I. J. Computer Network and Information Security, **2016, 10, 45-52**
Published Online October 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.10.06

A New Approach for Remote User Authentication in a Multi - Server Environment Based on DYNAMIC-ID using SMART-CARD

Shanu Gaharana
Hindustan Institute of Technology and Management, Agra, 282007, India
E-mail: shanugaharana@gmail.com

Darpan Anand
Hindustan Institute of Technology and Management, Agra, 282007, India
E-mail: darpan.anand.agra@gmail.com

Abstract—Internet and Communication Technologies operates widely in a multi-server environment. Authentication is one of a primary concern in multi-server environment. There are so many remote user authentication schemes using smart cards that operate in multi-server environment. But there are some authentication bottlenecks that these schemes suffer from. We have analyzed some schemes on the grounds of some specific security requirements and goals. In this paper, we propose a scheme that integrates key exchange and session key agreement in one phase and also supports traceability feature and resists denial of service attack.

Index Terms—The Internet and Communication Technologies (ICT), multi-server environment, dynamic Id, traceability, denial of service, authentication.

I. Introduction

The Internet has become an essential part of our daily life. We are living in an era, where we are surrounded by Internet and Communication Technology (ICT).The expeditious burgeoning of technology and the internet, is leading to the Internet of Things (IoT)[1] which is all about the proposed development of ICT in such a way that everyday objects are connected and allowed to send and receive data and information. Such a progressive scenario comes up with the concerns of security. Security involves ensuring confidentiality, integrity and availability of data [2].Authentication is a process in which an entity proves itself to be the one that it actually claims to be. In 1981, the classic technique is password based for authentication, which uses a one-way hash encryption function and it was proposed by Leslie Lamport [3]. However, this scheme could not resist interpolation attack [4]. To overcome the weakness of maintaining the verification table[5], Chang and Wu presented a new remote user password authentication scheme by using smart cards [6]. This scheme eliminated the need of maintaining verifier table. Several schemes and improvements [7]-[9] have been proposed, but these schemes were based on static login identity. The use of static login identity was found to be leaking some partial information in many applications and it is necessary to protect the partial information because an attacker may use this information to launch an attack. M.L. Das et. al. presented a new concept of dynamic ID based remote user authentication scheme [10] and later many schemes were developed that were based on the concept of dynamic identity [11]-[13]. In conventional user authentication schemes, a user is required to log into various remote servers by registering again and again and also he/she is supposed to remember the various user identities and passwords. Considering this problem in mind, Lee and Chang proposed a user identification and a key distribution scheme based on the difficulty of factorization and hash function for multi-server environment [14]. In multi-server architecture oriented schemes, the user is registered once in a registration server and can use all the permitted services on remote servers using single ID and password. Liao & Wang proposed a dynamic Id based remote user authentication scheme for multi server environments [15] where the user's identity changes dynamically in each session and this scheme was claimed to resist various attacks and achieve mutual authentication. Cheng Chi Lee et. al. proposed a scheme with the anonymity that can resist several attacks, but it was lacking in mutual authentication[16]. In 2012, S. S. Baboo and K. Gokulraj introduced a dynamic authentication scheme, which included a number of factors such as the password, password index, and date of modification are important factors, which decide the dynamicity in authentication. The basic idea behind this approach was vulnerability of static approach authentication schemes to different types of attacks in networked communication[17]. Xiong Li et. al. presented a scheme which was designed in order to protect the user from being tracked[18]. Kaiping Xue et. al. proposed dynamic pseudonym identity-based authentication and key agreement scheme that provides traceability and identity protection[19]. Hari Om et al proposed a method based on a 3-D Geometric approach, to authenticate the login request sent by a user located at

far distance [20]. Leu and Hsieh presented a comparatively more secure and practical scheme that uses few hashing operations in its implementation [21].

In this paper, we present an algorithm that not only eliminates the risks associated with the studied algorithms but also is reliable.

The rest of this paper is organized as follows. Section II describes the related work and Section III describes the proposed scheme. Section IV discusses the analysis of the proposed scheme and also presents the comparative analysis of the proposed scheme with other studied schemes. Finally, conclusions are given in Section V.

II. Related Work

This section presents a review of some dynamic Id based remote user authentication techniques operative in the multi server environment that we have studied and analyzed. There are some general notations used in the paper as explained in Table 1.

Table 1. General Notations used in Paper

S.N.	SYMBOL	DESCRIPTION
1	ID	Identity of User
2	PW	Password of User
3	h(.)	Hash function
4	$\oplus$	Bitwise XOR operation
5	||	Concatenation operation
6	y	Secret value of server(to be stored on the smart card)
7	x	Secret value of server
8	SID_j	Service Providing Server's identity

A. In Cheng Chi Lee Scheme [16], there are three participants involved:

- The User (U_i),
- The Service Providing Server (Sj)
- Registration Center (RC).

RC selects the master key x and a secret number y to compute h(x||y) and h(y) and then it shares h(x||y) and h(y) with S_j through a secure channel. The master secret key x and secret number y are known to RC only.

The scheme does not support traceability and also if an attacker will try to replay the login message $\{P_{ij}, CID_i, Q_i, N_i\}$ then S will compute $T_i, B_i, A_i, Q_i and\ M'_{ij}$ but M''_{ij} would not get verified by the and so replay attack won't succeed, but meanwhile if, several replay attacks occur, then the server will become busy in unnecessary computations leading to denial of service.

B. In Xiong Li, Jian Ma et al Scheme [17], three participants are there:

- The User(U_i)
- The Service Providing Server(Sj)
- Registration Center(RC)

RC selects the master key x and a secret number y to compute h(x|| y) and h(SID_j||h(y)) and then shares them with S_j through a secure channel.

An attacker will try to replay the login message $\{P_{ij}, CID_i, M_1, M_2\}$ then,the RC will compute $N_i, E_i, D_i, B_i, A_i, M_3\ and\ M_4\ but\ M_3$ does not get verified and so replay attack won't succeed, but during this time if several replay attacks are caused then it will make the registration server busy leading to denial of service.

C. In Kaiping Xue et al Scheme[18], there are three participants:

- The User (U_i)
- The Service Providing Server (S_j)
- Control Server (CS).

The scheme provides the unique feature of traceability which supports tracing the user's identity at the control server during the verification phase.

D. In Leu and Hsieh Scheme [19], a random number is used to represent the identity indirectly, which in turn results in difficulty to guess a random number rather than a logical identity. There are three participants in the scheme:

- The User (U_i)
- The Service Providing Server(Sj)
- Registration Server (RC)

RC selects the master key x and a secret number y to compute h(x||y) and h(y)parameters and then RC shares them with service providing server (Sj) through a secure channel. The master key x and a secret number y are known to RC only.

The password is not transmitted to the server in a plain text format and so an insider cannot easily perform an attack. But let a malicious insider user (U_f), possessing a legitimate smart card, can directly get h(y)from the elements stored in the smart card. The attacker U_f first computes T_f, B_f *and* V_f as:-

$$T_f = h(ID_f \parallel x)$$

$$V_f = T_f \oplus h\left(ID_f \parallel h(b_f \oplus PW_f)\right)$$

$$B_f = h(h(b_f \oplus PW_f) \parallel h(x \parallel y))$$

T_f, B_f, V_f and h(x // y) can be obtained by brute force attack. By knowing these two values, the attacker can perform eavesdropping attacks to find the session key shared among any other users, the related service providing servers and RC. An attacker will try to replay the login message $\{P_{ij}, CID_i, Q_i, N_i\}$ then S will compute $T_i, B_i, A_i, Q'_i and M_{ij}$. But M_{ij} does not get verified and so replay attack won't succeed, but during this time if several replay attacks are caused then it will make the server busy leading to denial of service.

III. Proposed Scheme

On the basis of analysis and thorough review of various schemes, we have identified that all the reviewed schemes provide identity protection, session key agreement and a separate phase for password update or change. Masquerade attack cannot be performed on all the schemes, except on the Leu and Hsieh scheme. A replay attack is only possible on the C.C. Lee scheme, but the rest of the schemes are safe from it as they make use of either timestamp or nonces.

Therefore, it is necessary to give a sight on these goals for future research and develop an algorithm that satisfies all the security requirements and attains all the goals. There are some requirements that an ideal password authentication scheme should hold the line against.

On the basis of analysis and thorough study of various schemes, we have developed our new scheme. Our scheme consists of three entities:

- The User (U_a),
- The Service Providing Server (S_j) and
- The Control Server (CS).

The CS is considered to be a trusted party. The CS selects the master key x and the secret number y. The scheme contains following phases:

- The Initialization and Registration Phase
- The Login and Verification Phase
- The Password Change Phase

A. The Initialization and Registration Phase:

When a user U_a wishes to access the services, he/she has to submit his/her identity ID_a and password PW_a to the CS. There are following steps:-

Step R1: $U_a -> CS: ID_a, A_a, b.$

The user U_a freely selects his/her identity ID_a, password PW_a and a random number b. Then, U_a computes A_a as

$$A_a = h(ID_a \| PW_a \| b) \quad (1)$$

Then submits ID_a and A_a and b to the control server CS for registration through a secure channel.

Step R2:

On receiving the registration message (ID_a, A_a, b),

CS chooses a random number c for the user U_a and computes

$$B_a = h(ID_a \| A_a \| b \quad (2)$$

$$P_a = h(B_a \| x) \quad (3)$$

$$Q_a = h(P_a \| C) \quad (4)$$

$$R_a = P_a \oplus Q_a \quad (5)$$

Step R3: $CS -> U_a$*:*

CS issues a smart card to U_a, and the card contains (Q_a, R_a, B_a,h())on card.

Step R4:

Then, U_a enters b into his/her smart card, the smart card contains (Q_a, R_a, B_a,h(),b).

For Service Providing Server S_a, he/she sends its ID, SID_j to CS. CS chooses a random number d and computes

$$PSID_j = h(SID_j \| d) \quad (6)$$

$$PID_j = h(PSID_j \| y) \quad (7)$$

CS sends PID_j to Service Providing Server.

B. Login and Verification Phase:

When the user wishes to use the services provided by the remote server S_j.

Step L1:

U_a inserts the smart card into reader and inputs the password PW_a and calculate as:-

$$A_a = h(ID_a \| PW_a \| b) \quad (8)$$

$$B_a{}^* = h(ID_a \| A_a \| b) \quad (9)$$

Now, Check whether

$$B_a{}^* = B_a \quad (10)$$

if yes then do

$$P_a = R_a \oplus Q_a \quad (11)$$

$$T_a = P_a \oplus N_{a1} \quad (12)$$

$$U_{aj} = h(P_a \oplus h(SID_j \| TS_a) \quad (13)$$

$$V_{aj} = h(P_a \| B_a \oplus N_{a1}) \| (append0(N_{a1}) \| append0(ID_a)) \quad (14)$$

$$CID_a = ID_a \oplus h(B_a \| U_{aj}) \quad (15)$$

and sends $(CID_a, B_a, P_a, V_{aj}, TS_a)$ to the service providing server.

Step L2:

When S_j receives the login message, it performs following operations:-

It checks whether $TS_j - TS_a <= 0$ (16)

if yes then do

$$D_a = PID_j \oplus N_{a2} \quad (17)$$

$$E_a = h(N_{a2} \| PID_j \| V_{aj}) \quad (18)$$

$$F_a = SID_j \oplus h(PID_j \oplus N_{a2}) \quad (19)$$

and sends $(CID_a, B_a, E_a, D_a, F_a, SID_j, V_{aj}, TS_a)$ to the control server.

Step L3:

On receiving the message, the control server performs following operations. At first, it checks

Whether $TS_{cs} - TS_j <= 0$ (20)

if yes then proceed as

$$PSID_j = h(SID_j \| d) \quad (21)$$

$$PID_j = h(PSID_j \| y) \quad (22)$$

$$N_{a2} = D_a \oplus PID_j \quad (23)$$

$$E_a^* = h(N_{a2} \| PID_j \| V_{aj}) \quad (24)$$

Then again checks whether $E_a^* = E_a$ (25)

if yes then do

$$P_a^* = h(B_a \| x) \quad (26)$$

Further checks whether $P_a^* = P_a$ (27)

if yes, Then the user is verified by CS.

$$ID_a = CID_a \oplus h(B_a \| U_{aj}) \quad (28)$$

Extract N_{a1} from V_{aj} and generate nonce N_{a3}

$$W_a = N_{a1} \oplus N_{a3} \oplus h(SID_j \| N_{a2} \| PID_j) \quad (29)$$

$$X_a = h(N_{a1} \oplus N_{a3}) \quad (30)$$

$$Y_a = N_{a2} \oplus N_{a3} \oplus h(ID_a \| N_{a1} \| B_a) \quad (31)$$

$$Z_a = h(N_{a2} \oplus N_{a3}) \quad (32)$$

Now, CS sends (X_a, Y_a, Z_a, W_a) to the service providing server.

Step L4:

On receiving the message from CS, *Sj* performs following operations:

$$N_{a1} \oplus N_{a3} = W_a \oplus h(SID_j \| N_{a2} \| PID_j) \quad (33)$$

$$X_a^* = h(N_{a1} \oplus N_{a3}) \quad (34)$$

Then checks whether $X_a^* = X_a$ (35)

If yes, then S_j sends (Y_a, Z_a) to the user.

Step L5:

On receiving the message from *Sj*, following operations are performed at user terminal:

$$N_{a2} \oplus N_{a3} = Y_a \oplus h(ID_a \| N_{a1} \| B_a) \quad (36)$$

$$Z_a^* = h(N_{a2} \oplus N_{a3}) \quad (37)$$

Then checks whether $Z_a^* = Z_a$ (38)

and if it does not hold true, U_a terminates the session otherwise the authentication of CS and *Sj* is verified by U_a.

Now, *Sj*, U_a and CS can compute a common session key

SK as

$$SK = h(N_{a1} \oplus N_{a2} \oplus N_{a3}) \quad (39)$$

C. Password Change Phase:

When the user U_a wants to change the password, he/she has to submit his/her identity ID_a and password PW_a to the CS. The steps of the password change phase are as follows:

$$A_a = h(ID_a \| PW_a \| b) \quad (40)$$

$$B_a^* = h(ID_a \| A_a \| b) \quad (41)$$

Check whether $B_a^* = B_a$ (42)

If yes, then it asks for a new password and sends it to the control server.

The whole algorithm is presented as following.

Algorithm1. Registration and Initialization Phase

1. Start
2. At User Terminal
3. User inserts card into terminal enters his ID_a and PW_a
4. b ← random number
5. $A_a = h(ID_a \| PW_a \| b)$
6. MSG $U_{a\,toCS} \leftarrow ID_a; A_a, b$
7. U_a sends $MSG_{U_{a\,toCS}\,to\,CS}$;
8. At Control Server
9. $B_a = h(ID_a \| A_a \| b)$
10. $P_a = h(B_a \| x)$
11. $Q_a = h(P_a \| c)$
12. $R_a = P_a \oplus Q_a$
13. CS stores $(B_a, Q_a, R_a, h(.))$ on smart card and send it to user.

Algorithm 2. Login and Verification Phase

1. Start

At User Terminal

2. User inserts card into terminal, enters ID_a and PW_a
3. $A_a = h(ID_a \| PW_a \| b)$
4. $B_a{}^* = h(ID_a \| A_a \| b)$
5. check if $B_a{}^* = B_a$,if yes then computes
6. $Pa = Ra \oplus Qa$
7. $T_a = P_a \oplus N_{a1}$
8. $U_{aj} = h(Pa \oplus h(SID_j) \| TS_a)$
9. $V_{aj} = h((P_a \| B_a \oplus N_{a1}) \| (append0(N_{a1}) \| append0(ID_a))$
10. $CIDa = IDa \oplus h(Ba \| U_{aj})$
11. $MSG_{U_a toCS} \leftarrow CID_a, B_a, P_a, V_{aj}, TS_a$
12. U_a *sends* MSG_{UatoCS}toCS;

At Service Providing Server, S_j

13. Checks if($TS_j - TS_a <= 0$)if yes then do
14. $Da = PID_j \oplus Na2$
15. $Ea = h(Na2 \| PID_j \| V_{aj})$
16. $Fa = SID_j \oplus h(PID_j \oplus N_{aj})$
17. $MSG_{S_j toCS} \leftarrow CID_a, B_a, V_{aj}, TS_a, E_a, D_a, F_a, SID_j$
18. S_j *sends* $MSG_{Sto\ CS}$to CS;

At Control Server, CS

19. checks whether $TS_{CS} - TS_j <= 0$, If yes then proceed as
20. $PSID_j = h(SID_j \| d)$
21. $PID_j = h(PSID_j \| y)$
22. $N_{a2} = D_a \oplus PID_j$
23. $E_a^* = h(N_{a2} \| PID_j \| V_{aj})$
24. Then again checks whether $E_a^* = E_a$, If yes then do
25. $P_a^* = h(B_a \| x)$
26. Further checks whether $P_a^* = P_a$, if yes, then the user is verified by CS.
27. $ID_a = CID_a \oplus h(B_a \| U_{aj})$
28. Extract N_{a1} from V_{aj} and generate nonce $N_{a3.}$
29. $W_a = N_{a1} \oplus N_{a3} \oplus h(SID_j \| N_{a2} \| PID_j)$
30. $X_a = h(N_{a1} \oplus N_{a3})$
31. $Y_a = N_{a2} \oplus N_{a3} \oplus h(ID_a \| N_{a1} \| B_a)$
32. $Z_a = h(N_{a2} \oplus N_{a3})$
33. Now, CS sends (X_a, Y_a, Z_a, W_a) to the service providing server.

At Service Providing Server, S_j

34. $N_{a1} \oplus N_{a3} = W_a \oplus h(SID_j \| N_{a2} \| PID_j)$
35. $X_a = h(N_{a1} \oplus N_{a3})$
36. Checks if X_a^*?=X_a , if yes then
37. $MSG_{S_j to\ U_a} \leftarrow Y_a, Z_a$
38. S_j *sends* $MSG_{S_j to\ U_a}$to User;

At User

39. $Na2 \oplus Na3 = Ya \oplus h(IDa \| Na1 \| Ba)$
40. $Z_a^* = h(Na2 \oplus Na3)$
41. Check if $Z^*{}_a$?=Z_a if yes then CS and S_j gets verified by user otherwise the process is terminated.
42. Finally, a common session key $SK=h(N_{a1} \oplus N_{a2} \oplus N_{a3})$ is computed by all the three parties.

The algorithm is represented pictorially in Fig1 and Fig 2.

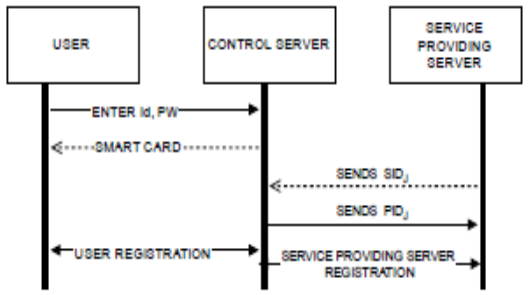

Fig.1. Registration Phase

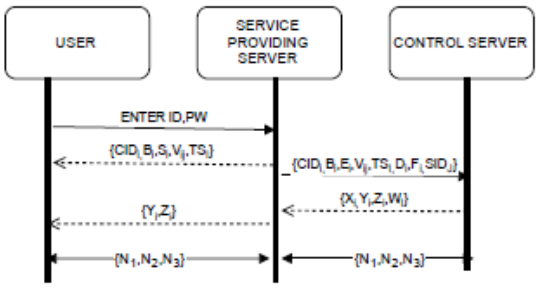

Fig.2. Login and Verification Phase

IV. Analysis

In this section, we are presenting the analysis of our scheme along with the analysis of the scheme studied for literature survey.

A. Identity protection and user anonymity –

Identity protection and preserving user anonymity are two fundamental requirements for an authentication algorithm. To ensure identity protection user's identity is passed on a secure channel and to preserve the user anonymity, the id is not passed directly to the communication channel.

In our scheme, id is passed on a secure channel in the registration phase to preserve the identity and in login phase, the id is not passed directly to preserve user anonymity.

B. Traceability –

During the verification phase control server can compute the original id of the user and this feature makes a user traceable on a control server.

There was no feature of traceability in C.C.Lee et al, Xiong Li et al and Leu & Hsieh et al scheme, but in our scheme, original id can be computed as in equation number 25 and hence the scheme supports traceability, which is a unique feature.

C. Mutual authentication –

Mutual authentication is described as the authentication of the user to control server and control server to the user. It is done to ensure tight security.

The proposed scheme ensures mutual authentication between the user, service providing server and CS.

D. Session key agreement –

A session key is computed by communicating parties to protect the communication between them. In this scheme, a session key SK is computed to protect the communication between the communicating parties. The calculation of SK is as:-

$$SK=h(N_{a1}\oplus N_{a2}\oplus N_{a3})$$

E. Password updating/changing –

For a user's convenience, it is very necessary to have a separate mechanism or phase to update or change the password.

In our scheme, the password can be changed anytime whenever a user wants to and it is done in coordination with control server.

F. Resistance to insider attack –

An insider attack is an intentional misuse of computers or networks by authorized persons such as administrators. An insider can perform an offline guessing attack to obtain users' passwords. If he becomes successful in gaining this then he /she may harm other users by accessing another server with same passwords. He may also try to forge the smart card for malicious purposes. So, a good scheme must provide resistance for an insider attack.

In the proposed scheme, a password is not transmitted to the server in plain text format and so an insider cannot easily perform an attack. But a malicious insider user, possessing a legitimate smart card, can't extract any secret information even after applying brute force attack on the elements (Q_a, R_a, B_a, h(), b) stored in the smart card. And hence insider attack will result in nothing to an attacker.

G. Resistance to stolen smart card attack –

A stolen smart card can help an adversary to break into the system. An algorithm must be designed in such a way that an attacker might not be able to derive secret information from the smart card.

Physical protection methods cannot prevent malicious attackers to get the stored elements. In Xiong Li et al scheme, an attacker can extract h(y) from stolen smart card and further compute $B_f = h(ID_i \parallel x)$ and then $B_f \oplus E_f = h(x \parallel y)$ and with these two parameters, he/she can spoof as a registration center to other legal users.

In Leu & Hsieh scheme, from the elements stored in the smart card, the user can directly get h(y). An attacker U_f first computes

$$T_f = h(ID_f \parallel x),$$

$$V_f = T_f \oplus h\big(ID_f \parallel h(b_f \oplus PW_f)\big)$$

$$B_f = h(h(b_f \oplus PW_f) \parallel h(x \parallel y))$$

And so T_f, V_f, B_f and h(x‖y) can be obtained by brute force attack. By knowing these two values, an attacker can trick a user as being a legitimate service providing the server.

Physical protection methods [22][23], cannot resist malicious attackers to get the stored elements, but our algorithm is so designed that finding stored elements won't help an attacker in obtaining credentials.

H. Resistance to replay attack –

Replay attack involves intercepting the previous messages and then replaying them to the intended entity (e.g. a server) with an intent to be considered a legitimate user. With this attack, a user can easily impersonate a legitimate user.

In C.C. Lee et al scheme, there is no resistance to replay attack, but our proposed scheme resists the attack by making use of time stamps.

I. Resistance of Denial of Service attack –

Denial of service attack prevents the normal operation of a server. It involves flooding the server with several packets so that it becomes busy in handling them leading to a denial of service to normal operations.

In Xiong Li et al scheme, An attacker will try to replay login message $\{P_{ij}, CID_i, M_1, M_2\}$ then RC will compute $N_i, E_i, D_i, B_i, A_i, M_3 \; and \; M_4 \; but \; M_3$ does not get verified and so replay attack won't succeed but the during this time if several replay attack are caused then it will make the registration server busy leading to denial of service.

An attacker will try to replay login message $\{P_{ij}, CID_i, Q_i, N_i\}$ then S will compute $T_i, B_i, A_i, Q_i' \; and \; M_{ij}$ but M_{ij} does not get verified and so replay attack won't succeed but the during this time if several replay attack are caused then it will make the server busy leading to denial of service.

But our scheme resists the attack by making use of time stamps.

J. Masquerade attack –

A masquerade attack is a man in the middle attack. Masquerading is an active attack. In this type of attack, an attacker is in between two communicating parties in such a way that both of them are unaware of its presence and attacker is monitoring and altering their messages. A masquerading attack involves eavesdropping the messages between communicating parties and then recording them for replay and after recording it may or may not alter the messages. It is an attack on confidentiality of data.

Table 2. Comparison of Our Proposed scheme with existing Techniques

S.N.	Security Requirements and Goals	C.C. Lee	Xiong Li	Leu & Hsieh	Our scheme
1	Anonymity of user &Identity protection	yes	yes	yes	yes
2	Traceability	no	no	no	yes
3	Mutual authentication	yes	yes	yes	yes
4	Session key agreement	yes	yes	yes	yes
5	Password updating/changing	yes	yes	yes	yes
6	Resistance of insider attack	yes	yes	yes	yes
7	Resistance of stolen smart card	yes	no	no	yes
8	Resistance to replay attack	no	yes	yes	yes
9	Resistance of Denial-of-Service attack	no	no	no	yes
10	Masquerade attack	no	no	Yes	No

In Leu & Hsieh scheme, the resistance of masquerade attack is provided by resisting replay attack even though with the help of stolen smart card and insider attack an attacker can masquerade as a legitimate server.

But in our scheme, presence of time stamp validity check makes replay attack impossible and the scheme is so designed that with the help of stolen smart card and insider attack, an attacker will not be able to masquerade as a legitimate server.

V. Conclusion

On the basis of security requirements and goals, we propose an improved dynamic identity-based authentication and key agreement scheme suitable for multi-server environment in this paper. Based on the comparative analysis, the scheme is found to be more efficient and reliable. It satisfies all the essential security requirements discussed in the paper.

In future, we can reduce the number of computations in the algorithm to increase the efficiency of the scheme.

References

[1] http://www.webopedia.com/TERM/I/internet_of_things .html. time accessed 20:42 01/05/2016

[2] http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm. time accessed 20:46 01/05/2016

[3] Lamport L. ,Password Authentication with Insecure Communication, Commun ACM 1981;24(11):7702.

[4] https://en.wikipedia.org/wiki/S/KEY. time accessed 21:00 01/05/2016

[5] R. S. Pippal, Jaidhar C. D. and ShashiKala Tapaswi, Security Vulnerabilities of User Authentication Scheme

using Smart Card, Data and Applications Security and Privacy XXVI, 26th Annual IFIP WG.
[6] Chang CC, Wu TC., Remote Password Authentication with Smart Card, Comput. Digital Tech., IEE Proc. E1991; 138(3):1658.
[7] Yoon, E.J., Ryu, E.K. and Yoo, K.Y. (2004) Further Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards. IEEE Transactions on Consumer Electronics, 50, 612-614. http://dx.doi.org/10.1109/TCE.2004.1309437.
[8] Tina, X., Zhu, R.W. and Wong, D.S. (2007) Improved Efficient Remote User Authentication Schemes. International Journal of Network Security, 4, 149-154.
[9] Yang, L. and Ma, J.F. (2011) Trusted Mutual Authentication Scheme with Smart Cards and Passwords. Journal of University of Electronic Science and Technology of China, 4, 128-133.
[10] Das ML, Saxana A, Gulati VP,A dynamic ID-based remoteuser authentication scheme, IEEE Trans ConsumElectr2004;50(2):62931.
[11] JIA-LUN Tsai, Tzong-Chen Wu and Kuo-Yu Tsai,New Dynamic Id Authentication Scheme Using Smart Cards, Int. J.Commun. Syst. 2010; 23:14491462.
[12] Fengtong Wen, XueleiLi., An improved dynamic ID-based remote user authentication with key agreement scheme, Com-puters and Electrical Engineering 38 (2012) 381387.
[13] Bae Ling Chen, Wen Chung Kuo and Lih Chyau Wuu, Robust Remote Authentication Scheme with Smart Card, Int. J.Commun. Syst. (2012).
[14] WB Lee, CC Chang. ,User identification and key distribu-tion maintaining anonymity for distributed computer networks, International Journal of Computer Systems Science & Engineering,2000;15(4):211214.
[15] Liao, Y. P., & Wang, S. S. ,A secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standard& Interfaces, 31(1), 2429.
[16] Cheng Chi Lee, Tsung Hung Lin, Rui Xiang Chang, A secure dynamic ID based remote user authentication scheme for multi server environment using smart cards, ,Expert Systems withApplications 38 (2011) 1386313870.
[17] S. S. Baboo & K. Gokulraj, An Enhanced Dynamic Mutual Authentication Scheme for Smart Card Based Networks, *I. J. Computer Network and Information Security*, 2012, 4, 30-38, DOI: 10.5815/ijcnis.2012.04.04.
[18] Xiong Li, Jian Ma, W. Wang,Y. Xiong, J. Zhang,A novel smart card and dynamic ID based remote user authentication scheme for multi - server environments, Mathematical and computer modeling, Vol58,Issues 1-2, July 2013, Pages 85-95.
[19] Kaiping Xue, P. Hong and C. Ma, A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture, Journal of Computer and System Sciences 80 (2014)195206.
[20] Hari Om, Vishavdeep Goyal and Kunal Gupta, A 3-D Geometry based Remote Login 2-Way Authentication Scheme using Smart Card, *I. J. Computer Network and Information Security*, 2015, 8, 72-79, DOI: 10.5815/ijcnis.2015.08.08.
[21] Jenq Shiou Leu, Wen-Bin Hsieh, Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards, IET Inf. Secur., 2014, Vol. 8,Iss. 2, pp. 104113
[22] Kocher, P., Jaffe, J. , Jun, B. ,Differential power analysis, Proc. Advances in Cryptology (Crypto99), Santa Barbara, USA, 1999, pp. 388397.
[23] T. S. Messerges,E. A. Dabbish and Sloan, *Examining smartcard security under the threat of power analysis attacks*, IEEE Transactions on computers, VOl. 51,No. 5,May 2002.

Authors' Profiles

Shanu Gaharana, born in 1988. M.Tech student in Uttar Pradesh Technical University, Lucknow of Computer Science and Engineering from India.

Her main research interests include cryptography and network security.

Darpan Anand is working as Assistant Professor in the Department of Computer Science and Dean (Student Welfare) at Hindustan Institute Technology & Management, Agra.

His research interest includes Network Security, Cryptography, Computer Network and Distributed Computing.

How to cite this paper: Shanu Gaharana, Darpan Anand,"A New Approach for Remote User Authentication in a Multi - Server Environment Based on DYNAMIC-ID using SMART-CARD", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.10, pp.45-52, 2016.DOI: 10.5815/ijcnis.2016.10.06