International Journal of Engineering & Technology, 7 (4.39) (2018) 677-680

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Kerberos System Based Security Model Using Two Factor Authentication for Cloud Computing

Young-Soo Kim[1], Byoung Yup Lee[2*]

[1,2]Department of Cyber Security, Pai Chai University, Korea
**Corresponding author Email: bylee@pcu.ac.kr*

Abstract

Background/Objectives: The authentication technology is important in the cloud environment where many users and data are mixed. Therefore, we suggest a Kerberos-based Two Factor Authentication model to address the vulnerability of password.
Methods/Statistical analysis: We design and implement our suggested model. To check the practicality of cloud computing security model adopting Kerberos system based authentication model and Two Factor Authentication, we materialized authentication security model and authorization model.
Findings: In order to decrease the vulnerability of the password, we suggests Kerberos system based Two Factor Authentication model. We found that the suggested model has no errors in running, ensures security and confidentiality of information of the user when applied to the cloud environment to prevent cyber attacks targeting cloud services,and is resistant to cloud server attack by an attacker so that it can be the solution.
Improvements/Applications: Our suggested model ensures the security and confidentiality of information of a user when applied to the cloud that underlies a variety of application fields such as big data so that it can prevent cyber attacks targeting cloud services and contribute to activation of cloud computing.

Keywords: *Kerberos System, Security Model, Challenge Response, Two Factor Authentication, Authorization, Cloud Computing*

1. Introduction

Cloud computing is a type which does not own the IT resource but outsource a part or whole of it; users can use the cloud computing service at any time, at any place, and with any devices. It creates a computer environment for unspecified users to use without restriction of time and space. The authentication technology is essential in the cloud environment in which many users and data are mixed. However, most of cloud servers implement ID and password based authentication, which is vulnerable not only in the public network but also to cyber attacks and the vulnerability is one of the main obstacles to block the activation of cloud computing[1-5].

Therefore, the authentication technology is important in the cloud environment where many users and data are mixed. Most of cloud servers, however, implement authentication based on ID and password, which is vulnerable in the public network. Therefore, we suggest a Kerberos-based Two Factor Authentication model to address the vulnerability of password. Two Factor Authentication means a type of authentication that combines 'thing you know' with 'thing you own' and Kerberos-based Two Factor Authentication model using ID/password and a smart phone proposed in this paper ensure the identity a user connected to the network, adding a security stage to the existing Kerberos authentication system.

User authentication issue is a bar to make it hesitant to utilize cloud computing with the risk to leak critical information of an individual or a business. Particularly, it would increase the risk for important data stored in the cloud to be exposed to an unauthorized user. It is a bar to many businesses adopting the cloud service. In order to address the problem, we propose cloud computing authentication security model applying Two Factor Authentication to Kerberos authentication system by utilizing research model as seen in Figure 1.

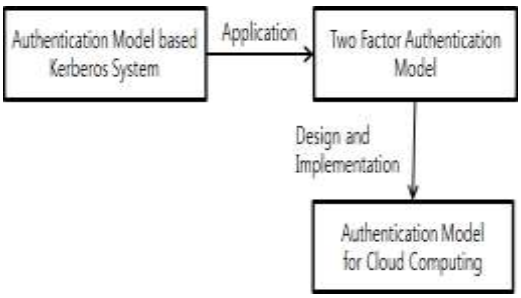

Figure 1: Research Model

Authentication security model is a means used to verify the qualification of a user who is able to access information. It is a technology to block inappropriate use or transmission of information and it has a significant meaning as a fundamental technology to secure access control over information resource and traceability to impose responsibility. This paper is written as follows. Chapter 2 analyzes the challenge/response based authentication model; Chapter 3 analyzes the Two Factor Authentication model with multiple authentication model. Chapter 4 proposes an authentication model for cloud computing applying Kerberos authentication and Two Factor Authentication model. Chapter 5 draws conclusion and implications.

2. Challenge-Response based Authentication Model

2.1. Challenge-Response Authentication Model

With Challenge-Response method, when a client has an access to a server, the server creates random number and sends Challenge to the client; the way the client encrypts the Challenge and gives it back to the server is called Challenges-Response authentication method[6-7]. Trial-Response authentication can improve security by utilizing authentication method with one-time random number that adds owning based security which is based in symmetric key to address the vulnerability to existing reply attacks using ID and password. With one-time random number, it is impossible to predict Challenge and it should vary. In this way, even though a hacker taps Response in the middle of communication, he is not able to reuse it. The authentication process utilizing Challenges-Response method is as shown in Figure 2.

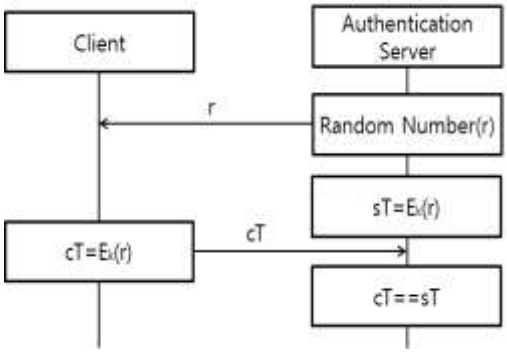

Figure 2: Challenges-Response Based Authentication Model

Authentication server generates a random number and sends it to the user in the form of Challenge. Simultaneously, the server has the password corresponding with identification number of the user and initiates encryption of the random number using the password. The user who received challenge(sT) encrypts it to be his password, EK(r), and gives response(cT) back to the authentication server. The server that received Response compares its own computation with the value of the Response; When they match, it verifies him to be an eligible user.

2.2. Kerberos System based Authentication Model

Kerberos is a system to provide identity authentication service, which was a part of the project, Athena, in MIT; it has the structure as shown in Figure 3. Kerberos system consists of AS(Authentication Server) and TGS(Ticket Granting Server). The authentication process of Kerberos system requires password of the user in the case when the user logs on the client system and it sends a message containing IDs of the user and the server and the password to AS. Authentication Server checks if the user input correct ID and password and he is authorized to have an access to the application server. When two stages are successfully made, AS accepts the user as an authorized entity and send TGT(Ticket to get Service Ticket) issued by TGS that enables him to access the application server. TGT is generated with ID of the user, network address, and ID of the service server to verify the authorized person. When the client sends TGT to TGS, TGS issues the service ticket that allows him to access the service server and gives it to the client. As the service ticket is encrypted with security key shared with TGS and the application server, it cannot be altered by the user or an attacker. With this service ticket, the client is able to have access to the application server to be provided with services[8]. The client sends the message containing his ID and ticket to the service server. The application server decrypts the ticket and checks if the ID in the ticket is identical to the plain ID in the message. It also checks if the network address in the ticket is identical to the connected address. When they match, the application server acknowledges the user as an authorized entity. Kerberos system based authentication model requires the password only once when the client wants to get the server service so that it is able to block the attack related to the password.

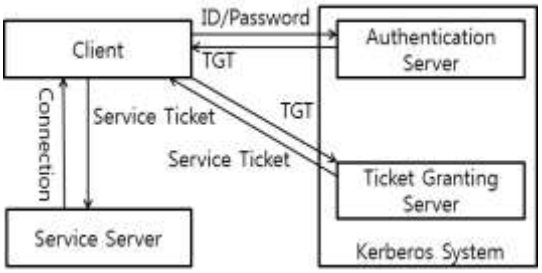

Figure 3: Kerberos System Based Application Model

3. Multiple Authentication Model

3.1. Password based Single Authentication Model

Password system authenticates the user after comparing inputted ID and password with those stored in the system and when they match, it accepts him as an authorized user, which is one of the most common authentication methods. It provides effective authentication in a controlled environment. The security of the password system depends on the confidentiality of the password. This method, however, can be targeted by an attacker using random attack when the password file is not protected under access control[9]. Thus, the password file should use one-way function and store the output of the hash function. This authentication method has the process that the user inputs his password into the system and the system inputs the password to one-way function and applies the output and firstly inputted password to the one-way function and compares the output with the value stored in the system to authenticate the user. Figure 4 describes the process in which the password is compared when the user A logs on to the computer.

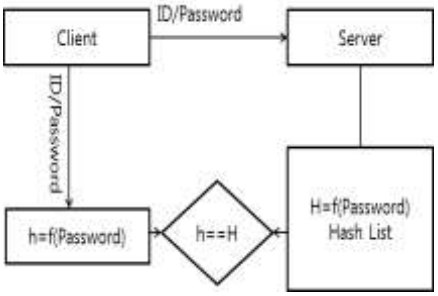

Figure 4: Password based Authentication Model Using One-Way Function

3.2. Smart Phone based Two-Factor Authentication Model

2FA(Two-Factor Authentication) is added with another authentication and checking stage to basic user name and encryption security model. Without 2FA, user name and password are enough to be authorized. Single authentication factor is password. However, when using same user name and password, identity information has the risk to be stolen. Utilizing 2FA, another step is added to the primary login process; two stage safeguards should be neutralized to be hacked. Therefore, the success rate to attack decreases and not being solely dependent on the password decreases the vulnerability[10]. As seen in Figure 5, smart phone based 2FA implements authentication by integrating user login including password with physical access to the smart phone. The user inputting ID and password can log on to AS and he receives

OTP(One-Time Password) in text message using SMS via a mobile device and sends OTP via PC; in this way, the authentication process is complete. When sending OTP generated in the server to the user, owning the smart phone used for receiving OTP is an important security factor in this authentication model. In fact, one who stole an end user's smart phone, user's name, and user's passphrase is able to disguise as the end user. Furthermore, an attacker could copy SIM card to receive SMS of the end user.

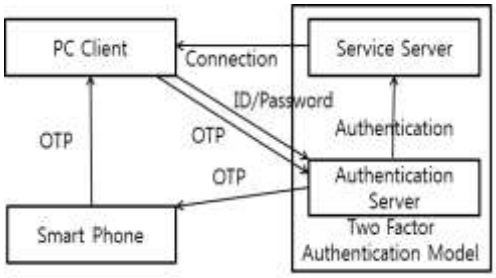

Figure 5: Smart Phone Based Authentication

4. Kerberos System Based Security Model Using Two Factor Authentication for Cloud Computing

4.1. Our Suggested Authentication Model

The key to cloud computing service is to control the access by checking identity of the user. However, many cloud servers implement authentication based on ID and password, which is vulnerable in the public network. For this reason, 2FA(Two Factor Authentication Model) is necessary to resolve the vulnerability of passwords. 2FA is a type of authentication that combines 'thing you know' with 'thing you own.' Utilizing this authentication model ensures that a user connected to a network is the authorized user. Strong authentication solution has an effect for a business to add another security stage. Therefore, it is imperative to make 2FA to be the standard of the cloud service. For this, we suggest Kerberos system based Two Factor Authentication model for cloud computing by applying Two Factor Authentication model to Kerberos system.

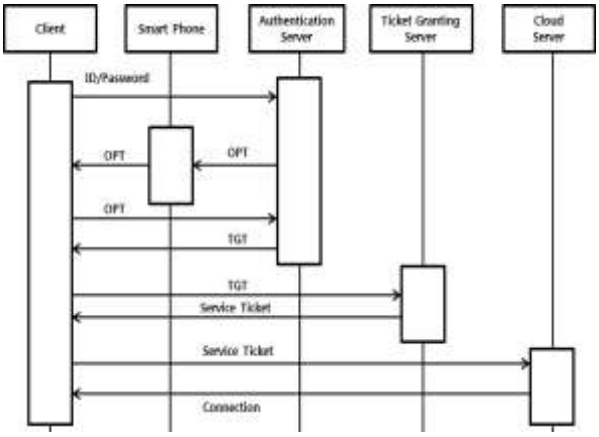

Figure 6: Kerberos System Based Security Model Using Two Factor Authentication for Cloud Computing

As seen in Figure 6, for cloud computing the user using the client of PC sends ID and password and the authentication server verifies the user first; for the second authentication, it generates disposable password to be sent to the smart phone of the user. Authentication is complete when the user inputs the disposable password on the client and it issues TGT(Ticket to get Service Ticket) to get the cloud service ticket and send it to the user. The user sends TGT(Ticket to get Service Ticket) to TGS(Ticket Granting Server) and gets the service ticket and is provided with services after the request.

4.2. Verification of Our Suggested Authentication Model

To check the practicality of cloud computing security model adopting Kerberos system based authentication model and Two Factor Authentication, we materialized authentication security model and authorization model. Figure 7 describes the process to approach a webpage implementing authentication and authorization as the process to verify practicality. It shows the process in which it identifies kim and authenticates him and allows him to access every webpage in the application after authorization.

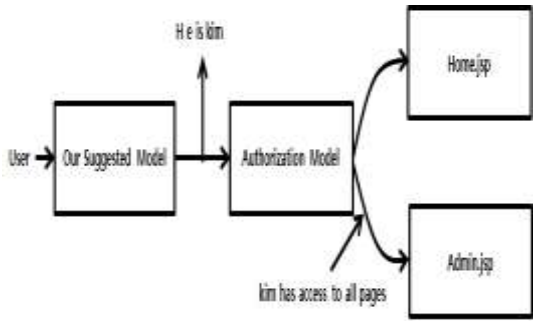

Figure 7: Process for Practicality Verification

The architecture of cloud computing security model applying our suggested model is as shown in Figure 8. The user is requested to complete the user registration before access to the webpage. After the user using the client is authenticated from the authentication system implementing our suggested model, it stores authentication information of the user and the accessible application list into the database and displays the list on the client of the user.

When the user chooses a certain web application on the list, with the reference of the authority information of the database, it issues a disposable token and stores information of the token and the user authentication into a new table of the database. When the user has access to a certain webpage, it sends the token and it allows the user to access as there is the token in the database.

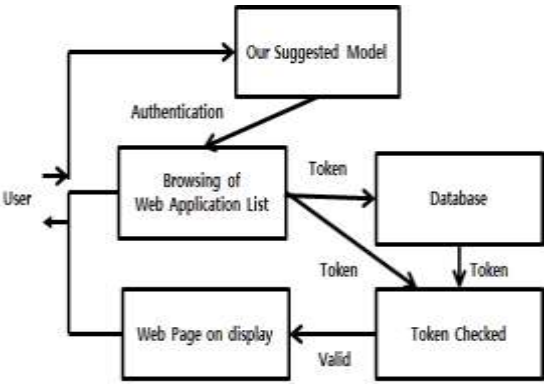

Figure 8: Application Model for Practicality Verification

We found that the suggested model has no errors in running, ensures security and confidentiality of information of the user when applied to the cloud environment to prevent cyber attacks targeting cloud services, and is resistant to cloud server attack by an attacker so that it can be the solution.

5. Conclusion

At present, cyber attacks targeting cloud services have severely increased and some cloud services have been occupied and weaponized. When virtual machine of the cloud service is hacked,

it can be abused with C&C server communicating with malicious IP addresses and it would attack another virtual machine and send junk mails. In the cloud computing environment where data of many users are stored, authentication technology of the user is essential. However, the common way of authentication in the cloud service is as follows; When the user sends Credentials and requests log-in, the service provider authenticates him after comparing it with user information stored in the back-end system. It is vulnerable in the public network. In order to decrease the vulnerability of the password, we suggests Kerberos system based Two Factor Authentication model. 2FA is a type of authentication combining thing you know with thing you own; the Kerberos system based Two Factor Authentication model utilizing ID, password, and smart phone suggested in this paper makes it possible to trust the user connected to the network is the rightful person, which provides an effect to add security stage to Kerberos authentication system. It consequently ensures security and confidentiality of important information of the user after applied to the cloud environment that underlies different application fields like big data so that it can prevent cyber attacks in advance and contribute to activating cloud computing.

Acknowledgment

This research was supported by the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT and Future Planning (NRF-2017R1A2B1003678).

References

[1] F. Cheng, Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm, Mobile Networks and Applications pp.304-336, 2011.

[2] Eldefrawy, Mohamed Hamdy, Khaled Alghathbar, and Muhammad Khurram Khan. OTP-Based Two-Factor Authentication Using Mobile Phones. Information Technology New Generations(ITNG), Eighth International Conference on. IEEE, pp. 327-331, 2011.

[3] FadiAloul, Syed Zahidi, Wassim El-Hajj, Two Factor Authentication Using Mobile Phones. IEEE/ACS International Conference on Computer Systems and application, pp. 641-644, 2009.

[4] Temkar, Rohini, Comparative Approach to Cloud Security Model, Springer Advaces in Computing, Communication and Control, Vol.125, pp 170-177, Jan 2011.Forman, G. 2003.

[5] Ganseo Zhao, ChunMingRong, Jin Li, Feng Zhang and YongTang, Trusted Data Sharing Over Untrusted Cloud Storage, IEEE International Conference on Cloud Computing Technology and Science, pp 97-103, Dec 2010.

[6] Hojabri M., Rao K. V., Innovation in cloud computing :Implementation of kerberos version5 in cloud computing in order to enhance the security issue, ICICES2013, pp452-456, 2013.

[7] H.M.N Al-Hamadi, C.Y. Yeun, M.J. Zemerly, and M. Al Qutayari, Distributed Lightweight Kerberos Protocol for Mobile Agent System, IEEE GCC2011, pp.233-236, 2011.

[8] InshilDoh, KijoonChae, Jiyoung Lim and Min Young Chung, An Improved Security Approach Based on Kerberos for M2M Open IPTV System, Tthe 15 International Conference on NBiS2012, pp.754-759, 2012.

[9] Abdul Raouf Khan, "Access Control in Cloud Computing Environment", APPN Journal of Engineering and Applied Sciences, Vol.7, No.5, pp.613-615, 2012.

[10] A. M. Axel Buecker. Protecting Data Assets by Deploying a Multi-Factor Authentication Solution with End-to-End Encryption. Technical report, IBM, 2013.