Cryptanalysis and An Efficient Secure ID-Based Remote User Authentication Scheme Using Smart Card

Ruhul Amin
Jakir Hossain Institute of Polytechnic
Department of Computer Science and Technology
Aurangabad, West Bengal-742224, India

ABSTRACT

Remote User authentication protocol is used for verifying the legitimacy of a remote user over insecure network environments. Recently, many secure ID based remote user authentication scheme using smart card have been proposed in the literature. In 2012, Ratan-Sanjay [1] proposed secure ID based remote user authentication scheme using smart card and claimed that their scheme can avoid all types of security flaws and feasible in terms of computation and storage cost. But We have pointed out that their scheme is insecure against user impersonation attack, server masquerading attack, off-line password guessing attack, off-line identity guessing attack, session key recovery attack and smart card stolen attack. So, their scheme can not be used for practical implementation in terms of security. Further, their scheme takes more computation and communication cost than the proposed scheme. To overcome these weakness, we have proposed an efficient secure ID based remote user authentication scheme using smart card based on cryptographic one way hash function. The proposed scheme resists all possible attacks and provides better computation and communication cost than Ratan-Sanjay's [1] scheme published earlier.

Keywords:

Attack, Authentication, Password, Secure ID, Smart Card

1. INTRODUCTION

Remote user authentication is important to identify whether the communicating parties are valid or not using password and smart card between the login user and remote server. Many password based remote user authentication scheme [2],[3],[5],[4] have been proposed in the literature over insecure networks. In 1981, first Lamport [5] proposed remote user authentication scheme based on identity and password. In Lamport scheme, server maintain verification table at the server end. But it is insecure against stolen verifier attack. Then in 2000, Hwang et. al.'s [2] scheme overcome the Lamport's [5] drawback. In 2004, Das et. al.'s [6] proposed dynamic identity based remote user authentication scheme and claimed that their scheme is secure against user anonymity. Later, Chein and chen et. al.'s [7] pointed out that Das et. al's [6] scheme fail to protect user anonymity and also Liao and Hwang et. al.'s [8] pointed out that Das et. al.'s [6] scheme is insecure against password guessing attack and it could not achieve mutual authentication. Then Chein and chen et. al.'s [7] proposed a scheme to preserve user anonymity using modular exponentiation. In 2007, Hu et. al.'s [10] pointed out that Chein and chen et. al.'s [7] scheme is insecure against sever masquerading attack, insider attack, replay attack and denial of service attack and proposed an improved scheme to overcome these weaknesses. In 2009, Xu et. al.'s [9] proposed remote user authentication scheme using non-temper resistant and modular exponentiation. Then R. Song [11] showed that Xu et. al.'s [9] scheme is insecure against user impersonation attack. In 2010, R. Song [11] proposed more secure authentication scheme using symmetric key cryptosystem and modular exponentiation. However W. B. Horng Cheng [12] showed that R. Song et. al.'s [11] scheme is insecure against password guessing attack, insider attack and denial of service attack. In 2011, Li and Lee proposed robust remote user authentication scheme using smart card to provide better authentication process and to resist all possible attacks. Then in 2011, Yoon and Yoo [13] demonstrated that Jia et. al.'s [14] remote user authentication scheme is insecure against forgery attack, insider attack and server spoofing attack.

In this paper, we have demonstrated that Ratan-Sanjay's [1] scheme is vulnerable to off-line password guessing attack, off-line identity guessing attack, user impersonation attack, server masquerading attack, smart card stolen attack and session key recovery attack. we have presented proposed scheme in section 4, To overcome these weaknesses and to provide better security and communication cost than Ratan-Sanjay's [1] scheme published earlier.

The remainder of this paper is organized as follows: Section 2 briefly reviews the Ratan-Sanjay's [1] scheme. Section 3 shows the brief description of attacks on Ratan-Sanjay's [] scheme. Section 4 describes the proposed scheme which withstand the weaknesses of Ratan-Sanjay's [1] scheme. Section 5 describes cryptanalysis of proposed improved scheme and section 6 compares the performances of proposed scheme with previously published scheme. Conclusion of this paper appears in section 7. Finally References are given in section 8.

2. BRIEF REVIEW OF RATAN-SANJAY'S SCHEME

This section presents briefly description of Ratan-Sanjay's [1] secure ID based remote user authentication scheme using smart card. The notations used throughout this paper are summarized in Table 1:

A one-way hash function $h : (0,1)^* \longrightarrow (0,1)^n$ takes an arbitrary length input $X \in (0,1)^*$, and produces a fixed-length(say, n-bits) output $h(X) \in (0,1)^n$ called the message digest.The

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
N_1	$\longrightarrow$	random nonce generated by U_i
N_2	$\longrightarrow$	random nonce generated by remote server RS
$h(\cdot)$	$\longrightarrow$	cryptographic one way hash function
SK	$\longrightarrow$	shared secret session key between user U_i and server RS
$\oplus$	$\longrightarrow$	bitwise xor operation
$\|$	$\longrightarrow$	concatenate operation

hash function is the fingerprint of a file, a message, or other data blocks, and has the following attributes:

(1) Hash function can be applied to a data block of all sizes.
(2) For any given variable $X, h(X)$ is easy to operate, enabling easy implementation in software and hardware.
(3) The output length of h(X) is fixed.
(4) Deriving X from the given value $Y = h(X)$ and the given hash function $h(\cdot)$ is computationally infeasible.
(5) For any given variable X, finding any $Y \neq X$ so that $h(Y) = h(X)$ is computationally infeasible.
(6) Finding a pair of inputs (X, Y), $X \neq Y$, so that $h(X) = h(Y)$ is computationally infeasible.

Their scheme consists of following four phases: Registration phase, Login phase, Authentication phase and Password Change phase.

2.1 Registration Phase

Whenever a new user wants to access the services from the server, he/she must have to register with the trusted remote server. Then, he/she choose his/her desired identity ID_i and password PW_i and sends $h(ID_i)$ and $h(ID_i \| PW_i)$ to the remote server through secure channel. After receiving registration request, remote server computes A_i = $h(ID_i) \oplus h(x \| h(ID_i))$, B_i = $A_i \oplus h(ID_i \| PW_i)$, C_i = $h(A_i)$ and D_i = $h(ID_i \| PW_i) \oplus h(x)$. Then issues the smart card for user U_i after storing some parameter into memory of smart card.

2.2 Login Phase

U_i inserts his/her smart card to the card reader and then supply ID_i^* and PW_i^*. The smart card computes A_i^* = $B_i \oplus h(ID_i^* \| PW_i^*)$ and C_i^* = $h(A_i^*)$ and check whether C_i^* is equal with stored C_i. If not, smart card terminates the login process otherwise smart card generates a random nonce R_i and computes $E_i = A_i^* \oplus R_i$, $Cid = h(ID_i \| PW_i) \oplus R_i$ and $F_i = h(A_i \| D_i \| R_i \| T_u)$, where T_u is the current login time stamp. Then sends login request message $\{F_i,\ E_i,\ Cid,\ T_u,\ h(ID_i)\}$ to remote server RS through insecure channel.

2.3 Authentication phase

After receiving login request message $\{F_i,\ E_i,\ Cid,\ T_u,\ h(ID_i)\}$, server verifies the validity of time interval $T_u^{'} - T_u <= \triangle T$, where $\triangle T$ denotes expects valid time interval for transmission delay and $T_u^{'}$ is the travel time of the message. If it holds, server computes A_i^* = $h(ID_i) \oplus h(x \| h(ID_i))$, $R_i^* = A_i^* \oplus C_i$, $G = h(ID \| PW_i^*)$ = $Cid \oplus R_i$, D_i^* = $h(ID \| PW_i^*) \oplus h(x)$ and computes F_i^* = $h(A_i^* \| D_i^* \| R_i^* \| T_u)$. Then checks whether F_i^* is equal with received F_i. If not then rejects the login request otherwise server RS further computes F_s = $h(h(ID_i) \| D_i \| R_i \| T_s)$, where T_s is the server current time stamp and sends reply message $\{F_s,\ G,\ T_s\}$. After receiving reply message, smart card computes G^* = $h(ID_i \| PW_i)$, F_s^* = $h(h(ID_i) \| R_i \| D_i \| T_s)$ and checks whether G^* = G and F_s^* = F_s are same or not. If the above condition holds, the mutual authentication is complete otherwise terminate the session. Then both user and remote server computes session key SK = $h(h(ID_i) \| T_s \| T_u \| A_i)$ for secure communication.

2.4 Password Change phase

This phase is involved whenever an existing user U_i wants to change the password PW_i with a new Password PW_i^{new}. User U_i inserts the smart card to the card reader/client machine and keys in ID_i^* and PW_i^* and request to change password. The card reader checks whether C = C* are equal or not. If it is satisfy User U_i is a legitimate bearer of the smart card. Then the card reader asks the User U_i to input new password PW_i^{new}. After entering the new password the card reader computes B_i^{new} = $A_i \oplus h(ID_i \| PW_i^{new})$ and D_i^{new} = $h(ID_i \| PW_i^{new}) \oplus h(ID_i \| PW_i) \oplus D_i$ and then replace B_i^{new} and D_i^{new} with B_i and D_i respectively into memory of smart card.

3. CRYPTANALYSIS OF RATAN-SANJAY'S SCHEME

In this section, the cryptanalysis of Ratan-Sanjay's [1] scheme is presented. To analyze the security weaknesses of Ratan-Sanjay's scheme, Our assumption are given in the following:

Assumption 1. It can be assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [15][16].

Assumption 2. Due to the low entropy of ID_i and PW_i selected by U_i, we assume an adversary is able to off-line guess U_is 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. [17].

Assumption 3. It can be assume that a valid user can provide secret information of the remote server to an attacker or a valid user can acts as an attacker after extract secret information of the remote server. In Ratan-Sanjay's [1] scheme, a valid user can computes hash value of server secret key $h(x)$ = $D_i \oplus h(ID_i \| PW_i)$ since valid user knows D_i using Assumption 1 and his/her personal identity and password ID_i and PW_i respectively. So an attacker or valid user knows $h(x)$of the remote server.

Under these assumption, we will show the various attacks on Ratan-Sanjay's [1] scheme such as user impersonation attack, Server masquerading attack, Off-line identity guessing attack, off-line password guessing attack smart card stolen attack and Session key recovery attack. So Ratan-Sanjay's [1] scheme should not use for the real application in terms of security.

3.1 User Impersonation Attack

After extracting login request message $\{F_i,\ E_i,\ Cid,\ T_u,\ h(ID_i)\}$ and reply message $\{F_s,\ G,\ T_s\}$, an attacker can perform user impersonation attack as follows:

Step 1: Attacker generates a random number r^* and computes D_i^a = $G \oplus h(x)$ then derives R_i = $G \oplus Cid$, A_i^* = $E_i \oplus R_i$ and again attacker computes E_i^a = $A_i^* \oplus r^*$, Cid^a = $G \oplus r^*$ and F_i^a = $h(A_i^* \| D_i^a \| Cid^a \| r^* \| T_a)$, T_a is the attacker current timestamp. Then attacker sends forged message $\langle F_i^a,\ E_i^a,\ Cid^a,\ T_a,\ h(ID_i)\rangle$ to the remote server.

Step 2: After receiving the forged message, RS checks the validity of time interval T^* - $T_a \leq \Delta T$ where T^* is the server's

time stamp and ΔT is the expected time interval for transmission delay. If it is valid then computes A_i^* = $h(ID_i) \oplus h(x \parallel h(ID_i))$, $r^* = A_i^* \oplus E_i^a$, $G = Cid \oplus r^*$, $D_i^* = G \oplus h(x)$ and $F_i^* = h(A_i^* \parallel D_i^* \parallel r^* \parallel T_a)$. Then server checks whether F_i^* is equals with F_i^a or not. It can be shown that the above condition is true. Then authenticated server will be convinced the message sent from the legal user.

Thus, an attacker can perform user impersonation attack on Ratan-Sanjay's [1] scheme.

3.2 Server Masquerading Attack

After intercepting login request message $\{F_i,\ E_i,\ Cid,\ T_u,\ h(ID_i)\}$ and reply message parameter G, an attacker can perform server masquerading attack as follows:

Step 1: Attacker generates random number r^* and then computes $D_i^a = G \oplus h(x)$ and $F_s^a = h(h(ID_i) \parallel D_i^a \parallel r^* \parallel T_a)$, where T_a is the attacker current time stamp and $h(x)$ obtained by using assumption 3. Then sends $\{F_s^a,\ G,\ T_a\}$ to user U_i.

Step 2: After receiving $\{F_s^a,\ G,\ T_a\}$, smart card computes G^* = $h(ID_i \parallel PW_i)$ and F_s^* = $h(h(ID_i) \parallel D_i \parallel r^* \parallel T_a)$. Then check the conditions whether G^* equals with received G and further checks whether F_s^* equals with received F_s^a. It can be easily shown that both condition are true. Then user U_i will be convinced the message sent from the legal remote server.

Thus, an attacker can perform successfully server masquerading attack on Ratan-Sanjay's [1] scheme.

3.3 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 $B_i, C_i, D_i, h(\cdot)$ from the user's smart card. Using these secret information of smart card, Assumption 3 and login message $h(ID_i)$, an attacker can create valid login message as follows:

Attacker computes $h(ID_i \parallel PW_i)$ =$D_i \oplus h(x)$ and A_i = $h(ID_i \parallel PW_i) \oplus B_i$. Then generates a random number r and computes $E_i = A_i \oplus r$, $Cid = h(ID_i \parallel PW_i) \oplus r$ and F_i = $h(A_i \parallel D_i \parallel r \parallel T_a)$, where T_a is the attacker current time stamp. Then, sends $\{F_i,\ E_i,\ Cid,\ T_u,\ h(ID_i)\}$ to the remote server as valid login message. So, their scheme is insecure against smart card stolen attack.

3.4 Off-line Identity Guessing Attack

After intercepting login message $h(ID_i)$, an attacker can successfully launched off-line identity guessing attack as follows:

Step 1: Attacker chose identity ID_i^a and computes $h(ID_i^a)$. Then check the correctness whether $h(ID_i^a)$ is equals with $h(ID_i)$.

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 ID_i. So, their scheme is insecure against off-line identity guessing attack.

3.5 Off-line Password Guessing Attack

After successfully getting static parameter identity ID_i of user U_i, an attacker can guess user correct password by performing the following steps:

Step 1: Attacker knows the value $h(ID_i \parallel PW_i)$. Then attacker chose password PW_i^a and computes $h(ID_i \parallel PW_i^a)$, where ID_i is the correct user identity. After that Attacker checks the correctness whether $h(ID_i \parallel PW_i)$ is equals with $h(ID_i \parallel PW_i^a)$.

Step 2: An attacker repeats the above process until the correct password is obtained. After some guessing, an attacker can find out the correct password. So, their scheme is insecure against off-line password guessing attack.

3.6 Session Key Recovery Attack

In remote user authentication system, session key is used to communicate securely between the user and the server. In Ratan-Sanjay's [1] scheme, an attacker can computes session key. So an attacker can gets confidential information between the client and server after decrypting using session key. As a result, Ratan-Sanjay's [1] scheme is inapplicable for practicable implementation. Session key computation by an attacker are as follows:

An attacker can computes A_i described in smart card stolen attack procedure in section 3. We assume that an attacker stores $i-th$ login and reply message parameter $T_u,\ T_s$ respectively between the user and server. Then attacker computes session key SK = $h(h(ID_i) \parallel A_i \parallel T_u \parallel T_s)$. Thus, an attacker can computes session key between the user and server.

3.7 Mutual Authentication

If any remote user authentication scheme is insecure against user impersonation attack and server masquerading attack then that scheme generally fails to provide mutual authentication. We have shown in section 3 that Ratan-Sanjay's scheme is insecure against user impersonation and server masquerading attack. Hence Ratan-Sanjay's scheme fails to provide mutual authentication.

4. PROPOSED SCHEME

In this paper, we have shown that Ratan-Sanjay's [1] scheme is insecure against various attack. To overcome these weaknesses, in this section we proposed an efficient secure ID based remote user authentication using smart card. It is assumed that Remote server (RS) is a trusted authority.

The proposed scheme consists of mainly four phases namely Registration phase, Login phase, Authentication phase and password change phase. All these phase of the proposed scheme is as follows:

4.1 Registration Phase

Whenever a new user wants to get services from the remote server, he/she first must have to register with the trusted registration center. User choose his/her desired identity ID_i and password PW_i and then computes masked password PWR_i = $h(PW_i \parallel r)$ to resists privileged insider attack, where r is the random number chosen by the user U_i. Then sends registration message ID_i, PWR_i to the remote server RS. After receiving it, remote server computes CID_i = $h(ID_i \parallel x \parallel T)$ and checks whether CID_i is exists or not in the server database, where x is the secret key of the remote server and T is the time stamp at the time of registration maintained by the remote server. If CID_i is exists, then server sends a message to the user to choose another identity otherwise remote server computes A_i = $h(ID_i \parallel PWR_i)$, C_i = $h(CID_i \parallel x)$ and Z_i = $C_i \oplus PWR_i$. Then server issues smart card securely for the user U_i after storing $\{A_i,\ Z_i,\ CID_i, h(\cdot)\}$ into memory of smart card. After getting smart card, user U_i stores random number r into memory of smart card.

4.2 Login Phase

Whenever an existing user U_i wants to get the services from the remote server, first inserts his/her smart card into the card reader or terminal and submits his/her identity ID_i^* and password PW_i^*. Then card reader computes $PWR_i^* = h(PW_i^* \parallel r)$, $C_i^* = Z_i \oplus PWR_i^*$, $A_i^* = h(ID_i^* \parallel PWR_i^*)$ and checks whether computed A_i^* equals with stored A_i or not. If true, card reader generates a random nonce N_1 and computes $B_i = PWR_i^* \oplus N_1$, $D_i = h(CID_i \parallel B_i \parallel C_i^*)$ and $G_i = C_i^* \oplus B_i$. Then, sends login request message $\{D_i,\ G_i,\ CID_i\}$ to the remote server.

4.3 Authentication Phase

After receiving the login request message $\{D_i,\ G_i,\ CID_i\}$ first check the format of CID_i. If it is valid then computes $C_i^s = h(CID_i \parallel x)$, $B_i^s = C_i^s \oplus G_i$, $D_i^s = h(CID_i \parallel B_i^s \parallel C_i^s)$ and checks whether computed D_i^s equals with received D_i. If it is not equals then server terminates the session otherwise; server computes $K_i = h(CID_i \parallel B_i^s \parallel N_2)$ and $L_i = B_i^s \oplus N_2$, where N_2 is random number chosen by the remote server. Then sends reply message $\{K_i,\ L_i\}$ to the smart card user U_i for mutual authentication. After receiving it, smart card computes $N_2^* = L_i \oplus B_i$, $K_i^* = h(CID_i \parallel B_i \parallel N_2^*)$ and checks whether computed K_i^* equals with received K_i. If equals, then mutual authentication is achieved and both the parties agree with a common shared session key SK by computing $SK = h(B_i \parallel N_2 \parallel C_i^s)$ for securing future data communications otherwise terminates the session.

4.4 Password Change Phase

This phase is invoked whenever U_i wants to change his/her password. U_i inserts the smart card into the card reader and submits ID_i^* and PW_i^*. Then card reader computes $PWR_i^* = h(PW_i^* \parallel r)$, $A_i^* = h(ID_i^* \parallel PWR_i^*)$ and checks whether computed A_i^* equals stored A_i. If true, U_i enters a new password PW_i^{new}. Then card reader computes $PWR_i^{new} = h(PW_i^{new} \parallel r)$, $A_i^{new} = h(ID_i^* \parallel PWR_i^{new})$, $Z_i^{new} = C_i \oplus PWR_i^{new}$ and stores A_i^{new} and Z_i^{new} instead of A_i and Z_i respectively into the memory of smart card. Thus, U_i can change the password without taking any assistance from remote server.

5. CRYPTANALYSIS OF PROPOSED SCHEME

This section describes cryptanalysis of proposed scheme. In this paper, to analyze the security analysis of proposed scheme, it can be assumed that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [15][16] and can intercept messages communicating between the user and the server. Also it can be assumed that an attacker may possess the capabilities to thwart the security scheme.

5.1 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 secret values $\{A_i,\ Z_i,\ CID_i, h(\cdot)\}$ stored in the user's smart card, because the attacker can not compute the valid login request message $\{D_i,\ G_i,\ CID_i\}$ without knowing the secret password PW_i of valid user U_i and server secret key x. In proposed scheme if the attacker wants to get the secret parameter PW_i and server secret key x, he/she must have to solve the inversion of cryptographic hash function which is computationally hard. So, the proposed scheme is secured against user impersonation attack.

5.2 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 users login request message. However, the attacker can not masquerade as the server by forging the reply message, because it is hard to compute $\{K_i,\ L_i\}$ by an attacker without knowing the secret parameter user's password PW_i. Hence, the attacker can not masquerade as the legitimate server to the user by launching the server masquerading attack.

5.3 Off-line Identity Guessing Attack

After getting secret values $\{A_i,\ Z_i,\ CID_i, h(\cdot)\}$ stored in the user's smart card and after intercepting login message, the attacker attempts to guess user identity ID_i using CID_i, A_i in the registration phase. To guess user's identity from CID_i, attacker has to guess user's identity, server secret key x and registration time T simultaneously but which is not possible in polynomial time and also from A_i is not possible because he/she has to guess user identity and user password simultaneously which is not possible in polynomial time. So, the proposed scheme is secure against Off-line identity guessing attack.

5.4 Off-line Password Guessing Attack

As described in section 5, the proposed scheme is secure against off-line identity guessing attack. So attacker has no way to guess user's correct password from A_i parameter stored in user's smart card because he/she can not guess user identity and password simultaneously in polynomial time. Also attacker can not guess user's password from PWR_i because he/she can not compute valid PWR_i from the known parameters. So, the proposed scheme is secure against off-line password guessing attack.

5.5 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 $\{A_i,\ Z_i,\ CID_i, h(\cdot)\}$ from the smart card. Also can be assumed that attacker stores the $i-th$ login message $\{D_i,\ G_i,\ CID_i\}$ of the user U_i. After getting all these parameter, attacker has no way to guess or derive user identity and password. So attacker can not create valid login message. As a result, the proposed scheme is secure against smart card stolen attack.

5.6 Session Key Recovery Attack

In the proposed scheme, an attacker can not compute session key $SK = h(B_i \parallel N_2 \parallel C_i^s)$. Because to compute session key attacker has to know user's correct password PW_i, identity ID_i and server secret key x. But there is no way to get these secret information from the proposed scheme. If an attacker wants to get these secret information, he/she must have to solve cryptographic one way hash function which is computationally hard. So, the proposed scheme provides strong security in terms of session key.

5.7 Privileged Insider Attack

Generally, many user uses same password for their convenience of remembering and easy of use whenever required. However if the system manager or privileged insider of the server knows user's password, he/she may try to access user's U_i other accounts in other server. But in proposed scheme, the system manager or privileged insider of the server can not derive user's password PW_i because user have submitted masked password $h(PW_i \parallel r)$ instead of PW_i. To get correct PW_i, system manager must have to solve Inversion of cryptographic one way

hash function problem which is computationally hard. Hence, the proposed scheme resists insider attack.

5.8 Mutual Authentication

As described the attack procedure in section 5, proposed scheme can withstand the user impersonation attack and the server masquerading attack. So the proposed scheme provides strong mutual authentication because without knowing user's password PW_i and server secret key x, attacker can not compute valid login and reply message of the proposed scheme.

6. PERFORMANCE ANALYSIS OF PROPOSED SCHEME

In this section, we evaluated the performance of proposed scheme with Ratan-Sanjay's [1] scheme. We have compare login and authentication phases of proposed scheme with Ratan-Sanjay's [1] scheme because these phases are used frequently. Table 2 shows the computation over head and Table 3 shows the communication cost and storage cost of proposed scheme and Ratan-Sanjay's [1] scheme. In Table 2, T_h is the time required for hashing operation. Though, proposed scheme resists different possible attacks of Ratan-Sanjay's scheme, in spite of proposed scheme provides better computation and communication cost than the related scheme.

It can be reasonably assumed that the length of ID_i and PW_i is 64 bits each and $h(\cdot)$, random nonce returns 128 bits each. The communication cost (capacity of transmitting message) of proposed scheme and related scheme [1] is 640 $bits$ = $(128 + 128 + 128 + 128 + 128)$ and 1024 $bits$ = $(128 + 128 + 128 + 128 + 128 + 128 + 128 + 128)$ respectively. Also the storage cost (stored into the memory of smart card) takes almost same bits of proposed scheme and their scheme that is 640 $bits$, 512 $bits$ respectively. Table 4 shows that their scheme is insecure against different possible attacks. Further proposed scheme provides strong authentication against different attacks described in section 5. After resisting all possible attacks of related scheme, proposed scheme provides low computational and low communication cost than their scheme. Hence the proposed scheme is more efficient and secure than Ratan-Sanjay's scheme.

Table 2. comparison of computational cost of proposed scheme with related scheme

Scheme ⇒ Phase ⇓	Ratan-Sanjay's	Proposed Protocol
Login Phase	$4T_h$	$3T_h$
Authentication Phase	$7T_h$	$6T_h$
Total	$11T_h$	$9T_h$

Table 3. comparison of communication and storage cost of proposed scheme with related scheme

Scheme ⇒ Item ⇓	Ratan-Sanjay's	Proposed Protocol
Communication Cost	1024 bits	640 bits
Storage Cost	512 bits	640 bits

7. CONCLUSION

This paper shows that Ratan-Sanjay's [1] scheme suffers from different attacks. To overcome these weaknesses a proposed scheme is given in this paper. Further, the proposed scheme is more efficient in terms of computational and communication cost than that of Ratan-Sanjay's [1] scheme. In addition, proposed scheme provides mutual authentication between user and remote server and also user can change his/her password freely without help of remote server.

Table 4. attack comparison of proposed scheme with related scheme

Scheme ⇒ Attack ⇓	Ratan-Sanjay's	Proposed Protocol
User Impersonation Attack	Yes	No
Server Masquerading Attack	Yes	No
Off-line Password Guessing Attack	Yes	No
Off-line Identity Guessing Attack	Yes	No
Smart Card Stolen Attack	Yes	No
Mutual Authentication	No	Yes
Session key Recovery Attack	Yes	No

It is shown that the proposed scheme provides strong security protocol based on the user's password. For the better security, biometric feature as well as password can be incorporate in the protocol.

8. REFERENCES

[1] R.R Ahirwal, S.S. Sonwanshi, "An Efficient and Secure ID-based Remote User Authentication Scheme using Smart Card", International Journal of Applied Information Systems (IJAIS) ISSN : 2249-0868, vol. 1, no. 6, pp. 35-41, February 2012.

[2] Min- Shiang Hwang, Li Hua Li., "A new remote password authentication scheme using smart card", IEEE Transaction on Consumer Electronics, 46 (1), pp. 28-30, 2000.

[3] J.K.Jan and Y.Y.Chan, "paramita wisdom password authentication scheme without verification tables", The journal of system and software, 42(1), pp. 45-57, 1998.

[4] Chun Ta Li, Cheng Chi Li., "A password authentication scheme over insecure networks", Journal of computer and system science, vol. 72,No. 4 pp. 727-740, 2006.

[5] L. Lamport, "Password authentication with insecure communication", Communication of the ACM, vol. 24, No 11 pp. 770-772, 2001.

[6] M.L. Das, A. Saxena and V.P. Gulati., "A Dynamic ID-based remote user authentication scheme", IEEE Transaction on consumer Eleectronice, vol. 50, pp. 629-631, 2004.

[7] H.Y. Chien and C.H. Chen., "A remote authentication scheme preserving user anonymity", proc. advanced information networking and application, vol.2.pp 245-248, march, 2005.

[8] I.E. Liao, Chenge-chi Lee and Min-shiang Hwang., "Security Enhancement for a Dynamic ID-Based Remote User Authentication Scheme", Proc. Conference on Next Generation Web Services Practice, pp.437-440, July,2005.

[9] J. Xu, W.T. Zhu and D.G. Feng., "An improved smart card based password authentication scheme with provable security", Computer Standards and Interfaces, vol. 31, no. 4, pp. 723 728, 2009.

[10] L.I.Hu, X.X. Niu, and Y.X. Yang., "Weaknesses and improvements of a remote user authentication scheme using smart cards", The Journal of China Universities of Posts and Telecommunications, vol. 14, pp. 91-94, 2007.

[11] R. Song., "Advanced smart card based password authentication Protocol", Computer Standards and Interfaces, Volume 32, Issue 4, June, PP 321-325, 2010.

[12] W B Horng and Cheng p Lee., "Security weaknesses of song.s advanced smart card based Password authentication

Protocol", IEEE trans. Computer, vol.978-4244-6789 1/10,2010.

[13] Eun-Jun Yoon, and Kee-Young Yoo., "Three Attacks on Jia et al..s Remote User Authentication Scheme using Bilinear Pairings and ECC", World Academy of Science, Engineering and Technology 60 (JULY 2011).

[14] Z. Jia, Y. Zhang, H. Shao, Y. Lin and J. Wang, "A remote user authentication scheme using bilinear pairings and ECC", Proceeding Of 6th International Conference on Intelligent Systems Design and Applications (ISDA.06), Vol.2, Oct., pp. 1091-1094, 2006.

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

[16] 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.

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