International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 24452-24462

http://www.ripublication.com

An Efficient Password Based Authentication Scheme Using Dynamic Identity and Smart Card

Dr. B. Indrani
Assistant Professor, Department of Computer Science,
DDE-Madurai Kamaraj University, Madurai
Tamil Nadu, INDIA
Dr. M. Amutha Prabakar
Associate Professor and Head,
Department of Information Technology,
R.V. S. College of Engineering and Technology, Dindigul Tamil Nadu, INDIA

Abstract

User authentication is a most important problem, particularly with mobile devices such as PDA's, smart card, laptops. User authentication is a primary and foremost problem for every system for providing safe access to access personal information. Password and Personal Identification Number (PIN) based authentication is the leading and classical mechanism for verifying the identity of actual device user. In this paper, we proposed an efficient remote authentication scheme using dynamic identity and smart card. The proposed protocol is based on RSA cryptosystem. The proposed scheme provides basic security requirements with minimum computational cost. The session key can be created by the common known values from the communicating parties.

Keywords: Authentication, Passwords, smartcard, RSA, Session Key

Introduction

The fundamental of data communication is derived from the primary concept of data sharing, which relates to the heterogeneous mechanism. The current Internet is vulnerable to various attacks such as denial of service attack, forgery attack, forward secrecy attack, server spoofing attack, parallel session attack, guessing attack, replay attack, smartcard loss attack and stolen verifier attack. In this paper, we proposed a new remote mutual authentication scheme using smart cards without password table, which circumvents most of these attacks. In the proposed method the remote system does not maintain the password table, but instead maintains the onetime registration date and time of the users. User authentication is the primary part of information security. In a heterogeneous environment, we can expect the plenty of possibilities for

information snoop from nodes by any unauthorized user that are pretending as the valid one, thus being the reason for the several security issues. Authentication is the process verifying the user identity. Authentication is the process verifying the user identity. All security access methods are based on three fundamental pieces of information: who you are, what you have and what you know. Password authentication is the foremost mechanism for verifying the identity of computer users. In the existing traditional setup the ID and password are maintained by the remote system in a verification table. If a user wants to log in a remote server then he has to submit his ID and PW to the server. The remote server receives the login message and checks the eligibility of the user key referencing the password or verification table. If the submitted ID and PW matches with the corresponding pair stored in the servers verification table, the user will be granted access to the server.

In this paper, we propose an efficient remote user authentication scheme using dynamic identity based RSA cryptosystem. We have incorporated session key generation mechanism, which enhances the security mechanism further.

This paper is organized as follows, in section 2 we provide brief review of Remote User authentication schemes. In section 3, we proposed an efficient remote user authentication scheme using RSA cryptosystem. In section 4, we provide a security analysis of our proposed scheme. In section 5, we analyze the cost and functionality of the related schemes. Finally, in section 6, we conclude our paper.

Related Work

In 1981, Lamport proposed his onetime password with one way hash function against replay attacks. However, Lamport's (1981) scheme has the three drawbacks as follows:

1. It has high hash overhead
2. It requires password resetting
3. A password table should be stored on the server's side.

Later papers were developed to avoid these drawbacks. To prevent the password table from being stolen or modified by attackers, solutions have been proposed where the password table is no longer required to be kept by the server.

To solve draw backs (a) and (b) of Lamport's scheme, Shimizu (1990) proposed a new protocol called CINON. Later Shimizu et al. proposed their PERM protocol to solve the random number memorizing problem of the CINON protocol. Haller (1994) developed the famous S/KEY one–time password for an Internet draft RFC1760. However, some researchers have pointed out that the security of the S/KEY scheme can be broken by replay attacks, server spoofing attacks, and password guessing attacks. Sandirigama et al (2000) and Lin et al (2001) proposed the SAS and OSPA protocol, respectively, which turn out superior to Lamport's (1981) protocols, the CINON protocol, and the PERM protocol, in terms of storage utilization computing time, and transmission overhead. However, Chen and Ku (2002) later proved that the SAS and OSPA protocol can be broken by two stolen verified attacks. Recently, quite a number of password authentication schemes with smart card have been proposed.

These smart card based authentication schemes are classified into three main types as follows:

1. RSA–Based Password Authentication Schemes
2. ElGamal–Based Password Authentication Schemes
3. Hash–Based Password Authentication Schemes

Hwang and Li (2000) proposed ElGamal–based remote user authentication scheme using smart card. This scheme is based on ElGamal's (1985) public key cryptosystem. The Hwang–Li (2000) scheme does not need a password table to check the validity of the login request. Additionally, it can withstand replay attacks. However, Awasthi and Lal (2004), Chan and Cheng (2000), and Shen–Lin–Hwang (2003) showed that the Hwang–Li (2000) scheme cannot withstand forgery attacks. Shen et al (2003). and Awasti et al (2004) proposed an improved scheme to counter forgery attacks. Besides, Awasthi et al's (2003) scheme can achieved forward secrecy, ensuring that the previously generated user's passwords are secure even if the systems secret key is stolen or has been revealed in public by accident.

Later, Kumar (2004 b) proposed a new remote user authentication scheme using smart cards. This scheme is a modified form of Shen et al's (2003) scheme and uses one more function C_K to generate the check digit for each registered identity.

Yang and Shieh (1999) proposed two password authentication schemes with smart cards. The two schemes are based on RSA public key cryptosystem. This scheme does not store password or verification table in the server, and let users freely change their own passwords. However, Chan and Cheng (2000), Fan–Li–Zhu(2002), Shen–Lin–Hwang (2003) and Sun et al (2003) pointed out that Yang and Shieh's (1999) schemes have a drawback; an intruder is able to impersonate a legal user by constructing a valid login request. Fun et al (2002) proposed a simple improvement to remedy the damage done by forgery attacks. The improved scheme puts a strict limit on the ID. In the authentication phase, the remote system will check the ID's form. However, Ku et al (2004) and Wang and Yang (2006) showed that Fan et al's (2002) scheme cannot seem to withstand forgery attack.

Shen et al (2003) also proposed an enhancement of the Yang–Shieh (1999) scheme. The proposed scheme can withstand forgery attacks and provide mutual authentication to withstand server spoofing attacks. However, Yang et al pointed out that Shen et al's (2003) scheme is still vulnerable to forgery attacks. Sun et al (2003) pointed out that the cryptanalysis in Chan and Cheng (2000) scheme was unreasonable and proposed their forgery attacks on the Yang–Shieh (1999) scheme. To resist Sun et al's (2003) attack, Yang et al (2005) proposed an improvement of the Yang – Shieh (1999) scheme.

Recently, lots of password authentication schemes based on one–way hash function have been proposed with computation cost lower than that of RSA–based and ElGamal–based password authentication schemes. Sun et al (2003) proposed an efficient and practical remote user authentication scheme. No password table is required to be kept in his system and therefore the communication and computation costs are reduced. Hwang et al (2002 c). and Chien et al (2002) respectively proposed their simple remote user authentication schemes. In these schemes, the authors claimed that their schemes could achieve the following goals: no verification or

password table required on the server's side, low communication cost and computational cost, the replay attack problem completely solved, and freedom to choose their password. Hwang et al (2002 c) pointed out, the scheme can not achieve mutual authentication, and the scheme can not let users freely change their passwords. Further more, Yoon et al (2004). pointed out that the Hwang et al (2002 c) scheme is insecure if the secret key of the server leaked out or stolen. Hsu (2004) showed that the Chien et al (2002) scheme is vulnerable to the parallel session attacks. Later, Lee et al (2004) proposed an improved efficient scheme to remedy the parallel session attack problem. Chen et al (2002) proposed two secure SAS–like password authentication schemes with lower storage processing, and transmission overhead. These two schemes can withstand the stolen verifier attack on SAS and OSPA protocol. Nowadays, all password authentication schemes are based on the static login ID, which, however, can have partial information about the user's login message leaked out. Hence, Das et al.( ) proposed a dynamic ID–based remote user authentication scheme with smart cards. However, their scheme has some security flows. Later, Liao et al (2006) further proposed a new scheme to achieve all of their proposed requirements. This scheme proposed a session key to encrypt/decrypt the communicated message using the symmetric cryptosystem.

Tian et al (2007) showed that Yoon et al (2004) scheme is subject to forgery attacks if the information stored in the smart card is stolen. This violates the "two factor security" objective of the smart cards based on remote user authentication scheme. Tian et al (2007) propose an amendment to this problem and proposed two new schemes, which are more efficient and secure than Yoon et al (2004) scheme.

Liu Yongliang et al (2007) proposed a ECC–based wireless authentication protocol. Although so many schemes have been proposed to authenticate a legitimate user, none of them can solve all possible attacks. Pathan-Hong (2008), established that some kind of attacks are possible on Yang-Wang-Chang (2005) scheme.

However, Kim et al. (2005) pointed out that Yang et al.'s (2005) improvements still cannot withstand forgery attacks. At the same time, Kim et al. (2005) proposed improved methods. Wang and Yang (2006) pointed that Kim et al.'s (2005) improvements also cannot resist the forgery attacks.

Kumar(2010) proposed a scheme wherein the server and user authenticate one another, and then generate a secret session key for secure communication. In this scheme, the remote user is free to change his/her password without connecting to server.

Kumar (2010) proposed a secure remote user authentication scheme with smart cards. This scheme not only provides mutual authentication between the user and server, but also establishes a common session key to provide message confidentiality. In addition, this protocol provides the explicit key authentication property for establishing common session keys. Kumar pointed out that this protocol is provably secure to withstand the replay attack and the stolen verifier attack. In the password change phase of this protocol

In the real environment, it is not impossible for many applications to adopt smart cards due to its poor flexibility, especially for applications over Internet in which the service provider need to take into account the additional implementation cost [35]

Proposed Scheme

In this paper, we proposed an efficient remote authentication scheme using dynamic identity and smart card. The proposed protocol is based on RSA cryptosystem. The proposed scheme has four phases: 1) Initial Phase, 2) Registration Phase, 3) Login Phase and 4) Authentication Phase and verification Phase. Whenever a new user registers through the registration phase, the server issues the smart card and password which holds the related information, and sends it through the secure channel. To access the remote server, user inserts his smart card into the device and keys the password. The server will verify and authenticate the user.

1) Initial Phase

Authentication Server will have the following parameters,

a. p, q are two large prime numbers
b. Compute $n = p \times q$ and $\phi(n) = (p-1) \times (q-1)$
c. Select a primitive element g
d. Select a server key pairs (d_s, e_s)

2) Registration Phase

Whenever a new user register with the server, the user Ui must have a unique identity ID_i and PW_i is register with authentication server through secure channel. Then the server has to perform the following steps.

Step1: The Server computes the smart card identity value SID_i for the user's smart card as follows:

$$SID_i = ID^{T_r} (mod\ n)$$

Server will maintain the SID_i andPW_i.

Step2: Compute $H = g^{SID_i \times PW_i \times d} (mod\ n)$

Step3: The smart card will contain $(n, e, g, ID_i, SID_i, H, T_r)$

3) Login Phase

If user U_i wants login to the remote server, then the user first insert his smart card in the smart card reader and enters his ID_i and PW_i. The smart card reader performs the following steps

Step1: Generate the dynamic *ID* (DID_i) as follows

$$DID_i = SID_i^T (mod\ n)$$

Step2: Select a random number r and compute $X = g^{PW_i \times r \times T} (mod\ n)$ and $Y = H^{r \times T} (mod\ n)$

The login request will contain the following parameters (DID_i, X, Y, T)

4) Authentication and Verification Phase

The server will verify the login request when ever a new request receives.

Step1: The server will verify the user *ID*, it checks the dynamic *ID* value as folows:

$$if (DID_i == SID_i^T (mod\ n)?\ TRUE : FALSE)$$

If the check condition returns TRUE then go to step2; otherwise reject the request

Step2: Check the time interval for the communication

$$if(T^{'} - T) \leq \Delta T ? TRUE : FALSE)$$

Here T' is a login request arrival time of server and T is the login time of client or user. The check condition compute the time interval between login time and login request arrival time, if it is less than or equal to ΔT (legal time interval between a normal communication) then accept and go to step3; otherwise reject the login request.

Step3: Check the correctness of the following equation $Y^e = X^{SID_i}(mod\ n)$

$$if(Y^e == X^{SID_i}(mod\ n)\ ?\ TRUE : FALSE)$$

If the condition returns TRUE then accept the login request; otherwise reject the request

Step4: From Step1 to Step3 check all the conditions, if any one of the condition fails then login request will be expired or terminated. If all the conditions are TRUE then accept the login request.

Correctness of the Equation

Proof:

$Y^e = X^{SID_i}(mod\ n) \quad \rightarrow \quad (1)$

Substitute the values for Y and X in eq1.

$$(H^{r.T})^e = (g^{PW_i.r.t})^{SID_i}(mod\ n)$$

$$(g^{SID_i.PW_i.d})^{r.T})^e = g^{PW_i.r.t.SID_i}(mod\ n)$$

$$g^{SID_i.PW_i.r.T} = g^{PW_i.r.t.SID_i}(mod\ n)$$

Both the side is equal.

Session Key Generation

The session key for the new login session is generated as follows:

$$SessionKey = X^{SID_i}(mod\ n)$$

Security Analysis

An ideal password authentication scheme should satisfy the basic security requirements. The security analysis of the password based authentication schemes discussed in the chanpter 1.4 in [9]. The security analysis of the proposed scheme is discussed in this section. In this section, we provide an in depth security analysis and discussion of the RSA based authentication scheme

a. Denial of service attack

The login request is generated based on password, current time and user's secret information. The login request generation is not based on any previous information; every time it is a new one with current time. The attacker cannot create or update the false information for login. DOS attacks might result from the computation

consumption also. The attackers might send the forged login request message to S. If the DIDi is a valid user identity and T is a valid timestamp, the server S will perform the authentication. The more forged login request messages are sent, the more computation load the server performs. In the proposed scheme, if the login request is rejected three times then automatically the user account is locked and he has to contact server to unlock the account. The proposed protocol overcomes the DOS attack over the computation power of the server.

b. Parallel Session attack

Suppose an adversary intercepts the login request (DIDi, X, Y, T). He cannot create a valid new login request because X is calculated using a random number and password PW_i, and Y value is calculated using user secret information and current time. The adversary cannot create a valid login request with out knowing secret information.

c. Smart card Loss Attack

Suppose user U_i loses his smart card, the adversary cannot use this card without knowing the password of the user U_i. Suppose an adversary wants to change the password, he must know the original password. Thus his attempt to impersonate user U_i fails.

d. Off line password guessing attack

In the proposed scheme, the password PW_i is calculated by using certain functions selected by user U_i. Suppose an adversary intercepts the login request (DIDi, X, Y, T) of a user U_i. It is not possible to recover the original password from this login request message.

Cost Analysis

This section, presents the cost comparison of the proposed scheme with other smart card based authentication schemes. Yang-Shieh (1999), Fan-Li-Zhu (2002), Yang-Wang-Chang (2005) and Rajaram et al (2012) schemes are based on RSA. Table 2 compares the computational cost for each phase. The proposed scheme has high time complexity due to the improved security level than existing

Table 2: Computation Cost comparison between Proposed Scheme and Related Schemes

Schemes	E1	E2	E3
Yang-Shieh (1999)	$2T_{mexp}+1T_{mmul}$	$2T_{mexp}+3T_{mul}+1T_h$	$2T_{mexp}+1T_{mul}+1T_h$
Fan-Li-Zhu (2002)	$2T_{mexp}+1T_{mmul}$	$2T_{mexp}+3T_{mul}+1T_h$	$2T_{mexp}+1T_{mul}+1T_h$
Yang-Wang-Chang (2005)	$2T_{mexp}+2T_{mmul}$	$2T_{mexp}+3T_{mmul}$	$3T_{mexp}+1T_{mmul}$
Kumar (2010)	$T_{mexp}+T_{C_K}$	$3T_{mexp}+2T_h$	$2T_{mexp}+T_h+T_{C_K}$
Kumar (2010)	$T_{mexp}+T_{C_K}$	$2T_{mexp}+T_h$	$T_{mexp}+T_h+T_{C_K}$
Rajaram et al (2012)	$2T_{mexp}+3T_{mmul}$	$2T_{mexp}+3T_{mmul}$	$3T_{mexp}+2T_{mmul}$
Proposed scheme	$2T_{mexp} + 3T_{mmul}$	$3T_{mexp} + 3T_{mmul}$	$2T_{mexp}$

E1 – Computation cost for Registration Phase
E2 – Computation cost for Login Phase
E3 – Computation cost for Authentication Phase

T_{mexp} -time taken for executing a modular exponentiation operation

T_{mmul} -time taken for executing a modular multiplication operation

T_h -time for executing a one-way hash function

T_{C_K} -time for executing a function to generate check digit for the registered identity

Implementation Results and Discussions

This section, discusses the implementation results of the proposed scheme (EPAS) and related schemes. Table 3 presents the time estimate incurred for various operations.

Table 3:Time Estimate Taken For Various Operations

Operations (128 bit)	**Estimated Time in ms**
T_{mexp}	$\approx 1.527932 ms$
T_{mmul}	$\approx 1.513726 ms$
T_h	$\approx 2.139810 ms$
T_{C_K}	$\approx 2.078715 ms$

Table 4 compares the computational cost for all the phases in all the related schemes.

Table 4: Execution Time Comparison For Registration, Login And Authentication Phases

Schemes	**E1**	**E2**	**E3**
Yang-Shieh (1999)	$\approx 5.80752ms$	$\approx 10.37142ms$	$\approx 7.32128ms$
Fan-Li-Zhu (2002)	$\approx 5.80752ms$	$\approx 10.37142ms$	$\approx 7.32128ms$
Yang-Wang-Chang (2005)	$\approx 7.33484ms$	$\approx 8.86346ms$	$\approx 7.94752ms$
Kumar (2010 a)	$\approx 3.60653ms$	$\approx 8.86346ms$	$\approx 7.27489ms$
Kumar (2010 b)	$\approx 3.60653ms$	$\approx 5.19364ms$	$\approx 5.74657ms$
Rajaram et al (2012)	$\approx 8.86346ms$	$\approx 8.86346ms$	$\approx 9.47594ms$
Proposed scheme	$\approx 7.59702ms$	$\approx 9.12492ms$	$\approx 3.05586ms$

Conclusion

In this paper, we proposed an efficient remote authentication scheme using dynamic identity and smart card. The proposed protocol is based on RSA cryptosystem. The proposed scheme provides basic security requirements with minimum computational cost. The experimental result shows that the proposed scheme is efficient and robust compare to other related schemes. In Rajaram et al (2012) scheme does not provide the session key creation concept. In our proposed scheme, the session key can be created by the common known values from the communicating parties.

Reference

[1] Awasthi .A .K and Lal .S (2003), "A Remote User Authentication Scheme using Smart Cards with Forward Security", IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp. 1246–1248, 2003.

[2] Awasthi .A .K and Lal .S (2004), "An enhanced remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 583–586, May

[3] Chan .C .K and Cheng .L .M (2000), "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, pp. 992–993.

[4] Chen .C .M and Ku .W .C (2002), "Stolen-verifier attack on two new strong-password authentication protocols," IEICE Trans. Communication. E85-B pp.2519–2521.

[5] Chien .H .Y, Jan .J .K, and Tseng .Y .M (2002), "An efficient and practical solution to remote authentication: smart card," Computers & Security, Vol. 21, No. 4, pp. 372–375

[6] Haller .N (1995), "The S/KEY one-time password system," RFC Technical Report 1760, February.

[7] Hsu .C .L, (2004), "Security of Chien et al's remote user authentication scheme using smart cards," Computer Standards and Interfaces, Vol. 26, No. 3, pp. 167–169.

[8] Hwang .M .S, and Li .L .H, (2000), "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28–30, February.

[9] Hwang .M .S, Lee .C .C, and Tang .Y .L, (2002 c), "A simple remote user authentication scheme," Mathematical and Computer Modeling, Vol. 36, pp. 103–107

[10] Kim .M and Koc .C .K, (2005) "A Simple Attack on a Recently Introduced Hash-Based Strong-Password Authentication Scheme," International Journal of Network Security, Vol.1, No.2, PP.77–80.

[11] Kim .K .W, Jeon .J .C, and Yoo .K .Y, (2005) "An improvement on Yang et al.'s password authentication schemes," Applied Mathematics and Computation, vol. 170, pp. 207-215

[12] Ku .W .C, Chen .C .M, (2004), "Weakness and improvement of an efficient password based user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 204–207.

[13] Ku .W .C, (2004), "A hash-based strong-password authentication scheme without using smart cards," ACM Operating System Review, vol. 38, no. 1, pp. 29–34.

[14] Kumar .M, (2004 a), "Some Remarks on a Remote User Authentication Scheme Using Smart Cards with Forward Secrecy," IEEE Transactions on Consumer Electronics, Vol 50. No 2.

[15] Kumar .M, (2004 b), "New remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 597–600.

[16] Kumar .M, (2010), "An Enhanced Remote User Authentication Scheme with Smart Card," International Journal of Network Security, Vol.10, No.3, PP.175–184.

[17] Kumar .M, (2010), "A New Secure Remote User Authentication Scheme with Smart Cards," International Journal of Network Security, Vol.11, No.3, PP.128-133.

[18] Lamport .L, (1981), "Password authentication with insecure communication," Communication of the ACM, Vol. 24, No. 11, pp. 770–772

[19] Lee .S, Kim .H, and Yoo .K, (2004), "Comment on a Remote User Authentication Scheme using Smart Cards with Forward Secrecy," IEEE Transactions on Consumer Electronics, Vol 50, No 2

[20] Fan L., Li J. H., and Zhu H. W., (2002) "An enhancement of timestamp-based password authentication scheme", Computer & Security, Elsevier Vol. 21, pp. 665-667.

[21] Liao, Lee .C.C. Hwang .M.S., (2006), "A password authentication scheme over insecure networks," Journal of Computer and System Sciences, vol. 72, pp.727–740.

[22] Lin .C.L., Sun .H.M., Hwang .T, (2001), "Attacks and solutions on strong-password authentication," IEICE Trans. Communication, E84-B, pp.2622–2627

[23] Wang .B and Li .Z.Q., (2006) "A Forward-Secure User Authentication Scheme with Smart Cards," International Journal of Network Security, Vol.3, No.2, PP.116–119.

[24] Wang .R.C. and Yang .C.C., (2006) "Cryptanalysis of Two Improved Password Authentication Schemes Using Smart Cards," International Journal of Network Security, Vol.3, No.3, PP.283–285.

[25] Yang, W.H. and Shieh, S.P. (1999), "Password Authentication Schemes with Smart Cards", Computers & Security, Vol. 18, No. 8, Elsevier, pp. 727-733.

[26] Yang, C. C., Wang, R. C, and Chang, T. Y., (2005) "An improvement of the Yang-Shieh password authentication schemes", Applied Mathematics and Computation 162, Elsevier, pp. 1391-1396.

[27] Yoon E.J., Ryu E.K., and Yoo .K.Y., (2004 a), "Further Improvement of an Efficient password based Remote Authentication Scheme using smart cards," IEEE Transaction on Consumer Electronics, Vol. 50, No. 2, pp. 612–614.

[28] Yoon E.J., Ryu .E.K, and Yoo .K.Y., (2004 b), "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," IEEE Transaction on Consumer Electronics, Vol. 50, No. 2, pp. 568–570

[29] Sun .H.M., and Yeh .H.T., (2003), "Further cryptanalysis of a password authentication scheme with smart cards," IEICE Transactions on Communication, vol. E86-B, no. 4, pp. 1412-1415.

[30] Tian .X., Zhu .R.W., and Wong .D.S., (2007), "Improved Efficient Remote User Authentication Schemes," International Journal of Network Security, Vol.4, No.2, PP.149–154.

[31] Shen .J.J, Lin .C.W., and Hwang .M.S., (2003), "A modified Remote User Authentication Scheme using Smart Card," IEEE Transactions on Consumer Electronics, Vol. 49, No. 2, pp. 414–416

[32] K. Altinkemer and T. Wang, "Cost and benefit analysis of authentication systems," *Decision Support Systems*, vol. 51, pp. 394-404, 2011

[33] S. K. Sood, "An improved and secure smart card based dynamic identity authentication protocol," *International Journal of Network Security*, vol. 14, no.1, pp. 39-46, 2012

[34] K. Awasthi, K. S. Srivastava, and R. C. Mittal, "An improved timestamp-based remote user authentication scheme," *Computers and Electrical Engineering*, vol.37, pp. 869-874, 2011

[35] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search", *International Journal of Network Security*, vol. 15, no. 2, pp. 71-79, 2013