A Strong User Authentication Framework for Cloud Computing

Amlan Jyoti Choudhury[1], Pardeep Kumar[1], Mangal Sain[1]

[1]Department of Ubiquitous IT, Dongseo University, Busan, 617-716, South Korea
choudhuryamlanjyoti@gmail.com, pradeepkhl@gmail.com, mangalsain1@gmail.com

Hyotaek Lim[2], Hoon Jae-Lee[2]

[2]Division of Computer and Information Engineering, Dongseo University, Busan, 617-716, South Korea

htlim@dongseo.ac.kr, hjlee@dongseo.ac.kr

Abstract— **Cloud computing is combination of various computing entities, globally separated, but electronically connected. As the geography of computation is moving towards corporate server rooms, it bring more issues including security, such as virtualization security, distributed computing, application security, identity management, access control and authentication. However, strong user authentication is the paramount requirement for cloud computing that restrict illegal access of cloud server. In this regard, this paper proposes a strong user authentication framework for cloud computing, where user legitimacy is strongly verified before enter into the cloud. The proposed framework provides identity management, mutual authentication, session key establishment between the users and the cloud server. A user can change his/her password, whenever demanded. Furthermore, security analysis realizes the feasibility of the proposed framework for cloud computing and achieves efficiency.**

Keywords— **Cloud Computing, Virtualization, SAAS, PAAS, IAAS, User authentication, OOB**

I. INTRODUCTION AND MOTIVATION

With the advancement of IT, cloud computing has evolved through a number of different services, such as, virtualization, software as a service (*SAAS*), infrastructure as a service (*IAAS*) and platform as a service (*PAAS*). For instance, cloud computing refers to both the applications delivered as services over the internet and the hardware and system software in the data centres, that provide those services [1]. The basic goal of cloud computing is to provide great flexibility to users, where users can process, store and access their data on the cloud server anytime, anywhere using the internet. In addition, users do not need to concern with the processing details. Generally cloud systems are divided into three categories, namely, public cloud, private cloud and hybrid cloud [2-4].

The new cloud computing technology offers many advantages such as, information shared in virtual environment, dynamic scalability, storage utility, software utilization, platform and infrastructure utilization, managed distributed computing power, and many more. However, the cloud computing technology comes with many issues, for example; performance, resiliency, interoperability, data migration and transition from legacy systems. One of the main issues is security, such as, virtualization security, distributed computing, application security, identity management, access control and authentication [5-7]. Furthermore, in [8], [9] authors have pointed out that the identity and access control management is a core requirement for cloud computing. Thus, strong authentication becomes paramount requirement in cloud computing service environment.

So far significant researches have been proposed, to provide adequate security to cloud computing [10-13]. However, these existing security mechanisms have some lack of security measures (*as discussed in section II*) in practical implementation. Moreover, the openness nature of internet has many inherent security flaws [14]. A lot of security attacks have been proven on different clouds such as, Google App Engine, Amazon web services, Salesforce (Salesforce.com). As a result, illegal users can exploit these security flaws and either steal secret information or disturb the normal operation of internet using different types of attacks and threats. Thus, strong user authentication and authorization have not yet been extending into the cloud.

In this regard, the above challenges motivate us to introduce a reliable and strong user authentication framework for cloud computing, where a legitimate user prove his/her authenticity before entering into the cloud. The proposed scheme verifies user authenticity using two-step verification, which is based on password, smartcard and out of band (i.e. strong two-factor) authentication. In addition, the proposed scheme provides mutual authentication, identity management, session key establishment, user privacy and secure against many popular attacks.

The rest of the paper is organized as follows. In section II we discuss some existing literatures. In section III, cloud security architecture and in section IV, the proposed strong two-factor user authentication protocol for cloud computing. Section V performs security analysis of the proposed framework. Section VI, conclusion are drawn and future research directions for secure cloud computing.

978-0-7695-4624-7/11 $26.00 © 2011 IEEE
DOI 10.1109/APSCC.2011.14

II. LITERATURE REVIEW

Before addressing cloud security, we will review some existing authentication schemes, which are based on client-server architecture. One of the most popular and elderly remote user authentication schemes was suggested by Lamport [15] in 1981, in which, the server stores the hashed value of a user's password. In Lamport's scheme, password table was used to verify the legitimacy of users, but if this password table is compromised, stolen, or modified by an adversary, then the system could be partially or completely compromised [16],[17]. Some more recent smart card based password authentication schemes have been proposed in [18] – [21], and many of the schemes have been broken as shown by [22] - [26].

Shoup-Rubin [27] proposed extension of Bellare-Rogaway model [28] which is based on three party key distribution protocol and smartcard is used to store the long term secret keys. In their scheme, smartcard is used to prevent the adversaries and it is assumed that smartcard is never compromised. So basically the scheme falls in one factor category as two factor schemes can be broken by compromising both the factors only.

Liao et al. [19] tried to consolidate a number of passwords and smartcard based properties and proposed two factor smartcard and password authentication scheme, which is still vulnerable to many attacks, as demonstrated in [29].

Cloud computing is a variant of client server architecture, where, thousands of clients use the same infrastructure at a large scale. Consequently, it needs stronger authentication than conventional client server inter-networking system.

Lee et al [10] have proposed public key and mobile out of band based authentication for cloud computing. However, the scheme transmits data (e.g. *ID, PW,* and *PKI*) in a plaintext form which can be easily intercepted by the adversaries. In addition, their scheme does not care about data confidentiality, data integrity, user privacy and users are not allowed to change their password. As result, their scheme is not fit for real time cloud computing.

In [11], authors study the challenges regarding confidentiality, integrity and availability for cloud computing and mainly concerned about efficient handling of IAM using protocols. However, prior to identity and access management, access control is more important so that any unauthorised adversary cannot access legal user's data. Furthermore, identity and access control management represents identity assertion relationships to connect services in the cloud. But what do we do to verify end users to establish their identities and raise a question to researchers, how to protect cloud data from illegal users?

Li and Wu [12] proposed a theoretical prototype system, in which cloud computing system is combined with trusted platform support service. Celesti et al [13] proposed reference architecture to address identity management problem for cloud computing. However, these schemes did not address access control for cloud computing users.

As we can see from above literature, the exiting user authentication schemes have many security flaws. This paper address most of the security concerns of cloud computing and propose a strong user authentication framework for cloud computing.

III. CLOUD SECURITY ARCHITECTURE

This section describes a secure cloud architecture, where strong user authentication framework is proposed. The proposed secure cloud architecture has two major advantages as follows.

1) The scheme posses an extra OOB (out of band) factor (other than only two factors) which undoubtedly provide better security over two factor authentication.

2) Two separate communication channels, making it very difficult for the adversaries to attack in two different channels schematic security architecture of the proposed protocol is shown in figure 1.

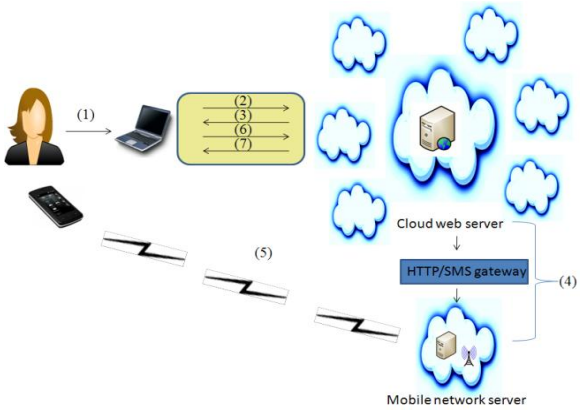

Figure 1: Architecture of the proposed scheme

As shown in the fig1, the basic idea of proposed scheme is as follows.

1. The user inserts the smartcard in the terminal and enter user *ID* and Password (*PW*). The local system verifies the authenticity of the user based on smartcard, *ID* and *PW*.
2. Once the local verification is over, the user send login request to the cloud server.
3. Upon receiving the login request, the cloud server sends some authentication data based on the specific user.
4. The cloud server sends the onetime key to the mobile network through HTTP/SMS gateway [10].
5. The mobile network delivers the onetime key to the user via SMS.

6. The user authenticates the server and sends some message based on smartcard, *ID* and onetime key.
7. The server authenticates user based on data sent by the user in step 6.

The notations used in this paper are mentioned below in table 1.

TABLE 1
DESCRIPTION OF NOTATIONS USED IN THIS PAPER

Notation	Description
A	Specifies a user
S	Denote server
ID	Represents user identity
PW	Denote user's password
K	Onetime key
x	A user's secret number
y	A servers secret number stored at the server
p	A large prime number
g	Primitive element in the Galois field *GF(p)*
h(.)	One way hash function, e.g. SHA1, SHA2
||	Denotes concatenation operation
X→Y: M	Message *M* is sent *X* to *Y* through public channel
X=>Y: M	Message *M* is sent *X* to *Y* through secure channel
$\oplus$	Denote XOR operation

IV. PROPOSED SCHEME

Before, detailed discussion of the proposed scheme, some assumptions are made are not supposed to be violated while executing the scheme. The assumptions are mentioned below.

1. All the clients and service providers are supposed to be honest in the registration phase.
2. After registration phase is over, no client and server is trusted. The clients need to verify themselves during login phase by providing exact identification data to access services and applications.
3. Once mutual authentication is performed, the server is always trusted and it is assumed that the server never compromises with the network adversaries.

The proposed scheme consists of three phases; registration phase, login phase and authentication phase and one activity, called password change.

A) Registration phase:

In the registration phase, user needs to register at the server by providing appropriate identification details. The server process user's data and issue a smartcard to the user. The procedure is as follows:

1. *A* generate a random number *x* and compute $h(PW \oplus x)$.
2. *A=>S: ID,* $h(PW \oplus x)$, *h(x)*
3. *S* checks *ID* (new)=*ID* (existing). If equal, then reject registration request and go back to the step 1. Otherwise, proceed to the step 2.
4. *S* generates *y* and compute
   $J=h(ID \oplus h(PW \oplus x))$, $I= h(ID||y)$ and
   $B= g^{h(I||J)+h(x)+h(y)} \bmod p$.
5. *S* store {*I,J, B, p, g, h(.)*} in the smartcard.
6. Upon receiving the smartcard, the user enters *x* into the smartcard. Now smart card having {*I, J, B, p, g, h(.),x*}.
7. *S* stores *ID* in the *ID* table maintained in the server.

B) Login Phase:

This phase is invoked when user wants to login into the clouds. The users are verified before access to the cloud. The procedure is described below:

1. *A* insert the smartcard and enter *ID* and *PW*.
2. Local system compute $J_1= h(ID \oplus h(PW \oplus x))$, and check if $J_1=J$ then proceed to the next step, otherwise abort.
3. Compute, $C=h(I||J)$ and $A \rightarrow S: M_1$. *A* send login request message, M_1 to the server over the public channel. Here, $M_1=<B, C>$is login request message,.
4. Subsequently, the server generate *K*, compute $B''=g^{C+h(y)} \bmod p$, $h(B'')$, $L=h(B''||K)$, and $h(L)$. And the server generate message $M_2= <h(B''),h(L)>$.
5. $S \rightarrow A: M_2$, *S* sends M_2 to *A* using public channel. Also, S=>A*: K*, S sends *A*, onetime key, *K* using secure *OOB* channel to user's mobile phone.
6. Upon receiving message M_2, *A* computes*:* $B'=Bg^{-h(x)} \bmod p$ and $h(B')$ and $L*=h(B'||K)$, and $h(L*)$.
7. *A* Check the two conditions, $h(B')=h(B'')$ and $h(L*)=h(L)$, whether true or not .
   If both conditions are true, then proceed to the next step, otherwise terminate the login session.
8. *A* compute $R=h(T||B')$, and generate $M_3=<I,h(R),T>$. $A \rightarrow S$: M_3. *A* send message M_3 to the server over the public channel. Here *T* is the current time stamp of the user.

C) Authentication Phase:

Authentication phase is processed in the server where, the server will decide whether *A* should be allowed to login or not. The authentication phase process is as follows.

1. Check if $T' - T \leq \Delta T$ holds true or not. If the condition is false, then rejects the session. Otherwise, proceed to the next step. Here, ΔT is the maximum legal time difference for an authentication session defined for a networking system and T' is the current time stamp of the server.
2. Compute $I'=h(ID||y)$ and $R*=h(T||B'')$.

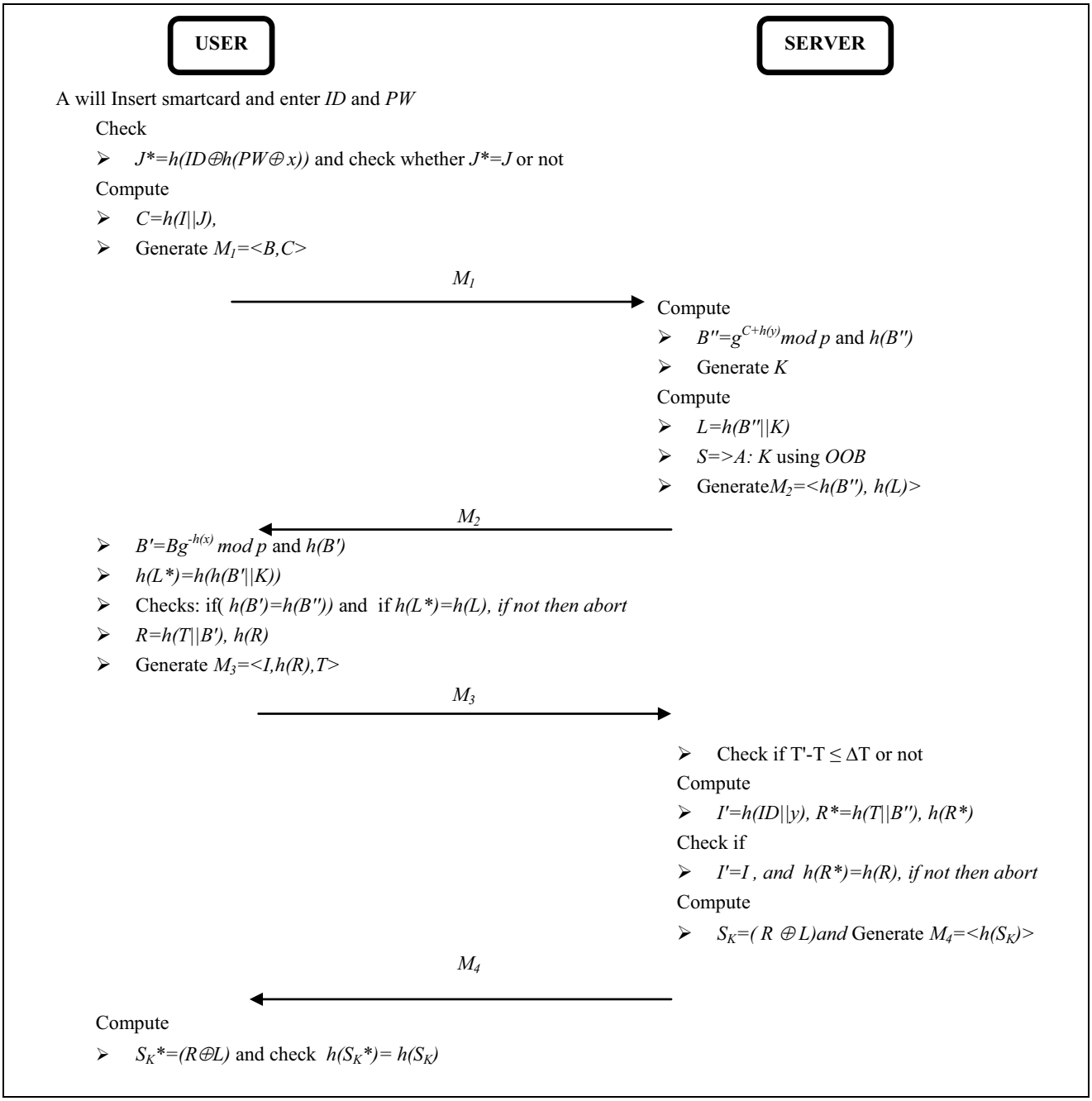

Figure 2: Login and authentication Phase

3. Check whether $h(R^*)=h(R)$ and $I'=I$. If both conditions are true, then proceed to the next step. Otherwise, terminate the login session.
4. The server generate a session key $S_K= (R \oplus L)$ and compute $h(S_K)$, which is message $M_4 <h(S_K)>$. $S \rightarrow A$: M_4 The message M_4 is sent to the user over public channel which contain the hash of a session key, *i.e.,* $h(S_K)$.

The flow of login and authentication phase is shown in figure 2.

The session key S_K is needed for final authentication for the user which is valid for some constant definite time. The session key (S_K), can be calculated by the user as $S_K= (R \oplus L)$.

D) Password change:

Password change is a user friendly facility, which is a very important requirement in user authentication schemes. It allows users to change their password anytime whenever user wishes to change their password. The procedure for password change is discussed below.

1. User chooses a change of password, in the self system.
2. *A* enter *ID* and *PW* and compute $J^*=h(ID \oplus h(PW \oplus x))$.
3. Local system will check $J^*=J$, if yes, then go to the next step, otherwise rejects the request.
4. *A* enter new password, PW' and generate x'.
5. Compute, $J'= h(ID \oplus h(PW' \oplus x'))$.
6. Replace J by J' and x by x' in the smartcard.

V. SECURITY ANALYSIS

1. *Identity management:* The server stores all the registered *ID*s in the *ID* management table and check availability of unique *ID* in each new registration.
2. *User privacy:* The proposed scheme never transmits user private data in plaintext form. The messages $M_1=<B,C>$, $M_2=<h(B''),h(L)>$, $M_3=<I, h(R),T>$ and $M_4=<h(Sk)>$ are transmitted over the public channel. Clearly, these messages cannot be decoded easily to get *ID, PW* etc. Hence, the scheme provides user privacy.
3. *Mutual authentication:* In the 7th step of login phase, the user checks whether $h(B')= h(B''), h(L^*)=h(L)$ and authenticates the server. Subsequently, in the 3rd step of authentication phase, the server checks $h(R^*)=h(R)$ and $I'=I$ or not. This way the server validates user. Hence, mutual authentication is performed.
4. *Password change:* Proposed scheme facilitate users to change password any time as shown in section IV(D). Password change facility makes a schemes inherently stronger compared static password based schemes. Moreover, it gives flexibility to users such that, users can change password if they forget or if they get hacked. Hence, it is user friendly.
5. *Session key agreement:* A session key, S_K is established between the user and the server after authentication process. This key is different in every login session and cannot be replayed after the session expires.
6. *Replay attack:* The onetime key is valid for one login session, and the key is delivered to the user via mobile out of band channel. Moreover, the scheme provides session key agreement between the user and the server which is also valid for only one login session. Hence our scheme is strong against Replay attack.
7. *Man in the middle attack:* In the message M_1, even if attacker knows *B* and *C*, they cannot calculate B'', without the knowledge of *y*. In message M_2, *L* can be verified only when someone knows both B' and *K*. B' is very difficult to compute and *K* is transmitted using secure *OOB* channel. In message M_3, no one can compute and verify I' and R^* without the knowledge of y and B''. Hence MITM attack is not applicable to the proposed scheme.
8. *Denial of service attack:* In the login phase step 1, (Section *V(B)),* the user's legitimacy is verified in the local system before communicating with the cloud server. The password change activity is also performed in the local system only. Hence, login phase step 1 and password change step (1-3) confirms our scheme to be strong against DOS attack.
9. *Stolen verifier attack and data modification attack*: The server secret value y is not known to the user. Smartcard contain *{I,J,B,p,g,h(.),x},* but without the knowledge of *ID, PW* and *K* it is very difficult to find B', *L, R,*. Thus, even if smartcard is stolen or lost, stolen verifier attack and data modification attack is not applicable in the scheme.
10. *Impersonation attack:* The proposed scheme never transmits user *ID* and *PW* directly through the public channel. Instead, *ID* and *PW* are hashed and performed some operations over it. Also the scheme uses high entropy onetime key, delivered to user using separate out of band channel for proper authentication. Hence the proposed scheme is strong against impersonation attack.
11. *Phishing attack*: Mutual authentication between the user and the server is performed (section VI step 3) in the scheme. Only the genuine server can send proper user identification data ($h(B'')$), which will be verified by the user. Hence, the scheme is also strong against phishing attack.
12. *Password guessing attack:* The scheme uses complex password term ($J=h(ID \oplus h(PW \oplus x))$) using one way hash function. Moreover, the scheme uses onetime key (*K*) using different communication channel (*OOB*), which provide more robustness to the scheme. Hence, without knowing *x, y and K*, the scheme cannot be broken by password guessing attack.
13. *Insider attack:* Insider attack is the most hazardous threat to any inter-networking system. In the proposed scheme, the password is never used openly, instead, it is digest with ($J=h(ID \oplus h(PW \oplus x))$), which is very difficult to invert. Moreover, attackers need the user secret number *x*, and onetime key *K*, and the smartcard to get access to the cloud. Only a genuine user can provide *x*, *K*, and smartcard simultaneously. Hence, the scheme is strong against insider attack.

VI. CONCLUSION

This paper proposes a strong user authentication framework for cloud computing with many security features, such as identity management, mutual authentication, session key agreement between the users and the cloud server, and user friendliness (i.e., password change phase). The term, strong two factor signifies one factor in 'something you know' (password) and two factors in 'something you have' (smartcard and *OOB*). In addition, cloud computing being a combination of computing resources; resource constrains are given less priority to provide high security to the cloud. Hence, this paper has not performed any performance comparison with some

existing schemes. The proposed protocol can resist many popular attacks such as replay attack, man in the middle attack, and denial of service attack. Currently, study on some formal security proofing technique of is on process, and providing formal security proof to the proposed framework will be the future research goal.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2011-0004833 and 2011-0023076)

REFERENCES

[1]. M. Armbrust, A. fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Above the Clouds: A Berkely view of Cloud Computing" Technical Report No. UCB/EECS-2009-28. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (Accessed in May 2011).

[2]. S. Ramgovind, MM. Eloff, E. Smith, "The Management of Security in Cloud Computing", Information Security for South Africa (ISSA), 2010.

[3]. "Introduction to Cloud Computing architecture", whitepaper 1st edition, June 2009, or http://webobjects.cdw.com/webobjects/media/pdf/Sun_Cloud Computing.pdf.

[4]. Global Netoptex Incorporated, 2009, demystifying the cloud. Important opportunities, crucial choices, http://www.gni.com, pp 4-14, viewed 13 December 2009.

[5]. R. Chakraborty, S. Ramireddy, T.S. Raghu, H. R. Rao, "The Information Assurance Practices of Cloud Computing Vendors". IT Professional,vol.12, 2010. pp.29-37.

[6]. H. G. Miller and J. Veiga, "Cloud Computing: Will Commodity Services Benefit Users Long Term?" IT Professional, vol.11, 2010, Pp.29-37.

[7]. M. S. Blumenthal, "Hide and Seek in the Cloud". Security & Privacy, IEEE, vol 8, 2010, Pp 57-58.

[8]. L. Ponemon, "Security of Cloud Computing Users," Ponemon Institute, Research Report, May 2010. http://www.ca.com/files/industryresearch/security-cloud-computing-users_235659.pdf

[9]. F. Gens, 2009,' New IDC IT Cloud Services Survey: Top Benefits and Challenges',IDC eXchange, viewed 14 July 2011, http://blogs.idc.com/ie/?p=730.

[10]. S. Lee, I. Ong, H.T. Lim, H.J. Lee, "Two factor authentication for cloud computing", International Journal of KIMICS, vol 8, Pp. 427-432

[11]. S. A. Almulla, C. Y. Yeun," Cloud Computing security Management", IInd International Conf. engg systems management and its applications(ICESMA),2010.

[12]. Z. Shen, L. Li, F. Yan, X. Wu, "Cloud Computing System Based on Trusted Computing Platform", Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on , vol 1, Pp 942-945.

[13]. A. Celesti, F. Tusa, M. Villari, A Puliafito, "Security and Cloud Computing: InterCloud Identity Management Infrastructure", 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 , Pp 263-265.

[14]. C. Danwei, H. Xiuli, and R. Xugyi, "Access control of cloud services based on UCON," CloudCom 2009, LNCS 5931, pp. 559-564, 2009.

[15]. L. Lamport, "Password authentication with insecure communication," Comm. ACM 24(11), Nov 1981, 770–771.

[16]. M.S.Hwang, and L.H. Li, "A New Remote User Authentication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics 46 (1) (2000) 28-30.

[17]. M.K. Khan, "Cryptanalysis and Security Enhancement of Two Password Authentication Schemes with Smart Cards", Multitopic Conference, 2007. INMIC 2007. IEEE International.

[18]. H.Y. Chien, J.K. Jan, Y.M. Tseng, "An efficient and practical solution to remote authentication: Smart card," Comput. Secur. 21 (4) (2002) 372–375.

[19]. I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, "A password authentication scheme over insecure networks," J. Comput. System Sci. 72 (4) (2006) 727–740.

[20]. E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," IEEE Trans. Consum. Electron. 50 (2) (May 2004) 568–570.

[21]. E.J. Yoon, K.Y. Yoo, "New authentication scheme based on a one-way hash function and Diffie–Hellman key exchange," 4th International Conference of Cryptology and Network Security, CANS 2005, LNCS vol. 3810, Springer-Verlag, 2005, pp. 147–160.

[22]. M.-S. Hwang, "Cryptanalysis of remote login authentication scheme," Comput. Commun. 22 (8) (1999). Pp. 742–744.

[23]. M.-S. Hwang, C.-C. Lee, Y.-L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," Internat. J. Inform. 12 (2) (2001).pp. 297–302.

[24]. M. Scott, "Cryptanalysis of an id-based password authentication scheme using smart cards and fingerprints," SIGOPS Oper. Syst. Rev. 38 (2) (2004). Pp. 73–75.

[25]. B. Wang, J.H. Li, Z.P. Tong, "Cryptanalysis of an enhanced timestamp-based password authentication scheme," Comput. Secur. 22 (7) (2003). pp. 643–645.

[26]. E.J. Yoon, K.Y. Yoo, "New authentication scheme based on a one-way hash function and Diffie–Hellman key exchange," 4th International Conference of Cryptology and Network Security, CANS 2005, LNCS, vol. 3810, Springer-Verlag, 2005, pp. 147–160.

[27]. V. Shoup, A. Rubin, "Session key distribution using smartcards", in: Proc. EUROCRYPT 96, in: LNCS., vol 1070, Springer-Verlag, 1996, pp 321-333

[28]. M. Bellare, P. Rogaway, Provably secure session key distribution—The third party case, in: Proc. 27th ACM Symp. on Theory of Computing, ACM, Las Vegas, 1995, pp 57-66.

[29]. G.Yang, D. S. Wong, H. Wang, X. Deng, "Two-factor mutual authentication based on smart cards and passwords", Journal of Computer and System Sciences, vol 74, 2008, Pp. 1160-1172.