thus, Sood *et al.*'s scheme is vulnerable to steal information from a database attack.

3. Proposed Scheme

This section describes the process for a new dynamic ID-based remote user authentication scheme, a scheme that is based on one-way hash function and symmetric cryptography (Figure 2).

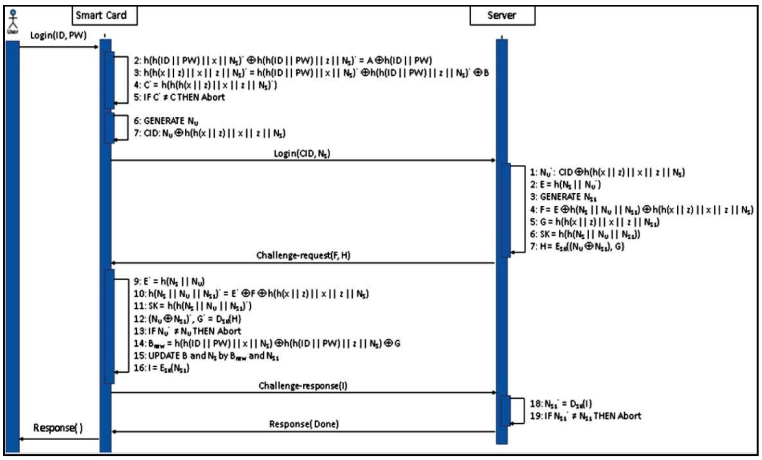

Figure 2. Authentication phase of the proposal scheme

The scheme allows the user to establish a session key and get access to the server, but at the same the user not need to reveal its *ID*. The initial assumptions are:

1) The bit length of the secret keys and nonce is 256,
2) The one-way function used is SHA-2, and
3) The one-way function is public.

3.1 Registration phase

When the user wants to be part of the system, it chooses an *ID* and *PW*, and then hashes the *ID* and *PW* to create a message digest. Next, the user sends the message digest to the server over a secure channel. Upon receiving the message digest from the user, the server computes the security parameters (step 2 to 5) using exclusive-or operation, string concatenation operation and one-way hash function. Then, the server stores the security parameters (N_S, *A*, *B*, *C*, $h(\cdot)$) into the user's smart card and delivers the smart card to the user. The process is as follows:

1. U ➔ S: $h(ID||PW)$
2. S: GENERATE N_S
3. S: $A = h(h(ID||PW)||x||N_S) \oplus h(h(ID||PW)||z||N_S) \oplus h(ID||PW)$
4. S: $B = h(h(ID||PW)||x||N_S) \oplus h(h(ID||PW)||z||N_S) \oplus h(h(x||z)\ ||x||z||N_S)$
5. S: $C = h(h(h(x||z)||x||z||N_S))$
6. S ➔ U: SC containing N_S, A, B, C, $h(\cdot)$

Note: In this case, the user keeps secret its *ID* and *PW* because it sends a message digest instead of a clear text.

3.2 Login phase

Whenever a user wants to get access to the server, it inserts the smart card into the smart card reader and keys the correct *ID* and *PW*. Then, the smart card verifies the correctness of *ID* and *PW* by means of the steps 2, 3, 4 and 5. If the verification is positive, the smart card computes the login request message. As result, the user gets a unique login request message (N_S, *CID*) which does not contains its *ID* or *PW* in clear text and it is dynamic. In the step 8, the user sends the login request message to the server over an open channel. The process is as follows:

U ➔ SC: ID, PW

SC: $h(h(ID||PW)||x||N_S)^* \oplus h(h(ID||PW)||z||N_S)^* = A \oplus h(ID||PW)$

SC: $h(h(x||z)||x||z||N_S)^* = h(h(ID||PW)||x||N_S)^* \oplus h(h(ID||PW)||z||N_S)^* \oplus B$

SC: $C^* = h(h(h(x||z)||x||z||N_S)^*)$

SC: IF $C^* \neq C$ THEN Abort

SC: GENERATE N_U

SC: CID: $N_U \oplus h(h(x||z)||x||z||N_S)$

U ➔ S: N_S, CID

Note: In this case, the login request message is based on a dynamic login *ID*; this means that, the user sends a different login request message to the server every time, keeping secret its *ID*.

3.3 Authentication phase

Upon receiving the login request message, the server retrieves sensitive information from *CID*. Then, it generates a nonce (N_{S1}) and uses it to compute new security parameters (*F*, *G*). Next, it computes the session

key using a nonce and information received from the user. Then, the server encrypts sensitive information using the session key ($E_{SK}\{N_U, N_{S1}, G\}$)). In the step 8, the server sends a challenge message (F, H) to the user over an open channel.

After the user receives the challenge message, its smart card retrieves sensitive information from F and computes the session key. Then, the smart card decrypts H to recover: 1) the nonce generated (N_U) during the login phase (step 6); 2) new security parameter (G); and 3) the nonce generated by the server (N_{S1}). In the step 13, the smart card verifies the legitimacy of the server. If the verification is positive, it updates the value of B and N_S by B_{new} and N_{S1}, and computes the challenge-response message. In the step 17, the smart card sends the challenge-response message to sever over an open channel. Finally, the server verifies the legitimacy of the user.

The process is as follows:

1. S: N_U^*: CID $\oplus$ h(h(x||z)||x||z||N_S)
2. S: E = h(N_S||N_U^*)
3. S: GENERATE N_{S1}
4. S: F = E $\oplus$ h(N_S||N_U||N_{S1}) $\oplus$ h(h(x||z)||x||z||N_S)
5. S: G = h(h(x||z)||x||z||N_{S1})
6. S: SK = h(h(N_S||N_U||N_{S1}))
7. S: H = $E_{SK}\{(N_U \oplus N_{S1}), G\}$
8. S ➔ U: F, H
9. SC: E^* = h(N_S||N_U)
10. SC: h(N_S||N_U||N_{S1})* = E^* $\oplus$ F $\oplus$ h(h(x||z)||x||z||N_S)
11. SC: SK = h(h(N_S||N_U||N_{S1})*)
12. SC: $(N_U \oplus N_{S1})^*$, G^* = $D_{SK}\{H\}$
13. SC: IF $N_U^* \neq N_U$ THEN Abort
14. SC: B_{new} = h(h(ID||PW)||x||N_S) $\oplus$ h(h(ID||PW)||z||N_S) $\oplus$ G
15. SC: UPDATE B and N_S by B_{new} and N_{S1}
16. SC: I = $E_{SK}\{N_{S1}\}$
17. U ➔ S: I
18. S: N_{S1}^* = $D_{SK}\{I\}$
19. S: IF $N_{S1}^* \neq N_{S1}$ THEN Abort
20. S ➔ U: Done

Mutual authentication is done

Note: In this case, the server does not maintain a database. Moreover, the schemes do not require time synchronization because it uses nonce.

3.4 Password Change phase

This phase is invoked whenever the user requires changing the password for a new one (PW_{new}). The process is as follows:

1. U ➔ SC: ID, PW, PW_{new}
2. SC: $h(h(ID||PW)||x||N_S)^* \oplus h(h(ID||PW)||z||N_S)^* = A \oplus h(ID||PW)$
3. SC: $h(h(x||z)||x||z||N_S)^* = h(h(ID||PW)||x||N_S)^* \oplus h(h(ID||PW)||z||N_S)^* \oplus B$
4. SC: $C^* = h(h(h(x||z)||x||z||N_S)^*)$
5. SC: IF $C^* \neq C$ THEN Abort
6. SC: $A_{new} = h(h(ID||PW)||x||N_S) \oplus h(h(ID||PW)||z||N_S) \oplus h(ID||PW_{new})$
7. SC: UPDATE A by A_{new}

4. Security Evaluation

This section describes a cryptography study of the scheme proposed in this paper, demonstrating that it overcomes the security flaws found in Sood, Sarje & Singh (2010, 19). Moreover, we explain that the proposed scheme achieves all the security goals desired in a secure remote user authentication scheme. Finally, the section presents a security comparison between the proposed scheme and Sood *et al.*'s scheme.

4.1 Security analysis

The proposed scheme can resist very well-known attacks making it more secure than Sood *et al.*'s scheme.

4.1.1 Guessing secret key attack. In this scenario, a malicious user can extract the secret information stored in its smart card (N_S, *A*, *B*, *C*) by means of Kocher, Jaffe & Jun (1999, 2) and Messerges, et al., (2002, 543) techniques and computes:

1. Attacker: $h(h(ID||PW)||x||N_S)^* \oplus h(h(ID||PW)||z||N_S)^* = A \oplus h(ID||PW)$
2. Attacker: $h(h(x||z)||x||z||N_S)^* = h(h(ID||PW)||x||N_S)^* \oplus h(h(ID||PW)||z||N_S)^* \oplus B$

Although the attacker can recover security information from *A* and *B*, it cannot recover *x* and *z* by means of any combination among *A*, *B*, *C*, and *D*. Moreover, the adversary needs to guess the value of *x* and *z* at the same time because both values are concatenated and hashed by

SHA-2. Furthermore, the hash value of *x* and *z* are concatenated and hashed with different values, making it hard to guess the correct value of *x* and *z* by a malicious user.

4.1.2 Impersonation attack. In this scenario, an eavesdropper has one of the user's previous login request message (N_S, *CID*). However, the adversary cannot extract sensitive information from *CID* which can be used to compute an imitative login request message.

4.1.3 Replay attack. In this scenario, an eavesdropper has one of the user's previous login request message (N_S, *CID*) and sends it to the server. Under this circumstance, the attack does not work because the server sends a challenge message (*F*, *H*) to the eavesdropper and waits the corresponding response. Although, the adversary knows (N_S, *CID*) and (*I*) it cannot retrieve the nonce (N_{S1}) generated by the server for this specific connection. When, the server receives the challenge-response message (*I*) and carries out the verification process (step 19), the mutual authentication will fail. In this scheme, the server generates a nonce for each new session making the scheme resistant against replay attack.

4.1.4 Steal information from a database attack. In this scheme, the server does not maintain a database, making it secure against this attack.

4.2 Achieving security goals

According to Li (2011, 157) and Madhusudhan & Mittal (2012, 1237) a secure remote user authentication scheme should achieve the following security goals: 1) without verification table; 2) users can choose their password freely; 3) without password reveal; 4) password dependent; 5) mutual authentication; 6) session key agreement; 7) forward secrecy, 8) without time-synchronization; 9) user anonymity; and 10) efficiency for wrong password login.

The following list demonstrates how the proposed scheme achieves all the security goals mentioned above:

- Without verification table: the server does not maintain a verification table; it keeps secret two keys which represents 512 bits of storage.
- Users choose their password freely: the user chooses freely its *ID* and *PW* during the registration phase and password change phase.
- Without reveal password: the user does not share its *ID* and *PW* with the server during the registration phase or password change phase. Moreover, the server does not know the user's *ID* and *PW* and it does not store any personal information into a database.

- Password dependent: the smart card verifies the legitimacy of the owner by means of the knowledge of *ID* and *PW* before it computes the login request message.
- Mutual authentication: the server and the user verify the legitimacy of each other by means of the knowledge of secret information and agreement of the session key.
- Session key agreement: the server and the user compute one-time session key using information which both entities known.
- Forward secrecy: the password of the user is not stored in clear text into the smart card or database. Although an attacker obtains the smart card of the user, it cannot recover the user's password by means of any combination of the information stored in the smart card.
- Without time-synchronization: the server and the user do not use time-synchronization in any phase.
- User anonymity: the user does not share personal information with the server in the registration phase. Moreover, the login request message does not contain personal information which can be used by an eavesdropper to trace the identity of the user during or after the communication with the server.
- Efficiency for wrong password login: the smart card verifies the validity of the user's ID and password during the login phase. If the user's *ID* and *PW* are wrong, the smart card does not compute the login request message or does not change the password.

4.3 Security comparison

Table 2 shows that the proposed scheme is more secure than Sood *et al.'s* scheme.

Table 2. Security comparison between the present proposal and Sood et al.'s scheme

Security goal	Sood et al.	New scheme
Without verification table	No	Yes
Users choose their password freely	Yes	Yes
Without password reveal	No	Yes
Password dependent	Yes	Yes
Mutual authentication	Yes	Yes
Session key agreement	Yes	Yes
Forward secrecy	No	Yes
No time-synchronization	No	Yes
User anonymity	Yes	Yes
Efficiency for wrong password login	Yes	Yes

The proposal scheme does not maintains a verification table while the scheme proposed by Sood, Sarje & Singh (2010, 19) requires a database, as a result a malicious user or adversary can obtain sensitive information. Moreover, the proposed scheme keeps the user's password secret, during the registration phase, because the user sends a message digest instead of a message with the *ID* and password in clear text. Furthermore, the scheme of Sood, Sarje & Singh (2010, 19) cannot provide forward secrecy because a malicious user or attacker can compute the future session keys, compromising the entire system. Finally, the proposed scheme.

5. Conclusion

A very important feature of the proposal scheme is that none login request message contains the user's ID or password, making it secure against identity theft attack. In addition, the security analysis demonstrates that the scheme resists guessing secret key attack, impersonation attack, steal information from a database attack, and replay attack, and it achieves one by one the security goals proposed by Li and Madhusudhan & Mittal.

Bibliographical references

CHEN, T.H.; HSIANG, H.C. & SHIH, W.K. (2011). Security Enhancement on an Improvement on Two Remote User Authentication Schemes Using Smart Cards. In: Future Generation Computer Systems, FGCS, Vol. 27, No. 4 (Apr.). Amsterdam (The Netherlands): North-Holland. p. 377-80. ISSN: 0167-739X.

CHUNG, H.R.; KU, W.C. & TSAUR, M.J. (2009). Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments. In: Computer Standards & Interfaces, Vol. 31, No. 4 (Jun.). Amsterdam (The Netherlands): Elsevier Science Publishers B. V. p. 863-68. ISSN: 0920-5489.

DAS, M.L.; SAXENA, A. & GULATI, V.P. (2004). A Dynamic Id-Based Remote User Authentication Scheme [online]. In: IEEE Transactions on Consumer Electronics, Vol. 50, No. 2 (may). Reading (Berkshire, UK): IEEE Consumer Electronics Society. p. 629-631. ISSN: 0098-3063 <doi:10.1109/TCE.2004.1309441> [consult: 12/03/2016].

KHAN, M.K.; KIM, S.K. & ALGHATHBAR, K. (2011). Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. In: Computer Communications, Vol. 34, No. 3 (Mar.). Amsterdam (The Netherlands): Elsevier Science Publishers B. V. p. 305-09. ISSN: 0140-3664.

KOCHER, P.C.; JAFFE, J. & JUN, B. (1999). Differential Power Analysis. In: 19th Annual International Cryptology Conference on Advances in Cryptology, Crypto'99 (15-19/08/1999). Santa Barbara (CA, USA): International Association for Cryptologic Research, IACR. WIENER, M. (ed.). Advances in Cryptology - CRYPTO'99. London (UK): Springer-Verlag. p. 388-397. ISBN: 3-540-66347-9.

LEE, Y.C.; CHANG, G.K.; KUO, W.C. & CHU, J.L (2008). Improvement on the Dynamic Id-Based Remote User Authentication Scheme. In: 7th International Conference on Machine Learning and Cybernetics, ICMLA'08 (12-15/05/2008), Kunming (China): Association for Machine Learning and Applications, AMLA. Proceedings of the ICMLA'08, Vol 7, New York (NY, USA): IEEE. p. 3283-3287. ISBN: 978-1-4244-2095-7.

LI, C.T. (2011). Secure Smart Card Based Password Authentication Scheme with User Anonymity [online]. In: Information Technology and Control, Vol. 40, No. 2. Kaunas (Lithuania): Kaunas University of Technology. p. 157-162. e-ISSN: 2335-884X <http://www.itc.ktu.lt/index.php/ITC/article/view/431/682> [consult: 12/05/2016].

LIAO, I.E.; LEE, C.C. & HWANG, M.S. (2005). Security enhancement for a dynamic ID-based remote user authentication scheme [online]. In: International Conference on Next Generation Web Services Practices, NWeSP'05 (22-26/08/2005), Seoul (Korea): IEEE Computer Society - Technical Committee on Business Informatics and Systems, TCBIS. Proceedings of the NWeSP'05, New York (NY, USA): IEEE. <doi:10.1109/NWESP.2005.67> [consult: 09/05/2016]

LIOU, Y.P.; LIN, J. & WANG, S.S. (2006). A New Dynamic Id-Based Remote User Authentication Scheme Using Smart Cards. In: 16th Information Security Conference, ISC 2006 (08-09/06/2006), Taichung (Taiwan): Feng Chia University. Proceedings of 16th Information Security Conference, p. 198-205.

MADHUSUDHAN, R. & MITTAL, R.C. (2012). Dynamic ID-Based remote user password authentication schemes using smart cards: A review [online]. In: Journal of Network and Computer Applications, Vol. 35, No. 4 (Jul.). p. 1235-1248. ISSN: 1084-8045. <doi:10.1016/j.jnca.2012.01.007>, <http://www.sciencedirect.com/science/article/pii/S1084804512000215> [consult: 19/03/2016].

MARTÍNEZ PELÁEZ, R.; RICO NOVELLA, F.; SATIZÁBAL, C. & POMYKALA, J. (2011). Efficient remote user authentication scheme using smart cards [online]. In: International Journal of Internet Technology and Secured Transactions, Vol. 3, No. 4. Olney (UK): Inderscience Publishers. p. 407-418. ISSN: 1748-569X. <http://www.inderscienceonline.com/doi/pdf/10.1504/IJITST.2011.043137>, <DOI: 10.1504/IJITST.2011.043137> [consult: 09/05/2016].

MARTINEZ PELÁEZ, R.; RICO NOVELLA, F. & VELARDE ALVARADO, P. (2013). Cryptanalysis and improvement of Chen-Hsiang-Shih's remote user authentication scheme using smart cards [online]. In: Revista Facultad de Ingeniería, No. 68 (sep). Medellín (Colombia): Universidad de Antioquia. p. 27-35. e-ISSN: 2422-2844 <http://aprendeenlinea.udea.edu.co/revistas/index.php/ingenieria/article/view/17038/14755> [consult: 10/04/2016].

MESSERGES, T.S.; DABBISH, E.A. & SLOAN, R.H. (2002). Examining Smart-Card Security under the Threat of Power Analysis Attacks [online]. In: IEEE Transactions on Computers, Vol. 51, No. 5 (may). Washington, DC (USA): IEEE Computer Society. p. 541-552. ISSN: 0018-9340. <DOI: 10.1109/TC.2002.1004593> [consult: 10/05/2016].

SOOD, S.K.; SARJE, A.K. & SINGH, K. (2010). An improvement of Liou et al.'s authentication scheme using smart cards [online]. In: International Journal of Computer Applications, Vol. 1, No. 8 (feb). New York (NY, USA): Foundation of Computer Science. p. 16-23. ISSN: 0975-8887 <DOI: 10.5120/188-325>, <http://www.ijcaonline.org/journal/number8/pxc387325.pdf> [consult: 23/04/2016].

STEVENS, M. (2013). New Collision Attacks on Sha-1 Based on Optimal Joint Local-Collision Analysis [online]. In 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2013 (26-30/05/2013), Athens (Greece): International Association for Cryptology Research. JOHANSSON, T. & NGUYEN, P. (eds.). Advances in Cryptology – EUROCRYPT 2013. Berlin (Germany): Springer-Verlag Berlin Heidelberg. p. 245-261. e-Book ISBN: 978-3-642-38348-9 <http://link.springer.com/chapter/10.1007%2F978-3-642-38348-9_15#page-1>, <DOI: 10.1007/978-3-642-38348-9_15> [consult: 12/05/2016].

WANG, Y Y.; LIU, J.Y.; XIAO, F.X. & DAN, J. (2009). A more efficient and secure dynamic ID-based remote user authentication scheme [online]. In: Computer Communications, Vol. 32, No. 2 (mar). Amsterdam (The Netherlands): Elsevier Science Publishers B. V. p. 583-585. ISSN: 0140-3664 <DOI: 10.1016/j.comcom.2008.11.008>, <http://www.sciencedirect.com/science/article/pii/S0140366408005756> [consult: 11/05/2016].

WEN, F. & LI, X. An improved dynamic ID-based remote user authentication with key agreement scheme. In: Computers & Electrical Engineering, Vol. 38, No. 2 (mar). Amsterdam (The Netherlands): Elsevier Science Publishers B. V. p. 381-87. ISSN: 0045-7906 <http://www.sciencedirect.com/science/article/pii/S0045790611001868>, <doi:10.1016/j.compeleceng.2011.11.010> [consult: 10/05/2016].

YEH, K.H.; SU, C.; LO, N.W.; LI, Y. & HUNG, Y.X. (2010). Two robust remote user authentication protocols using smart cards [online]. In: Journal of Systems and Software, Vol. 83, No. 12 (dec). Amsterdam (The Netherlands): Elsevier Science Publishers B. V. p.2556-2565. ISSN: 0164-1212<http://www.sciencedirect.com/science/article/pii/S0164121210002128>, <doi:10.1016/j.jss.2010.07.062> [consult: 12/05/2016].

YOON, E.J. & YOO, K.Y. (2006). Improving the dynamic ID-based remote mutual authentication scheme [online]. In: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops (29/10-03/11/2006). Montpellier (France): On The Move, OTM. Meersman, R.; TARI, Z. & Herrero, P. (eds.): Lecture Notes in Computer Science - OTM 2006 Workshops. Berlin (Germany): Springer-Verlag Berlin Heidelberg. p. 499-507. e-ISBN: 978-3-540-48276-5 <http://link.springer.com/chapter/10.1007%2F11915034_73> [consult: 09/05/2016].