# Analysis and Improvement of User Authentication Framework for Cloud Computing

Nan Chen, Rui Jiang
School of Information Science and Engineering, Southeast University, Nanjing, China
chennseu@126.com, R.Jiang@seu.edu.cn

***Abstract* — Cloud Computing, as an emerging, virtual, large-scale distributed computing model, has gained increasing attention these years. Meanwhile it also faces many secure challenges, one of which is authentication. Amlan Jyoti Choudhury et al proposed a user authentication framework to ensure user legitimacy before entering into the cloud. However, the scheme is found to suffer from some attacks through our analysis. In this paper, we firstly analyze few attacks and the make an improvement on the user authentication framework. Our new protocol ensures that only legitimate users can access the cloud service based on smartcard. Security analysis shows our proposed scheme is secure under standard cryptographic.**

***Keywords—Cloud Computing; Remote user authentication; Smartcard; Security***

## I. INTRODUCTION

Recently, cloud computing has been greatly interested by both academic and industry communities. It is like a "resource pool", which can provide the cost-effective and on-demand services to meet the needs by outsourcing data [1]. However, as an attractive paradigm, it also faces many challenges, and the security issues are the most important. As mentioned in [2], cloud security issues can be classified into four categories: authentication, data integrity, data confidentiality and access control. User authentication is the paramount requirement for cloud computing that restricts illegal access of cloud server and so far many schemes have been proposed. In this paper, we mainly discuss the identity authentication between the user and cloud server.

In many circumstances the weakest link is the password used to access a web-based application. Therefore rather than using just a password to login to a website, users couple a password with a second authentication mechanism called two factor authentication. With two factor authentication even if someone has stolen your password, they'll need physical access to your secondary authentication mechanism in order to access your data [3]. And nowadays two factor authentication has been introduced into cloud.

In 1981, Lamport [4] proposed a remote user authentication system, in which, the server stores the hash value of the user's password for the later verification. However, in 2000, M.S.Hwang et al [5] presented that if the password table was compromised, the whole system could be invalid. Then they proposed a new remote user authentication scheme using smart cards. But this scheme does not resist impersonate attack. In 2010, Chen and Huang [6] proposed a user participation-based authentication combining CAPTCHA and visual secret sharing. Later Chun-Ta Li et al [7] pointed out that Chen et al's scheme existed masquerading attack when the smartcard had been stolen. Recently the user login security is more and more concerned in the case of smartcard lost [7][8].

In 2011, Amlan Jyoti Choudhury et al [9] presented a user authentication frame for cloud computing. They applies identity authentication with smartcard to cloud computing and it is a new idea. The scheme verifies user authenticity using two-step verification, which is based on password, smartcard and out of band authentication. However, through our security analysis, the scheme exist extremely serious attacks.

In this paper, we focus on secure user authentication in cloud computing. We analyze the vulnerability and attacks existing in Amlan et al's protocol. To overcome these issues, we propose an advanced authentication protocol. In our scheme, we realize the basic requirements for evaluating a password authentication scheme [10].

The rest of the paper is organized as follows. Section 2 gives a brief introduction of the related authentication frame proposed by Amlan Jyoti Choudhury et al and points out the vulnerabilities and attacks to the protocol. The new remote user authentication scheme against smartcard security breach is proposed in Section3 and security analysis of our protocol is explained in Section4. Finally, we make a conclusion in Section5.

## II. REVIEW OF RELATED WORKS

Recent years, a few password-based remote authentication schemes using smartcard have been proposed in cloud computing. In this section, we review one of the recent password-based remote authentication schemes. For convenience of description, we will list the common notations used throughout this paper first.

### *A. Notations*

A: A login user
S: The cloud server
*ID*: Identity of the user
*PW*: The password of the user
*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)
$h(\cdot)$: One way hash function

Published by Atlantis Press, Paris, France.
© the authors

$E_K(\cdot)/D_K(\cdot)$ :The symmetric encryption/decryption function with key *K*

||: Concatenation operation

X→Y: Message M is sent X to Y through public channel

X=>Y: Message M is sent X to Y through secure channel

$\oplus$ : The XOR operation

### *B. Brief review of Amlan et al's Frame*

There are four phases in Amlan et al's scheme [9]: registration, login, authentication and password change. Different phases work as follows.

1. Registration phase

1. A selects a random number $x$ and computes $h(PW \oplus x)$.

2. A=>S: $ID$, $h(PW \oplus x)$, $h(x)$

3. Cloud server checks whether the $ID$ has existed firstly. Then the server generates $y$ and computes $J = h(ID \oplus h(PW \oplus x))$, $I = h(ID \| y)$ and $B = g^{h(y)+h(I\|J)+h(x)} \bmod p$.

4. S=>A: a smartcard containing $\{I, J, B, p, g, h(.)\}$.

5. Upon receiving the smartcard, the user enters $x$ into the smartcard.

6. S stores $ID$ in the $ID$ table maintained in the server.

2. Login phase

1. A inserts the smartcard and enters $ID$ and $PW$.

2. Local system computes $J_1 = h(ID \oplus h(PW \oplus X))$, and check whether $J_1 = J$ or not. If true, proceed to the next step, otherwise abort.

3. A computes $C = h(I \| J)$

4. A→S: $M_1 =< B, C >$

5. The server generates onetime key $K$ and send it to user's mobile phone using secure OOB channel. Then S computes $B'' = g^{C+h(y)} \bmod p$, $h(B'')$, $L = h(B'' \| K)$ and $h(L)$.

6. S→A: $M_2 =< h(B''), h(L) >$

7. Upon receiving $M_2$, A computes $B' = Bg^{-h(x)} \bmod p$, $h(B')$, $L^* = h(B' \| K)$ and $h(L^*)$. Then A checks whether $h(B') = h(B'')$ and $h(L^*) = h(L)$ or not. If both conditions are true, then proceed to the next step. Otherwise terminate the login session.

3. Authentication phase

1. A computes $R = h(T \| B')$. Here, T is the timestamp of the current time.

2. A→S: $M_3 =< I, h(R), T >$

3. The server checks if $T' - T \le \Delta T$ .Here, $\Delta T$ 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. Then, S computes $I' = h(ID \| y)$ and $R^* = h(T \| B'')$, and checks whether $h(R^*) = h(R)$ and $I' = I$. If both equations are true, S will generate $S_k = (R \oplus L)$ . Otherwise the server terminates the communication.

3. S→A: $h(S_k)$

4. The user checks $h(S_k)$ by computing $h(S_k^*) = h(R \oplus L)$.

4. Password change phase

The User A chooses a change of password in the self system. Then A enters $ID$ and $PW$, and computes $J^* = h(ID \oplus h(PW \oplus x))$ .Local system will check $J^* = J$, if $J^* \neq J$, then rejects the request, otherwise A enters a new password $PW'$ and generates $x'$. The smartcard computes $J' = h(ID \oplus h(PW' \oplus x'))$ and replace $J$ by $J'$ and $x$ by $x'$ in the smartcard.

### *C. The Attacks*

1. Masquerading attack

If a user's smartcard is lost or stolen and it is got by an attacker, the attacker can extract the secret information stored in the smartcard. As the messages sent from A to S are only related with secret data stored in the smartcard, the attacker can masquerade as a legal user. The attacker can compute $C = h(I \| J)$ , $B' = Bg^{-h(x)} \bmod p$ , $h(R) = h(h(T \| B'))$. Therefore, the messages in login phase step2 and authentication phase step1 can be generated by the attacker so that the attacker can successful makes a valid login request as a legal user.

Besides, at the end of the authentication phase, S sends $h(S_K)$ to A. A computes $S_K{}^*$ and checks whether $h(S_K{}^*) = h(S_K)$ or not. If the attacker modifies $h(S_K)$, A will not be able to authenticate server. Therefore, it will cause that the server completes the authentication while the client doesn't think so. The communication between user and server cannot be established. Mutual authentication is imperfect.

2. OOB attack

In this scheme, the authors think the major advantage of the scheme is the OOB (out of band) factor. To improve the security, the cloud server generates the onetime key for the mobile network through HTTP/SMS gateway. The mobile network delivers the onetime key to the user's mobile phone via SMS. However, some facts show that this method is not as good as the authors think.

Lots of attacks for out-of band have been proposed such as SMS interception, phone flooding or SMS phishing. The details are described in [11][12]. In the cybercrime trend of future, these attacks will become a great threat for the out-of-band authentication.

3. Password change phase flaw

In the phase of password changing, the user only makes the change of $J$ and $x$ in the smartcard. But the user does not change $B$, which is used in the authentication. This may lead to login failures once the user change the password. For example, the original parameters were $PW$, $J$ and $x$. After the user altered the password, these


© the authors

parameters change to $PW^{'}$, $J^{'}$ and $x^{'}$ .Then when the user logins into the cloud server, in the step3 of the login phase, the server computes $B^{"} = g^{C+h(y)} \bmod p = g^{h(I\|J^{'})+h(y)} \bmod p$ . Then the server sends $h(B^{"})$ to the user for verification. The user computes $B^{'} = Bg^{-h(x^{'})} \bmod p = g^{h(I\|J)+h(y)+h(x)+h(x^{'})} \bmod p$ in step4. Obviously, $h(B^{'}) \neq h(B^{"})$ . The authentication fails and the login fails.

## III. OUR PROPOSED SCHEME

In this section, we improve the Amlan et al's scheme. Our proposed scheme resolves their security flaws and enhances the security. This scheme has four phases: registration phase, login phase, authentication phase and password change phase. The details are described as follow.

### A. Registration Phase

In the registration phase, user provides appropriate identification details to the cloud server. Then the cloud server issues a smartcard to the user according user's data.

1. A selects a random number $x$ and computes $h(PW \oplus x)$.

2. A=>S: $ID$, $h(PW)$, $h(PW \oplus x)$.

3. S checks whether the $ID$ has existed in server. If it is true, S rejects registration request. Otherwise, S generates $y$ and computes:

$I = h(ID \| y)$

$B = g^{ID+h(PW)+h(y)} \bmod p$

4. S=>A: a smartcard containing $\{I, B, p, g, h(\cdot)\}$.

5. A enters $x$ into his smartcard. Now smartcard contains $\{I, B, p, g, h(\cdot), x\}$.

6. S stores $ID$ and $h(PW \oplus x)$ in the serve.

### B. Login Phase

This phase is invoked when user wants to login into the cloud.

1. A inserts his smartcard and enters $ID$ and $PW$.

2. The smartcard computes $C = h(I \| h(PW \oplus x) \| T_u)$, where $T_u$ denotes A's current timestamp.

3. A→S: $ID, C, T_u$.

### C. Authentication Phase

After receiving the login request message $\{ID, C, T_u\}$, the server verify the identity of the user. The procedure is as follows.

1. If $T_u^{'} - T_u < \Delta T$ , S rejects A's login request. Otherwise, S performs the following computations: $I^{*} = h(ID \| y)$, $C^{*} = h(I^{*} \| h(PW \oplus x) \| T_u)$. Here, $T_u^{'}$ is the current timestamp of server and $\Delta T$ is the maximum time interval for transmission delay. If $C^{*}$ equals $C$, S accepts A's login request and computes $K^{'} = g^{ID+h(y)} \bmod p$, $h(K^{'})$ and $R = h(K^{'} \| T_s)$. $T_s$ is S's current timestamp. S generates a random number $a$.

2. S→A: $E_{h(K^{'})}\{R, T_s, a\}$.

3. A computes $K^{"} = Bg^{-h(PW)} \bmod p$ and $h(K^{"})$. Then A uses $h(K^{"})$ to decrypt $E_{h(K^{'})}\{R, T_s, a\}$ and gets $\{R, T_s, a\}$. A checks the timestamp. If $T_s$ is invalid, A terminates this session. Otherwise, A computes $R^{'} = h(K^{"} \| T_s)$ and compares $R^{'}$ to the received $R$. If equal, A successfully authenticates S.

4. A→S: $h(a)$

5. S checks $h(a)$. If $h(a)$ is correct, mutual authentication successes. Now both user A and server S can compute the session key $S_K = h(K^{'} \| a) = h(K^{"} \| a)$.

### D. Password Change Phase

This phase is invoked when the user wants to change his password.

1. A insert his smartcard into smartcard reader and enter $ID$ and $PW$.

2. A→S: $E_{S_K}\{h(PW \oplus x) \| h(PW^{'} \oplus x) \| b\}$

A and S execute the login and authentication phase mentioned above. If A passes the verification, A will send a password change request to S, and then submit $h(PW \oplus x)$ and $h(PW^{'} \oplus x)$ .Here $PW^{'}$ is A's new password, $b$ is a random number.

3. S checks $h(PW \oplus x)$ and replaces it by $h(PW^{'} \oplus x)$.

4. S→A: $h(b)$

5. A checks $h(b)$. If it is correct, the smartcard performs the following computations:

$Z = Bg^{-ID-h(PW)} \bmod p$

$B^{'} = Zg^{ID+h(PW^{'})} \bmod p$

6. A replaces $B$ by $B^{'}$ in the smartcard.

## IV. SECURITY ANALYSIS

In this section, we evaluate the security of the proposed scheme.

1. Identity management: The cloud server stores all the registered users' $ID$ s, and checks $ID$ in registration phase and login phase.

2. User privacy: The messages related to user's private data (i.e. $PW$ etc) are never transmitted in plaintext in our protocol. The attacker cannot crack these from the messages.

3. Replay attack: In the login and authentication phases, the transmitted messages contain timestamp. $C = h(I \| h(PW \oplus x) \| T_u)$ , $R = h(K^{'} \| T_s)$ . Hence our scheme is strong against replay attack.

4. Man in the middle attack: In our protocol, no matter


© the authors

which message is modified by adversary, the communication will terminate. For example, if $ID$ is modified into $ID^*$ in login phase, $I^* = h(ID^* \| y)$, $C^* = h(I^* \| h(PW \oplus x) \| T_u)$. Then $C^* \neq C$, terminate the communication.

5. Stolen verifier attack and insider attack: Usually the server stores some verification or password table in its database to verify the legality of the login user. Thus server's database may be the attacker's target. In our scheme, even if the attacker has obtained the verification table, the attacks is not existed. Because only knowing $ID$ and $h(PW \oplus x)$, the attacker cannot compute $C = h(I \| h(PW \oplus x) \| T_u)$ and $K' = g^{ID+h(y)} \bmod p$.

In addition to the above advantages, our protocol has greatly enhanced the security compared to Amlan et al's in the following aspects.

6. Withstanding masquerade attack: our proposed scheme can withstand masquerade attack with smartcard revealing. When A's smartcard has been stolen, the attacker can breach the data $I, B, p, g, h(\bullet)$ stored in the smartcard. The attacker cannot compute $h(I \| h(PW \oplus x) \| T_u)$ according these parameters. And neither $K'$ nor $K''$ can be got by the attacker without knowing $PW$ or $y$. So even if the smartcard is stolen, our protocol can protect users' login security.

Besides, our proposed scheme can provide mutual authentication. At the step2 of authentication phase, S sends $E_{h(K')}\{R, T_s, a\}$ to A. A checks $R$ to verify S. Meanwhile A sends a response $h(a)$ to S for verification. Thus the mutual authentication is performed.

7. Avoiding OOB attack: our proposed scheme does not use onetime key $K$. Instead, we use $h(K')$ to encrypt the message to ensure protocol secure. Thus we avoid transmitting $K$ through OOB channel and avoid OOB attack. In Amlan et al's scheme since the final session key is related to the onetime key $K$, the final session key is different in every login. Although we don't use onetime key $K$, our final session key is related to a random number, which is different in every session. Therefore a different session key will be generated between user and server in every login.

8. Password change: our proposed scheme facilitates users to change password. As described in password change flaw, Amlan et al's scheme cannot achieve the function of changing password. In our scheme, when we change the password, we change $h(PW \oplus x)$ in the server and $B$ in the smartcard at the same time for the later authentication. It is inherently stronger compared static password based scheme.

## V. CONCLUSION

In this paper, we make a security analysis on the user authentication framework proposed by Amlan Jyoti Chouhury et al and point out some security attacks to it. Then we proposed a improved scheme for cloud computing. Our scheme inherits the merits of Amlan's protocol and enhances the security for user communicating with cloud server. Security analysis is presented in section 4, and our scheme can resist most current attacks. Performance simulation will be our future work.

## ACKNOWLEDGEMENTS

This work is supported by the Program of Changzhou Key Laboratory of Hi-tech under contract CM20103003, the Key Lab of Information Network Security, Ministry of Public Security under contract C12602, and the Program of Science and Technology Supporting Project under contract CE20120030.

## REFERENCES:

[1] Michael Armbrust , Armando Fox , Rean Griffith , Anthony D. Joseph , Randy Katz , Andy Konwinski , Gunho Lee , David Patterson , Ariel Rabkin , Ion Stoica , Matei Zaharia, "A view of cloud computing," Communications of the ACM, v.53 n.4, April 2010.

[2] Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Ku, "Multimedia Storage Security in Cloud Computing: An Overview," 13th International Workshop on Multimedia Signal Processing (MMSP), 2011.

[3]Jack Newton,Beyond Passwords: Two Factor Authentication Comes to t he Cloud.

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

[5] 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.

[6] T. H. Chen and J. C. Huang, "A novel user-participating authentication scheme," The Journal of Systems and Software, 83(5):861–867, 2010.

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

[8] H. C. Hsiang and W. K. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Computer Communications, 32(4):649–652, 2009.

[9] Amlan Jyoti Choudhury, Pardeep Kumar, Managal Sain, Hyotaek Lim, Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing", Asia-Pacific Services Computing Conference, 2011 IEEE.

[10] I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, "A password authentication scheme over insecure networks", Journal of Computer and System Sciences 72(2006) 727-740.

[11] S21sec blog report, "ZeuS Mitmo: Man-in-the-mobile",2010

[12] Szu yu Lin. "Enhancing the security of out-of-band one-time password two factor authentication in cloud computing". Department of Electrical Engineering, 2010.


© the authors