IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. III (Mar – Apr. 2015), PP 08-16
www.iosrjournals.org

Cryptanalysis and Security Enhancement of a Khan et al.'s Scheme

Eman T. Jasim[1], Hameed A. Younis[2]
University of Basra, College of Science, Department of Computer Science, Basra, Iraq.[1,2]

Abstract: *Remote user authentication, in which the resources are distributed among the recipients and they are shared across the network in the form of network services provided by the remote systems. Before supply such services, the remote system should have the skill to authenticate the users. Otherwise, a discount could impersonate a legitimate user login to get access to the system. Currently, an efficient remote authentication in which using smart card have been widely adopted due to their low computational cost and convenient portability for the authentication purpose. In smart card this field, there are many studies have relied upon them, including a study by Khan et al. who claimed that he exceeded the weaknesses of Wang et al.'s scheme. But unfortunately Khan et al.'s scheme is still suffer from several the identified weaknesses which is include preserve anonymity of a user, efficiency for wrong password login, forward secrecy and efficiency session key agreement. So our propose which it includes the construction of authentication system depending on 2FA , which is authentication scheme based on smart card, where it is surpassed the identified weaknesses of Khan et al.'s scheme which including preserve anonymity of a user, efficiency for wrong password login, forward secrecy and efficiency session key agreement.*

Keywords: *2FA , Authentication, Remote user authentication, Smart card, Password.*

I. Introduction

Remote user authentication is one of the results of the rapid development of the Internet where from which the user can access to the source of his whereabouts One contact applications remotely and the most popular of which are the smart card in addition to this area over several stages to be arrived at what it now In 1981, Lamport [1] claimed that his a remote user authentication scheme is secure by it is presented a scheme using password table. In 2000, Hwang and Li [2] identified that Lamport's scheme is susceptible to the risks of hacking and modifying the password table. Thus, Hwang and Li proposed a remote user authentication scheme without using the password table, which was based on El Gamal public key encryption method [3].In 2004, Das et al.[4] proposed a dynamic ID-based remote user authentication scheme using smart cards which it resist the reply attacks, forgery attacks, guessing attacks, insider attacks and stolen verifier attacks through allowing the users to select and alter their password freely with it is not preserve any verifier table by employing a dynamic ID-based remote user authentication scheme using smart cards for each login .In 2005 Liao et al.[5] proposed scheme with a little alteration can enhance the security of Das et al.'s scheme[4]. Despite this proposed scheme does not add many computational costs, but it is also efficient. In 2006 Yoon et al. [6] proposed scheme including an amended dynamic identity based mutual authentication scheme that excludes the security weaknesses of Liao et al.'s scheme[5], where they explained a reflection attack on Liao et al.'s scheme[5] that breaks the mutual authentication. In the same year Liou et al.[7] proposed scheme which overcomes the weaknesses of Das et al.'s scheme[4] by proposition a new dynamic identity based remote user authentication scheme using smart cards that realizes mutual authentication. In 2009, Wang et al.[8] proposed scheme which overcomes the weaknesses of Des et al.'s scheme[4] which it did not achieve mutual authentication and could not resist impersonate remote server attack by improvement the password authentication scheme which still keeps the merits of the original scheme. In 2011 Khan et al.[9] proposed scheme which overcomes the identified weaknesses of Wang et al.'s[8] dynamic ID-based remote user authentication scheme which include vulnerable to insider attack, does not preserve anonymity of a user, long and random password for a user to remember, no provision for revocation of lost or stolen smart card and no support for session key agreement during authentication process.

However, in this paper, firstly, we show that Khan et al.'s scheme suffers from attacks and have some practical security pitfalls. Moreover, we discuss that their scheme has weaknesses and is insecure, inefficient, and infeasible for implementation in the real environment. To overcome the security flaws of Khan et al.'s scheme, we propose an improved dynamic ID-based remote user authentication scheme which including preserve anonymity of a user, efficiency for wrong password login, forward secrecy and efficiency session key agreement. Rest of the paper is organized as follows: II. Materials And Methods which includes 1. briefly reviews Khan et al.'s scheme 2. examine the weaknesses and security problems of their scheme 3. Details of

our proposed scheme based on smart card 4. Cryptanalysis of our proposed scheme based on smart card. III. Result and discussion which includes Comparison with Related Works. and IV. Conclusion

II. Materials And Methods

Review Khan et al.'s scheme

Khan et al.'s have proposed an enhanced smart card-based authentication scheme, dependent on Wang et al.'s scheme who achieve mutual authentication and could resist impersonate remote server attack. However, Khan mentioned that Wang et al.'s scheme is still suffer from weaknesses, so Khan et al.'s scheme improves all the identified weaknesses of Wang et al.'s dynamic ID-based remote user authentication scheme which include vulnerable to insider attack, does not preserve anonymity of a user, long and random password for a user to remember, no provision for revocation of lost or stolen smart card and no support for session key agreement during authentication process.

Khan et al. Presented scheme consists of five different phases, namely; registration phase, login phase, authentication phase, password-change phase, and revocation of lost or stolen smart card phase. These phases work as follows:

A. Registration Phase

This phase includes two function, the first function when Ui wants to registration and the second function when Ui wants to re-registration to authentication server S. Khan et al.'s scheme includes two secret key x_s and y_s which is used for providing with user anonymity during authentication server, while they used value of N to revoke a smart card in the case of theft or stolen, which is stored in database as account for number of the registration of Ui, with all that Khan et al.'s assume founding high security condition such as, e.g., strong administration policies and procedures, firewalls, intrusion detection software to protect the sensitive data on the server. The following steps are performed to complete the registration phase:

Step1 ID_ichooses his ID_i and pw_i and generates a random number r and computes $RPW_i = h(r \parallel pw_i)$.

Step2 U_i submits his ID_i and RPW_i to the S over a secure channel.

Step3 S checks the registration credentials of U_i and checks whether his chosen $ID_i$is already in the database or not. If ID_i already exists in the database, S intimates U_i to choose anotherID_i. In addition, S checks the registration record of U_i and if U_i is a new user then S sets value of $N = 0$, otherwise if $U_i$is re-registering in the system the S sets $N = 1$ and stores values ID_i and N in the database.

Step4 S computes $J_i = h(x_s \parallel IDU)$ where $IDU = (ID_i \parallel N)$.

Step5 S computes $L_i = J_i \oplus RPW_i$.

Step6 Now, S issues smart card to U_i which contains values of L_i and y_s over a secure channel.

Step7 U_i securely stores random number r in the smart card and does not need to remember its value. This step completes the registration process.

B. Login Phase

When U_i wants to login into S, he inserts his smart card in the terminal and inputs his ID_i and pw_i. Smart card performs the following steps:

Step1 Computes $RPW_i = h(r \parallel pw_i)$ and $J_i = L_i \oplus RPW_i$, where random number r is securely pre-stored in the smart card.

Step2 Acquires the current time stamp $T_i$and computes$C_1 = h(T_i \parallel J_i)$.

Step3 Generates a random number d and computes an anonymous ID_i of U_i by $AID_i = ID_i \oplus h(y_s \parallel T_i \parallel d)$.

Step4 At the end of login phase U_i sends a login message $m = \{AID_i, T_i, d, C_1\}$ to S for the authentication process.

C. Authentication Phase

Upon receiving the login request message $m = \{AID_i, T_i, d, C_1\}$ the authentication server S verifies its authenticity by the following steps:

Step1 Verifies the validity of time interval between $T_i$and $T^{'}$. If $(T^{'} - T_i) \geq \Delta T$, then S rejects the login request and intimates Ui about the time stamp expiry and refuse the further operations. Here, ΔT denotes the expected valid time interval for transmission delay and $T^{'}$ denotes receiving time stamp of login message m.

Step2 Computes $ID_i = AID_i \oplus h(y_s \parallel T_i \parallel d)$ and validates if ID_i is a valid user's ID_i then performs further operations, otherwise terminates the operation and informs U_i about it.

Step3 Checks the value of N in the database and computes $IDU = (ID_i \parallel N)$.

Step4 Computes $J_i = h(x_s \parallel IDU)$and checks whether $h(T_i \parallel J_i) \stackrel{?}{=} C_1$. If they are equal, it means U_i is an authentic user and S accepts the login request, otherwise the login request is rejected and user is informed about the decision.

Step5 For mutual authentication, S acquires current time stamp T_s and computes $C_2 = h(C_1 \oplus J_i \oplus T_s)$ and then sends the mutual authentication.
Step6 $S \rightarrow U_i$: authentication message $\{C_2, T_s\}$.
Step7 Upon receiving the mutual authentication message, U_i verifies the the mutual authentication, message was received. If $(T^{"} - T_s) \geq \Delta T$, then U_i rejects this message and terminates the operation, otherwise step8 is performed.
Step8 U_i checks whether $h(C_1 \oplus J_i \oplus T_s) \stackrel{?}{=} C_2$. If this holds, U_i authenticates S, otherwise login request is given up by U_i.
Step9 Now, U_i and S share the symmetric session key $S_k = h(C_2 \oplus J_i)$ for performing further operations during a session.

D. Password-change Phase

In the password-change phase, when a user wants to change his password pwi with a new password pw'_i, he inserts his smart card into the smart card reader and enters his ID_i and password. The smart card performs the following operations without interacting with remote server S:
Step1 Computes $RPW_i^* = \mathrm{h}(\mathrm{r} \parallel pw_i)$ and $J_i^* = L_i \oplus RPW_i^*$. If $J_i = J_i^*$ hold, then Ui is allowed to change the password, otherwise password-change phase is terminated.
Step2 Computes $L_i = J_i \oplus RPW_i \oplus RPW_i^* \oplus h(r \parallel pw_i)$ and replaces the old value of L_i with the new value.
Now, the new password is successfully changed and this phase is terminated

E. Lost Smart Card Revocation Phase

In the case of loss or stolen of smart card, U_i requests S for its revocation. S first validates the U_i by his secret credentials, e.g., mother's maiden name, date of birth, national ID_i card number, or some other values known to U_i. After validating the revocation request, S changes the value of N to revoke the smart card. In every case of stolen or lost of smart card, the value of N is incremented by one. Later on, U_i can re-register to S without changing his Di . Here, U_i is strongly recommended not to use any previous values for his new registration, e.g., password and random number, otherwise anybody can impersonate U_i by using the same credentials previously saved in the lost or stolen smart card.

2. Weaknesses of Khan's Scheme

In this section, we explain the weaknesses of Khan et al.'s scheme as they appear in [10][11]:

2.1 User Anonymity

In some application of authentication, we need to save confidentiality of identity of a user because the adversary sniffing the communication channel can eavesdrop between parties which been in communication to achieve authentication process.

In Khan et al.'s scheme, in which they claimed with providing user anonymity by in the login phase specifically, in step3 $AID_i = ID_i \oplus h(y_s \parallel T_i \parallel d)$ but in fact in the authentication phase the sever computes the clear ID_ithat means this step break any user anonymity because the user become known to the adversary sniffing in the case of attack, so we assume adversary Ua stolen smart card and password, and by eavesdrops:
1. the attack can be extract $AID_i, T_i$and d.
2. With $T_i$and d the attacker can computes his own AID_j, ID_j and pw_j.
3. Now by computing $AID_i \oplus AID_j \oplus ID_j$ the attacker can obtain about IDi, because as we mentioned earlier U_j the attacker completely control of smart card and the value of T_i and d so:

$AID_i \oplus AID_j \oplus ID_j$
$= ID_i \oplus h(y_s \parallel T_i \parallel d)) \oplus (ID_j \oplus h(y_s \parallel T_i \parallel d) \oplus ID_j$
$= ID_i$

In addition, if the attacker can obtain any smart card, he can get the secret information as y_s which stored in stolen smart card by monitoring the power consumption [13] or by analyzing the leaked information [12] and can compute:

$AID_i \oplus h(y_s \parallel T_i \parallel d)$
$= ID_i \oplus h(y_s \parallel T_i \parallel d) \oplus h(y_s \parallel T_i \parallel d)$
$= ID_i$

2.2 Efficiency for Wrong Password Login

It discovers the mistake of password in early phase as login phase without any delay the client by display error message this option availability not sending a request message to the server to verify from the identity of a user, leading non transition to authentication phase and thus saves a lot of time.

In Khan's scheme, if the client's password is wrong, he/she will not know it is wrong until he finishes login pass and begin authentication phase arriving to step4 when the server check $h(T_i \parallel J_i) \stackrel{?}{=} C_1$ and send message to client finding wrong in password all that leading waste of time and inefficiency.

2.3 Forward Secrecy

In fact, Khan et al.'s scheme can't provide the forward secrecy, because if the attacker get the value $x_s$and y_s , he can calculate the session key by conducting some accounts:
1. From method above the attacker can get the value $ID_i$with let $N_i$be zero.
2. The attacker have $ID_i$and guess N= 0, he computes $IDU = (ID_i \parallel N)$ then $J_i = h(x_s \parallel IDU)$.
3. If the attacker get the value of J_i, he can get the session key by computes $S_k = h(C_2 \oplus J_i)$.
If the attacker does not get the session key, he will increment of N by one and repeat all above steps until to get its current value.

2.4 Inefficiency of The Double Secret keys

Khan et al.'s use two secret keys $x_s$and y_s, while they can achieve user authentication and agreement service by using one key, so using two keys are more expensive.

3. Details of Our Proposed Scheme Based on Smart Card

The notations used throughout our proposed scheme based on smart card can be summarized as follows:

Table (1.1): The notations used throughout our proposed scheme based on smart card.

Notation	Description
U_i	User
S	Remote server
ID_i	User's ID
pw_i	User's password
$h(.)$	One-way hash function
$\oplus$	Bitwise XOR computation
$\parallel$	Concatenation operation
x_s	Secret value of server
ΔT	Expected valid time interval
T	Time stamp
A$\Rightarrow$B:M	A sends M to B through a secure channel
A$\rightarrow$B:M	A sends M to B through a common channel.

We use simple hash functions to propose our scheme based on smart card. Our presented scheme includes five different phases these are: registration phase, login phase, authentication phase, password-change phase, and revocation of lost or stolen smart card phase. These phases work as follows:

A. Registration Phase

Step1 U_i selects his ID_i , pwi and creates a random number r to calculates $RPW_i = h(r \parallel pw_i)$.
Step2 $Ui \Rightarrow S: ID_i , RPW_i$.
Step3 S checks if the U_i initial registration , S creates a new record for credentials of Ui in database and sets value of N=0, otherwise sets value of N=N+1and store in database.
Step4 S Calculates $J_i = h(x_s \parallel IDU)$ where $IDU = (ID_i \parallel N)$.
Step5 S Calculates $L_i = J_i \oplus RPW_i$.
Step6 S Calculates $B_i = h(L_i \parallel ID_i)$.
Step7 Now, $S \Rightarrow U_i$:a smart card containing $\{B_i, J_i\}$
Step8 U_i does not need to remember the value of random number r because it will be saved in smart card securely.

B. Login Phase

U_i enters his smart card smart card reader, then Ui enters his $ID_i{}'$, pwi' to smart card then it carries out the following steps:
Step1 Calculates $RPW_i{}' = h(r \parallel pw_i), L_i{}' = J_i \oplus RPW_i{}'$ and $B_i{}' = h(L_i{}' \parallel ID_i{}')$,where random number r is securely pre-stored in the smart card.
Step2 If $B_i{}' \neq B_i$reject the smart card, otherwise computes next steps.
Step3 Get the current time stamp $T_i$and calculates $C_1 = h(T_i \parallel B_i{}')$.
Step4 Produces a random number d and calculates an anonymous
ID_i of U_i by $CID_i = RPW_i{}' \oplus h(L_i{}' \parallel T_i \parallel d)$.

Step5 $U_i \longrightarrow S$: $m = \{CID_i, T_i, d, C_1\}$.

C. Authentication Phase

After arriving the login request message $m = \{CID_i, T_i, d, C_1\}$ the authentication server S verifies its validity by the following steps:

Step1 Checks the of authenticity time interval between $T_i$and T'. If $(T' - T_i) \geq \Delta T$, then S rejects the login request. Here ΔT refers to the expected valid time interval for transition delay and T' refers to receiving time stamp of login message m.

Step2 Calculates $RPW_i = CID_i \oplus h(L_i \parallel T_i \parallel d)$ and verifies if RPW_i a valid then executes further operations, otherwise finishes the operation and reports U_i about it.

Step3 Calculates $L_i = h(Ji \parallel RPW_i)$ to Calculates $B_i = h(L_i \parallel ID_i)$ then check whether $h(T_i \parallel B_i) \stackrel{?}{=} C_1$. If they are equal, it means U_i is an authentic user and S accepts the login request, otherwise the login request is rejected and user is informed about the decision.

Step4 For mutual authentication, S acquires current timestamp T_s and Calculates $C_2 = h(C_1 \oplus L_i \oplus T_s)$ and then sends the mutual

Step5 $S \rightarrow Ui$:authentication message $\{C_2, T_s\}$.

Step6 After arriving the mutual authentication message, Ui checks the time interval between $T_s$and $T^{"}$, where T" is the time stamped when the mutual authentication, message was arrived. If $(T^{"} - T_s) \geq \Delta T$, then U_i rejects this message and terminates the operation, otherwise step8 is performed.

Step7 U_i checks whether $h(C_1 \oplus L_i \oplus Ts) \stackrel{?}{=} C_2$. If this holds U_i authenticates S otherwise login request is given up by U_i .

Step8 Now, U_i and S, share the symmetric session key $S_k = h(C_2 \oplus B_i)$ for carrying out further operations during a session.

D. Password-change Phase

In the password-change phase, when a user wants to change his password $pw_i$with a new password pw_i' , he enters his smart card into the smart card reader and enters his ID_i , password. The smart card carries out the following operations with interacting with remote server S:

Step1 Calculates $RPW_i^* = h(r \parallel pw_i)$ and $L_i^* = J_i \oplus RPW_i^*$. If $L_i = L_i^*$ hold, then U_i is allowed to change the password, otherwise password-change phase is finished.

Step2 Calculates $J_i = L_i \oplus RPW_i \oplus RPW_i^* \oplus h(r \parallel pw_i)$ and replaces the old value of $J_i$with the new value. Now, the new password is successfully modified and this phase is finished

F. Lost Smart Card Revocation Phase is equal to the original one in Khan et al.'s scheme.

4. Cryptanalysis of Our Proposed Scheme Based on Smart Card

4.1 User Anonymity

In our proposed scheme which is based on smart card, we perform to change ID dynamic CID_i in step3 existing in login phase by $CID_i = RPW_i \oplus h(L_i \parallel d \parallel T_i)$, where the attacker based on eavesdropping on the victim's login request message$m = \{CID_i, T_i, d, C_1\}$.

In the case of the attacker who obtains CID_i, T_i, d from eavesdropping, he/she cannot extract RPW_i because, he need to know the value of L_i which is not stored in smart card, and he cannot compute L_i because he need to know another information like J_i, so it leads to failed this attack.

4.2 Forward Session

In the case of this attack could reveal the server's secret key that is not lead to getting the key session. In our proposed scheme based smart card it is assumed the adversary $U_a$has gotten the value of x_s, he/she need to get the value of Bi because $ks = \{T_s, Bi\}$, but that need to compute $B_i =_i h(L_i \parallel ID_i)$, where $L_i = J_i \oplus RPW_i$, $J_i = h(x_s \parallel IDU)$ and $IDU = (ID_i \parallel N)$ that means he/she need to know ID_i with x_s, but the value of ID_i become difficult getting it after we have achieved user anonymity, so this attack cannot achieve with just know x_s.

4.3 Efficient Secret Key

In our proposed scheme based on smart card, we use only one secret key x_s, where it meets with our purpose. While khan et al.'s use two secret server's keys $x_s$andy_s, where the use of the first to save unique of ID_i, in addition Khan et al.'s use it in authentication phase to verify from the ownership of the user for ID_i, while the use of the second key y_s for compute ID-dynamic, but with our proposed we use one to save the unique of $ID_i$and we do not need another one to use in ID-dynamic.

4.4 Efficiency for Wrong Password Login

In our proposed scheme based on smart card, we treat this problem by adding step $B_i = h(L_i \parallel ID_i)$ in registration phase where it reveals if a user enters his/her password or username mistake and this detection happen in login phase when the value of $B_i'$is compared between B_i, this step save a lot of time and if the user make mistake in his/her data he/she cannot pass the login phase to the authentication phase, that means this step represents as the step of authentication.

4.5 Denial of Service

This attacker causes the server rejects the logins of specific user until re-registration. That means making the user change password verification information in his smart card to another. As a result this attack prevents this user of communications facilities.

In our proposed scheme based smart card, the attacker needs the values of $ID_i$and pw_i, which are hidden in other information e.g., to get the value of ID_i the attacker need to know x_s which is not stored in smart card where $J_i = (x_s \parallel IDU)$, and in the pw_i he need to know L_i which is not stored in smart card and pw_iwhich is not stored clearly in verification server in addition to random number r_i which is stored securely in smart card where $L_i = J_i \oplus RPW_i$. So all of ambiguous values make the attack of denial of service is difficult.

4. 6 Forgery Attacks

An attacker attempts to manipulate sensitive data to impersonate as the legal user or server to access the resource on the remote system. As to compute the dynamic CID_i we do not only use XOR operation but also concatenate operation e.g., $pw_i$and ID_i where password hidden by RPW_i and ID_i by J_i using one-way hash function$h()$, it's difficult to extract ID_i by modify random number secret key x_s which contacted with$IDN = (ID_i \parallel N)$, which all of them compute with hash function$J_i = h(x_s \parallel IDU)$. And it's difficult to extract pw_i by modify random number r which hidden with clear pw_i in hash function$RPW_i = h(pw_i \parallel r)$. In the case of the attacker who obtains login request message $m = \{CID_i, T_i, d, C_1\}$, the modify$T_i$, d unavailing because the attacker need to obtain $x_s$to compute ID_i, and L_i to compute the clear pw_i for forgery the legal user.

4.7 Password Guessing Attack

It is difficult to guess the sensitive data of user e.g., password, username, because our proposed scheme based on smart card, hidden $pw_i$by $RPW_i$and ID_i byJ_i. In the case of the attacker who obtains request login massage by eavesdropping between Ui and S, he cannot obtain RPW_i and ID_i because need to obtain L_i andx_s.

4.8 Revocation of Smart Card

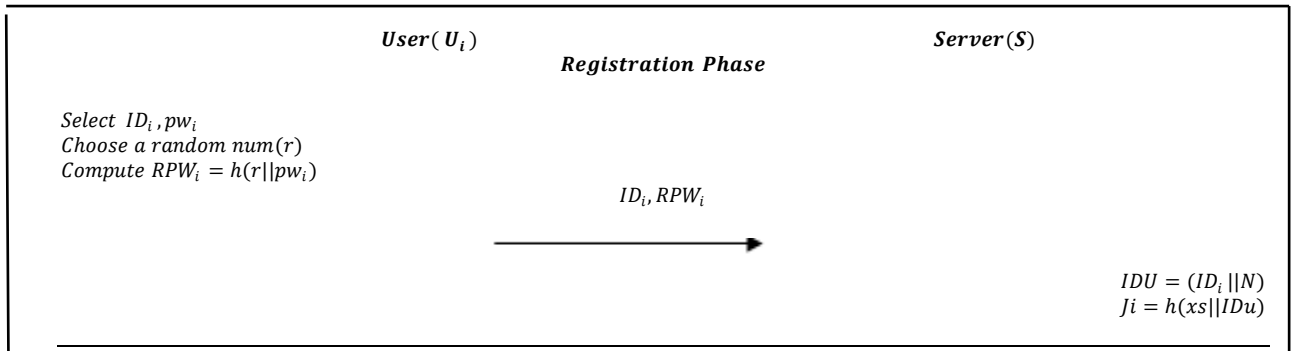
In our proposed scheme based on smart card, if registered user's smart card is stolen or lost, he can request the remote server to cancel his smart card by incrementing the value of N by one in its secure database, also an adversary who stole or theft smart card of a user wants to login into server, he cannot pass this phase unless to load fingerprint feature from his external advice that means addition of fingerprint feature robust to our proposed scheme based password.

4.9 Securely Chosen and Update Password

In our proposed scheme based on smart card , the user can freely choose password and include phase in which change the user's password without any hassle of contacting the remote server S and another one cannot change this password unless has valid ID_i and password of the smart card holder.

4.10 Mutual Authentication

To keep trust between U_i and S, our proposed scheme based on smart card is performed mutual authentication of both communication parties. Where the server S send $\{C_2, T_s\}$ to U_i and U_i calculated the value of C_2 by J_i which is only know to U_i and S.



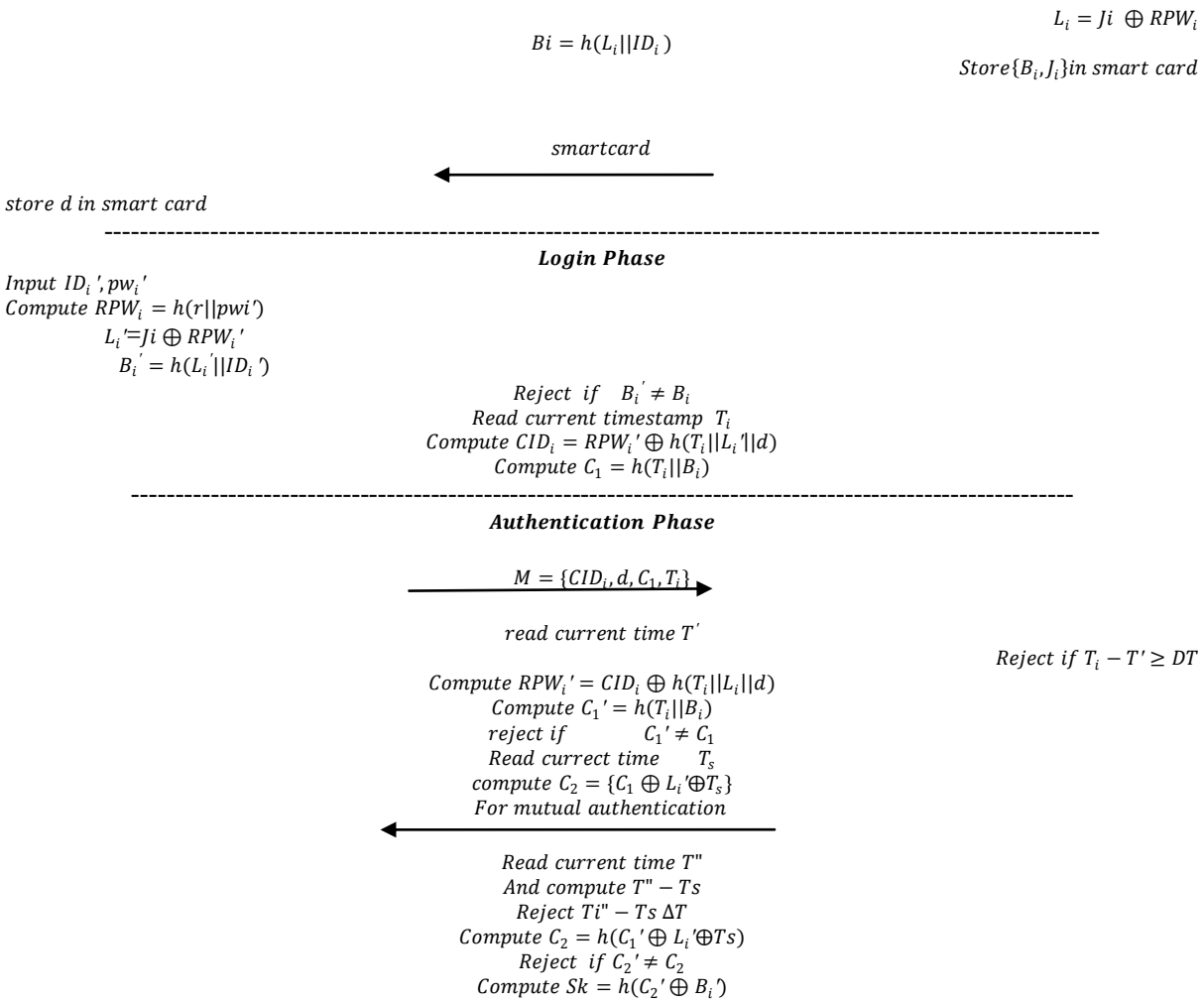


Fig.(1.1): Our proposed scheme based on smart card.

III. Result And Discussion

1. Comparison with Related Works

In this section**,** comparisons with related works which include three tables there are a comparison of computational cost, comparison of communication cost and analysis security feature.

1.1 Computational Cost: We compare our proposed schemes with six authentication schemes, including Das et al. (2004), Liao et al. (2005), Yoon and Yoo (2006), Liou et al. (2006), Wang et al. (2009), and Khan et al. (2011),it is depend on the results which existing in paper [10], in general Table (2) shown the evaluation parameters.

Table (2): Evaluation Parameters.

Symbol	Definition
T_h	Represents the execution time of the one-way hash function h(.)
$T_\oplus$	The execution time of the XOR operation
$T_\parallel$	Represents execution time of the concatenation operation.

The detail of comparison of computational for our proposed scheme based on smart card is explained in Table (3).

Scheme	Registration	Login and Verification	Total cost
Our scheme based on smart card	$4T \parallel +3Th + 1T\oplus$	$6T \parallel +7Th + 7T\oplus$	$10T \parallel +10Th + 8T\oplus$

Khan et al.(2011)	$3T \parallel +2Th + 1T\oplus$	$8T \parallel +10Th + 9T\oplus$	$11T \parallel +12Th + 10T\oplus$
Wang et al.(2009)	$2T \parallel +2T\oplus$	$8T \parallel +14T\oplus$	$10T \parallel +16T\oplus$
Liou et al. (2006)	$3T \parallel +5T\oplus$	$9T \parallel +12T\oplus$	$12T \parallel +17T\oplus$
Yoon et al.(2006)	$3T \parallel +3Th + 2T\oplus$	$21T \parallel +10Th + 3T\oplus$	$24T \parallel +13Th + 5T\oplus$
Liao et al. (2005)	$1T \parallel +2Th + 1T\oplus$	$9T \parallel +20T\oplus$	$1T \parallel +11Th + 21T\oplus$
Das et al. (2004)	$2T \parallel +1T\oplus$	$7T \parallel +14T\oplus$	$9T \parallel +15T\oplus$

Table (3): Comparison of computational for our proposed scheme based on smart card

From Table (3), it is noticed that computational cost of our proposed scheme based on smart card is less compared to computational cost of other schemes the Khan et al., Liou et al., Yoon et al. and Liao et al., despite of our proposed provides more security than other, whereas computational cost of Das et al.'s computational cost is the least but it provides least security compared to other schemes, as it is noticed there is no much difference between the Das et al. and Wang et al. schemes in terms of computational efficiency, but Wang et al. scheme is better than that of Das et al. in terms of performance, because it provides mutual authentication.

1.2 Communication cost: To compute these values ,it is assumed that the result size of secure one-way hash function is 128 bits, the lengths of IDs and PWs are 128 bits, with the sizes of timestamps and random numbers are 64 bits. The details of communication cost for our proposed scheme based on smart card is explained in Table (4).

Table (4): Comparison of communication cost for our proposed scheme based on smart card.

Scheme	Registration	Cost(bits)	Message	Cost(bits)	Total communication cost (number of bits)
Our scheme based smart card	$CIDi, Ti, d, Ci$	384	C_2, Ts	192	576
Khan et al.(2011)	$CIDi, Ti, d, Ci$	384	C_2, Ts	192	576
Wang et al.(2009)	$IDi, CIDi, Ni, T$	448	a', Tn	192	680
Liou et al. (2006)	$CIDi, Ei, T$	320	R, T	192	512
Yoon et al.(2006)	$CIDi, Ni, Ci, T$	448	D, Tn	192	680
Liao et al. (2005)	$CIDi, Ni, Ci, T$	448	D, Tn	192	680
Das et al. (2004)	$CIDi, Ni, Ci, T$	448	-----	192	448

From Tables (4) it is noticed that the communication cost of our proposed scheme based on smart card and our proposed scheme based on 3FA does not exceed the communication cost of Khan et al.'s scheme, and they are less compared to the Liao et al.'s, Yoon et al.'s and Wang et al.'s schemes, while it is noticed that the communication cost of Das et al.'s scheme is the least with 448 bits, because, it does not support mutual authentication.

1.3 Security Features: In general, Table (5) describes the security features, and Table (6) describes the comparison of security properties for our proposed scheme based on smart card with related works.

Table (5): Security Features.

Feature	Definition
C1	Forward secrecy
C2	User anonymity
C3	Smart card revocation
C4	Efficiency for wrong password login
C5	Freely chosen password by the users
C6	Secure password change
C7	No password reveal
C8	Mutual authentication

Table (6): Comparison of authentication schemes for our proposed scheme based on smart card.

Scheme	C1	C2	C3	C4	C5	C6	C7	C8
Our scheme based on smart card	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Khan et al.(2011)	No	No	Yes	No	Yes	Yes	Yes	Yes
Wang et al.(2009)	Yes	No	Yes	No	No	No	No	Yes
Liou et al. (2006)	No	Yes	No	No	No	Yes	No	Yes
Yoon et al.(2006)	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Liao et al. (2005)	No	Yes	No	No	Yes	Yes	Yes	Yes
Das et al. (2004)	No	Yes	No	No	No	Yes	No	No

IV. Conclusion

Remote user authentication has become an important technique that distributes environment in which the services are distributed and devices are untrusted. An efficient remote authentication, in which smart cards are based on multi-factors authentication.In present study, it is proposed scheme, which is based 2FA there are password and smart card, where it has been compared with related works which is include three parts there are computational cost, communication cost and security features.In computational cost, our proposed scheme based on smart card takes less computational cost compared to Khan et al.'s scheme where the total cost of our proposal equal to $10T \parallel +10Th + 8T\oplus$, while the total cost of Khan et al.'s scheme equal to $11T \parallel +12Th + 10T\oplus$. In communication cost, our proposed scheme based on smart card does not exceed the communication cost of Khan et al.'s scheme, where both of them equal to 576 bit.

Moreover, in security features we overcome the shortcoming of Khan et al.'s scheme, where we focus on user's anonymity, efficiency for wrong password login, forward key secrecy, and efficient of keys.

References

[1]. L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770–772.
[2]. M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28–30.
[3]. T. El Gamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (4) (1985)469–472.
[4]. ML. Das, A. Saxena, and V.P. Gulati, " A Dynamic ID-based Remote User Authentication Scheme", IEEE Trans. Consumer Electron., 50(2),(2004) 629-631.
[5]. I. Liao, I., C.-C. Lee ,M.-S. Hwang, " Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme", In Proceedings of the International Conference on Next Generation Web Services Practices, NWeSP'05, Seoul, Korea,(2005) 437–440.
[6]. E.J. Yoon, and K.Y. Yoo, "Improving the Dynamic ID-Based Remote Mutual Authentication Scheme", Proc.OTM Workshops, LNCS 4277,(2006) 499–507.
[7]. Y.P. Liou, J. Lin, and S.S. Wang, "A New Dynamic ID-Based Remote User Authentication Scheme Using Smart Cards", In Proceedings of 16_{th} Information Security Conference, Taiwan,(2006)198–205.
[8]. Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan," A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme", Computer Communications, 32(4),(2009)583–585.
[9]. M. K. Khan, S.-K. Kimb, and K. Alghathbar, " Cryptanalysis and Security Enhancement of 'a More Efficient & Secure Dynamic ID-based Remote User Authentication Scheme'", Computer Communications, 34,(2011)305–309.
[10]. R. Madhusudhan and R.C. Mittal, " Dynamic ID-based Rremote User Password Authentication Schemes Using Smart Cards: A Review", Journal of Network and Computer Applications,35, (2012)1235–1248.
[11]. H. Debiao, C. Jianhua, and H. Jin, " Weaknesses of a Dynamic ID-Based Remote User Authentication Scheme", International Journal of Network Security,13,(2011)58-60.
[12]. P. Kocher, J. Jaffe, and B. Jun," Differential Power Analysis", Proc. Advances in Cryptology (CRYPTO'99),(1999) 388–397.
[13]. S.T. Messerges, E.A. Dabbish, and R.H. Sloan," Examining Smart-Card Security Under The Threat of Power Analysis Attacks", IEEE Transactions on Computers, 51(5),(2002) 541–552.