A User Authentication Scheme on Multi-Server Environments for Cloud Computing

Jen-Ho Yang
Department of Multimedia and
Mobile Commerce,
Kainan University,
Taoyuan County, Taiwan
e-mail: jenhoyang@mail.knu.edu.tw

Ya-Fen Chang
Department of Computer Science
and Information Engineering,
National Taichung University of
Science and Technology, Taiwan
e-mail: cyf @cs.ccu.edu.tw

Chih-Cheng Huang
Department of Information
Management,
Kainan University,
Taoyuan County, Taiwan
e-mail: mdb525@gmail.com

Abstract—**In the cloud computing, user authentication is an important security mechanism because it provides the functions of authentication, authorization, and accounting for cloud servers. However, the previously proposed user authentication schemes have many security and efficiency problems. In addition, these schemes can only work on single server environments. To solve the above problems, we propose a new user authentication scheme on multi-server environments for cloud computing in this paper. Compared with the related works, the proposed scheme has less computation costs. In addition, the proposed scheme can be applied to multi-server environments because the ID-based concept is used. Therefore, the proposed user authentication scheme provides efficiency, security, and flexibility for the cloud computing applications.**

Keywords-User authentication; cloud computing; ID-based scheme; multi-server environment; mobile device

I. INTRODUCTION

With the development of computer technologies, more and more e-commerce applications are implemented on cloud computing environments [1, 2]. Thus, the cloud computing becomes a popular network technology in recent years. In the cloud computing, the user authentication scheme is very important because it can be applied to many applications, such as SaaS (Software as a Service), PaaS (Platform as a service), and IaaS (Infrastructure as a service) [3]. Moreover, the user authentication scheme provides the authentication, authorization, and accounting for cloud users and servers. Thus, the users can securely access their services provided by the cloud servers.

In recent years, most cloud services adopt the OpenID [4] to implement the user authentication. This is because the OpenID allows the cloud user to use a single identity (ID) to require various services from different cloud servers. That is, the cloud users do not have to manage many different identities. However, the OpenID relies on an ID provider to generate each user's identity. While authenticating the cloud users, the server needs to connect to the ID provider on the Internet. Thus, the authentication time and communication load are very high. To solve the above problems, we try to use the ID-based technique [5-13] to propose a new user authentication scheme for cloud computing.

The ID-based scheme utilizes the user's ID to be the authentication information, and thus the verifier can directly use the ID to authenticate the validity of the cloud user. Recently, many ID-based schemes [5-13] have been proposed to solve the user authentication problem. In 2004, Das et al. [6] proposed an ID-based scheme to handle the user authentication in cloud computing. Then, Wang et al. [7] pointed out Das et al.'s scheme has some security problems and proposed an enhanced ID-based scheme in 2009. Unfortunately, Wen et al. [9] found that Wang et al.'s scheme still has some security issues, and then they proposed a improvement scheme in 2012.

However, we find that Wen et al.'s scheme still has some problems. First, their scheme has high computation costs so that it is not suitable for mobile devices. Second, their scheme cannot be applied to multi-server applications for the cloud computing. Thus, we propose an ID-based authentication scheme in multi-server environments for cloud computing in this paper. The proposed scheme has low computation costs because it is implemented by one-way hash functions and exclusive-or operations. In addition, the proposed scheme uses the ID-based technique to generate the user's identity. Thus, it can be applied to multi-server environments for cloud computing in practice.

II. THE RELATED WORK

In this section, we introduce Wen et al.'s scheme [9] as follows. Their scheme can be divided into four phases: the registration phase, login phase, user authentication phase, and mutual authentication phase. The notations used in Wen et al.'s scheme are shown in Table I.

TABLE I. THE NOTATIONS OF WEN ET AL.'S SCHEME

ID_i	Identity of the user *i*
PW_i	Password of the user *i*
$\|$	String concatenation operation
$h(\cdot)$	One-way hash function
$\oplus$	Exclusive-or operation

978-1-4799-0434-1/13/$31.00 ©2013 IEEE

x	The secret value of the server
T	Timestamp
ΔT	The time difference of the timestamp

A. The registration phase

Step 1. The user *i* sends ID_i and PW_i to the server.

Step 2. The server computes $n_i = h(ID_i \| PW_i)$, $m_i = n_i \oplus x$, and $N_i = h(ID_i) \oplus h(PW_i) \oplus h(x) \oplus h(m_i)$ and stores $\{h(\cdot), N_i, n_i\}$ into a smart card.

Step 3. The server sends the smart card to the user.

B. The login phase

Step 1. The user uses the smart card to compute $A_i = h(ID_i) \oplus h(PW_i)$ and $B_i = N_i \oplus h(ID_i) \oplus h(PW_i) = h(x) \oplus h(m_i)$.

Step 2. The user computes $CID_i = h(A_i) \oplus h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T)$ and sends $M_1 = \{CID_i, n_i, N_i, T\}$ to the server.

C. The user authentication phase

Step 1. The server checks if ΔT is in a valid time. If it is valid, then the server computes $m_i = n_i \oplus x$, $B_i = h(x) \oplus h(m_i)$, and $A_i = N_i \oplus B_i = h(ID_i) \oplus h(PW_i)$.

Step 2. The server computes $CID_i \oplus h(A_i) = h(B_i \oplus h(N_i) \oplus h(n_i) \oplus T)$ and $C_i' = h(A_i \oplus T' \oplus h(n_i))$.

Step 3. The server computes $SK = h(A_i \| T \| B_i \| T')$ and $KC' = h(B_i \| SK \| T')$ and sends $M_2 = \{C_i', KC', T'\}$ to the user.

D. The mutual authentication phase

Step 1. The user checks if ΔT is in a valid time. If it is valid, then the user computes $C' = h(A_i \oplus T' \oplus h(n_i))$.

Step 2. The user checks if C' is equal to C or not. If they are equal, then the user computes $KC' = h(A_i \| SK \| T'')$.

Step 3. The user sends $M_3 = \{KC, T''\}$ to the server. Then, the server computes $KC = h(A_i \| SK \| T'')$ to check the user's validity.

III. THE PROPOSED SCHEME

The proposed scheme can be divided into two phases: the registration phase and the mutual authentication phase. The notations used in the proposed scheme are shown in Table II.

TABLE II. THE NOTATIONS OF THE PROPOSED SCHEME

ID_u	User's identity
PW_u	User's password
ID_{S_i}	Server's identity
$\|$	String concatenation operation
$h(\cdot)$	One-way hash function
$\oplus$	Exclusive-or operation
N	Random number
x	Secret key of the ID provider
TS	Timestamp generated by the mobile user
TS'	Timestamp generated by the server
ΔTS	Time difference of the timestamp

A. The registration phase

Step 1. The mobile user sends ID_u and PW_u to the ID provider. Then, the ID provider computes $A = h(ID_u \| x) \oplus PW_u$ and sends it to the mobile user in a secure channel.

Step 2. The user sends ID_{S_i} to the ID provider. Then, the ID provider computes $B = h(h(ID_u \| x) ID_{S_i})$ and sends it to the server in a secure channel.

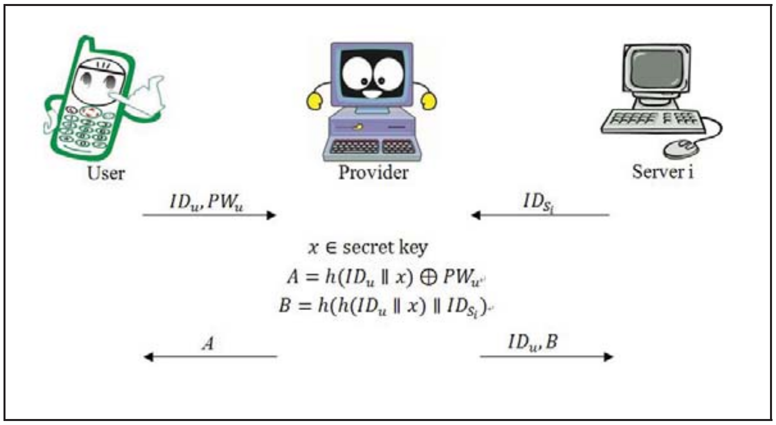

Figure 1. The registration phase of the proposed scheme

B. The mutual authentication phase

Step 1. The user generates N to computes $D = h(B \| TS) \oplus N$ and $C = h(N \oplus TS)$. Then, the user sends (D, C, TS) to the server.

Step 2. The server checks if ΔTS is valid or not. If ΔTS is valid, then the server computes $N' = h(B \| TS) \oplus D$ and $C' = h(N' \oplus TS)$.

Step 3. If $C' = C$, then the server ensures that the mobile user is valid. Then, the server computes $SK = h(N' \| TS \| C' \| TS')$ and $KC = h(C' \| SK \| TS')$ and sends (KC, TS') to the user.

Step 4. The user checks if ΔTS is valid or not. If it is valid, then the user computes $SK' = h(N \| TS \| C \| TS')$ and

$KC^{'} = h(C \,\|\, SK^{'} \,\|\, TS^{'})$. If $KC^{'} = KC$, then the user ensures that server is valid.

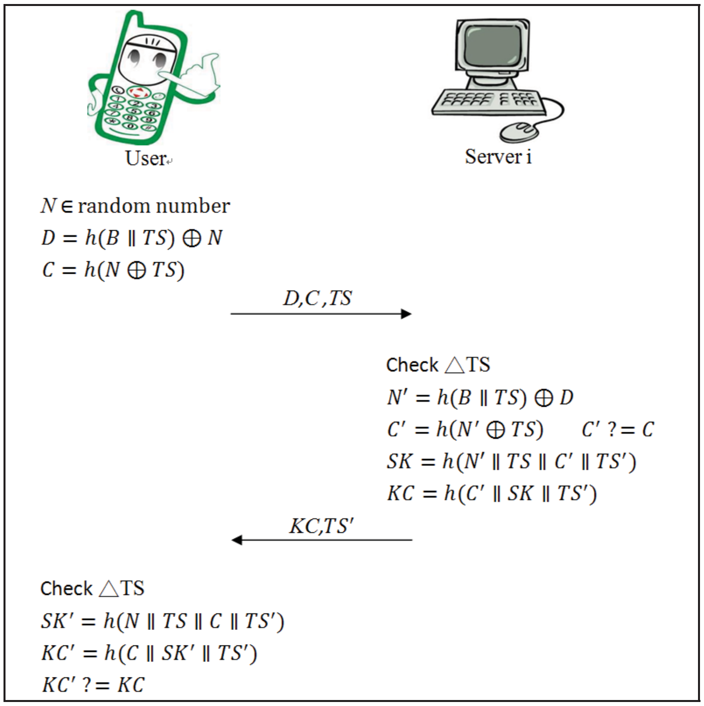
User
Server i
$N \in$ random number
$D = h(B \,\|\, TS) \oplus N$
$C = h(N \oplus TS)$
D,C,TS
Check △TS
$N' = h(B \,\|\, TS) \oplus D$
$C' = h(N' \oplus TS)$
$C' \,?= C$
$SK = h(N' \,\|\, TS \,\|\, C' \,\|\, TS')$
$KC = h(C' \,\|\, SK \,\|\, TS')$
KC,TS'
Check △TS
$SK' = h(N \,\|\, TS \,\|\, C \,\|\, TS')$
$KC' = h(C \,\|\, SK' \,\|\, TS')$
$KC' \,?= KC$

Figure 2. The mutual authentication phase of the proposed scheme

According to the above description, the proposed scheme is designed by the one-way hash function and the XOR operation. Thus, the proposed scheme has low computation costs and it is suitable for mobile devices. In addition, the ID provider uses the ID-based concept to generate the authentication information for the mobile user and the server. Therefore, the proposed scheme can be applied to the multi-server environments for the cloud computing.

IV. DISCUSSIONS OF THE PROPOSED SCHEME

In this section, we perform some attacks on the proposed scheme to analyze the security. The security analyses are shown as follows.

Assume that an attacker wants to obtain the authentication information $h(B \,\|\, TS)$, and then he/she eavesdrops the communication to get $D = h(B \,\|\, TS) \oplus N$. However, the attacker cannot get $h(B \,\|\, TS)$ because it is protected by the random number N. Besides, the attacker cannot get the session key $SK = h(N^{'} \,\|\, TS \,\|\, C^{'} \,\|\, TS^{'})$ from $KC = h(C^{'} \,\|\, SK \,\|\, TS^{'})$ because SK is protected by the one-way hash function $h(\cdot)$. According to the above analysis, the outsider is impossible for the proposed scheme.

A. Insider Attack

Assume that a mobile user wants to obtain the secret key x of the ID provider, and he/she may compute x from $A = h(ID_u \,\|\, x)$. However, this attack is infeasible because x is protected by the one-way hash function $h(\cdot)$. Similarly, computing x from $B = h(h(ID_u \,\|\, x) \,\|\, ID_{S_i})$ on the server side is also infeasible because x is protected by $h(\cdot)$.

B. Impersonation Attack

Assume that an attacker wants to impersonate a mobile user to log in to the server, and he/she may choose a fake $B^{''}$ to compute $D^{''} = h(B^{''} \,\|\, TS^{''}) \oplus N^{''}$ and $C^{''} = h(N^{''} \oplus TS^{''})$. Then, the attacker sends $(D^{''}, C^{''}, TS^{''})$ to the server. However, the server will find that $(D^{''}, C^{''}, TS^{''})$ is sent from an attacker because $B^{''} \neq B$, $N^{''} \neq N^{'}$, and $C^{''} \neq C^{'}$. Thus, the attacker cannot impersonate a mobile user in the proposed scheme. According to the same reason, an attacker cannot impersonate the server because he/she does not know the secret value B.

C. Replay Attack

Assume that an attacker intercepts the communications between the mobile user and a server, and he/she can get (D, C, TS). The attacker replaces TS by $TS^{''}$ and sends $(D, C, TS^{''})$ to log in to the server, and then the server computes $N^{'} = h(B \,\|\, TS^{''}) \oplus D$ and $C^{'} = h(N^{'} \oplus TS^{''})$. Then, the server knows that $C^{'} \neq C^{''}$ because $TS^{''} \neq TS$. Therefore, the server will discover that $(D, C, TS^{''})$ is sent by an attacker. That is, the proposed scheme can prevent the replay attack.

V. CONCLUSIONS

In this paper, we propose an ID-based user authentication scheme on multi-server environments for the cloud computing. The proposed scheme has low computation costs because it is designed by the XOR and one-way hash function operations. Moreover, the proposed scheme can be used on multi-server environments because the ID-based concept is used. Thus, the proposed scheme is more efficient and flexible than the related works. In the future, we will use the proposed scheme to investigate various cloud computing applications, such as user authorization, bill accounting, and access control.

ACKNOWLEDGMENT

This work was supported by National Science Council of Taiwan under the grants NSC 102-2410-H-424-019 and NSC 101-2410-H-025-009-MY2.

REFERENCES

[1] IMC Advanced Learning Solutions, “What is cloud computing,” Available Online: http://www.im-c.com/en/products/learning-management-system/clix-saas/what-is-cloud-computing/.

[2] Todd in Cloud-based Security, Securing the Cloud, Defining the Cloud, Available Online: http://www.cloudsecurity.trendmicro.com/defining-the-cloud.

[3] Michael Miller, Cloud Computing: Web-based Applications That Change the Way You Work and Collaborate Online, Que Publishing, USA, Aug. 2009.

[4] W. Bin, H. H. Yuan, L. X. Xiao and X. J. Min , “Open Identity Management Framework for SaaS Ecosystem,”, Proceedings of 2009 IEEE International Conference on e-Business Engineering (ICEBE '09), Macau, China, pp. 512–517, Oct. 2009.

[5] H. Lee, D. Choi, Y. Lee, D. Won, and S. Kim, “Security weaknesses of dynamic ID-Based remote user authentication protocol,” Proceedings of World Academy of Science, Engineering and Technology, vol. 59, pp. 190–193, 2009.

[6] M. L. Das, A. Saxena, and V. P. Gulati, “A dynamic ID-based remote user authentication scheme,” IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629–631, 2004.

[7] Y. Wang, J. Liu, F. Xiao, and J. Dan, “A more efficient and secure dynamic ID-based remote user authentication scheme,” Computer Communications, vol. 32, no. 4, pp. 583–585, 2009.

[8] J. S. Xu, R. C. Huang, W. M. Huang, and G. Yang, “Secure document service for cloud computing,” Proceedings of the 1st International Conference on Cloud Computing(CloudCom '09), LNCS 5931, pp. 541–546, 2009.

[9] F. Wen, X Li, “An improved dynamic ID-based remote user authentication with key agreement scheme,” Computers and Electrical Engineering, vol. 38, no.2, pp. 381–387, Mar. 2012.

[10] D. Recordon and D. Reed , “OpenID 2.0: A Platform for User-Centric Identity Management,” Proceedings of the second ACM workshop on Digital identity management(DIM '06), New York, pp. 11–16, 2006.

[11] H. Li, Y. Dai, L. Tian and H. Yang , “Identity-Based Authentication for Cloud Computing,” Proceedings of the 1st International Conference on Cloud Computing(CloudCom '09), LNCS 5931, pp. 157–166, 2009.

[12] T. Hwang, J. L. Chen, “Identity-Based Conference Key Broadcast System,” IEE Proceedings of Computers and Digital Technology, vol. 141, pp. 57– 60, 1994.

[13] M. S. Hwang, J. W. Lo, S. C. Lin, “An Efficient User Identification Scheme Based on ID-Based Cryptosystem,” Computer Standards and Interfaces, vol. 26, no.6 , pp. 565–568, Oct. 2004.