ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Survey of Remote User Password Authentication Scheme Using Smart Cards

***Ajay Kumar Sahu[1], Dr. Ashish Kumar[2], Dr. Tarun Gupta[3]**

1. Department of Computer Science, RKGIT, Ghaziabad, Uttar Pradesh Technical University, Lucknow, India.
2. Department of Computer Science, ITS Greater Noida, Uttar Pradesh Technical University, Lucknow, India.
3. Department of Computer Science, RGEC, Meerut, Uttar Pradesh Technical University, Lucknow, India

Manuscript Info

Manuscript History:

Received: 12 February 2015
Final Accepted: 22 March 2015
Published Online: April 2015

Key words:

Authentication, Smart Cards, Network Security, Password, Hash function, Cryptography.

****Corresponding Author***

Ajay Kumar Sahu

Abstract

Password authentication has been adopted as one of the most commonly used solution in the network environment to protect resources from unauthorized access. Password authentication based on smart cards is one of the simplest and the most convenient authentication scheme and is mostly used to authenticate the legitimacy of remote users. Many schemes based on cryptography have been proposed by various researchers to solve the problem. However, previous schemes are vulnerable to various attacks and are neither efficient, nor user friendly. Today, there are many potential attacks that are targeted at authentication including masquerade attack, insider attack, parallel session attack, offline password guessing attack, server spoofing attack, and many more. In this paper, we have studied a number of schemes proposed by many researchers, their applications, merits and demerits and found that none of the schemes meet all the security requirements and goals, which are necessary for secure password authentication scheme. Here, we have defined and suggested all the security requirements and the goals an ideal password authentication scheme must satisfy and achieve.

INTRODUCTION

With recent developments in internet and e-commerce technologies, many services, such as online shopping, online game, e-learning, internet-banking, e-health, online trading etc. are provided through the internet, which makes life very easy and convenient. However, with the increase of network attacks, such as password guessing attacks, server-spoofing attacks, replay attacks, forgery attacks etc, network and information security has become an important issue for internet-based services. Remote user authentication schemes are common approaches to verify the legitimacy of service seeker users. By employing a remote user authentication scheme, servers first authenticate the remote users, and only after successful authentication, grant access to resources/services to those who are authorized: whereas neglect the unauthorized or malicious entities whose target is to spoil the network security and take undue advantage. Generally, there are three types of authentication methods used. 1. Identity authentication of something known, such as passwords. This is called single factor authentication. 2. Identity authentication of something possessed, such as smart cards. This is called two-factor authentication. 3. Identity authentication of some personal characteristics, such as iris scans, fingerprint scans and Voiceprint scans. This is called three-factor authentication.

In recent years, the authentication schemes are based only on the password which is easiest and most convenient security mechanism used in those days. Example of password authentication applications includes remote login systems, database management system, automated teller machines (ATMs), and Personal Digital Assistants (PDAs), etc., although such schemes are relatively easy to execute, but they have several vulnerabilities

(Daniel V. Klein, 1990). After some time When researchers dug more into this field (Jan J. K, Chen YY., Chang CC, Wu TC.), they found that only password is not sufficient to fulfill the security need of various application areas like database management systems, corporate sector, and the banking sector, etc.. Which gave rise to the introduction of smart card based remote user authentication schemes, which provide two-factor authentication that is; a successful login requires the user to have a legal smart card and a proper password. Normally, a strong, smart card based, password authentication scheme should satisfy some security requirements and withstand different types of attacks such as password guessing attacks, forgery attacks, replay attacks, parallel session attacks, stolen-smart-card attacks, leak-off-verifier attacks, etc. Besides, an ideal password authentication scheme should be user friendly and achieve some functional requirements such as that:
1. Any un-authorized login should be quickly detected when any user inputs a wrong password in the login phase. 2. Allow users to freely choose and change the passwords without interacting with the server, thus, it can decrease the communication overheads 3. The server does not need to store a password table or verification table to avoid leak-of-verifier attacks. 4. It must provide mutual authentication between the server and the user, which makes the server confirm the user is a legal user and the user makes sure that he/she has login to a valid server. 5. It must allow the user and the server to negotiate a shared session key, after which they can communicate to each other.

In the three-factor authentication scheme, it is very similar to the smart card based, password authentication scheme, with the only difference is that it requires some biometric characteristics that can add as an additional authentication factor (He et al., 2014). The three- factor authentication scheme is more expensive than single or two-factor authentication because of the high implementation cost. Hence, the password authentication scheme using smart card is one of the simplest and most convenient authentication methods for handling secret data in the insecure network environment. Several password authentication schemes using smart cards have been proposed in the past, some of which are discussed below.

2. Literature Review

In 1981, Lamport proposed a password-based remote user authentication scheme that used a one-way hash function. However, this method has some drawbacks: 1. the requirement of a password table to be stored in the server to verify the legitimacy of a user; 2. the necessity of password resetting; 3. High hash overhead. After some duration several improved password-based authentication schemes (Hwang T-Y, 1983; Laih et al., 1989; W-H Yang et al., 1997) have been proposed to overcome the drawbacks 2 and 3. All these schemes having verification table, stored securely on the server and contains the user's password. In 1990 a scheme was proposed without password tables; this scheme requires the use of a smart card by the user, the login credentials of the user is not stored by the user. The main drawback of this scheme is that the password cannot be modified easily. In 1991, (C. -C. Chang, S. -J. Hwang) proposed a remote user password authentication scheme using smart cards. In this scheme, it is assumed that the information stored on the smart card could be easily read out by a smart card user. The main drawback of this scheme is that any smart card user can be easily found another user's password by intercepting the login transmitting messages. In the duration of 1993-1999, many authors proposed different authentication schemes with smart cards (Yang W-H, 1999; Chang and Hwang S-J, 1993; Jeng and Jin-Fu C., 1996).

In 2000, M-S Hwang et. al., (2000) identified that Lamport's scheme was vulnerable to the risks of hacking and modifying the password table. They proposed a remote user authentication scheme without using the password table, which was based on El Gamal public key encryption method (El Gamal T., 1985). However, Hwang et al.'s scheme does not allow users to freely choose and change their passwords. Furthermore, this scheme has been found to be vulnerable to various impersonation attacks (Chang, 2003; Her-Tyan et al., 2004). Until now, there have been ample of remote user authentication schemes (I-En Liao et. al. 2006, Deepchand Ahirwal, 2012, Kwang Cheul Shin et al., 2013) published in the literatures and each published scheme has its own merits and demerits.
In (2000), sun proposed an efficient and convenient remote user authentication scheme based on smart card which uses cryptographic hash functions. The major drawback of the scheme of sun et al. is, passwords are not easily memorable and that the user cannot freely choose or change his/her password. In 2002, Chien et al. (2002) criticized the scheme of sun et. al. by pointing out that this scheme only achieves one-sided user authentication and subsequently proposed an enhanced verifier-free password authentication scheme that is capable of mutual authentication. Additionally, the user can freely choose his/her password in the scheme of Lizhen Yang, Kefei Chen (2004) showed that Shieh et al.'s authentication scheme (Yang and Shieh, 1999) was insecure against forgery attack.

Hwang M-S. et al. (2003) devised an enhancement of the Yang et al. (1999) scheme. The devised scheme introduced the mutual authentication to handle server spoofing attackes and tackled problems of forgery attacks. However, Yang et al. pointed out that Hwang M-S et al's (2003) scheme is still prone to forgery attacks. All

the published schemes suffered with the risk of ID theft during the message transmission over an insecure channel. Das et al. (2004) devised a dynamic ID based remote user authentication scheme to overcome the risk. It was a novel scheme since avoids impersonation. It was based one way hash functions and provides the flexibility of choosing and changing the password. Later on many researchers raised concerns over Das et al. scheme. Awasthi (2004) observed that Das et al. scheme was insecure and did not fulfill all the basic needs of authentication schemes. Chien and chen (2005) noticed that Das et al. scheme does not protect an user's anonymity and proposed an improved remote authentication scheme. Furthermore, Ku and Chang also revealed some of the weaknesses of Das et al.'s scheme. In 2005, Lee et al. (2005) improved Chien et al.'s scheme by adding the ability to resist parallel session attacks.

In 2006, Lee, C-C et al. proposed a password authentication scheme that could be implemented over insecure networks. Unfortunately, Yoo K-Y et al.(2006) showed that , Lee C-C et al. scheme is vulnerable to offline password guessing attacks, replay attacks, and denial-of-service attacks. However, none of these authors suggested any modification over the vulnerabilities to above attacks. Later, Kumari S. et al. (2011) improved Liao et al.'s scheme by enabling it to resist the attacks pointed out by E J Yoon et al. and Xiang et al. In 2007, Wang et al.. (2007) proved that both Ku and Chen (2004) and Yoon et al. (20004) schemes cannot resist forgery attacks, denial-of-service attacks or offline password guessing attacks. Additionally, these authors proposed an improved scheme for real application in resource-limited environments.

In 2008, Ku W-C et al. (2009) proved that Wang et al.'s schemes are vulnerable to offline password guessing attacks and impersonation attacks and is unable to achieve perfect forward secrecy. Additionally, these authors proposed an improved scheme with greater security strength. Later, Juang et al. (2008) proposed a robust and efficient user authentication and key agreement scheme using smart cards. Unfortunately, Sun et al. (2009) showed that Juang et al.'s scheme suffers from three weaknesses. Inability of the password changing operations the session key problem and inefficiency of the double secret keys, and then presented improved schemes. Later in (2014), Huang et al. (2013) analyzed Jung et al., s scheme and sun et al.'s scheme, and showed that these two schemes are insecure against offline-dictionary attack. In (2009), Wang et al. Proposed a password authentication scheme; but Wen and Li (2012) proved that YY. Wang et al.'s scheme is insecure against impersonation attack and then proposed an enhanced scheme.

In 2010, R. Song introduced a new and more secure authentication scheme based on a symmetric key cryptosystem and modular exponentiation. However W.B Horng-Cheng demonstrates that R. Song et al. scheme is vulnerable to the offline password guessing attack, insider attack, and denial-of-service attack and proposed a scheme which does not provide perfect forward secrecy for session keys. In the same year, sood et al. (2010) showed that Xu et al.'s scheme is vulnerable to offline dictionary attacks, forgery attacks and then presented an improved scheme. In 2011, Chen et al. analyzed Wang et al., 2007 scheme and proved that it is insecure against parallel session attack, impersonation attack, and then proposed an enhanced scheme. Later, Fan et al. (2011) proposed a two-factor authentication scheme, but wang and wang (2014) showed that the scheme is vulnerable to smart card security breach attack; insider attack and node capture attack and fails to preserve user anonymity.

In 2012, Chen et al. (2012) proved that sood et al., 2010) does not achieve mutual authentication and that song's scheme (Song, 2010) is vulnerable to stolen-smart-card and offline password guessing attacks. Then Chen et al. proposed a robust smart card- based remote user password authentication scheme. In the same year, Hsieh and Leu (2012) reanalyzed the Hsiang et al.'s scheme (Hsiang and Shih, 2009) and showed that the scheme cannot withstand off line password guessing attack, masquerading user/server attack.

In 2013, Kumari and Khan reanalyzed the Chen et al.'s scheme (Chen et al., 2012) and showed that the scheme cannot resist impersonation attacks or insider attacks; they then presented an improved scheme. In the same year, Li et al. (2013) also showed that Chen et al.'s scheme cannot ensure perfect forward secrecy and that it cannot detect incorrect password in the login phase, they then proposed an improved scheme. Jiang et al. showed that Chen et al.'s scheme (Chen et al., 2012) is vulnerable to password guessing attack. Furthermore, Jiang et al., proposed a solution to overcome the shortcoming of chen et al.'s scheme. However, Mishra et al. showed that Jiang et al.'s scheme cannot resist insider attack, password guessing attack and user impersonation attack, and fails to ensure perfect forward secrecy and user anonymity. Later on, Chang et al. proposed a dynamic identity based remote user authentication scheme. Most recently (2014), Kumari et al. Analyze the Chang et al.'s scheme and showed that the scheme is vulnerable to offline password guessing attack, impersonation attack and insider attack, and they then proposed an improved scheme.

3. Security Requirement and Goals

In general, an ideal smart card-based, password authentication scheme should satisfy some of the security requirements (SR) described in (Madhusudhan and Mittal, 2012). Here, we list out and define the security attacks that an ideal password authentication scheme should withstand.
SR1: The ability to resist smart card loss attacks, SR2: The ability to resist offline password guessing attacks, SR3: The ability to resist denial of service attacks, SR4: The ability to resist forgery attacks or impersonation Attacks, SR5: The achievement of mutual authentication, SR6: The ability to resist replay attacks, SR7: The ability to resist parallel session attacks and reflection attacks, SR8: The ability to resist stolen-verifier attacks and modification attacks, SR9: The ability to resist insider attack, SR10: Perfect forward secrecy, SR11: The ability to resist server spoofing attacks, SR12: The achievement of session key agreement, SR13: The achievement of user anonymity, SR14: Resist online password guessing attack.
An ideal password authentication scheme should withstand all of the above attacks. Besides, it should achieve the following goals: G1: No verification table, G2: Freely chosen password by the user, G3: No password reveal, G4: Password dependent, G5: Mutual authentication, G6: Session key agreement, G7: Forward secrecy, G8: User anonymity, G9: Smart card revocation, G10: Efficiency for wrong password login. Furthermore, Ma et al. suggested three principles that are important to design a secure remote user mutual authentication scheme. These principles include the following:

1. Public-key techniques are very important to with stand offline password guessing attack and to preserve user anonymity.
2. There is an unavoidable trade-off when fulfilling the goals of local password updates and resistance to smart card loss attack.
3. At least two exponentiation operations conducted on the server side are necessary for achieving forward secrecy.

An ideal password authentication scheme withstands all above attacks and achieves goals. Surprisingly none of the existing password authentication schemes passed requirements. Therefore, there are opportunities to develop an ideal scheme satisfying all the requirements.

4. The Password Authentication Sschmes

Recently, a number of password authentication schemes with smart card have been proposed. These smart card based authentication schemes are based on cryptography, which can classified into three main types are as follows:
a) The one-way hash function based, password authentication scheme, for eg. (MD5 and SHA-1).
b) The discrete logarithm problem (El Gamal) based, password authentication scheme.
c) The Diffie Hellman Problem (RSA) based, password authentication scheme.

4.1 One Way Hash Function

A one-way hash function h: a (b is a function with the following properties:
The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output

- The function h is one-way in the sense that given a, it is easy to compute h (a) =b. However, given by, it is hard to compute h^{-1} (b) =a.
- It is computationally infeasible to find any pair a,a' such that a'≠a, but h(a')=h(a).
- The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output
- Given a, it is computationally infeasible to find a' such that a'≠a; but h(a')=h(a).

4.2 Discrete Logarithm Problems

- Until now, solving discrete logarithm problem is still a hard problem. We describe this problem as follows. Assume that g is a generator of Zp^* and p is a large prime number. Consider the following equation:
$$J = g^j \bmod p. \quad (1)$$
- If we know g, j, and p, it is very easy to compute J, however, if we know g, J, and p, it is very difficult to solve the equation for j. The difficulty is due to factoring prime numbers as that required for RSA. The problem of solving equation (1) for j is called discrete logarithm problem.

4.3 Diffie-Hellman Key Agreement

In 1976, Diffie and Hellman proposed a key agreement scheme for making agreement on a session key over insecure networks. The scheme allows two parties communicate each other in a secure communication with the agreed session key. Its security is based on solving discrete logarithm problem. Assume that sameer and mohan are to agree on a session key over insecure networks. The parameters g and p are public. Then, they do the following steps to agree on a session key.

- Sameer randomly chooses a large number a and sends Mohan $A=g^a \bmod p$.
- In the meantime, Mohan also randomly chooses a large number b and sends sameer $B=g^b \bmod p$.
- After that, sameer and Mohan can calculate their session key as $K=B^a \bmod p=A^b \bmod p=g^{ab} \bmod p$.

Without knowing a and b, no one can listen on the sameer –Mohan channel. To derive a and b, it is the discrete logarithm problem.

5. Performance and Security Requirements Comparison

In this section, we evaluate some schemes and compare to each other. Here, we compare the schemes of Yoon et al. (2004), Liao et al.(2006), Wang et al. (2007), Xu et al. (2009), Song (2010), and Chen et al. (2012), in terms of security requirements satisfied and performance. To analyses the computational cost, we define the following notation;

t_h : the computational cost of one hash operation.
t_{mexp} : the computational cost of one modular exponent.
t_{sym}: the computational cost of one symmetric key encryption/decryption.
t_m: the computational cost of one multiplication/division.
t_{xor}: the computational cost of one XOR operation.

Here we consider only the computational cost of the login phase and authentication phase because these two phases are executed much more frequently in password authentication schemes. Here we do not consider t_{xor} into account because as compared to the other four operations, the computational cost of XOR operation is negligible. Table 1 illustrates the results of the performance comparisons of some related schemes; from this table; It can be observed that the overall computational costs of the schemes of Yoon et al.(2004), Liao et al. (2006), Wang et al. (2007), Xu et al. (2009), Song (2010) and Chen et al. (2012) respectively. The comparisons of the security requirements satisfied by related schemes are summarized in table 2; From this table, it can be seen that no one such scheme proposed by various researchers fulfills all the security requirements.

Table1- Computational cost of the proposed scheme and other related schemes

Schemes	Login phase	Authentication phase	Total
Yoon et al.(2004)	$2t_h$	$4t_h$	$6t_h$
Liao et al. (2006)	$4t_{mexp}+3t_h$	$3t_{mexp}+3t_h$	$7t_{mexp}+6t_h$
Wang et al. (2007)	$4t_h$	$4t_h$	$8t_h$
Xu et al. (2009)	$2t_{mexp}+3t_h$	$2t_{mexp}+4t_h$	$4t_{mexp}+7t_h$
Song (2010)	$1t_{sym}+2t_h$	$1t_{mexp}+1t_{sym}+6t_h$	$1t_{mexp}+2t_{sym}+8t_h$
Chen et al. (2012)	$2t_{mexp}+2t_m+2t_h$	$1t_{mexp}+1t_m+6t_h$	$3t_{mexp}+3t_{m+}8t_h$

Table2- Security requirements of the proposed scheme and other related schemes

Schemes	Security requirements (SR)

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9	SR10	SR11	SR12	SR13	SR14
Yoon et al.(2004)	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N
Liao et al. (2006)	N	Y	Y	Y	N	N	Y	Y	Y	Y	N	Y	N	N
Wang et al. (2007)	Y	N	Y	Y	N	Y	Y	Y	Y	N	N	Y	N	N
Xu et al. (2009)	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N	Y	N	N
Song (2010)	Y	Y	Y	Y	N	Y	N	Y	Y	Y	N	Y	N	N
Chen et al. (2012)	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y	N	Y

Y: achieved; N: not achieved.

- t_h: the computational cost of one hast operation;
- t_{mexp}: the computational cost of one modular exponent;
- t_m :the computational cost of one multiplication/division;
- t_{sym}: the computational cost of one symmetric key encryption/decryption;
- t_{xor} : the computational cost of one XOR operation;

6. CONCLUSION

In this paper, the survey of the several password-based authentication schemes over insecure networks has been done. Here, we studied the various schemes proposed by a number of researchers, their drawbacks of these schemes and the modifications proposed by various researchers. Here, we have defined the security requirements and goals an ideal password authentication scheme must satisfy and achieve. Unfortunately, none of the schemes can satisfy all the security requirements and achieve all the goals. Thus, it is expected that the authentication scheme which will propose by various researchers must efficiently solve the specified vulnerabilities while maintaining the advantages of the existing smart-card based user authentication scheme. In the future, we aspect more secure and efficient authentication protocol using smart card will be proposed by various researchers, whose computational cost is very low and resist to all possible attacks. We hope an ideal smart card based, password authentication scheme, which meets the entire security requirement and all the goals can be developed.

REFERENCES

Klein DV. Foiling the cracker: a survey of, and improvements to, password security. In: Proceedings of the 2nd USENIX security workshop; 1990. p. 5-14.

Chang C-C, Wu T-C. Remote password authentication with smart cards. Comput Digit Tech IEE Proc E 1991; 138 (3) :165-8.

He D, Kumar N, Lee J-H, Sherratt RS. Enhanced three-factor security protocol for consumer USB mass storage devices. IEEE Trans Consum Electron 2014; 60(1):30-7.

Hwang T-Y. Password authentication using public-key encryption. Proc IEEE Int Carnahan Conf Security Technol 1983:141-4.

Harn L, Huang D, Laih C. Password authentication using public key cryptography. Comput Math Appl 1989;18 (12): 1001-17.

Shieh S-P, Yang W-H, Sun H-M. An authentication protocol without trusted third party. IEEE Commun Lett 1997;1 (3): 87-9.

Yang W-H, Shieh S-P. Password authentication schemes with smart cards. Comput score 1999;18 (8): 727-33.

Chang C-C, Hwang S-J. Using smart cards to authenticate remote passwords. Comput Math Appl 1993; 26 (7): 19-27.

Shiuh-Jeng W, Jin-Fu C. Smart card based secure password authentication scheme. Comput Secur 1996;15(3):231-7.

Hwang M-S, Li L-H. A new remote user authentication scheme using smart cards. IEEE Trans Consum Electron 2000;46 (1): 28-30.

ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: Advances in cryptology. Springer; 1985. p. 10-8.

Chang C-C. Some forgery attacks on a remote user authentication scheme using smart cards. Informatica 2003; 14(3):289-94.

Yang W-H, Shieh S-P. Password authentication schemes with smart cards. Comput Secur 1999;18(8):727-33.

Yoon E-J, Yoo K-Y. Drawbacks of Liao et al.'s password authentication scheme. In: NWeSP 2006. International conference on Next generation web services practices, 2006. IEEE; 2006. p. 101-8.

Kumari S, Khan M K, Cryptanalysis and improvement of a robust smart-card-based remote user password authentication scheme, Int J Comm Syst., http://dx.doi.org/ 10.1002./dac.2590.

Chang C-C, Wu T-C. Remote password authentication with smart cards. Comput Digit Tech IEE Proc E 1991;138(3):165-8.

Liao I-E, Lee C-C, Hwang M-S. A password authentication scheme over insecure networks. J Comput Syst Sci 2006;72(4):727-40.

Chien H-Y, Jan J-K, Tseng Y-M. An efficient and practical solution to remote authentication: smart card. Comput Secur 2002;21(4):372-5.

Yang WH, Shieh SP. Password authentication schemes with smart cards. Compu- ters and Security 1999;18(8):727–33.

Shen JJ, Lin CW, Hwang MS. Security enhancement for the timestamp-based, password authentication scheme using smart cards. Comp Sec 2003;22 (7): 591–5.

Das ML, Saxena A, Gulati VP. A dynamic ID-based remote user authentication scheme. IEEE Trans Consum Electron 2004;50 (2): 629–31.

Awasthi AK, Lal S. An enhanced remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 2004;50 (2): 583–6. May.

Liao IE, Lee CC, Hwang MS. Security enhancement for a dynamic ID-based remote user authentication scheme. In: Proceedings of the international conference on next generation web services practices, August 2005. p. 437–40.

Tsai CS, Lee CC, Hwang MS. Password Authentication Schemes. Current Status and Key Issues, International Journal of Network Security 2006;3 (2): 101–15.

Wang X-M, Zhang W-F, Zhang J-S, Khan MK. Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Comput Stand Interfaces 2007;29 (5): 507-12.

Ku WC, Chen SM. Weakness and improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Trans Consum Electron 2004;50 (1): 204–7.

Yoon EJ, Ryu EK, Yoo KY. Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Trans Consum Electron 2004;50 (2): 612–4.

Chung H-R, Ku W-C, Tsaur M-J. Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments. Comput Stand Interfaces 2009;31 (4): 863-8.

Juang, W. S., Chen, S. T., & Liaw, H. T. (2008). Robust and efficient password authenticated key agreement using smart cards. IEEE Transactions on Industrial Electronics, 55 (6), 2551–2556.

Huang X, Chen X, Li J, Xiang Y, Xu L. Further observations on smart-card-based, password-authenticated key agreement in distributed systems. IEEE Trans Parallel Distrib Syst 2013;25 (7): 1767-75.

Wang et al.'s remote user password authentication scheme for resource-limited environments. Comput Stand Interfaces 2009;31 (4): 863-8.

Sood SK, Sarje AK, Singh K. An improvement of Xu et al.'s authentication scheme using smart cards. In: Proceedings of the third annual ACM Bangalore conference. ACM; 2010. p. 15.

Wang X-M, Zhang W-F, Zhang J-S, Khan MK. Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Comput Stand Interfaces 2007;29 (5): 507-12.

Wang D, Wang P. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. Ad Hoc Netw 2014;20:1-15.

Wang D, Ma C-G, Wang P, Chen Z. Robust smart card based, password authentication scheme against smart card security breach. 2012. Tech. Rep., Cryptology ePrint Archive, Report 2012/439.

Sood SK, Sarje AK, Singh K. An improvement of Xu et al.'s authentication scheme using smart cards. In: Proceedings of the third annual ACM Bangalore conference. ACM; 2010. p. 15.

Hsieh W-B, Leu J-S. Exploiting hash functions to intensify the remote user authentication scheme. Comput Secur 2012;31(6):791-8.

Hsiang H-C, Shih W-K. Weaknesses and improvements to the yooneryueyoo remote user authentication scheme using smart cards. Comput Commun 2009;32 (4): 649-52.

Kumari S, Khan M K, Cryptanalysis and improvement of a robust smart-card-based remote user password authentication scheme, Int J Comm Syst., http://dx.doi.org/ 10.1002./dac.2590

Chen B-L, Kuo W-C, Wuu L-C. Robust smart-card-based remote user password authentication scheme. Int J Comm Syst 2012;27(2):377-89.

Li X, Niu J, Khurram Khan M, Liao J. An enhanced smart card based remote user password authentication scheme. J Netw Comput Appl 2013;36(5):1365-71.

Chen B-L, Kuo W-C, Wuu L-C. Robust smart-card-based remote user password authentication scheme. Int J Comm Syst 2012;27(2):377-89.

Kumari S, Khan MK, Li X. An improved remote user authentication scheme with key agreement. Comput Electr Eng. 2014;40(6):1997-2012.

Chang YF, Chang HC. Security of dynamic ID-based remote user authentication scheme. In: Proceedings of NCM. Seoul, Korea; 2009. p. 2108–10.

Yoon E-J, Ryu E-K, Yoo K-Y. Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Trans \Consum Electron 2004;50 (2): 612-4.

Liao I-E, Lee C-C, Hwang M-S. A password authentication scheme over insecure networks. J Comput Syst Sci 2006;72(4):727-40.

Wang X-M, Zhang W-F, Zhang J-S, Khan MK. Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Comput Stand Interfaces 2007;29 (5): 507-12.

Xu J, Zhu W-T, Feng D-G. An improved smart card based, password authentication scheme with provable security. Comput Stand Interfaces 2009;31 (4): 723-8.

Song, R. Advanced smart card based, password authentication protocol. Comput Stand Interfaces 2010;32 (5): 321-5.

Chen B-L, Kuo W-C, Wuu L-C. Robust smart-card-based remote user password authentication scheme. Int J Comm Syst 2012;27(2):377-89.

Li X, Niu J, Khurram Khan M, Liao J. An enhanced smart card based remote user password authentication scheme. J Netw Comput Appl 2013;36(5):1365-71.

Chen B-L, Kuo W-C, Wuu L-C. Robust smart-card-based remote user password authentication scheme. Int J Comm Syst 2012;27(2):377-89.

Kumari S, Khan MK, Li X. An improved remote user authentication scheme with key agreement. Comput Electr Eng. 2014;40(6):1997-2012.

Chang YF, Chang HC. Security of dynamic ID-based remote user authentication scheme. In: Proceedings of NCM. Seoul, Korea; 2009. p. 2108–10.

Chang YF, Tai WL, Chang HC. Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update. Int J. Commun. Syst 2013. http://dx.doi.org/10.1002/dac.2552.

Yoon E-J, Ryu E-K, Yoo K-Y. Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Trans \Consum Electron 2004;50 (2): 612-4.

Liao I-E, Lee C-C, Hwang M-S. A password authentication scheme over insecure networks. J Comput Syst Sci 2006;72(4):727-40.

BIOGRAPHY

Ajay Kumar Sahu is an Assistant Professor in the department of Computer Science and Engineering in Raj Kumar Goel Institue of Technology (RKGIT) Ghaziabad, affliated to Uttar Pradesh Technical University(UPTU), Uttar Pradesh, India. His area of research interest include Global Information Systems, Organizational Impact of IT, Software Development and Support, Network Security and Technology Adoption. He has done his M.Tech from Guru Gobind Singh Indraprstha University (GGSIPU), Delhi and B.Tech. (CSE) from G.L.A institute of Technology, Mathura. He has total twelve years of teaching experience Academics. He has published more than ten research papers in national and international journals and proceedings.

Ashish Kumar received the M.Tech. degree in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in 2008 and Ph.D. in Computer Science and Engineering from University of Petroleum and Energy Studies, Dehradun. He is a Professor in the Department of Computer Science and Engineering at I.T.S. Engineering College, Gr. Noida, India. His research interest includes Mobile Adhoc Networks, Reverse Engineering and Object Oriented Systems.