International Journal of Computer Applications (0975 - 8887)
Volume 75 - No. 13, August 2013

An Improvement of Wang. et. al.'s Remote User Authentication Scheme Against Smart Card Security Breach

Ruhul Amin
Haldia Institute of Technology
Haldia, West Bengal-721657, India

Tanmoy Maitra
Haldia Institute of Technology
Haldia, West Bengal-721657, India

Soumya Prakash Rana
Jadavpur university
Jadavpur, West Bengal-721657, India

ABSTRACT

User authentication is one of the fundamental procedures to provide secure communications between user and server over an insecure public channel. Recently, Wang et. al. proposed password-based user authentication scheme based on hash function and modular exponentiation and they claimed that their scheme provides strong authentication than related scheme. But in this paper, it is pointed out that their scheme suffers from off-line password guessing attack, off-line identity guessing attack, user impersonation attack, server masquerading attack, smart card stolen attack and password change attack. Then an improved scheme over Wang et. al.'s scheme has been proposed to overcome their weaknesses. The proposed scheme resists all possible attacks and provides more security than wang et. al's scheme, published earlier.

Keywords:

Attack, Authentication, Password, Smart Card

1. INTRODUCTION

A user authentication scheme provides a legitimate user to log onto a remote server over an insecure channel. There are so many applications of user authentication protocol such as e-commeres, wireless sensor networks etc. In the ordinary authentication system server maintains a password verification table to verify the authenticated users. But the password verification table takes huge maintenance cost and also has a risk of tempering for the server end. First Lamport proposed a password-based authentication scheme based on one way hash function [1] to withstand the above mention problem. But his scheme suffers from different possible attacks [2]. After that so many remote user authentication schemes [3, 4, 5, 6] based on one way hash function has been proposed. But those schemes can not fulfill the properties of good user authentication scheme such that time synchronization problem, strong mutual authentication, freely changing of password etc. In 2005, Fan et. al. [7] and in 2007, Khan-Zhang [8] proposed user authentication scheme to provide strong authentication. But in 2009, Hyun et. al. [9] pointed out that both schemes [7],[8] suffer from impersonation attack and dictionary attack and also proposed an extension to authentication scheme without using smart cards. In 2011, Li and Lee proposed an enhanced remote authentication scheme [10]. Wang et. al. [11] shows that [10] scheme cannot withstand denial of service attack and is still vulnerable to off-line password guessing attack.

Recently, Wang et. al. proposed a secure password-based remote user authentication scheme [11] against smart card security breach. But in this paper it is pointed out that Wang et. al.'s scheme [11] suffers from different possible attacks such as off-line password guessing attack, off-line identity guessing attack, user impersonation attack, server masquerading attack, smart card stolen attack and password change attack.

The remainder of this paper is organized as follows: Section 2 briefly introduces some preliminary mathematical concepts for introducing the proposed scheme. Section 3 briefly reviews the Wang et. al.'s scheme [11]. Section 4 shows the brief description of attacks on Wang et. al.'s scheme [11]. Section 5 describes the proposed scheme which withstand the weaknesses of Wang et. al.'s scheme [11]. Section 6 describes cryptanalysis of the proposed improved scheme. Section 7 shows the security comparison between proposed scheme and Wang et. al.'s scheme [11]. Conclusion of this paper appears in section 8. Finally References are given in section 9.

2. PRELIMINARIES

In this section, a briefly review the basic concepts on hash function and a related mathematical problem are introduced.

2.1 Cryptographic Hash Function

A hash function is a deterministic function which takes a string of arbitrary length and produces a string of fixed length called the hashed value. Cryptographic hash functions are used universally in cryptography such as digital signatures, public-key cryptosystems, the random sequence generators used in key agreement, authentication protocols etc. Collisions in hash function is possible. Consider two messages m_0 and m_1 which are two arbitrary elements $\in$ hash function $H(\cdot)$, $\exists\ m, m'$ such that $H(m) = H(m')$, where $m \neq m'$. Cryptographic hash function satisfies the following additional properties:

(1) *Mixing-Transformation:* On any input m, the output hashed value $H(m)$ is computationally indistinguishable from a uniform binary string in the interval $[0, 2^{|H|}]$, where $|H|$ denotes the output length of H.

(2) *Preimage Resistant:* On any input m, given y from the range $H(\cdot)$, it is hard to find m such that $H(m) = y$.

(3) *Second-Preimage Resistant:* Given m from the domain of $H(\cdot)$, it is hard to find $m' \neq m$ such that $H(m) = H(m')$.

(4) *Collision Resistant:* It is hard to find a pair of distinct messages m, m' such that $H(m) = H(m')$.

2.2 Diffie-Hellman Problem

The Diffie-Hellman problem [12] is stated as follows: given an element g and the values of g^x and g^y, find the value of g^{xy} is impossible without knowing the values of x and y, where g is a generator of some group (multiplicative group of a finite field or an elliptic curve group) and $x, y \in_R Z^*$.

3. BRIEF REVIEW OF WANG ET. AL.'S SCHEME

This section presents briefly description of Wang et. al.'s secure password-based remote user authentication scheme against smart card security breach [11]. The notation used throughout this paper are summarized in Table 1.

Table 1. notation used

RS	$\longrightarrow$	remote server
U_i	$\longrightarrow$	$i-th$ remote user
ID_i	$\longrightarrow$	identity of U_i
PW_i	$\longrightarrow$	password chosen by U_i
ID_i^a	$\longrightarrow$	identity guessed by an adversary
PW_i^a	$\longrightarrow$	password guessed by an adversary
PW_i^{new}	$\longrightarrow$	new password chosen by U_i
x	$\longrightarrow$	secret key of RS
y	$\longrightarrow$	public key of RS
b	$\longrightarrow$	random number chosen by user U_i
$H(\cdot)$	$\longrightarrow$	cryptographic one way hash function
g	$\longrightarrow$	primitive element over $GF(p)$
n	$\longrightarrow$	a large prime number
Z_n	$\longrightarrow$	set of integer numbers over modulo n
SK	$\longrightarrow$	shared secret key between user and server
$\oplus$	$\longrightarrow$	bitwise xor operation
$\|$	$\longrightarrow$	concatenate operation

Wang et. al.'s scheme [11] consists of four phases: registration phase, login phase, verification phase and password change phase.

3.1 Registration Phase

In this phase, user U_i submits ID_i and $PWR_i = H(PW_i \| b)$ to the remote server for registration, where b is a random number chosen by user U_i. After receiving registration message ID_i and PWR_i, remote server computes $N_i = PWR_i \oplus H(x \| ID_i)$ and $A_i = H(ID_i \| PWR_i)$. Then RS issues smart card for user U_i by storing the parameters $\langle N_i, A_i, n, g, y, H(\cdot)\rangle$ into memory of smart card, where $y = g^x \bmod n$ is the public key of remote server RS. After getting smart card user U_i stores b into the smart card.

3.2 Login Phase

This phase will be invoked whenever an existing user wants to get the service from the remote server. In this phase, user U_i first inserts his/her smart card into the card reader and submits ID_i and PW_i to the terminal. Then smart card computes $PWR_i^* = H(PW_i \| b)$, $A_i^* = H(ID_i \| PWR_i^*)$ and checks whether computed A_i^* equals to the stored A_i. If it holds good then smart card further computes $C_1 = g^u \bmod n$, $Y_1 = y^u \bmod n$, $H(x \| ID_i) = N_i \oplus PWR_i^*$, $CID_i = ID_i \oplus H(C_1 \| Y_1)$ and $M_i = H(CID_i \| C_1 \| H(x \| ID_i))$. Then terminal sends login message $\langle C_1, CID_i, M_i\rangle$ to the remote server RS over public channel.

3.3 Verification Phase

After receiving login request message $\langle C_1, CID_i, M_i\rangle$, remote server performs the following operations to verify user U_i. First, remote server computes $Y_2 = {C_1}^x \bmod n$, $ID_i = CID_i \oplus H(C_1 \| Y_2)$ and $M_i^* = H(CID_i \| C_1 \| H(x \| ID_i))$. Then checks computed M_i^* equals with the received M_i or not. If it equals then remote server RS generates a random number v and computes the session key $SK = {C_1}^v \bmod n$, $C_2 = g^v \bmod n$ and $C_3 = H(SK \| C_2 \| H(x \| ID_i))$. Then sends $\langle C_2, C_3\rangle$ to the user U_i. After receiving the reply message from the remote server RS, user U_i computes $SK = {C_2}^u \bmod n$, $C_3^* = H(SK \| C_2 \| H(x \| ID_i))$ and checks computed C_3^* equals with the received C_3 or not. If equality holds U_i computes $C_4 = H(C_3 \| H(x \| ID_i) \| SK)$ and sends it to the remote server. After getting C_4, RS derives $C_4^* = H(C_3 \| H(x \| ID_i) \| SK)$ and checks C_4^* equals to sending C_4 or not. If it holds good then both user and remote server agree upon a common shared secret key SK for future communication.

3.4 Password Change phase

If user U_i wants to change his/her password, user submits correct ID_i, PW_i and new password PW_i^{new} to the smart card. Then smart card computes $PWR_i^* = H(PW_i \| b)$, $A_i^* = H(ID_i \| PWR_i^*)$ and checks whether computed A_i^* equals to the stored A_i. If it holds good then smart card stores N_i^{new} and A_i^{new} instead of N_i and A_i by computing $N_i^{new} = N_i \oplus PWR_i^* \oplus H(PW_i^{new} \| b)$, $A_i^{new} = H(ID_i \| H(b \| PW_i^{new}))$ into the memory of smart card. Thus user U_i can change his/her desired password without help of remote server RS.

4. CRYPTANALYSIS OF WANG ET. AL.'S SCHEME

In this section, the cryptanalysis of Wang et. al.'s scheme [11] is presented. To analyze the security weaknesses of [11] scheme, the assumptions are given in the following:

Assumption 1. It can be assumed that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [13][14].

Assumption 2. Due to the low entropy of ID_i and PW_i, it can be assumed that an adversary is able to off-line guess U_i's identity ID_i and password PW_i individually. However, he/she cannot off-line guess ID_i and PW_i simultaneously in polynomial time as pointed out by Sood et. al. [15].

4.1 Off-line Password Guessing Attack

After extracting smart card parameter N_i and after intercepting login message $\langle C_1, CID_i, M_i\rangle$, the attacker can easily find out PW_i using following steps:

Step 1: Attacker knows $M_i = H(CID_i \| C_1 \| H(x \| ID_i))$. Then replace $H(x \| ID_i)$ with $N_i \oplus H(b \| PW_i)$, where N_i is the stored smart card parameter. So, $M_i = H(CID_i \| C_1 \| N_i \oplus H(b \| PW_i))$. Now from M_i, attacker knows all parameters except user password PW_i.

Step 2: Attacker chooses a password PW_i^a and computes $M_i^a = H(CID_i \| C_1 \| N_i \oplus H(b \| PW_i^a))$. Then checks the correctness whether M_i^a is equal with M_i or not.

Step 3: An attacker repeats the above process until the correct password is obtained. After some guessing, an attacker can find out the correct password. Thus an attacker can successfully launch off-line password guessing attack.

4.2 Off-line Identity Guessing Attack

Under assumption 2, an attacker can successfully launch off-line identity guessing attack after successfully perform off-line password guessing attack. The procedure for performing off-line identity guessing attack as follows:

Step 1: Attacker can extract A_i from memory of smart card by monitoring power consumption. Then attacker chooses an identity ID_i^a and computes $A_i^a = H(ID_i^a \parallel H(PW_i \parallel b))$, where PW_i, b are known parameter to the attacker. Then attacker checks the correctness whether computed A_i^a is equal with stored A_i or not.

Step 2: An attacker repeats the above process until the correct identity is obtained. After some guessing, an attacker can find out the correct identity. Thus an attacker can successfully launch off-line identity guessing attack.

4.3 User Impersonation Attack

After successfully perform off-line password guessing attack and under assumption 1, an attacker can perform user impersonation attack as follows:

Step 1: Attacker computes $H(x \parallel ID_i) = Ni \oplus H(b \parallel PW_i)$ using user's correct password PW_i. Then attacker chooses a random number r and computes $C_1^* = g^r \bmod n$, $Y_1^* = y^r \bmod n$, $CID_i^* = ID_i \oplus H(C_1^* \parallel Y_1^*)$ and $M_i^* = H(CID_i^* \parallel C_1^* \parallel H(x \parallel ID_i))$. Then attacker sends forged message $\langle CID_i^*, {C_1}^*, M_i^*, \rangle$ to the remote server.

Step 2: After receiving the forged message, remote server computes $Y_2^* = C_1^x \bmod n$, $ID_i = CID_i^* \oplus H(C_1^* \parallel Y_2^*)$, $G_1 = H(x \parallel ID_i)$ and $M_i^s = H(CID_i^* \parallel C_1^* \parallel G_1)$ then checks whether computed M_i^s with received M_i^* It can be shown that the above condition are equal. Then authenticated server will be convinced the message sent from the legal user.

Thus, an attacker can perform user impersonation attack.

4.4 Server Masquerading Attack

After successfully perform off-line password guessing attack and under assumption 1, an attacker can perform server masquerading attack as follows:

Step 1: Attacker computes $H(x \parallel ID_i) = Ni \oplus H(b \parallel PW_i)$ using user's correct password PW_i. Then attacker generates a random number v^* and computes $SK_a = {C_1}^{v^*} \bmod n$, $C_{2a} = g^{v^*} \bmod n$ and $C_{3a} = H(SK_a \parallel C_{2a} \parallel H(x \parallel ID_i))$. Then attacker sends C_{2a}, C_{3a} to the user U_i.

Step 2: After receiving C_{2a}, C_{3a}, smart card computes $SK = C_{2a}^u \bmod n$ and $C_{3a}^* = H(SK \parallel C_{2a} \parallel H(x \parallel ID_i))$ and checks whether computed C_{3a}^* is equals with received C_{3a}. It can be easily shown that the above condition is holds good. Then smart card user's will be convinced the message sent from the legal server.

Thus an attacker can perform server masquerading attack on wang et. al.'s scheme [11].

4.5 Smart Card Stolen Attack

Suppose a user U_i either lost or stolen by an attacker of his/her smart card. After getting the smart card, the attacker can extract the secret information $\langle N_i, A_i, n, g, y, H(\cdot)\rangle$ from the user's smart card. It also can be assumed that attacker stores the $i-th$ login message of the user U_i. As a result attacker can store the values, $\langle C_1, CID_i, M_i\rangle$. By using these secret information and stored parameters, attacker can create valid login message, described in user impersonation attack procedure in subsection 4.3. So their scheme is insecure against smart card stolen attack.

4.6 Password Change Attack

After intercepting login message $\langle C_1, CID_i, M_i\rangle$ from login messages, the attacker can easily find out user's correct password PW_i by performing the password guessing technique as describe in subsection 4.1. After getting correct PW_i, the attacker can change the valid user's password from the password change phase. So card reader will always reject the valid user in login phase.

5. PROPOSED SCHEME

In this section, we will present the improvement of wang et. al.'s scheme [11] to overcome their weaknesses. The proposed scheme consists of four phases namely registration phase, login phase, authentication phase and password change phase. Fig. 1 shows the layout of the proposed scheme. The all phases of the proposed scheme are as follows:

5.1 Registration Phase

In this phase, user U_i submits ID_i and $PWR_i = H(PW_i \parallel b)$ to the remote server for registration where b is a random number chosen by user U_i. After receiving ID_i and PWR_i, remote server computes $N_i = PWR_i \oplus H(x \parallel ID_i)$ and $A_i = H(ID_i \parallel PWR_i)$. Then RS issues smart card for user U_i by storing the parameters $\langle N_i, A_i, n, g, y, H(\cdot)\rangle$ into memory of smart card, where $y = g^x \bmod n$ is the public key of remote server RS. After getting smart card user U_i stores b into the smart card.

5.2 Login Phase

This phase will be invoked whenever an existing user wants to get the service from the remote server. In this phase, user U_i first inserts his/her smart card into the card reader and submits ID_i and PW_i to the terminal. Then smart card computes $PWR_i^* = H(PW_i \parallel b)$, $A_i^* = H(ID_i \parallel PWR_i^*)$ and checks whether computed A_i^* equals to the stored A_i. If it holds good then smart card further computes $C_1 = g^u \bmod n$, $Y_1 = y^u \bmod n$, $H(x \parallel ID_i) = N_i \oplus PWR_i^*$, $CID_i = ID_i \oplus H(C_1 \parallel Y_1)$ and $M_i = H(CID_i \parallel C_1 \parallel H(x \parallel ID_i) \parallel ID_i)$. Then terminal sends login message $\langle C_1, CID_i, M_i\rangle$ to the remote server RS over public channel.

5.3 Verification Phase

After receiving login request message $\langle C_1, CID_i, M_i\rangle$, remote server performs the following operations to verify user U_i. First, remote server computes $Y_2 = {C_1}^x \bmod n$, derives $ID_i = CID_i \oplus H(C_1 \parallel Y_2)$ and $M_i^* = H(CID_i \parallel C_1 \parallel H(x \parallel ID_i) \parallel ID_i)$. Then checks computed M_i^* equals with the received M_i or not. If it equals then remote server RS generates a random number v and computes the session key $SK = {C_1}^v \bmod n$, $C_2 = g^v \bmod n$ and $C_3 = H(SK \parallel C_2 \parallel H(x \parallel ID_i))$. Then sends $\langle C_2, C_3\rangle$ to the user U_i. After receiving the reply message from the remote server RS, user U_i computes $SK = {C_2}^u \bmod n$, $C_3^* = H(SK \parallel C_2 \parallel H(x \parallel ID_i))$ and checks computed C_3^* equals with the received C_3 or not. If equality holds U_i computes $C_4 = H(C_3 \parallel H(x \parallel ID_i) \parallel SK)$ and sends it to the remote server. After getting C_4, RS derives $C_4^* = H(C_3 \parallel H(x \parallel ID_i) \parallel SK)$ and checks C_4^* equals to sending C_4 or not. If it holds good then both user and remote server agree upon a common shared secret key SK for future communication.

6. SECURITY ANALYSIS OF PROPOSED SCHEME

In this section, we will analyze the security of the proposed scheme under the following assumption.

Assumption 1. It can be assumed that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [13][14] and intercept messages communicating between the user and the server.

Assumption 2. Due to the low entropy of ID_i and PW_i, it can assumed that an adversary is able to off-line guess U_i's identity

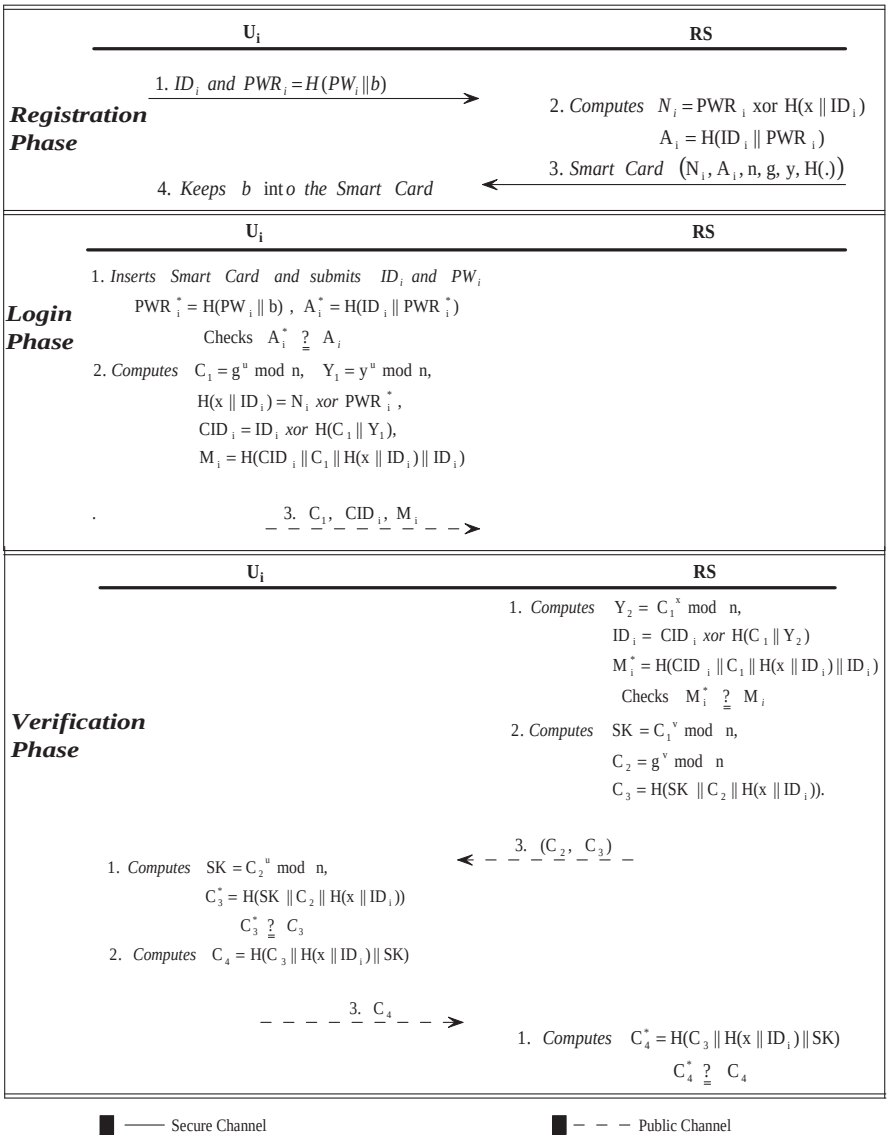

Fig. 1. Layout of proposed scheme

ID_i and password PW_i individually. However, he/she cannot off-line guess ID_i and PW_i simultaneously in polynomial time as pointed out by Sood et. al. [15].

6.1 Off-line Password Guessing Attack

Attacker can derived or guessed valid user's password using either (i) stored parameters in the memory of smart card (ii) all communicating messages between the user and server or from both. After getting smart card parameters and communicating message, attacker can not perform off-line password guessing attack described as follows:

(1) It can be assumed that an attacker has got secret values $\langle N_i, A_i, n, g, y, b, H(\cdot)\rangle$ from the memory of smart card. Then attacker attempts to guess user's correct password using N_i, A_i. But under assumption 2, attacker can not guess ID_i and PW_i simultaneously in polynomial time. So off-line password guessing attack is not possible using N_i and A_i.

(2) It can be assumed that an attacker has got $\langle C_1, CID_i, M_i\rangle$ and $\langle C_2, C_3\rangle$ from communicating messages between user and server. To guess correct password of a valid user U_i, the attacker have to guess ID_i and PW_i simultaneously which is not possible described by Sood et. al. [15].

It can be easily shown that if attacker extract all parameters from the memory of smart card and from all communicating messages, then also he/she can not guess valid user's password. As a result, the proposed scheme provides strong security on off-line password guessing attack.

6.2 Off-line Identity Guessing Attack

After getting secret values $\langle N_i, A_i, n, g, y, b, H(\cdot)\rangle$ stored in the user's smart card and after intercepting login message, the attacker attempts to guess user identity ID_i using N_i, A_i in the registration phase. To guess user's identity attacker has to guess at least user's identity, and user's password PW_i simultaneously but it is not possible in polynomial time. So the proposed scheme is secure against Off-line identity guessing attack.

6.3 User Impersonation Attack

To impersonate as a legitimate user, an attacker attempts to make a forged login request message which can be authenticated

to a server. However, the attacker can not impersonate as the legitimate user by forging the login request message even if the attacker can extract the stored secret values $\langle N_i, A_i, n, g, y, b, H(\cdot)\rangle$ from the user's smart card, because the attacker can not compute the valid login request message $\langle C_1, CID_i, M_i\rangle$ without knowing the secret password PW_i and ID_i of valid user U_i, and server secret key x. If the attacker wants to get the secret parameters ID_i, PW_i, x, he/she must have to solve the inversion of cryptographic hash function which is computationally hard. So the proposed scheme is secure against user impersonation attack.

6.4 Server Masquerading Attack

To masquerade as a legitimate server, an attacker attempts to make the forged reply message which can be masqueraded to the user when receiving the user's login request message. However, the attacker can not masquerade as the server by forging the reply message because it is hard to compute $\langle C_2, C_3\rangle$ by an attacker without knowing the secret values user's password PW_i, random number v and server secret key x. Hence the attacker can not masquerade as the legitimate server to the user by launching the server masquerading attack.

6.5 Smart card stolen attack

It can be assumed that the user U_i has either lost his/her smart card or stolen by an attacker. After getting the smart card, an attacker can extract the secret information $\langle N_i, A_i, n, g, y, b, H(\cdot)\rangle$ from the memory of smart card. It also can be assumed that attacker stores the $i-th$ login message $\langle C_1, CID_i, M_i\rangle$ of the user U_i. After getting all these parameters from login message and from memory of smart card, it is hard to derive or guess user's identity ID_i, password PW_i and server secret key s by the attacker. So attacker can not create the valid login message. As a result proposed scheme is secure against smart card stolen attack.

6.6 Privileged Insider Attack

The proposed scheme is secure against privileged insider attack because in proposed scheme, user U_i provides PWR_i which equals to $H(PW_i, y)$ instead of PW_i. As a result, system manager or privileged insider of the server can not derive valid user's password. So the proposed scheme provides security against privileged insider attack.

6.7 Password Change Attack

As described in this section, the proposed scheme can withstand the Password guessing attack and smart card stolen attack. To perform password change attack, an attacker have to provide correct ID_i and PW_i to the card reader. But in proposed scheme, there is no way to get or guess correct user's password PW_i to the attacker. So proposed scheme is secure against password change attack.

7. PERFORMANCE COMPARISON

In this section, we will compare the performance of the improved proposed scheme with wang et. al.'s scheme [11]. We have shown that [11] scheme is not applicable for the practical implementation in terms of security because [11] scheme is insecure against off-line password guessing attack, off-line identity guessing attack, user impersonation attack, server masquerading attack, smart card stolen attack and password change attack described in section 4. The improved proposed scheme and [11] scheme takes equal bits for computation and storage cost. Hence the proposed scheme is better than wang et. al.'s scheme [11] in terms of security. Table 2 shows the attack comparison of proposed scheme and related scheme.

Table 2. comparison of security analysis of proposed scheme with related scheme

Schemes ⇒ Attacks ⇓	Wang et. al.'s [11]	Our
Off-line password guessing attack	Yes	No
Off-line identity guessing attack	Yes	No
User impersonation attack	Yes	No
Server masquerading attack	Yes	No
Smart Card Stolen Attack	Yes	No
Password Change Attack	Yes	No

8. CONCLUSION

This paper demonstrated that the wang et. al.'s scheme is insecure against different possible attacks described in section 4. To overcome these weaknesses, an improved scheme over wang et. al.'s scheme has been proposed. The proposed improved scheme is more strong and efficient than related scheme in terms of security, described in section 6. Communication and storage complexity of both the scheme that is proposed improved scheme and wang et. al's scheme are same but in future, we will reduces both the complexity. Further, it can be incorporated biometric features to achieve high security in remote user authentication scheme.

9. REFERENCES

[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, Vol. 24, No. 11, PP. 770-772, 1981.

[2] A. Shimizu, T. Horioka and H. Inagaki, "A password authentication methods for contents communication on the Internet", IEICE Transactions on Communications, Vol. 81, No. 8, PP. 1666-1673, 1998.

[3] C.C. Chang and T.C. Wu, "Remote password authentication with smart cards", IEE Proceedings-E, Vol. 138, No. 3, PP. 165-168, 1993.

[4] S.B. Wilson, D. Johnson and A. Menezes, "Key agreement protocols and their security analysis", in proceedings of 6th IMA International Conference on Cryptography and Coding, Cirencester, LNCS, Vol. 1355, PP. 30-45, 1997.

[5] W.C. Ku and S.M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, PP. 204-207, 2004.

[6] E.J. Yoon, E.K. Ryu and K.Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, PP. 612-614, 2004.

[7] C.I. Fan, Y.C. Chan and Z.K. Zhang, "Robust remote authentication scheme with smart cards", Computers & Security, Vol. 24, No. 8, PP. 619-628, 2005.

[8] M.K. Khan and J. Zhang, "Improving the security of a flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, Vol. 29, No. 1, PP. 82-85, 2007.

[9] Hyun Sook Rhee, Jeong Ok Kwon and Dong Hoon Lee, "A remote user authentication scheme without using smart cards", Computer Standards & Interfaces, Vol. 31, PP. 6-13, 2009.

[10] C.T. Li and C.C. Lee, "A Robust Remote User Authentication Scheme using Smart Card", Information Technology and Control, Vol. 40, No. 3, PP. 231-238, 2011.

[11] Ding Wang, Chun-Guang Ma, Qi-Ming Zhang and Sendong Zhao, "Secure Password-based Remote User Authentication Scheme against Smart Card Security

Breach", Journal of Networks, Vol. 8, No. 1, PP. 148-155, January 2013.

[12] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, No. 6, PP. 644-654, November 1976.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis", Proceedings of Advances in Cryptology, PP. 388-397, 1999.

[14] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, Vol. 51, No. 5, PP. 541-552, 2002.

[15] S. K. Sood, A. K. Sarje and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture", Journal of Network and Computer Applications, Vol. 34, No. 2, PP. 609-618, 2011.