International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 1– No.6, February 2012 – www.ijais.org

An Efficient and Secure ID-based Remote User Authentication Scheme using Smart Card

Ram Ratan Ahirwal
Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha (M.P.) 464001 India

Swarn Sanjay Sonwanshi
Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha (M.P.) 464001 India

ABSTRACT

The User Authentication mechanism technology has enjoyed strong growth in recent year, but security threats and facing attacks in authentication have grown equally fast. Today, there are many potential attacks that are targeted at authentication including insider attack, masquerade attack, server spoofing attack, parallel session attack, offline password guessing attack and many more. Recently, In 2010 R. Song proposed advanced smart card based password authentication protocol with such non-tamper resistant smart card based on symmetric key cryptosystem as well as modular exponentiation. R. Song et al Scheme is vulnerable to the offline password attack, insider attack; forward secrecy and denial of service attack are cryptanalyses by W B Horng. In this article, we will propose an efficient ID-based authentication scheme which can avoid all type of security flaws. The functionally, performance and security analysis show that our proposed scheme is feasible in terms of computation cost, storage capacity and the scheme can resist server attack.

Keywords

Password authentication, smart card, network security, one-way hash function

1. INTRODUCTION

In an insecure network environment, User authentication is an important component of security. Remote user authentication mechanisms are used to verify the validity of the user login request. The first user authentication scheme introduced by Lamport [1] in 1981, in which the remote server should authenticate the remote user based on identity and password over an insecure network .In this scheme, the remote server must maintains a password table for verifying legal user. This password table makes Lamport's [1] scheme vulnerable to a stolen verifier attack, if the attack is capable of accessing the server password table.

The Revolution changed to storing password in verifying password table in server. In 2002 Hwang et al. [2] proposed a remote user authentication scheme, which does not require any password table in the remote server; moreover any legal user could choose and change their password freely without the help of the remote system. Hwang [2] claimed that it scheme provided an efficient authentication and required much fewer computations then other scheme. While Yoon and Yoo et al.[3] in 2005, cryptanalysis their scheme, previously generate user's secret hash values are insecure if the server secret key is prevail to real world, and also when

Smart card is stolen. An unauthorized user can easily change new password of the smart card.

In 2004, M.L. Das et al. [4] proposed a dynamic ID-based remote user authentication scheme and they claimed their scheme protect user anonymity from the adversary. While in 2005 Chien and Chen al et [5] point out that in das et al.'s scheme user Ui sends the data (Cid,Ni,Ci,T) to the remote server. In each login request, although the Cid dynamically changes every time, the value Ni is same and unique to each user. So that das al et scheme failed to protect the user antonymic. In addition, Liao lee and Hwang et al. [6] Point out the Das et al's [4] could not protect against password guessing attack .password could be revealed by remote system and it could not achieve mutual authentication .Chien and Chen al et. [5] Also proposed a mutual authentication scheme to preserve user anonymity based on modular exponentiation. This efficient is low. In 2007 Hu [8] found the Chien and Chen's [5] scheme is vulnerable to strong masquerade user or server attack, insider attack, replay attack and denial of service attacks and improved it to avoid these weakness. In 2009, Xu et al. [9] presented an authentication scheme using such non-tamper resistant smart card based on costly modular exponentiation. However R. Song [10] point out Xu et al. [9]'s scheme is vulnerable to the user impersonation attack. In 2010, he introduced a new and more secure authentication scheme based on symmetric key cryptosystem and modular exponentiation. However W. B. Horng -Cheng [12] demonstrates that R. Song et al. [10] scheme is vulnerable to the offline password guessing, insider attack, denial-of service and proposed scheme does not provide perfect forward secrecy for session keys.

In 2011, Chun-Ta Li and Cheng-Chi Lee [15] present a robust remote user authentication scheme using smart card. They claim that their proposed scheme is provide better authentication process and resistance to all possible attacks. But in this scheme is not provide security to the denial-of-service attack. Moreover, in 2011 E.J Yoon and K.Y Yoo [17] demonstrated that Jia's [16] remote authentication scheme is vulnerable to insider attack, forgery attack and server spoofing attack. They point out jia's scheme does not provide mutual authentication between user and server.

In this article, we shall present a secure and an efficient ID-based remote authentication scheme with mutual authentication and session key agreement. Moreover our scheme provides the user to choose and change their password by their own choice. In contrast, The propose scheme can resist masquerade, insider attack, parallel session attack, server spoofing attack, Further provides security analysis to compare with other published scheme. By performance analysis, the propose scheme is shown to be very efficient both in the storage and computation cost.

The reminder of the article is organized as fallows. In section 2 reviews of R. Song and its drawback. In Section 3 we Introduce our efficient and secure ID-based user authentication scheme, and we discuss the security analysis in session 4, compare the performance and efficiency of the propose scheme with other related scheme in session 5.and finally concludes the paper in Section 6.

2. REVIEW OF R. SONG's SCHEME

In the section, we are going to review R. Song [10] scheme "Advanced smart card based password authentication Protocol", and security weakness of its [12]. The Security of R. Song et al. Scheme depends on hybrid approach using both symmetric key cryptosystems and modular exponentiations. Their scheme consist of five phases: Initial phase, registration phase, login phase, verification phase and password change phase. [12]

1. Initial Phase-

Server Si selects two large prime numbers p and q such that $p = 2q + 1$ and choses a secret key "x". Server keeps both p and x secret. Then S selects a symmetric key cryptography algorithm with encryption Ek (.) and decryption Dk (.) a secure one way hash function.

2. Registration Phase-

User Ui submits his/her Identity IDi and Password PWi to the remote server through a secure channel for registration. Upon receiving the registration request, it computes A = h (ID^X mod p) $\oplus$ h (PWi). Then Si issues a smart card to Ui containing (IDi, Ai, h (.), E (.)} over a secure channel.

3. Login Phase-

User Ui wishes to log on the remote server Si; he/she must insert the smart card into card reader and type his Identity ID and password PWi. The card reader first generates a random number R. and gets the current timestamp Tu. Then it computes $K = A \oplus h(PWi)$, $W = EK(R \oplus Tu)$, and $Cu = h(Tu || R || W || ID)$. Where EK is the symmetric key encryption operation with the key K, Finally the smart card sends the login request message {IDi, Cu, W, Tu} to Server Si.

4. Authentication Phase-

Upon receiving the login request from user Ui at time T' the server Si first checks validity of the identity IDi and (T'-Tu) $\leq \Delta T$, where ΔT is a predefined transmission delay. If it is fail, the request is rejected else it consider for next step. The server Si computes K= h (ID^X mod p) and R' = DK (W) Tu and checks whether Cu = h (Tu || R' || W || ID). If they are equal, the user U is authenticated, then server computes Cs= h (ID ||R' ||Ts) and sends the reply massage {ID, Cs, Ts) to user Ui. Where, Ts is the current timestamp.

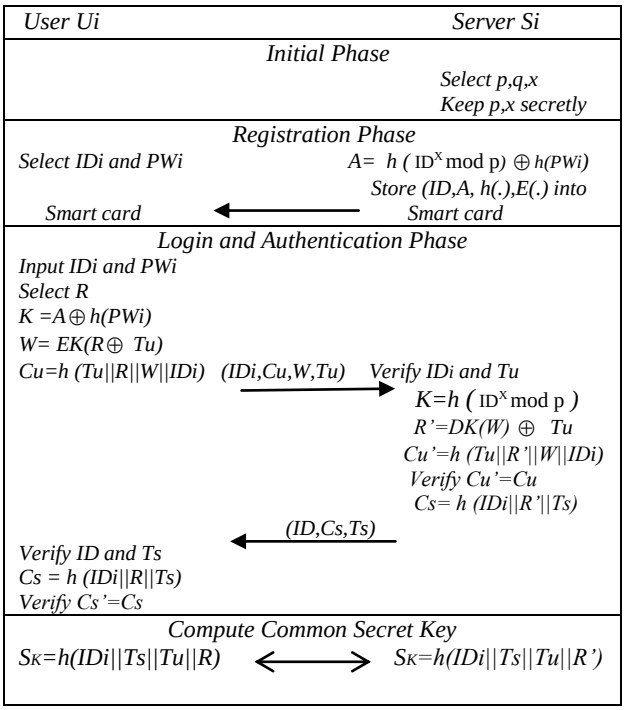

Figure1. R. Song's scheme

Upon receiving the relay massage from Si, the card reader checks the validate ID and freshness of Ts. Then compute h (IDi || R ||Ts) and checks Cs = h (IDi || R || Ts). If they are equal, the server is authenticated. After both user and server authenticated each other, they compute a common shared secret session key SK=h (IDi || Ts || Tu || R).

5. Password Change Phase-

User Ui is allowed to change his/her password from PW into PW'. He/she insert smart card into card reader and type IDi and PWi. Then, a mutual authentication between the server Si and the smart card is performed first. Then authentication is complete. The smart card asks Ui to enter a new password PW'. Then, it computes A' = A $\oplus$ h (PW) $\oplus$ h (PW') and replaces A with A'.

2.1 Security Analyses of R. Song

In this session, we show that R. Song's scheme will suffer from offline Password guessing Attack, Insider Attack and denial-of- Service Attack [12]. Moreover, R. Song's scheme does not hold the perfect forward security. [13]

2.1.1) Denial-of-Service Attack

If adversary can used to invalid ID and PW, and wants to send login request massage continuously to keep server busy, this attack is known as Denial-of-service attack. In R. Song scheme, adversary Ui inserts the smart card into card reader and keys in invalid IDi and PWi. Card reader generates an invalid login request and sends it to authenticate authority 'server'. The same process is repeated continuously by many other adversaries to overload the server. This holds the server accessibility for the valid users.

2.1.2) Insider Attack

In R. Song scheme, if an authorized insider (system manager) of the server Si knows the user's password, because server is receive User's IDi and PWi in plaintext form during

registration phase. He may try to impersonate Ui as a registered user.

2.1.3) Offline password Attack

The offline password guessing attack must satisfy two conditions. First user's password is not strong, and existence information's related to password are easily available. In R. Song's scheme, if an adversary has retrieved A stored in User's smart card and has intercepted one of previous login massage {IDi, Cu, W, Tu} transmitted between user and server.

Then the adversary can mount an offline password guessing attack. He first guesses a new password PW* and compute K= A⊕ h (PW*), then it calculated R*= DK (W) ⊕Tu and checks whether h (Tu || R* || W || IDi) =Cu or Cs= h (IDi || R* || Ts). If they are equal, the guessed password PW* is correct. Otherwise, continuous next guess until they are equal.

2.1.4) Forward secrecy

One of the important security properties is perfect forward secrecy. In R. Song's scheme security depends on encryption key K = h (ID^X mod p). This key is used to encrypt the login request such as W= EK (R Ts). Consider first case, if an adversary is previous insider (such as system manager), gets server secret key x, and large prime p and intercepts the massage (IDi, Cu, W, Ts) and (IDi, Cs, Ts) during login/ authentication process between user and server. An adversary can easily compute K = h (ID^X mod p), R = DK (W) Tu and session key Sk= h (IDi || Ts || Tu || R). Once he is successful in constructing an encryption key K, all future communication requests are readable. And second, if user's password PWi is compromised. Assume that if the adversary can retrieve A stored in user's smart card and intercepts previous login massage (IDi, Cu, W, Ts) and reply massage (IDi, Cs, Tu), then the adversary can easily compute the session key Sk =h(IDi, Ts, Tu, R) by computing K = A h(PWi) and R= DK (W) Tu . Therefore the R. Song's scheme is weak in perfect forward secrecy.

3. OUR PROPOSED SCHEME

In this section, we present a secure and an efficient ID-based remote user authentication protocol with smart card. We use one-way hash function and Bitwise XOR operation in this proposed scheme. Which execution time is extremely very low to compare to using Modular exponentiation. Our proposed scheme doesn't use any common key for encryption and decryption algorithm. Using one-way Hash function, it's computationally infeasible to invert operation. This scheme has four phases. 1-Registration phase 2-Login phase 3-authentication/verification phase and 4-password change phase. The flow diagram of our proposed scheme is shown in figure 2. The notations use in proposed scheme and phases are describe below-

The Notations

U – Remote User
ID – Identity of User
PW– password chosen by User
S– Remote authentication Server
X– Permanent secret key of S
H (·) – One-way hash Function
⊕ – Bitwise XOR operation
|| – concatenation

3.1 Registration Phase- In the registration phase, User Ui wants to register himself/herself in remote server S. Firstly User chooses his/her ID and PW. Before register on Server, registration authority computes h (ID) and h (ID||PW) and sends to remote server S over a secure channel. Upon receiving the registration request from User Ui. Server S computes same parameters related to the User Ui.

S computes $Ai = h(ID) \oplus h(X \,||\, h(ID))$

$$Bi = Ai \oplus h(ID \,||\, PW)$$
$$Ci = h(Ai)$$
$$Di = h(ID \,||\, PW) \oplus h(X)$$

And stored some of them in the smart card memory and issues this smart card to User Ui. This smart card is delivered to User Ui through a secure channel.

3.2 Login Phase- This phase provides the facility of a secure login to the user .User wants to access same services on remote server S. first it gain the access right on the remote server S. User Ui inserts the smart card to card reader and keys in ID* and PW*. The card reader computes –

$$Ai^* = Bi \oplus h(ID^* \,||\, PW^*)$$

And $Ci^* = h(Ai^*)$ and checks whether Ci (stored in the smart card memory) and Ci* are equal or not. If not, terminate to again login process. Otherwise yes, User Ui is legitimate bearer of the smart card. Then the card reader generates a random nonce Ri and computes –

$$Ei = Ai^* \oplus Ri$$
$$Cid = h(ID \,||\, PW) \oplus Ri$$
$$Fi = h(Ai \,||\, Di \,||\, Ri \,||\, Tu)$$

Where *Tu* is current time when login request proceed. And send the login request massage *{Fi, Ei, Cid, Tu, h (ID)}* to remote server S.

3.3 Verification Phase- Upon receiving the login request massage *{Fi, Ei, Cid, Tu, h (ID)}*. Server verifies the validity of time delay between *Tu*' and Tu. Where *Tu'* is the travel time of the massage.

$Tu' - Tu \leq \Delta T$ where ΔT denotes expects valid time interval for transmission delay.

Then server accepts the login request and go to next process, otherwise the server reject login request.

Server computes –

$$Ai^* = h(ID) \oplus h(X \,||\, h(ID))$$
$$Ri^* = Ai^* \oplus Ci$$
$$G = h(ID \,||\, PW)^* = Cid \oplus Ri$$
$$Di^* = h(ID \,||\, PW)^* \oplus h(X)$$

And computes $F^* = h(Ai^* \,||\, Di^* \,||\, Ri^* \,||\, Tu)$

And checks whether F and F* are equal or not. If they are not then reject the login request. If equal, then server S

Computes–

$$Fs = h(h(ID) \,||\, Di \,||\, Ri \,||\, Ts)$$

Where, *Ts* is remote server current time. And send acknowledge massage *{Fs, G, Ts}* to user Ui.
Upon receiving acknowledge massage smart card compute

$$G^* = h(ID \,||\, PW)$$
$$Fs^* = h(h(ID) \,||\, Di \,||\, Ri \,||\, Ts)$$

And checks where $G = G^*$ and $Fs = Fs^*$ are same or not. It is mutual authentication process. In which both Server and User verify to each other. If they are same then card reader makes session key (*Sk*) and both Server and User share it.

$$Sk = h(h(ID) \,||\, Ts \,||\, Tu \,||\, Ai)$$

Otherwise terminate to again login process.

3.4 Password change Phase- This phase is involved whenever User U want to change the password PW with a new Password *PWnew* .User U inserts the smart card to the card reader/client machine and keys in ID* and PW* and request to change password. The card reader checks whether C = C* are equal or not. If it is satisfy User U is a legitimate bearer of the smart card. Then the card reader asks the User Ui to input new password *PWnew*. After entering the new password the card reader calculate-

$$Bnew = Ai \oplus h(ID \,||\, PWnew) \text{ and}$$
$$Dnew = h(ID \,||\, PWnew) \oplus h(ID \,||\, PW) \oplus Di$$

And change B with *Bnew* and D with *Dnew* in smart card memory.

4. SECURITY ANALYSIS OF PROPOSED SCHEME

In this section, we analyze the security of our proposed scheme against all possible attacks. We just use one-way function and XOR operation to develop our scheme. The secure one-way function h (.) protects X server secret key, ID and PW since it is computationally infeasible to invert one-way function .It can resist the well-known attacks. In the paper, we not only concern with the specialties and the efficiency of our scheme, but also discuss for security and the computation complexity, storages capacities in our proposed scheme.

The security analysis is listed as fellow.

1) Resistance to Stolen smart card Attack-

Proof: In case a legitimate user losses his/her smart card. The adversary cannot use this card without knowing the valid password, and if adversary extracts information in its memory {*Bi, Ci, Di,*}. He cannot retrieve ID and PW, because it is computationally infeasible to invert the one-way hash function h (.) and without knowing the Server secret key X. The adversary can guess ID and PW correctly at the same time. It is not possible to guess out two parameters correctly at the same time. Therefore the proposed scheme is secure against stolen smart card attack.

2) Resistance to Denial-of- service-

Proof: In the proposed scheme, an adversary can used to invalid ID and PW, and wants to send login request massage continuously to keep server busy. This leads to denial-of-service attack. But he cannot send login request massage because in login phase, smart card reader checks the verification of smart card and correct password.

$$Ai^* = Bi \oplus h(ID^* \,||\, PW^*)$$
$$Ci^* = h(Ai^*) \text{ and check } (Ci = Ci^*)$$

Ci stores in smart card. Therefore, it's also resistance to denial-of service.

3) Resistance to Insider Attack-

Proof: If a privileged insider of the Server S obtains the smart card's secret information {*Bi, Ci* and *Di*} from user Ui. He cannot extract sensitive information like {*ID, PW, Ai* and *Di*} from *Bi, Ci* and *Di*.

$$Bi = Ai \oplus h(ID \,||\, PW),$$
$$Ci = h(Ai) \text{ and}$$
$$Di = h(ID \,||\, PW) \oplus h(X)$$

Because it is computationally infeasible to invert the one-way hash function h (.) and also he cannot extract Ai from Bi without the knowing of ID and PW.

4) Resistance to Parallel Session Attack-

Proof: if the attacker can masquerade as legitimate user *Ui* by a replaying a login request massage *{Fi, Ei, Cid, Tu, h (ID)}* with in the valid time frame window But attacker cannot compute the knowledge massage { *Fs, G, Ts*} because knowledge massage does not contains any information to construct next process.

$$G = h(ID \,||\, PW)^* = Cid \oplus Ri$$
$$Fs = h(h(ID) \,||\, Di \,||\, Ri \,||\, Ts)$$

Hence the proposed scheme is secure against parallel session attack.

5) Resistance to Replay Attack-

Proof: Suppose attacker intercepts the login request massage *{Fi, Ei, Cid, Tu, h (ID)}* from User U, and can replay the same massage to server, it is useless because the card reader used the current time stamp value "Tu" in each new login request,

$$Fi = h(Ai \,||\, Di \,||\, Ri \,||\, Tu)$$

This makes the "Fi" to be dynamic and valid for small time interval. Hence the proposed scheme is secure against massage replay attack

6) Resistance to Offline password guessing Attack: -

Proof: In the proposed scheme, if an adversary wants to guess the password. It can be prove to be impossible. Smart card is store with three values (*Bi, Ci* and *Di*). An adversary cannot guess valid "ID" and "PW" for computes

$$Bi = \{Ai \oplus h(ID \,||\, PW)\} \text{ and}$$
$$Di = \{h(ID \,||\, PW) \oplus h(X)\}.$$

Because it is impossible to guess right "ID" and "PW" in same time. All four phase has protected the "ID" and "PW" with one-way function h (.), which computationally infeasible to invert. If attacker know user's "ID", it's cannot extract *h (ID || PW)* without knowing server secret key.

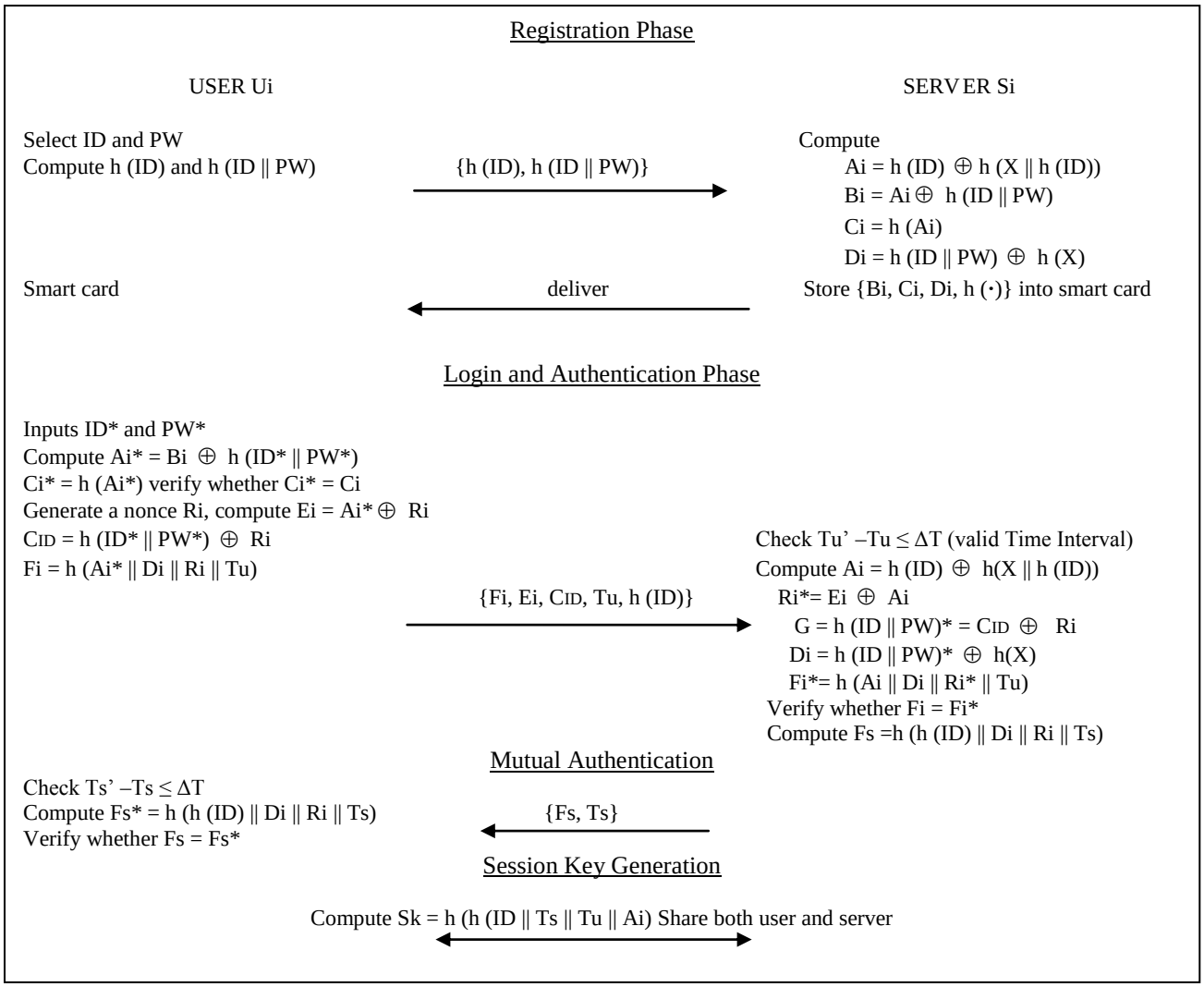

Figure 2. The Proposed Scheme

7) Leak of Server secret key: -

Proof: Unfortunately, if Server secret key "X" is prevail from Server S. The attacker cannot retrieve "ID" and "PW" from

$Di = \{h (ID || PW) \oplus h(X)\}$,

Because of using one-way function h (.), Server can easily Change and modify its secret key "X", and restore again in smart card.

8) Resistance to Server spoofing Attack: -

Proof: In the server spoofing attack, an attacker cannot masquerade as a legal server, because it cannot compute Ai, Bi and Di without knowing "ID", "PW" and X.

$Ai = \{h (ID) \oplus h(X || h (ID)\}$,

$Bi = \{Ai \oplus h (ID || PW)\}$ *and*

$Di = \{h (ID || PW) \oplus h(X)\}$

Moreover, malicious server cannot compute the session key *Sk= (h (h (ID) || Ts || Tu || Ai)* without knowing "*Ai*", and the session key is different for same user in different login session. Hence the proposed scheme is secure against server spoofing attack.

5. PERFORMANCE ANALYSIS AND COST COMPARISONS

From using the lightweight hash function and XOR operation, the proposed ID-based authentication scheme is very efficient. It is usually neglected considering its computation cost. We assume that secret server key X, ID, PW values and output hash function are all 160 bit long. If we use Secure hash function(SHA-I) implement each of the value is 160 bit long, time stamps are 40 bit length and identity by 32 bit long.

Table 1 shows, the storage comparison of the proposed scheme with the relevant user authentication based on smart card, Which shows our proposed scheme is reduced burden on the server, because the Server has store only server secret key (X).

Table 1. Storage Capacity Comparison

Storages /Scheme	Our Scheme	Yoon Yoo al et. [3]	Liou al et. [7]	R.Song al et.[10]
Smart Card	480 bits	480 bits	480 bits	320 bits
Server	160 bits	320 bits	320 bits	480 bits

Table 2 shows, the computation cost comparison of our proposed scheme with other related scheme. The computation cost is defined as the total time of various operation executed in each processes. The execution times for one-way hash function denote as "Th" and exclusive-OR operations require as very low execution time, it does not consider its computation cost. The modular exponential operation denotes as "Tm". The time complexity associated with the different operations can be express as

Exclusive OR << Th< Tm

Table 2. Computation cost caparisons

Phase/ Scheme	Our Scheme	Yoon Yoo et al. [3]	Liou et al. [7]	R.Song et al.[10]
Registration	4 Th	3 Th	3 Th	1 Tm + 1Th
Login	7 Th*	4 Th	5 Th	4 Th
Authentication	5 Th	4 Th	5 Th	1 Tm + 3Th

*The proposed scheme requires little more computation cost and equal to related user authentication scheme, Because our proposed scheme has strong secure mutual authentication scheme is resistance to insider attack, resistance to masquerade attacks, parallel session attack, replay attack, password attack, secure password change, protecting server spoofing attack, session key generation and agreement and other possible attack, that why some cost of execution are little more. Table 3 shows, the communication cost of the proposed scheme with the relevant user authentication based on smart card, which shows communication cost weightage between user and server in term of authentication.

Table 3. Communication Cost

Communication/Scheme	Our Scheme	Yoon Yoo et al. [3]	Liou et al. [7]	R.Song et al.[10]
Authentication (bits)	5*160	5*160	6*160	5*160

Moreover, the efficiency comparison among our proposed scheme and other previously proposed scheme are shown in Table 4. It shows resistance to aforementioned attacks in various processes. Our proposed scheme is secure in all phase, and related scheme are fail to resist attacks. This is mostly requiring for security enhancements in our proposed scheme.

6. CONCLUSION

In this paper, we review the authentication scheme proposed by R. Song is not secure enough against same weakness in section 2. We showed that his scheme is vulnerable to Denial-of-Service attack, Insider attack, Offline password attack Forward secrecy attacks. We present an efficient and secure ID- base remote user authentication scheme with smart card in section 3. Our proposed authentication scheme can satisfy all the requirements needed for achieving secure user authentication scheme with smart card. The proposed scheme is proved to be able to withstand the various possible attacks in session 4. In addition, through performance analysis and efficiency comparisons our scheme is better than with R.Song et al [10], Liou et al. [7] and Yoon Yoo et al. [3] in section 5. The efficiency of the proposed algorithm is very high because it is not involved in any time consuming modular exponential computing. In future, we invite to more secure, low cost and resist to all attacks authentication scheme with smart card.

Table 4. The Efficiency Comparison

Resistance to / Scheme	Our Scheme	Yoon Yoo et al. [3]	Liou et al. [7]	R.Song et al.[10]
Insider attack	Yes	No	Yes	No
Masquerade attack	Yes	No	Yes	Yes
Parallel session attack	Yes	No	Yes	No
Replay attack	Yes	Yes	Yes	No
Offline password attack	Yes	No	Yes	No
Secure password change process	Yes	Yes	Yes	Yes
Denial of service	Yes	No	Yes	No
Session key generation and agreement	Yes	No	No	Yes

7. ACKNOWLEDGMENT

The authors are thankful to Samrat Ashok Technological Institute, Vidisha (M.P.) India for extending their supports in this article.

8. REFERENCES

[1] L. Lamport, 1981 "Password authentication with insecure communication". Communications of the ACM, vol.24, no.11, , pp 770-772

[2] M. S. Hwang and L. H. Li. 2000 "A new remote user authentication scheme using smart card", In IEEE Transaction on consumer Eleclronic,"vol.40, no 1, pp 28-30.

[3] E. Yoon and Yoo, 2005 "More efficient and secure remote user authentication scheme using smart card", in proceeding of 11th international conference on Parallel and Distributed System, pp.73-77

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

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

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

[7] Y.P. Liou, J. Lin and S.S. Wang, 2006 "A New Dynamic ID Based Remote User Authentication Scheme using Smart Cards," Proc. 16th Information Security Conference, Taiwan, pp. 198-205, July.

[8] L.I.Hu, X.X. Niu, and Y.X. Yang, 2007 "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.

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

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

[11] Sandeep K. Sood, Anil K.Sarje and Kuldip Singh, 2010 "Secure dynamic identity-based remote user authentication scheme", Distributed Computing and Internet Technology, Lecture Notes in Computer Science, vol. 5966, pp. 224-235.

[12] W B Horng and Cheng p Lee, 2010 "Security weaknesses of song's advanced smart card based Password authentication Protocol."IEEE trans. Computer, vol.978-4244-6789 1/10,

[13] R S Pippal, Jaindhar C D, 2010"Comments on Symmetric Key Encryption based smart card authentication scheme". ICCTD 2010 IEEE vol. 978-1-4244-8845-2/10/2010

[14] William Stallings, "Cryptography and Network Security", *4/E*. Prentice Hall.

[15] Chun-Ta Li and Cheng-Chi Lee, 2011 "a robust remote user authentication scheme using smart card," Information Technology and Control, Vol.40, No.3 ,

[16] Z. Jia, Y. Zhang, H. Shao, Y. Lin and J. Wang 2006, "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.

[17] Eun-Jun Yoon, and Kee-Young Yoo, 2011, "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).