The New Territory of Lightweight Security in a Cloud Computing Environment

Shu-Ching Wang, Shih-Chi Tseng, Hsin-Met Chuan, Kuo-Qin Yan, Szu-Hao Tsai

The New Territory of Lightweight Security in a Cloud Computing Environment

Shu-Ching Wang[1], Shih-Chi Tseng[1], Hsin-Met Chuan[2], Kuo-Qin Yan[1]*, Szu-Hao Tsai[1]

[1] Chaoyang University of Technology, Taiwan, R.O.C.
{scwang, s10314901, kqyan*, s9914603}@cyut.edu.tw
[2] Hsing-Kuo University, Taiwan, R.O.C.
hn88780752@yahoo.com.tw
*: Corresponding author

Abstract. The cloud computing is an Internet-based resource sharing system in which virtualized resources are provided over the Internet. Cloud computing refers to a class of systems and applications that employ distributed resources for use in various applications; these computing resources are utilized over a network to facilitate the execution of tasks. However, cloud computing resources are heterogeneous and dynamic, connecting a broad range of resources. Thus, there are a large numbers of application and data center in the cloud computing environment. Therefore, the security issues of authentication and communication in application services and data center need to be considered in the cloud computing environment

Result

In this study, two security methods for client user are presented. (1) Group Key Authentication (GKA) is proposed for user to obtain the services from multiple servers quickly. And. (2) Authentication and Authorization within Two Factors (AATF) provides a more stringent authentication and authorization, and the security of cloud computing can be enhanced.

In a cloud-computing environment, each cloud service provider provides an authentication key to the user [3]. By using GKA, an authentication group key is generated by combining a set of authentication keys for different service providers at the same time. The generating steps of GKA are depicted in Fig. 1.

1. Group Key Req.: The user requests the Group Key.
2. ID Req.: AUTH Server requests the User's ID for identification when the server receives the Group Key Req.
3. ID Res.: User sends the account name and password to AUTH server to identify user.
4. Auth. ACK (Success/Failure): AUTH Server sends a message for User to notice the authentication is success or fail.
5. Services Sel.: If authentication is success, then User selects the services that user needed. In addition, a requirement is sent to AUTH server.

6. Key Req.: After AUTH Server receives the service request, it will send the Key Request and ID to Service Servers.
7. Key Res.: When Service Server receives the request and ID, an authentication key is generated, and the key and ID are stored. In addition, Service Server sends the authentication key to AUTH Server. When AUTH Server receives the authentication key; then the Group Key will be assembled and stored.

When the user authentication group key is established, a one-time identity verification for several services is available to users. The format of Group Key = ($SERVICE_1$||$SERVICE_2$||… ||$SERVICE_n$||ID). If a new service requirement is presented by user, the key of the certification of the new service will be given, and the new authentication key is combined to the GK. Moreover, every authentication key is generated by Service Server randomly.

AATF security mechanism for the user during authentication and authorization process is used to strengthen the legitimacy of authenticating users and improve the security of user accounts. The execution flow of AATF is shown in Fig. 2.

Step 1. The user generates a set of random numbers, and then a random number RN with Request sent to the application server side.
Step 2. Application server-side receives a random number RN with Request, return the SC to the user, and will direct users to the authentication server-side.
Step 3. Users will send UN, PWD and SC to the authentication server-side for authenticating.
Step 4. When the authentication is successful, the authentication server-side will sent the AuT and S to the user, if authentication fails then return a failure message to the user.
Step 5. The receiving AuT and S by user will be retrieved in accordance with the number of RN to generate sRN, and then S and sRN are sent to the application server-side authentication.
Step 6. The compare action of authentication and authorization will be started when application server received the S and sRN; the ApT is returned to user when authentication and authorization is passing; if fail, the fail message is returned.
Step 7. When Users receive the ApT, ApT and AuT are combined into a Token, and then Token can be passed to the application for using the service.

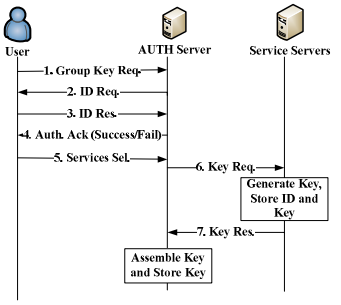

Fig.1 Group Key generating

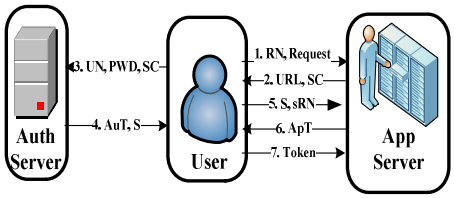

Fig. 2 The processes of AATF

There are a lot of services and users in the cloud computing environment, will be carried out to verify the identity through authentication and authorization protocol [4]. Therefore, the authentication and authorization are always making in cloud computing environments. When authentication and authorization requires a lot of steps and a large number of parameters, data exchange will be increased and the amount of resources needed to make authentication and authorization will be increased. Therefore, the number of steps, the total number of parameters and the amount of data exchanges will be used for comparison. Then, the authentication protocols proposed in this study can be verified as the lightweight computing security protocols. Form Table 1, the steps of certification, the total number of parameters and the amount of data exchange of GKA by AATF are less than OAuth [1] and the SAML[1].

Table 1 The comparisons with OAuth and SAML

	Step (times)	Parameter	Data Exchange
OAuth	10	11	30/time
SAML	8	12	14/time
GKA	7	4	8/time
AATF	7	11	13/time

Overall, our proposed lightweight security mechanisms can provide the security of information and communication and authentication, without wasting computing resources to enhance the security of cloud computing environment. Therefore, Group Key Authentication (GKA) is used to provide the services that users can quickly obtain multiple servers to improve security by reducing the transmission of secret information in the cloud computing environment. GKA also can reduced the number of users must be logged conversion services and waiting time. Authentication and Authorization within Two Factors (AATF) in the cloud computing environment at both ends of the server-side two-factor authentication through the authentication server-side services can provide more stringent authentication and authorization in order to verify the legitimacy of the identity of the user to enhance the cloud computing security.

Cloud computing is a concept in distributed systems. It is currently used mainly in business applications in which computers cooperate to perform a specific service together. In addition, the Internet applications are continuously enhanced with multimedia, and vigorous development of the device quickly occurs in the network system. As network bandwidth and quality outstrip computer performance, various communication and computing technologies previously regarded as being of different domains can now be integrated, such as telecommunication, multimedia, information technology, and construction simulation. Therefore, cloud computing is currently used many commodity computers that can cooperate to perform a specific service together [2]. Thus, applications associated with network integration have gradually attracted considerable attention.

In a cloud-computing environment, users can access the operational capability faster with Internet application, and the computer systems have the high stability to handle the service requests from many users in the environment [5]. Today, a new application service of operation system is emerged and it changes the user's usage in

the past. Originally, the Internet infrastructure is continuous grow that many application services can be provided in the Internet. The reliability is improved in a cloud computing by using the low-power hosts. In addition, cloud computing has greatly encouraged distributed system design and application to support user-oriented service applications. Furthermore, there are a large number of cloud applications and data centers provided in the cloud computing environment, so the information and communications, and authentication is one of the important security issue that must be considered. In other words, the security is one of the most important aspects of cloud computing as it ensures overall reliability and fluency. To ensure the cloud computing is safety, a mechanism to ensure the security of information and communication is thus necessary.

Therefore, Group Key Authentication (GKA) is used to provide the services that users can quickly obtain multiple servers to improve security by reducing the transmission of secret information in the cloud computing environment. GKA also can reduced the number of users must be logged conversion services and waiting time. Authentication and Authorization within Two Factors (AATF) in the cloud computing environment at both ends of the server-side two-factor authentication through the authentication server-side services can provide more stringent authentication and authorization in order to verify the legitimacy of the identity of the user to enhance the cloud computing security.

Through the above description, the proposed method can enhance the security in the cloud-computing environment. According to the characteristics of cloud computing, by using the proposed methods, the cost of resources can be reduced and the quality of service can be improved. The proposed security mechanisms can meet the cloud computing security step to ensure that users and service providers to enjoy the security of cloud computing environment with the service provider.

Acknowledgments. This work was supported in part by the Ministry of Science and Technology MOST 102-2221-E-324-008 and MOST 103-2221-E-324-025.

References

1. Almulla, S.A., Chan, Y.Y.: Cloud computing security management. In: the 2nd International Engineering Systems Management and Its Application, pp.1-7, April (2010).
2. Bertram, S., Boniface, M., Surridge, M., Bricombe, N., Hall, M. M.: On-demand dynamic security for risk-based secure collaboration in clouds. In: the 3rd IEEE Cloud Computing, pp. 515-525, July (2010).
3. Gong, Y., Ying, Z. Lin, M.: A survey of cloud computing. Lecture Notes in Electrical Engineering. 225, pp. 79-84, (2013).
4. Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.L. (2009): On technical security issues in cloud computing. In: the IEEE International Conference on Cloud Computing, pp. 109-116, (2009).
5. Ramgovind, S., Eloff, M.M., Smith, E.: The management of security in cloud computing. In: the Information Security for South Africa (ISSA), pp.1-7, August (2010).