A New Group Key Authentication Protocol in an Insecure Cloud Computing Environment

S.C. Wang[1], M.L. Chiang[2*], K.Q. Yan[3*], S.S. Wang[4*], S.H. Tsai [5]

[1]scwang@cyut.edu.tw

[*2]mlchiang@cyut.edu.tw

[*3]kqyan@cyut.edu.tw

[*4]sswang@cyut.edu.tw

[5]s9914603@cyut.edu.tw

Chaoyang University of Technology

[*]Corresponding author

Abstract—**Network bandwidth and hardware technology are developing rapidly, resulting in the vigorous development of the Internet. A new concept, Cloud computing, uses low-power hosts to achieve high quality service. According to the characteristics of Cloud computing, the enterprises can support the business services on the Internet. However, the authentication is one of the important problems in Cloud computing environment. In this paper, a protocol, Group Key Authentication (GKA), is proposed that the authentication time and data traffic in the Cloud computing can be reduced and the Quality of Service (QoS) can be increased.**

Keywords—**Cloud computing; Service oriented architecture; Group key; Distributed system; Quality of service**

1. INTRODUCTION

Today, network bandwidth and hardware technology must continuously advance so as to keep pace with the vigorous development of the Internet. The new concept of Cloud computing allows for more applications for internet users [2,5]. Cloud computing is a new 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 [1,4]. 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. Thus, applications associated with network integration have gradually attracted considerable attention. Similarly, Cloud computing facilitated through distributed applications over networks has also gained increased recognition. In a Cloud computing environment, users have access a safety service on the Internet [1,11], and the computer systems must have high security to keep pace with this level of activity.

In addition, Cloud computing has greatly encouraged distributed system design and application to support user-oriented service applications [2]. The Cloud computing must provide better confidentiality, integrity, availability and trust with application services for users. In order to lead users can smoothness to running their application in the Internet that the computer system has to make the stable network environment. Hence, the components in the system have to exclude the influence from abnormal components as like hacker. In addition, the Cloud computing is using many commodity computers to complete the specific service together for users. Therefore, the high security capability of a Cloud computing environment must be considered.

As Cloud computing becomes prevalent, more and more sensitive information are being centralized into the cloud, such as emails, personal health records, government documents, etc.. As a disruptive technology with profound implications, Cloud computing is transforming the very nature of how businesses use information technology. The Cloud computing makes

advantages more appealing than ever, it also brings new and challenging security threats towards users' private data [9].

Cloud computing is a style of computing where massively scalable IT-related capabilities are provided to multiple external customers "as a service" using internet technologies [6,8]. The cloud providers must achieve a large, general-purpose computing infrastructure; and they must use virtualization of infrastructure for different customers and services to provide the multiple application services. The users of Cloud computing environment can easily add or remove their individual service capacity; hence, the total capacity demands can be increased, and the user can deploy them at an additional low-cost.

As a disruptive technology with profound implications, Cloud computing is transforming the very nature of how businesses use information technology. From users' perspective, including both individuals and IT enterprises, using the cloud service form the cloud in a flexible on-demand manner brings appealing benefits such like avoidance of capital expenditure on hardware, software, and personnel maintenances, etc [3].

Moreover, the various cloud service providers provide several kinds of services for cloud users. Each user can ask a set of different services at the same time from the same cloud or same provider. Therefore, the providers should promise their services are high reliable and trusty in the Cloud computing environment when the amount of service requests is huge. Besides, the security of each cloud service provided by cloud service providers needs to be considered.

However, in a traditional internet service environment, the service is scattering in each provider's server. Thus, each provider has its own server. However, nowadays, the service of each provider is provided on the cloud. Thus, if user asks a service request need many times to authenticate, then user asks a set of service requests in the same server will waste a long time to wait.

Therefore, how to reduce the authentication time and data traffic in the Cloud computing and to increase the Quality of Service (QoS), is the problem we are going to tackle in this paper. In this paper, an authentication protocol on different services in the Cloud computing environment is proposed. Using the proposed authentication protocol, the several services requests in one time by user can be authenticated. According to the proposed authentication protocol, a group key for user's service requests is composed by several service keys. Therefore, the protocol can raise the authentication rate in Cloud computing environment.

The rest of the paper is organized as follows. Section 2 introduces the related work of this study. The detailed description of our proposed protocol is stated in Section 3. Section 4 gives the security analysis. Finally, the concluding remarks and future researches are given in Section 5.

2. RELATED WORK

In this section, the characteristics of Cloud computing, the security assertion markup language, the Open Authentication (OAuth) protocol, and the group based AKA protocol are given.

2.1 Characteristics of Cloud Computing

There are five main characteristics of Cloud computing are discussed in the subsection.

- **On-demand self-service.** A consumer can unilaterally provide computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote by heterogeneous thin or thick client platforms as well as other traditional or cloud-based software services.
- **Resource pooling.** The computing resources of provider are pooled to serve multiple consumers using a multi-tenant model. With different physical and virtual resources dynamically, the computing resources are assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction.
- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned. To the consumer, the capabilities available for provisioning are often appeared to be unlimited and can be purchased in any quantity at any time.
- **Measured service.** Cloud systems automatically control and optimize resource usage by leveraging a metering capability at

some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported. In other words, the cloud resources can be providing transparency for both the provider and consumer of the service [10].

2.2 Security Assertion Markup Language (SAML)

SAML is based on XML standards, used as a tool to exchange the authorization and authentication attributes between two entities, in the case of the cloud, between the Identity Provider (IdP) and Cloud Service Provider (CSP). The main goal of SAML is trying to support Single Sign On (SSO) using the internet. There are different versions of the SAML for example, SAML v1.0, SAML v1.1 and SAML v2.0. It supports digital signature and encryption. Following is an illustrative example to help in understanding of SAML used for SSO, between the user, IdP and CSP[1].

The communication process steps of SAML:

1. User requests a web page from the CSP.
2. CSP responds to the User by redirecting the user's browser to the SSO website located at the IdP.
3. Browser can redirect the processes.
4. Exchange authentication protocol between the Idp and user for identification.
5. IdP responds using encoded SAML to user.
6. User browser sends the SAML response to CSP to access the URL.
7. User is able to log in the CSP application.

2.3 Open Authentication (OAuth) Protocol

OAuth is a very interactive and interesting protocol, which allows users to share their private resources such as files, pictures located on one CSP with another CSP without exposing the personal identity information such as user names and passwords. The main objective of OAuth is to build an authorized access to a secure Application Programming Interface (API) used in mobile and desktops designs and it is based on the open source implementations. From the CSP perspective, it provides a service for users to access the programmable application hosted on different service provider without disclosing of the identity credentials. For instance, a consumer (a web site or an application that used to access stored files on behalf of the user) requests a print service from a service provider where the file is stored as a result, then the print will be executed without disclosing the file owner credentials [1].

To illustrate the communication process between the user and service provider using OAuthe protocol steps [1].

1. Web application asks Google Authorization for OAuth request token.
2. Google responds with unauthorized request token.
3. Web application directs users to Google web authorization page to request authorized token.
4. User accesses the Google Authorization page to verify their identity and either to allow or deny web application access to their data.
5. If user denies access then he/she will be directed to the Google page rather than the application page.
6. If user grants access, he/she will be redirected to the application web page, which includes authorized request Token.
7. The authorized request token is exchanged between the web application and Google Authorization.
8. Google verifies the request and sends Access Token.
9. The web application requests for user data from Google Authorization.
10. The Request in step 9 will be verified and signed by Google Authorization and if the access token is known by the Authorization, then the requested data will be sending.

2.4 Group Based AKA Protocol

Group based Authentication and Key Agreement (G-AKA) protocol facilitates users with subscribership in a common Home Network (HN) to roam form network to network. In the G-AKA, every Mobile Station (MS) provides its identity when visiting a Service Network (SN). Upon reception, the SN examines whether the MS belongs to an active group of which any member has completed full authentication. If not, the SN acquires the authentication data for the MS and its associated group from the concerned HN. This leads MSs of the same group to share the same authentication data, including group temporary authentication key and other necessary information [3].

3. GROUP KEY AUTHENTICATION

Although the benefits of Cloud computing are clear, so is the need to develop proper security for cloud implementations. In addition to the

usual challenges of developing secure IT systems, Cloud computing presents an added level of risk because essential services are often supported by several cloud service providers. The externalized aspect of outsourcing makes it harder to maintain data integrity and privacy, support data and service availability, and demonstrate compliance. For example, IDC recently conducted a survey (see Figure 1) of 244 IT executives/CIOs and their Line-Of Business (LOB) colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing [7].

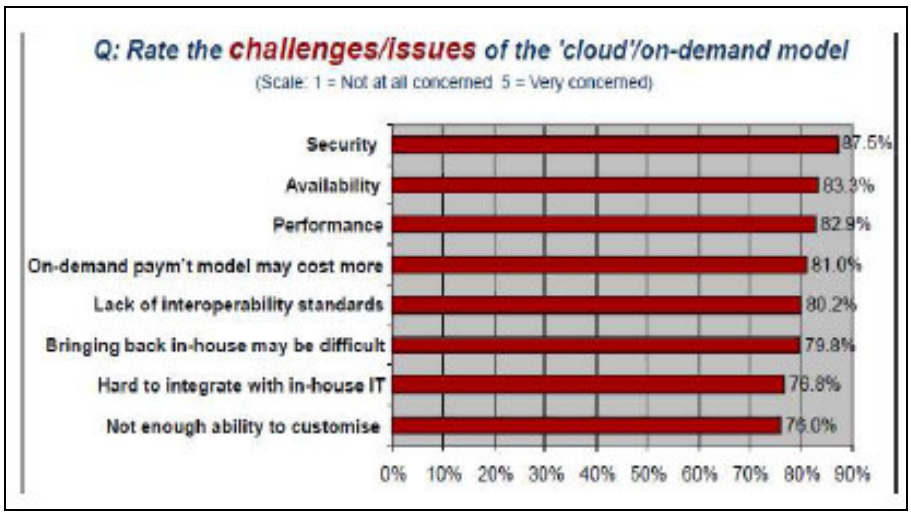

Figure 1. Cloud User Surveys 3Q09 – Security is the "Usual" Challenge (Source: IDC Enterprise Panel, September 2009)

Cloud computing has been envisioned as the next generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. As a disruptive technology with profound implications, Cloud computing is transforming the very nature of how businesses use information technology.

The main benefits of Cloud computing are therefore economies of scale through volume operations, pay-per-use through utility charging, a faster speed to market through componentizations and the ability to focus on core activities through the outsourcing of that which is not core (including scalability and capacity planning).

The protocol, Group Key Authentication (GKA) is proposed to facilitate to users with several services in a common cloud to roam from service to service. In the GKA protocol, each cloud service provider provides each user an authentication group key that the group key can be applied to several services at the same time. The group key is a combination key that is assembling the authentication key of several services. The order protocol is referred to provide the user that the services are user wanted. A group key is generated by the GKA protocol that composes a set key of each service for users' requests.

The communication process steps of GKA are shown in Figure 2.

1. Group Key Request: The user requests the Group Key.
2. ID Request: AUTH Server requests the User's ID for identification when the server receives the Group Key requirement.
3. ID Response: User sends the account name and password to AUTH server to identify user.
4. Authentication ACK (Success/Failure): AUTH Server sends a message for User to notice the authentication is success or fail.

5. Services Select: If authentication is success, then user will select the services that user needed. In addition, a requirement is sent to AUTH server.
6. Key Request: After AUTH Server receives the service request, it will send the Key Request and ID to Service Servers.
7. Key Response: When Service Server receives the request and ID, it will generate an authentication key and store the key and the ID. 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.

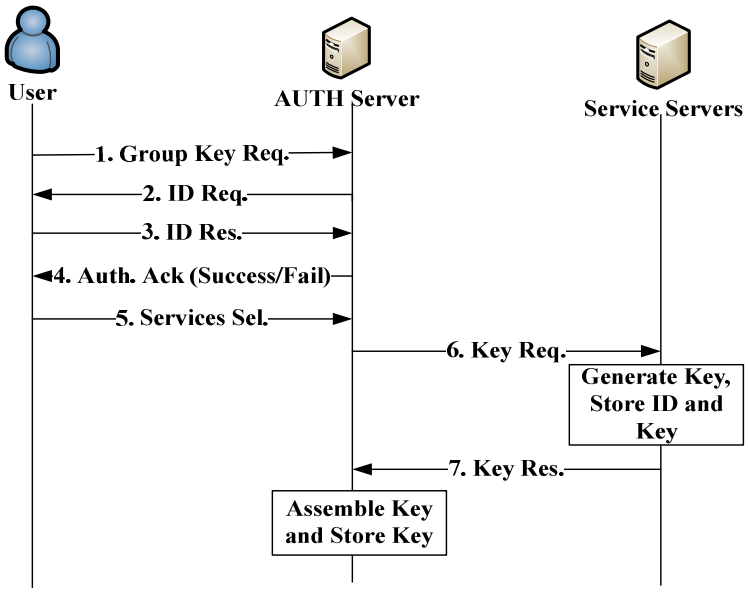

Figure 2. Group Key generating

After user created their own group key, the several services can be authenticated at the same time. The Group Key is GK = ($SERVICE_1$ ||$SERVICE_2$||…||$SERVICE_n$||ID). When user wants to apply a new service, then the authentication key of new service will be composed to the Group Key before ID. Moreover, every authentication key is creates by Service Server randomly.

An example of the authentication of user's several service requests is shown in Figure 3. The user applies the service just authenticating once. Users bring their own Group Key to each Service Server to request different services. At first, the Service Server verifies the Group Key and the ID of user. If the Group Key and the ID cannot be matched then Service Server will send a message to notice user to check their own Group Key and ID.

While Cloud computing makes the advantages more appealing than ever. Therefore, in the introduction we motivated the Group Key Authentication (GKA) for Cloud computing. By using the proposed GKA, the authentication time and data traffic in the Cloud computing can be reduced and the Quality of Service (QoS) can be increased.

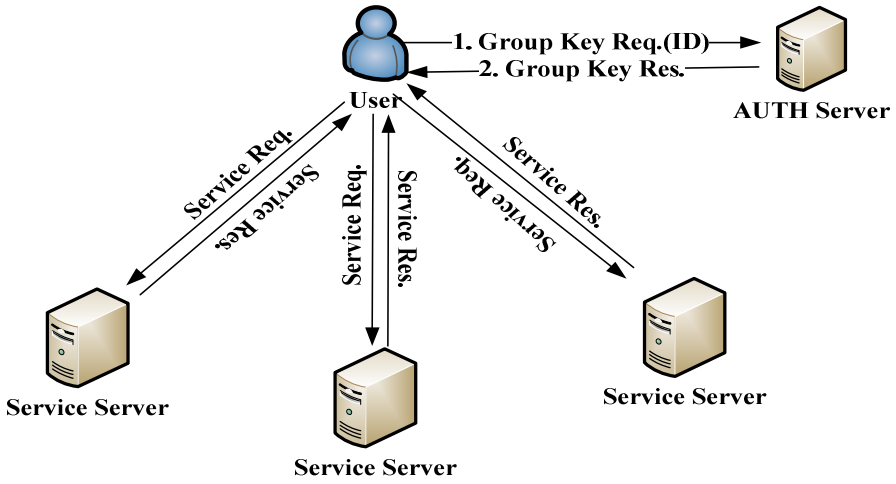

Figure 3. Apply to several services

4. DISCUSSIONS

In this section, the discussions of the advantages of the proposed GKA protocol are given. By using the proposed GKA, the authentication time and data traffic can be reduced

4.1 Reduce Authentication Time.

The proposed GKA protocol is compared with traditional authentication protocol. In the traditional way, the authentication requests should send many times to gain the identification of applied services. Therefore, if there are several services want to apply in different providers then the account name and password of user need to be inputted for each service. Hence, the wait time of the authentication is a long time.

The proposed GKA is composed with several service authentication keys for user that can gain the services of different servers in the one time. Therefore, user just needs to pass the AUTH Server authentication then user can obtain the service of server. User brings the Group Key to the services that have been chosen by user, and the Group Key can apply the requests to the chosen service servers. In other words, users do not need to authenticate repeatedly.

4.2 Reduce Data Traffic

In the Cloud computing environment, the cloud providers provide the multiple application services to users. There are a lot of service requests by cloud user; hence, a sequence of authenticated progressions for users needs to be done by Service Servers. In addition, the Service Server may send the same request to AUTH Server then many request packages for authentication are made. In the traditional way, this is a normal appearance, because the providers have own server to provide service to user. However, in the Cloud computing environment, there are so many services on the same server center. If the user request is frequently sent to the cloud service provider then there are a lot of authentications need to be executed. Therefore, the data traffic needs to be reduced effectively.

To use the proposed GKA protocol, the identification of user is authenticated only once. Then the Group Key is sent to user for applying the services with different providers. Comparing the traditional authentication protocol with the proposed GKA protocol, the steps of authentication of the proposed GKA protocol can be lessened. Owing to the data traffic for complicated authentication steps are reduced, the authentication messages between users and servers are lessened too.

5. CONCLUSION AND FEATURE WORK

Cloud computing provides an efficient, scalable, and cost-effective way for today's organizations to deliver business or consumer IT services over the Internet. A variety of different cloud computing models is available, providing

both solid support for core business functions and the flexibility to deliver new services.

In this paper, a Group Key Authentication (GKA) protocol is proposed which generates a composed group key to replace the traditional several authenticated keys. The proposed protocol can reduce the data traffic and authentication time on the Cloud computing environment. By using the proposed protocol, the several service requests in one time by user can be authenticated. In other words, a group key for user's service requests is composed by several service keys.

There are many security issues for protecting the sensitive information of user on the network. However, there is not a protocol to provide the flexibility security for users or companies needed. However, our proposed protocol will be extending to support the flexibility security.

ACKNOWLEDGMENT

This work was supported in part by the Taiwan National Science Council under Grants NSC99-2221-E324-022 and NSC97-2221-E-324–007-MY3.

REFERENCES

[1] S.A. Almulla and Y.Y. Chan, "Cloud Computing Security Management," *2010 2nd International Conference on Engineering Systems Management and Its Applications* (ICESMA), pp. 1-7, 2010.

[2] F.M. Aymerich, G. Fenu, S. Surcis, "An Approach to a Cloud Computing Network," *1st Int. Conf. Applications of Digital Information and Web Technologies*, pp. 113-118, August 2008.

[3] Y.W. Chen, J.T. Wang, K.H. Chi, and C.C. Tseng, "Group-based Authentication and Key Agreement," *Wireless Personal Communications* (Online, http://www.springerlink.com/content/tq650um81u38560 8/, DOI: 10.1007/ s11277-010-0104-7).

[4] R.L. Grossman, Y. Gu, M. Sabala and W. Zhang, "Compute and Storage Clouds using Wide Area High Performance Networks," *Future Generation Computer Systems*, Vol. 25, No. 2, pp. 179-183, Feb. 2009.

[5] M. Igor and B. Chris, "Cloud Security Technologies," *Information Security Technical Report*, Vol. 14, No. 1, pp. 1-6, 2009.

[6] J. Meiko, S. Jorg, G. Nils, and L.I. Luigi, "On Technical Security Issues in Cloud Computing," *IEEE International Conference on Cloud Computing* , pp. 109-116, 2009.

[7] J. Rittinghouse, J. Ransome, *Cloud Computing Implement, Management, and Security*, CRC, pp. 153.

[8] M.A. Vouk, Cloud Computing- Issues, Research and Implementations, *Proc. Information Technology Interfaces*, pp. 31-40, June 2008.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," *IEEE INFOCOM*, 2010.

[10] "Cloud guide," Cloud Security Alliance. December 2009.

[11] More Google Product, http://www.google.com/options/