An Improvement of User Authentication Framework for Cloud Computing

Jongho Mun, Jiye Kim, Dongho Won*
College of Information and Communication Engineering, Sungkyunkwan University, Korea.

* Corresponding author. Tel: +82-31-290-7107; email: dhwon@security.re.kr
Manuscript submitted July 15, 2015; accepted December 15, 2015.
doi: 10.17706/jcp.11.6.446-454

Abstract: Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as outsourcing services through the Internet. With cloud computing technique, the users are able to outsource their computing and storage tasks to the cloud servers. In cloud computing environments, the user authentication is very important issue because it provides the authorization while users access their data and cloud services. In 2014, Chen *et al.* improved Choudhury *et al.*'s scheme, and claimed that their scheme is more secure and practical remote user authentication scheme for cloud computing. However, we find that Chen *et al.*'s scheme is still insecure against outsider attack, server impersonation attack, smart card stolen attack and off-line password guessing attack. To overcome this drawback, we propose a robust and more secure user authentication scheme. Finally, we show that our proposed scheme is more secure and supports security properties than Chen *et al.*'s scheme.

Key words: Cloud computing, remote user authentication, smart card.

1. Introduction

Cloud Computing [1] is defined that refers to both the applications delivered as services via the Internet and the hardware and system software in the data center that provide those services. Thus, "cloud" can be defined a set of storages, services and interfaces those are provides by servers. Cloud computing allows users store and access all the data and services through the Internet instead of their own computers. The cloud computing can be categorized according to services available on the cloud namely IaaS (Infrastructure as a Service), SaaS (Software as a Service) and PaaS (Platform as a Service) [2]. According to [3], the security issues of cloud system can be classified into four categories: authentication, data integrity, data confidentiality and access control. Above all, the user authentication in cloud computing environments is very important issue because it provides the authorization while users access their data and cloud services. Since Lamport [4] proposed the first password-based authentication scheme over insecure communication in 1981, password-based authentication schemes [5]-[8] have been extensively investigated. However, a problem of password-based authentication scheme is that a server must maintain a password table for verifying the legitimacy of a remote user. Therefore, the server requires additional memory space for storing the password table for verifying user identity. Furthermore, password is generally simple and can be easily broken or forgotten. For this reason, many remote user authentication schemes using smart card [9]-[12] have been proposed. In 2011, Choudhury *et al.* [13] presented a user authentication frame for cloud computing. Choudhury *et al.* applies identity authentication with smart card for cloud computing. Their scheme verifies user authenticity using two-step verification, which is based on password, smart card and out of band authentication. However, in 2014, Chen *et al.* [14] found that Choudhury *et al.*'s scheme does not provide proper authentication and cannot resist impersonation attack. They proposed an improved scheme of Choudhury *et al.*'s scheme for cloud computing. However, Chen *et al.*'s scheme is still insecure. We find that their scheme cannot withstand outsider attack, impersonation attack, smart card stolen attack and off-line password guessing attack as well. Furthermore, Chen *et al.*'s scheme has no wrong password detection mechanism. To overcome this drawback, we propose a robust and more secure remote user authentication scheme which is an improvement of Chen *et al.*'s scheme. The remainder of the paper is organized as follows. We begin by reviewing Chen *et al.*'s remote user authentication scheme in Section 2. In Section 3, we describe security weaknesses of Chen *et al.*'s scheme. Our proposed scheme is presented in Section 4. Security analysis of our proposed scheme is given in Section 5. Finally, we conclude this paper in Section 6.

2. Review in Chen *et al.*'s Scheme

This section reviews the remote user authentication scheme proposed by Chen *et al.* in 2014. As previous researches, Chen *et al.*'s scheme consists of four phases: registration, login, authentication and password change phases which as follows. The notations used in this paper are summarized as Table 1.

Table 1. Notations Used in This Paper

Notations	Description
$A(U)$	A login user
S	The cloud server
SC	A smart card
$ID,\ PW$	Identity and password of the user
N	A random number unique to login user
K	One-time key
X	A user's secret number
Y	A server's 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
$E_k(\cdot)/D_k(\cdot)$	The symmetric encryption/decryption function with the key K
$\|\|$	Concatenation operation
$X \rightarrow Y$	Message M is sent X to Y through public channel
$X \Rightarrow Y$	Message M is sent X to Y through secure channel
$\oplus$	The XOR operation

2.1. Registration Phase

The registration phase is the initial phase of the scheme. In this phase, user provides appropriate identification details to the cloud server. Then the cloud server issues a smart card to user according user's data.

1) A selects a random number x and computes $h(PW \oplus x)$.
2) $A \Rightarrow S: ID, h(PW), h(PW \oplus x)$.
3) S checks whether the ID has existed in server. If ID has existed in server, S rejects registration request. Otherwise, S generates y and computes:

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

4) $S \Rightarrow A$: a smart card. S sends smart card which contains $\{I, B, p, g, h(\cdot)\}$ to user A over secure

channel.

5) A enters x into his smart card. Now, smart card contains $\{I, B, p, g, h(\cdot), x\}$.
6) S stores ID and $h(PW \oplus x)$ in the server.

2.2. Login Phase

This phase is invoked when user wants to login into cloud. To start any conversation, the user must first login to a specific terminal using smart card.

1) A inserts his smart card and inputs ID and PW.
2) The smart card computes $C = h(I||h(PW \oplus x)||T_u)$ where T_u denotes A's current timestamp.
3) $A \rightarrow S$: ID, C, T_u.

2.3. Authentication Phase

After receiving the login request messages $\{ID, C, T_u\}$, the server verifies 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:

$$\mathrm{I}^* = h(ID||y)$$

$$C^* = h(\mathrm{I}^*||h(PW \oplus x)||T_u)$$

where $T_u{}'$ is the current timestamp of server and ΔT is the maximum time interval for transmission delay.

If C^* equals C, S accepts the user 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. Then, S generates a random number a.

2) $S \rightarrow A$: $E_{h(K')}\{R, T_s, a\}$.
3) Upon receiving response message, A computes $K'' = Bg^{-h(PW)} \bmod p$ and $h(K'')$. Then, A decrypts $E_{h(K')}\{R, T_s, a\}$ with $h(K'')$ 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 and sends the value $h(a)$ to server S.
4) S checks $h(a)$. If $h(a)$ is correct, mutual authentication successes. Now both user A and server S can compute the session key $S_K = h(K'|| a) = h(K''|| a)$.

2.4. Password Change Phase

The phase is invoked when the user wants to change his/her password.

1) A inserts his/her smart card into card-reader and inputs ID and PW.
2) $A \rightarrow S$: $E_{S_K}\{h(PW \oplus x)||h(PW' \oplus x)||b\}$. A and S executes 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 $h(PW' \oplus x)$ where PW' is A's new password and b is random number.
3) After receiving password change request, S checks $h(PW \oplus x)$ and replaces it by $h(PW' \oplus x)$.
4) $S \rightarrow A$: $h(b)$.
5) When receiving response message, A checks $h(b)$. If it is correct, the smart card performs,

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

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

6) A replaces B by B' in the smart card.

3. Security Analysis of Chen *et al.*'s Scheme

In this section, we demonstrate the vulnerability of Chen et al.'s scheme in various communication scenarios.

3.1. Denial-of-Service via Wrong Password Login

This is the type of attack when a legal user is denied access to services which are meant for him. Suppose A inserts wrong password PW in login phase. Smart card has no mechanism to detect it, then A sends wrong login request $\{ID_a, C_a', T_a\}$ as login request, when S checks the equivalence $h(I_a||h(PW_a \oplus x)||T_a) =? C_a'$. Clearly, it will not hold. As a result, S will terminate the session and A will face the DoS.

3.2. Outsider Attacks

Any adversary O who is the legal user and owns a smart card can obtain information $\{I_o, B_o, p, g, h(\cdot), x_o\}$ and then he/she can compute $g^{h(y)} \bmod p = B_o g^{-h(PW_o)-ID_o} \bmod p$. If an adversary O intercepts any user A's login request message $\{ID_a, C_a, T_a\}$ and server S's response message $E_{h(K)}\{R_s, T_s, a_s\}$, then he/she can compute the encryption key $h(K')$ by calculating $h(g^{ID_a+h(y)} \bmod p)$. Hence, adversary O can decrypt server S's response message and compute the session key $S_K = h(K'|| a)$.

3.3. Server Impersonation Attacks

If user A sends login request message $\{ID_a, C_a, T_a\}$ to outsider adversary O which impersonates as the server S, then O easily can compute $K' = g^{ID_a+h(y)} \bmod p$ by using $g^{h(y)} \bmod p$. An adversary O performs following step.

1) The adversary generates a random number a_o and computes $h(K')$ and $R_o = h(K'||T_o)$ where T_o is O's current timestamp.
2) $O \rightarrow A$: $E_{h(K')}\{R_o, T_o, a_o\}$. After receiving response message $E_{h(K')}\{R_o, T_o, a_o\}$ from O, A will decrypt response message and check the timestamp T_o and R_o. However, R_a' is equal of R_o. Therefore, an outsider adversary O can impersonate the server S.

3.4. Smart Card Stolen & Off-line Password Guessing Attacks

If an adversary O intercepts legitimate user A's login request message $\{ID_a, C_a, T_a\}$ and steals A's smart card, he/she can obtain parameters $\{I_a, B_a, p, g, h(\cdot), x_a\}$. Then, an adversary O can perform off-line password guessing attacks.

1) An adversary guesses any password PW^*.
2) Then an adversary calculates $h(I_a||h(PW^* \oplus x_a)||T_a)$ and compares it with C_a. If the result is equal to C_a, the adversary infers that PW^* is user A's password. Otherwise the adversary selects another password nominee and performs the same processes, until he/she locates the valid password.

3.5. Requirement of Verifying Table

The server S must maintain the verifying table that stores each user's ID and $h(PW \oplus x)$ for verifying the legitimacy of the login users in Chen *et al.*'s proposed scheme. Therefore, the server S requires extra memory space to store the verifying table. Although the one-way hash functions and encryption algorithms are applied to prevent the passwords from being disclosed, the verifying table is still vulnerable. Because any insider adversary who knows the server's secret key y easily can impersonate any user by using ID and $h(PW \oplus x)$. Furthermore, if user wants to change his/her password, then server S should replace $h(PW \oplus x)$ to $h(PW' \oplus x)$ in verifying table.

4. Our Proposed Scheme

In this section, we describe more secure remote user authentication. Our improved scheme consists of four phase and works as follows.

4.1. Registration Phase

The registration phase is operated when the user U_i initially registers to the cloud server S and is described as follows.

1) U_i chooses his/her identity ID_i and password PW_i, then computes $h(PW_i)$.
2) $U_i \Rightarrow S$: $ID_i, h(PW_i)$. U_i sends $\{ID_i, h(PW_i)\}$ to the server S over a secure channel.
3) Upon receiving registration request message from U_i, S generates N_i and y where N_i is a random number to unique to U_i. Then, S computes,

$$F_i = h(y) \oplus N_i$$

$$D_i = h(y||N_i) \oplus ID_i$$

$$B_i = g^{ID_i + h(Pw_i) + h(N_i||y)} \ mod\ p$$

$$V_i = F_i \oplus h(ID_i \oplus h(PW_i))$$

where p is a large prime number and y is a server S's secret number stored at the server.

4) $S \Rightarrow A$: a smart card. S installs $\{F_i, D_i, B_i, V_i, p, g, h(\cdot)\}$ in the smart card and sends the smart card to user U_i via secure channel.

4.2. Login Phase

If U_i wishes to login cloud server S, U_i inserts his/her smart card into the card-reader and performs the following steps.

1) U_i inputs his/her identity ID_i and password PW_i.
2) Then, smart card computes $F_i^* = V_i \oplus h(ID_i \oplus h(PW_i))$ and compares F_i^* with stored F_i. If it holds, smart card computes,

$$W_i = B_i g^{-h(Pw_i)} \ mod\ p$$

$$C_i = h(W_i||T_i)$$

where T_i is the current timestamp. Otherwise, smart card rejects login request.

3) $U_i \rightarrow S$: F_i, D_i, C_i, T_i. Smart card sends login request $\{F_i, D_i, C_i, T_i\}$ to S through a common channel.

4.3. Authentication Phase

After receiving the login request message $\{F_i, D_i, C_i, T_i\}$ from U_i, the server S verifies the identity of the user U_i. The procedure is as follows.

1) If $T_u' - T_u > \Delta T$, S rejects U_i's login request. Otherwise, S performs the following computations:

$$N_i = F_i \oplus h(y)$$

$$ID_i = D_i \oplus h(y||N_i)$$

$$W_i^* = g^{ID_i + h(N_i||y)} \ mod\ p$$

$$C_i^* = h(W_i^*||T_i)$$

where T_i' is the current timestamp of server and ΔT is the maximum time interval for transmission delay.

If C_i^* equals C_i, S accepts the user U_i's login request and computes,

$$K_s = W_i^* g^{T_i} \, mod \, p$$

$$h(K_s)$$

$$R_s = h(K_s || T_s)$$

where T_s is S's current timestamp. Then, S generates a random number a.

2) $S \rightarrow U_i: E_{h(K_s)}\{R_s, T_s, a\}$. S encrypts $\{R_s, T_s, a\}$ with $h(K_s)$, and sends the response message $E_{h(K_s)}\{R_s, T_s, a\}$ to user U_i.

3) After receiving response message, U_i computes,

$$K_i = W_i g^{T_i} \, mod \, p$$

and decrypts $E_{h(K_s)}\{R_s, T_s, a\}$ with $h(K_i)$ and gets $\{R_s, T_s, a\}$. U_i checks the timestamp. If T_s is invalid, U_i terminates this session. Otherwise, U_i computes $R_i = h(K_i || T_s)$ and compares R_i to the received R_s. If equal, U_i successfully authenticates S.

4) $U_i \rightarrow S: h(a)$. U_i computes $h(a)$ and sends $h(a)$ to server S.

5) S checks $h(a)$. If $h(a)$ is correct, mutual authentication successes. Now both user U_i and server S can compute the session key $S_K = h(K_i || a) = h(K_s || a)$.

4.4. Password Change Phase

If U_i wants to change his/her password, he/she inserts his/her own smart card into a card reader, then enters identity ID_i and password PW_i. After receiving identity ID_i and password PW_i, smart card performs the following steps.

1) Smart card computes $F_i^* = V_i \oplus h(ID_i \oplus h(PW_i))$ and compares F_i^* with stored F_i. If it holds, smart card accepts U_i to enter a new password PW_i^*. Otherwise, smart card rejects password changing request.

2) After receiving new password PW_i^*, smart card computes,

$$B_i^* = B_i g^{-h(Pw_i)+h(PW_i^*)} \, mod \, p$$

$$V_i^* = F_i \oplus h(ID_i \oplus h(PW_i^*))$$

and updates B_i, V_i as B_i^*, V_i^*. Then, U_i can use the new password PW_i^* to login the authentication cloud server S.

5. Security Analysis of Our Proposed Scheme

In this section, we demonstrate that our scheme can withstand several possible attacks. We also show that our scheme supports several security properties. Our proposed scheme keeps the merits of Chen *et al.*'s scheme

5.1. Support User Anonymity

Suppose an adversary U_a intercepts on user U_i's login request message. However, he/she fails to guess the user U_i's identity from $\{F_i, D_i, C_i, T_i\}$. In our proposed scheme, we use random number N_i which is the unique to user U_i and the timestamp T_i in the login phase, then user U_i's login request message is changed each login time. An adversary U_a does not know N_i and y. Thus, our proposed scheme supports user anonymity.

5.2. Resisting Impersonation Attack

In the our proposed scheme, only U_i can compute $W_i = B_i g^{-h(Pw_i)}\ mod\ p$ and $C_i = h(W_i||T_i)$ since only he/she has the secrets N_i and password PW_i and S can compute $N_i = F_i \oplus h(y)$ and $ID_i = D_i \oplus h(y||N_i)$ since only he/she has the secrets y. The authentication server S authenticates U_i by checking $h(g^{ID_i + h(N_i||y)}\ mod\ p||T_i) =?\ C_i$ and the remote user U_i authenticates S by checking $\mathrm{h}(K_i||T_s) =?\ R_s$. Thus, our proposed scheme can resist impersonation attacks.

5.3. Resisting Smart Card Stolen Attack

If an adversary U_a steals U_i's smart card, then U_a can extract security parameters $\{F_i, D_i, B_i, V_i, p, g, h(\cdot)\}$ from legitimate user U_i's smart card. However, this information does not help them. He/she cannot obtain any information of U_i's ID_i and PW_i because these values are protected by secret parameters. An identity ID_i in D_i(=$h(y||N_i) \oplus ID_i$) is protected by S's long-term secret key y and the collision resistance one-way hash function $h(\cdot)$, and a password PW_i in V_i(=$F_i \oplus h(ID_i \oplus PW_i)$), B_i(=$g^{ID_i + h(Pw_i) + h(N_i||y)}\ mod\ p$) is encrypted with ID_i. Therefore, the our proposed scheme can resist smart card stolen attack.

5.4. Resisting Replay Attacks

In the proposed authentication scheme, an adversary cannot correctly modifies $\{F_i, D_i, C_i, T_i\}$ and $E_{h(K_s)}\{R_s, T_s, a\}$ without ID_i, PW_i, N_i and y, where $ID_i = D_i \oplus h(y||N_i)$, $N_i = F_i \oplus h(y)$ and $C_i = h(W_i||T_i)$. When and an adversary U_a tries to use the previous message $\{F_i, D_i, C_i, T_i\}$ to login S or $E_{h(K_s)}\{R_s, T_s, a\}$ to response U_i, a failed adversary will be detected by checking the invalid timestamp T_i and T_s. Thus, the proposed authentication scheme is secure against the replay attack.

5.5. Comparison of Security Properties

We compare the proposed scheme with the scheme of Choudhury *et al.* [13], Chen *et al.* [14] regarding resistance to possible attacks as depicted by Table 2. Our proposed scheme resists all those attacks to which the previous schemes are susceptible.

Table 2. Comparison of Security Properties

Security Properties	Choudhury *et al.*	Chen *et al.*	Our scheme
User impersonation attacks	No	No	Yes
Server impersonation attacks	No	No	Yes
Off-line password guessing Attacks	Yes	No	Yes
Denial-of-service attacks	Yes	No	Yes
Smart card stolen attacks	No	No	Yes
Modification attacks	No	No	Yes
Replay attacks	Yes	Yes	Yes
Support mutual authentication	Yes	Yes	Yes
Support user anonymity	Yes	No	Yes
Wrong password detection by SC	Yes	No	Yes

6. Conclusion

In 2014, Chen *et al.* proposed an enhanced scheme of Choudhury *et al.*'s scheme and demonstrated it is resistance to famous attacks such as impersonation attacks and out of band attacks. However, Chen *et al.*'s scheme is still insecure. Furthermore, their scheme has no wrong password detection mechanism then may deduce the DoS problem. In this paper, we shown how their scheme can suffer from outsider attacks, server impersonation attacks and smart card stolen attacks and proposed an improved protocol for authentication scheme that keeps the similar properties of Chen *et al.*'s scheme and make it more secure. The security analysis explains that our improved scheme rectifies the vulnerabilities of Chen *et al.*'s scheme.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0126-15-1111, The Development of Risk-based Authentication· Access Control Platform and Compliance Technique for Cloud Security)

References

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communication of the ACM, 53*, 50-58.

[2] Smith, E., *et al*. (2010). The management of security in cloud computing. *Proceedings of Information Security for South Africa* (pp. 1-7).

[3] Huang, C., Qin, Z., & Kuo, C. (2011). Multimedia storage security in cloud computing: An overview. *Proceedings of IEEE 13th International Workshop on Multimedia Signal Processing* (pp. 1-6).

[4] Lamport, L. (1981). Password authentication with insecure communication. *Communication of the ACM, 24,* 770-772.

[5] Gennaro, R., & Lindell, Y., (2006). A framework for password-based authenticated key exchange. *ACM Transactions on Information and System Security, 9,* 181-234.

[6] Yang, Y., Deng, R., & Bao, F. (2006). A practical password-based two-server authentication and key exchange system. *IEEE Transactions on Dependable and Secure Computing*, *3(2)*, 105-114.

[7] Jeun, I., Kim, M., & Won, D. (2012). Enhanced password-based user authentication using smart phone. *Advances in Grid and Pervasive Computing, 7296,* 350-360.

[8] Lee, Y., & Won, D. (2013). On the use of a hash function in a 3-party password-based authenticated key exchange protocol. *Grid and Pervasive Computing, 7681,* 730-736.

[9] Lee, J., Ryu, S., & Yoo, K. (2002). Fingerprint-based remote user authentication scheme using smart cards. *Electronics Letters, 38,* 554-555.

[10] Yi, W., Kim, S., & Won, D. (2009). Smart card based AKE protocol using biometric information in pervasive computing environments. *Computational Science and Its Applications*, *5593*, 182-190.

[11] Lee, Y. (2012). A new dynamic ID-based user authentication scheme to resist smart-card-theft-attack. *Applied Mathematics and Information Sciences, 6,* 355-361.

[12] Mun, J., Jin, Q., Jeon, W., & Won, D. (2013). An improvement of secure remote user authentication scheme using smart cards. *Proceedings of International Conference on IT Convergence and Security* (pp. 1-4).

[13] Choudhury, A., Kumar, P., Sain, M., Lim, H., & Lee, H. (2011). A strong user authentication framework for cloud computing. *Proceedings of 2011 IEEE Asia-Pacific Services Computing Conference* (pp. 110-115).

[14] Chen, N., & Jiang, R. (2014). Security analysis and improvement of user authentication framework for cloud computing. *Journal of Networks, 9,* 198-203.

Jongho Mun was born in Jinju, Korea on November 16, 1984. He received the B.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2012 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2014. He also worked as a malware analyzer in SECUI between 2014 and 2015.

He is currently pursuing the Ph.D. degree in electrical and computer engineering at Sungkyunkwan University. His current research interest includes cryptography, malware, forensic, and authentication or key management protocols.

Jiye Kim was born in Seoul, Korea on December 2, 1976. She received the B.S. degree in information engineering from Sungkyunkwan University, Korea, in 1999 and the M.S. degree in computer science education from Ehwa University, Korea, in 2007. She also worked as a software engineer for mobile phone manufacturers in Korea or Japan between 1999 and 2013. She is currently pursuing the Ph.D. degree in electrical and computer engineering at Sungkyunkwan University. Her current research interest includes cryptography, authentication or key management protocols, wireless sensor networks, and mobile security.

Dongho Won was born in Seoul, Korea on September 23, 1949. He received BSC, MSC and Ph.D. in electronic engineering from Sungkyunkwan University, Korea. After working in Electronics and Telecommunication Research Institute for two years, he joined Sungkyunkwan University, where he is currently a leader professor at Information and Communication Engineering. He also served as the president of Korea Institute of Information Security and Cryptography. He was the Program Committee Chair Man of 8th International Conference on Information Security and Cryptography in 2005. His research interests are cryptology and information security.