Chapter 17
Mutual Authentication Scheme for Cloud Computing

Shirly Lee, Tae Yong Kim and Hoon-Jae Lee

Abstract Cloud computing is known as one of the big next things in Information Communication Technology world. Cloud computing offers a lot of cost and efficiency benefits to the business, but it also introduce significant security vulnerabilities. Data security always becomes a big concern whenever customers lose physical control on their data. Sensitive data processed outside the enterprise need to be assurance that they are only accessible and propagate to the privileged users. In this paper, we proposed a mutual authentication that allow cloud user and cloud remote server to authenticate each other as we believed it is crucial to protect not only the server but also the legitimate users from security threats. Unlike one way authentication, in mutual authentication, client must proves its identity to server and the server must proves its identity to client before any access have been granted or any application traffic is sent over the client–server connection.

Keywords Cloud computing · Mutual authentication · Cloud data security · Cloud authentication

S. Lee
Intel Technology Sdn. Bhd, Malaysia, Malaysia
e-mail: l_shirly@yahoo.com

T. Y. Kim (✉) · H.-J. Lee
Division of Computer and Information Engineering, Dongseo University,
47 Jurye-ro, Sasang-gu, Busan 617-716, Korea
e-mail: tykimw2k@gdsu.dongseo.ac.kr

H.-J. Lee
e-mail: hjlee@gdsu.dongseo.ac.kr

H.-K. Jung et al. (eds.), *Future Information Communication Technology and Applications*, Lecture Notes in Electrical Engineering 235, DOI: 10.1007/978-94-007-6516-0_17,

17.1 Introduction

Cloud computing is known as the Next Big thing in today's information technology world. According to the survey result release by EquaTerra on 26th January 2011 as show in Fig. 17.1, cloud computing overall and cloud computing in lieu of outsourcing are predict to be the top business and IT service market trends indentified for 2011 [1]. This Pulse survey is regularly does in the fourth quarter of the year, with the objective to poll leading services providers and its advisors on what they projected as the most impactful trends in the business and IT services marketplace in the coming year.

Unlike the traditional computing methods, cloud computing is an internet based development and usage of computer technologies such as network infrastructures, applications, software platforms and etc. which allow its users to access anytime anywhere as they wish [2]. Cloud computing offers several cost and efficiency benefits to its users such as adaptive management of the cloud which allows applications to be scale on demand according to their need [3], provides the flexibility which allows clients to dynamically acquire more resources to host their services in order to handle peak workloads and release when the workload decrease, reducing organization's IT maintenance and administration costs [3]. However, without appropriate data security and privacy solution in place to certain degrees, cloud services cause some problems to the organization. In fact, security is one of the primary reasons why some organizations have been cautious in their adoption of cloud services based on the International Data Corporation (IDC) Q3 2009 survey. Security again ranked Top as the greatest challenge in cloud computing [4]. This is due to most of the corporate cannot afford the risk to

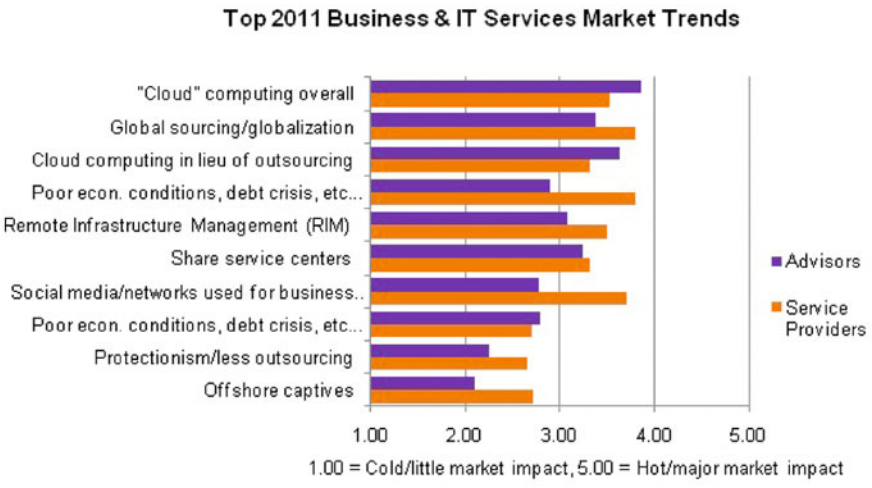


Fig. 17.1 EquaTerra Q4 year 2010 advisor and service provider pulse survey

compromise the security of their applications and data. Data security always becomes a big concern whenever customer loses physical control on their data.

In this paper, we proposed a mutual authentication that allow cloud user and cloud remote server to authenticate each other. It is crucial to protect not only the server but also the legitimate user.

17.2 Related Work

17.2.1 Security of Cloud Computing

Cloud computing is normally known as the fifth utility due to it pay per usage basic characteristic, cloud computing deliver on demand IT resources by allowing dynamically growing or shrinking the virtualized resources via internet [3]. It provides myriad virtual storage, computing resources and platform for its users to manipulate their data or utilize the processing resources conveniently over Internet without the need of knowing where exactly the infrastructure located [5]. It is widely accepted that, cloud services introduced a lot of benefits to their users by significantly reducing IT cost and help organizations to increase its service delivery efficiency, streamline IT management and better align IT services by breaking the physical bound between IT infrastructure and the user [3, 5] but at the same time, it also introduced a lot of new security risks. In December 2009, Cloud Security Alliance (CSA) has discovered top seven security risks [1, 6] which are (a) Abuse and Nefarious Use of Cloud Computing, (b) Insecure Application Programming Interface(API), (c) Malicious Insider, (d) Shared Technology Vulnerabilities, (e) Data Loss or Leakage, (f) Account, Service or Traffic Hijacking, and (g) Unknown Risk Profile.

17.2.2 Cloud User Authentication

Unlike others computing system, cloud computing is a paradigm that incorporates the software, platform and computer infrastructure as Internet based services so it is subject to external attackers perceived to public clouds [7]. Therefore authentication play a very important role in cloud computing.

Most common implemented authentication methods are knowledge-based, which user ID and password are requested only once during login. This ID password method provides higher level of convenience to users but also requires less effort for attackers to exploit.

Many attacks are manifested as phishing messages that masquerade as the one that sent by legitimate organizations and contain URLs that point to fraudulent web sites which have the same appearances as genuine ones [6]. The incident of

Salesforce.com, customers hit with phishing attack in year 2007 is the good example to show that user ID and password authentication method is not strong enough to against the access security attack in clouds [8, 9]. Therefore, we proposed a strong two factor user authentication [5] for cloud computing. However, the scheme does not provide mutual authentication, high computation cost and not robust enough. Thus in this paper, we propose a mutual authentication framework for cloud computing that can provide better security features with low computation cost.

17.3 Proposed Scheme

17.3.1 Notations

Our proposed mutual authentication scheme consists of three major phases: Registration phase, Login Phase and Authentication Phase. In the proposed scheme, there are two different entities: cloud client, *Uc* and Cloud Server, *Us*. The cloud server provides data storage services to a lot of clients. Clients store their data at the server and retrieve data on demand. Each client has a unique identification and password which she can prove her identity. Table 17.1 shows the list of the notations we used throughout our propose scheme.

17.3.2 Registration Phase

Firstly, a new cloud user, U_c is require to register to Cloud to register to Cloud Server U_s as illustrated in Fig. 17.2a:

Table 17.1 Notations

Notation	Description
Uc	Cloud user
Us	Cloud server
ID	*Uc*'s identity
PSW	*Uc*'s password
γ	Secret key maintained by *S*
h(.)	Collision-resistant one-way hash function
$\|\|$	String concatenation operation
N	*Uc*'s nonce(secret value)
Rc	*Uc*'s random validation factor
Rs	*Us*'s random validation factor
*S*1	The random one-time session key
$\oplus$	Exclusive-*OR* operation
V	Registration value
Ek[.]	Symmetric encryption function with respect to key *K*
Dk[.]	Symmetric decryption function with respect to key *K*

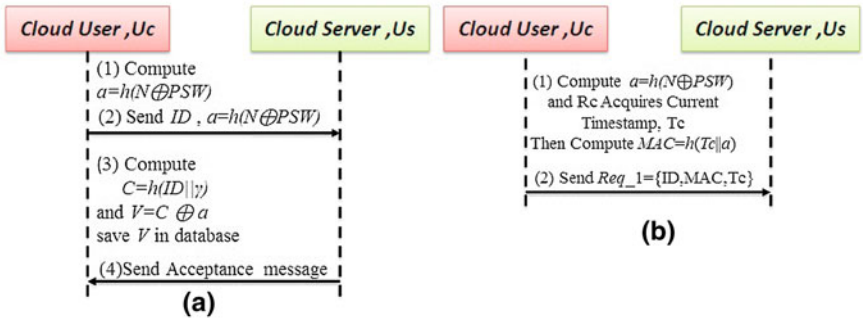


Fig. 17.2 **a** Registration phase. **b** Login phase

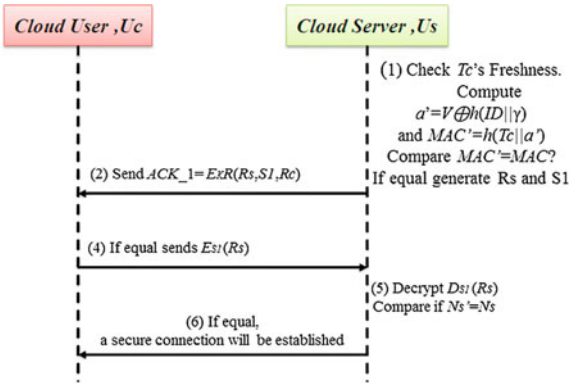
- U_c Selects a nonce, N and password, PSW and then compute $a = h(N \oplus PSW)$.
- Subsequently, U_c sends his ID and a to S_c for initial registration.
- Once S_c accepts the registration request, S_c will compute $C = h(ID \parallel \gamma)$ and the registration value, $V = C \oplus a$.

17.3.3 Login Phase

As presented in Fig. 17.2b, Login phase involved the below steps:

- Upon login, U_c computes $a = h(N \oplus PSW)$ and a random validation factor R_c,
- Then U_c acquires its current timestamp T_c to compute $MAC = h(T_c \parallel a)$.
- Subsequently U_c creates request message $Req\_1 = \{ID, MAC, T_c\}$.
- After that U_c encapsulates R_c with Req_1 and sends to S_c.

Fig. 17.3 Authentication phase



17.3.4 Authentication Phase

The summarized of the authentication phase can be found in Fig. 17.3. Upon receiving the *Req*_1, S_c performs the following steps:

- Firstly, S_c checks the freshness of T_c and rejects the request if T_c already existed in a current session of U_c. Otherwise, it continues to the next step.
- After that, S_c computes $a' = V \oplus h(ID \| k)$ and $MAC' = h(T_c \| a')$. If MAC' match with the received MAC, S_c generates a random validation factor R_s else rejects the login request.
- Then S_c generates a onetime random session key, S_1.
- Subsequently S_c acquires its current timestamp T_s and stores the paired of timestamps (T_c, T_s) and ID temporarily for the purpose of freshness checking until the end of session.
- S_c encrypt R_s, S_1, R_c to compute an acknowledgement message where $ACK\_1 = EK(R_s, S_1, R_c)$ and then sends to U_c.
- Once U_c received the ACK_1, U_c decrypts the message $DK(R_s, S_1, R_c)$ and then check if R'_c equal to its original R_c.
- If the valued is match, U_c encrypt $Es1(R_s)$ and then forwards to S_c. Otherwise terminate the authentication process.
- Once S_c received $Es1(R_s)$, it will decrypt $Ds1(R_s)$ and checks if value of R'_s equal to its original R_s.
- If the value is match, it means that both server and client have passed the mutual authentication. A secure connection will be established between U_c and S_c.

17.4 Security and Performance Analysis

17.4.1 Security Analysis

In this session, we discuss about the security of our proposed mutual authentication scheme.

(a) **Mutual Authentication**
As discuss earlier, our scheme not only just allow server to authenticate user but also provide the option to allow user to authenticate the server. We provide mutual authentication at the authentication phase, where S_c and U_c authenticate each other by verifying $R_c = R'_c$ and $R_s = R'_s$.

(b) **Defense Replay Attack**
Our proposed scheme able to resists the replay attack as it is based on challenge and response method which decides that a replay attack can't pass the subsequent challenges. Further to this, current timestamp is including in our scheme where access is only granted for the timestamp values which is fresh and within a reasonable tolerance time. Besides this, we used random

validation factors *(R_c, R_s)* and random one time session key S_1 to ensure there is just solely single authentication process, thus fraudulently replay messages will not be able to pass through the legality checking process.

(c) **Prevent Man-in the-Middle (MITM) Attack**
MITM attack is attacks where attack place himself in between client and server, attacker may interrupt and modify the communication [8]. We protect our *ACK*_1 by encryption, attacker would not able to obtain any content of *ACK*_1 without knowing key. Further to this, we enforce legality checking at U_c where R'_c have to match with R_c and at S_c $R_s = R'_s$ and *MAC* have to be matched. Different session used different T_c to compute MAC. Hence attacker will not able to pass through the authentication even if he able to collects all messages from others session.

(d) **Phising attack prevention**
We prevent phishing attack in cloud computing by providing strong mutual authentication. In our proposed scheme, client must prove its identity to server and the server must prove its identity to client before any access has been granted. S_c and, U_c authenticate each other by verifying $R_c = R'_c$ and $R_s = R'_s$ in the authentication phase.

(e) **Forward and backward Secrecy**
Since our session key, S_1 is randomly generated and unpredictable. Therefore our scheme is free from any used session key to be exposed.

(f) **User Proofing/Indentity theft Attack Protection**
U_c's authentication information, $V = h(ID \,||\, k) \oplus h(N \oplus PSW)$ is stored in S_c's database, if attacker able to steal V but he does not know the long-term secret, γ as γ is under strict protection as assumed. In this case, our scheme is free from user proofing and identity theft attack as it is infeasible for attacker to obtain $h(N \oplus PSW)$.

(g) **Server Spoofing Attack Protection**
Authentication process whenever U_c not able to decrypt the fraudulent message from masquerade S_c.

(h) **Side Channel Attack Prevention**
Cloud computing security could be compromise by attacker by placing a malicious virtual machine which masquerade as target cloud server and then perform side channel attack [8]. Our mutual authentication based authentication scheme able to prevent this, as we ensure both server and client authenticated each other before given any access to the application.

17.4.2 Performance Analysis

We proposed robust and trustworthy mutual authentication between cloud user and cloud service provider communicated over the internet. The main operation include the computation of *AND* exclusive *OR* operations of our proposed mutual authentication scheme are summarized in Table 17.2.

Table 17.2 Performance analysis of our propose scheme

	Operation	Registration	Authentication
Client	Xor	1	1
	Hash	1	2
	Symmetric cryptosystem	–	1
Server	Xor	1	1
	Hash	1	1
	Symmetric cryptosystem	–	1

Table 17.3 Security properties of the proposed scheme with other related schemes

Security properties	Proposed Scheme	Lee et al's scheme [6]
Prevent replay attack	Yes	Yes
No verification table	Yes	Yes
Prevent identity proofing	Yes	Yes
Prevent phishing attack	Yes	Yes
Certification establishment	No	Yes
Computation cost	Low	High
Provide mutual authentication	Yes	No
Prevent server spoofing attack	Yes	No

Further to this, Table 17.3 shows the comparison result of the security of the proposed scheme and the two-factor authentication for cloud computing.

17.5 Conclusion

Cloud computing is a new way of delivering computing resources which introduce a lot of benefits to its users. Despite its positive characteristics, it also brings in new security worries such as data security issues, illegal data access etc. We proposed mutual authentication scheme to minimize the cloud computing security risks such as man in-middle attack, identity theft, side channel attack and phishing attack. From the security analysis, it shown that our proposed scheme provides a robust and trustworthy mutual authentication between cloud user and cloud service provider communicated over the internet. While the from the performance analysis it show our proposed framework has good efficiency and suitable for cloud computing.

Acknowledgments This work was supported in part by the Dongseo Frontier 2009 and was supported by a research program of Dongseo University's Ubiquitous Appliance Regional Innovation Center supported by the grants from Ministry of Knowledge Economy of the Korean government and Busan Metropolitan City(No. B0008352).

References

1. Geelan J (2009) Twenty one experts define cloud computing virtualization: electronic magazine. http://virtualization.sys-con.com/node/612375
2. CloudImpact: cloud computing the stormy side/the upside. http://blogcloudimpact.com/?p=78
3. Duncan D, Chu X, Vecchiola C, Buyya R (2009) The structure of the new IT frontier: cloud computing-part 1. Strategic facilities magazine. Pacific & Strategic Holdings Pte Ltd, Singapore, Issue 9, pp 67–72
4. Gens F (2009) New IDC IT cloud services survey: top benefits and challenges in cloud computing. http://blogs.idc.com/ie/?p=730
5. Lee S, ong I, Lim HT, Lee HJ (2010) Two factor authentication for cloud computing. Int J Korea Inst Marit Inf Commun Sci (KIMICS) 8(4):427–432
6. Chou D (2008) Strong user authentication on web: Microsoft the architecture-journal. http://msdn.microsoft.com/enus/library/cc838351.aspx
7. Deloitte (2011) Information security briefing cloud computing. http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf
8. Gregg M (2010) 10 Security concerns for cloud computing. http://www.globalknowledge.ae/knowledge%20centre/white%20papers/virtualisation%20white%20papers/10%20security%20concerns%20for%20cloud.aspx
9. Kher V, Kim Y (2005) Securing distributed storage: challenges, techniques, and systems. In: Proceedings of the 2005 ACM workshop on storage security and survivability, pp 9–24