International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 221-234
http://dx.doi.org/10.14257/ijsia.2014.8.3.23

Privilege Management System in Cloud Computing using OAuth

Jeong-Kyung Moon[1,A], Hwang-Rae Kim[1,B] and Jin-Mook Kim[2]

[1] Division of Computer Science and Engineering, Kongju National University, Cheonan, 331717, Korea
[2] Division of Information Technology Education, Sunmoon University, Asan, 336708, Korea
{moonjk1018, plusone}@kongju.ac.kr, calf0425@sunmoon.ac.kr

Abstract

OAuth protocol has been developed of fast and easy-to-use proxy authentication structure over a surge in user demand for mobile cloud. However, OAuth involves some security and privacy problems. So, we propose ADAMS for user user authentication system mobile environments that can support user authentication, service authentication and access control services more convenience and easily. ADAMS simplify the authentication processing procedures to improve the structure of complex authentication of SSL or PKI. We developed a book research system in order to evaluate the safety of the ADAMS environment. It was assessment of ADAMS logicality using ASVO logic. ADAMS experimental results can improve confidentiality, integrity, availability, and non-repudiation services in mobile book research service.

Keywords: *OAuth, Cloud computing, Management System, BRS*

1. Introduction

Cloud computing is very fast increase that being used in accordance with the requirements of the efficient use of IT resources. The world's major companies provide cloud computing services. -Google App Engine, Amazon's EC2, Microsoft Azure Services Platform etc. And KT, SK, LG, and SKT are public and typical agencies to cloud computing service in domestic environment. 2013 World Mobile SNS number of subscribers is expected to reach 10 billion. Services such as Facebook, twitter, YouTube and each college Book Search App service for smartphones is on the rise. Most of these SNS services are using OAuth. OAuth as a way of authenticating users to access Web services are vulnerable to security. Virtualization technology can violated Infringement of malicious code and availability [1]. Therefore, it requires the use of a safer protocol and more reliable user authentication to access cloud computing services. We propose ADAMS for prevent the disorder that cloud computing can occur in the vulnerability of virtualization and information leakage occurs due to the centralization of information service. ADAMS was simplifying the certification authentication procedure to the structure of the complexity of the existing PKI and SSL. We build the appropriate database in the cloud environment, using the data of several university libraries to experiment with ADAMS and at other universities to search. Changes to OAuth for safe user authentication and service authentication and permission-based access control can be designed to Book Search. So, it was designed so that it can effectively handle the authentication problem that can occur when sharing data from various universities.

Composition of this treatise is as following. Chapter two, described about connection research about cloud computing and certification. And chapter three, Described about

[A] Jeong-Kyung Moon is First author, her mail address is moonjk1018@kongju.ac.kr
[B] Hwang-Rae Kim is Corresponding author, his mail address is plusone@kongju.ac.kr

ISSN: 1738-9976 IJSIA

Operate design and operational process for rights management system, user authentication and service authentication using OAuth. We descript the proposed model implementation results and logical evaluation in chapter four. Finally, chapter five is conclusion.

2. Related Works

We explain about related research in this chapter. First, Describe authentication technology using OAuth. In second section, we explain PMI and Cloud computing in third section.

2.1. OAuth (Open Authentication)

OAuth 1.0 protocol developed by the OpenAPI is an international standard authentication method. When authorized in a variety of applications, user authentication is used. OAuth is standardized authentication method each authentication method as a Google's AuthSub, AOL OpenAuth, Yahoo's BBAuth, Amazon's Web Services API. If you are using OAuth, this authentication application to share ours does not require a separate certification. OAuth can be authentication and authorization functions [2, 3]. Facebook, Google, Microsoft Messenger etc is using OAuth protocol.

OAuth consist three objects. There are User, Consumer, and Service Provider. User means a personal account to use the Service Provider and Consumer. Consumer is means the OAuth Service Provider to access the web site or application. Service Provider is means Web applications to support access via OAuth.

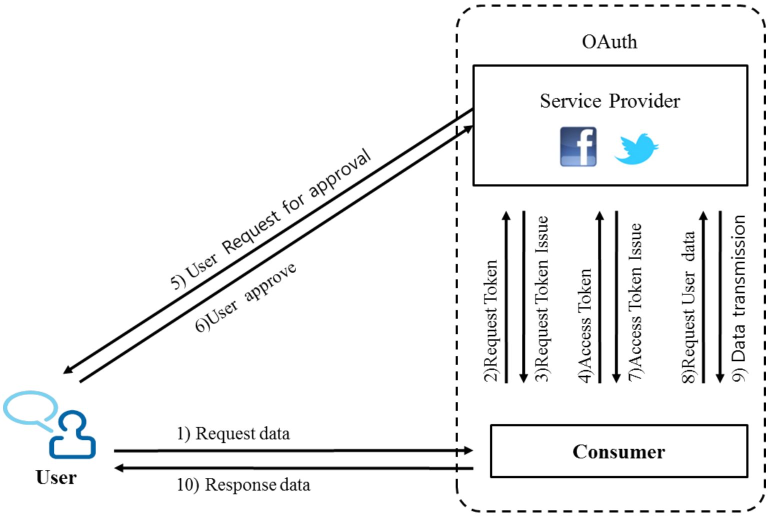


Figure 1. Procedure of OAuth Certification

Figure 1 User is subscribed to the Service Provider. When consumer is access to the users protect data, describe authorization procedure. Step 1 shows that user should be able to request the data. Step 2 and 3 shows that consumer is request to the service provider a temporary token. And Service Provider issue token and transit to Consumer. Step 4 shows that Consumer request access token for access to user's data. In step 5 and 6, Service Provider asks whether to approve access to the User. And User approved it. Step 7 shows that Service Provider is passing to the Consumer Access Token. Step 8 and 9 show that Consumer is request to the Service Provider to access the data requested by the User and Service Provider to transmit data. Finally, step 10 shows Consumer response to the User [4].

2.2. PMI (Privilege Management Infrastructure)

PMI attribute is authentication that provides information to users using the extension field of the X.509 certificate. PMI is simple because existing Public Key Infrastructure (PKI) can be used because the authentication procedure. However, the shorter the period for which the certificate is valid, there is a problem that different attribute certificates and Certificate Authority issuing authority.

PMI validate the attribute certificate to check the attribute information of the user. In this process, the privilege verifier to determine whether the user has a legitimate right that Connect a public-key certificates, attribute certificates and pointing it [5, 6].

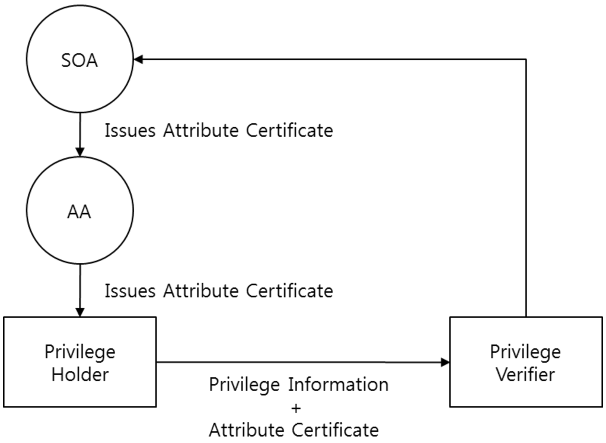


Figure 2. PMI Structure

Privilege Management Infrastructure of the overall structure shown in Fig. 1. OA and the CA of the PKI is similar to the self-authorization, SOA should blindly trust. AA rights of all or any certificate issued under delegated some tasks to perform from the SOA. Privilege Holder End-entity who received assurance from AA through a certificate authority for ownership. Privilege Verifier used to fit the application to receive this attribute certificate. Privilege Holder verify rightfully owns.

2.3. Cloud Computing

The cloud computing service is a novel service that can provide to a novel computer function by network infrastructure. Cloud computing service can divide by three categories. It is SaaS, PaaS, and IaaS. Below Table 1 divides cloud computing model by three and described explanation about it [7].

Table 1. Cloud Computing Model

	Feature	Examples
SaaS	It is way to lease and uses software that user is necessary in Internet. Against of elder way. User is different from thing which should buy and install direction software in existing when past-time [8].	Salesforce.com MobileMe, Google DOCS
PaaS	It is a Platform that borrows and uses tools that developer is used in development. By this way, software development is easy and fast, and price is cheap [9].	Google App Engine, Windows Azure,
IaaS	It is model that lent a computing infrastructure such as CPU, Memory, and Storage representatively.	Amazon AWS, GoGrid, At&T

Cloud computing services can divided depending on purpose to use Private Cloud, Public Cloud and Hybrid Cloud. Public Cloud provides flexible and affordable services in order to provide a variety of solutions to the services offered to the general user. Google AppEngine or Amazon's EC2 services are included here. Private Cloud within an enterprise cloud service closed, and the agency or organization responsible for the management and control for the user, and security is a powerful. Hybrid Cloud is a cloud service that maximizes the benefits of Public Cloud and Private Cloud. Hybrid cloud is enhanced security model proposed as a new model. It provides that reliable of Public Cloud service and confidential data management services of private cloud [10].

Cloud computing is Virtualized resources. From virtualization to cloud computing security issues that need to be addressed, is the biggest problem. Integrated into a single resource to manage multiple servers exist on the Host OS is installed on top of it, there will be an application. Cloud environment, the charging information, resource sharing, due to the diversity of the terminal, there are a variety of risks [11].

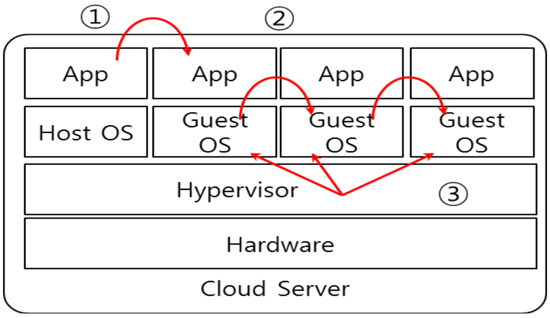


Figure 3. Virtualization of Vulnerability

Figure 3 Guest OS is infected with secondary infection takes place. And hypervisor infection leads to all the virtual machines that can be infected after shows. In addition, cloud computing due to the trustee. it is impossible to verify the user's information even if copy/move/modify. By the service provider of insider information leakage possibilities also exist.

3. Proposal System

3.1. Structure of Proposal System

ADAMS proposes to form a separate independent delegation of authority by changing the OAuth protocol. Independent privilege management provide in the form of Web-proxy server existing structure of PKI and CA permission from government agencies or provide one of both consumer or service provider of the system administrator role. This can cause high cost. However, reliability can be achieved. In addition, the privilege management system of the proposed system is simple processing procedures compared to OAuth. Figure 4 Shows structure of proposal system.

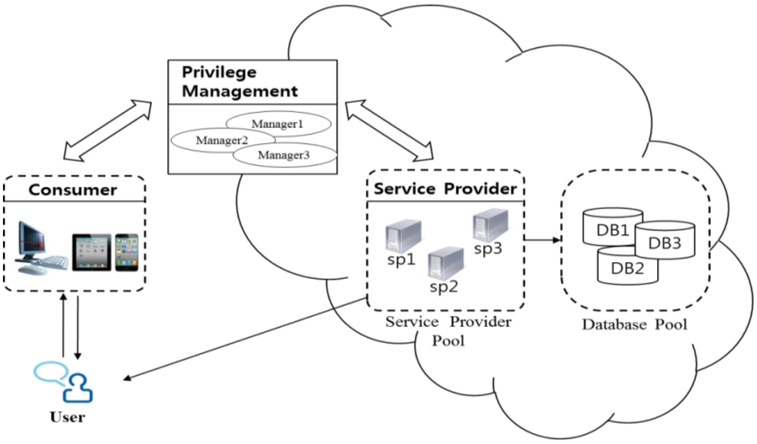


Figure 4. Overview of ADAMS

Figure 5 shows the components of the proposal system. These systems have user, consumer, service provider, privilege manager. User is request the service. Consumer is download or data group. Service Provider is consists of database group and service provider of book search for certification that can be handled easily and quickly group. Privilege Management is privilege management group to perform mutual authentication between the Consumer and Service Provider Administrator Group.

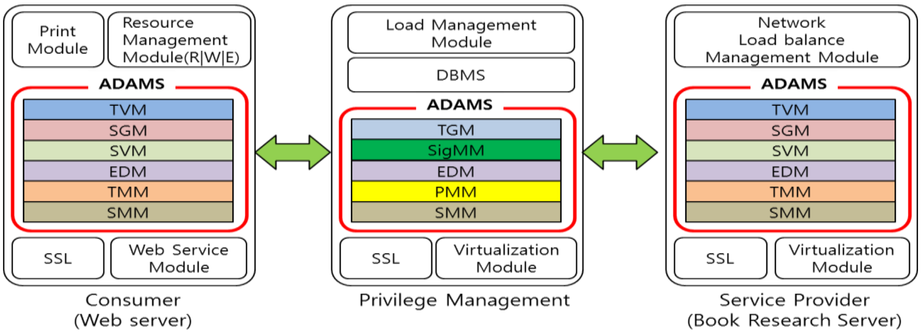


Figure 5. Components and Relation of ADAMS

Each component of the Proposal system with each of the internal structure is shown in Figure 5.

Table 2. Component Description

Component	explanation
TVM	Token Verify Module
SGM	Signature Generate Module.
SVM	Signature Verify Module
SMM	Session Management Module.
EDM	Encrypt & Decrypt Module
TMM	Transaction Management Module.
TGM	Token Generate Module
SigMM	Signature Management Module
EDM	Encrypt & Decrypt Module.
TMM	Transaction Management Module.
PMM	Privilege Management Module.

ADAMS consists of the user, consumer, service provider, privilege management. User, consumer and the service provider should handle authentication for user authentication and interaction devices for the service requested. it has six modules, in order to convey information about the service it requested. Unlike the existing OAuth, privilege management has five modules to centrally control the consumer and the service provider. Table 2 descript for each components.

3.2. Procedure of Proposal System

Proposal system has 13 details procedures. It can divide two big processes. First processing is verifying the user identity authentication. It consists of two steps. Figure 6 shows proposal system.

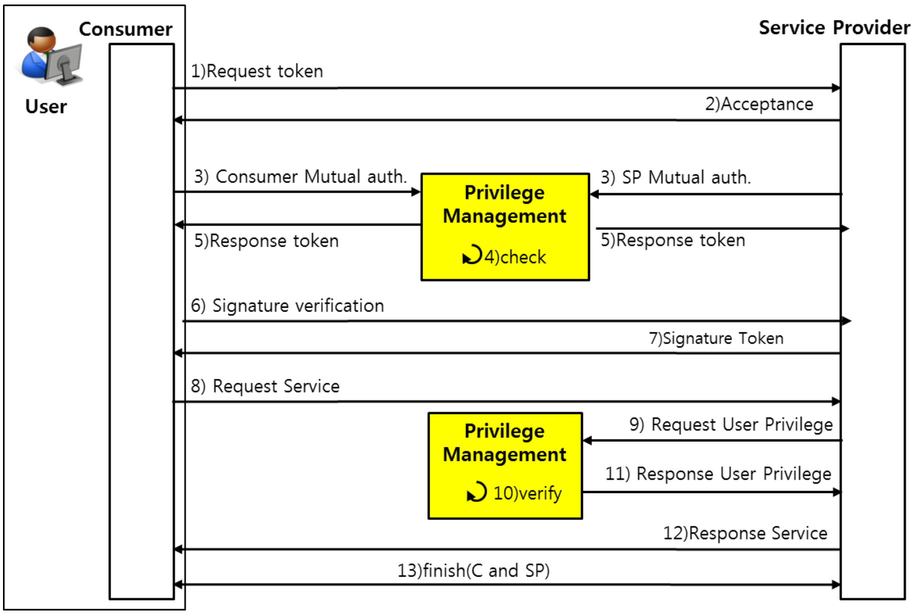


Figure 6. Procedures of our Proposal System

First process has two procedures.

1) Consumer transmits to the Service Provider User login information. In this time, the consumer transmits information of encrypted by user ID, PWD, TS and nonce using Session Key for legitimate visitor check.

User_Info = ENC_{SK}\{ ID | PWD | TS | nonce\}

2) Service Provider permits the User into login after confirming information.

The second process is authentication procedures to the Service Provider and Consumer objects for identification. In this step, privilege management creates identification token to the Consumer and Service Provider after confirming information.

This work consists of five steps. From step 3 to 7 is describe detail procedure.

3) Consumer and Service to Privilege Management request authentication. In this time, Consumer or Service Provider generate encrypted by IP, MAC, TS and Session ID. and pass.

Obj_Info = ENC_{SK}\{ C_IP | Obj_MAC | TS | Se_ID \} / Obj_Info = ENCSK\{ SP_IP | Obj_MAC | TS | Se_ID \}

4) Privilege Management verifies justice and generates a token.

5) Privilege Management is generated token then Encrypt and passed

Obj_Token=ENC$_{SK}${ C_IP | SP_IP | TS | Se_ID | D_MAC }

6) Consumer signed Obj_Token by HMAC_SHA1 algorithm and his own secret key value. And Passed it to the other party's public key to encrypt.

Sig_Token=EN$_{SK}$(HMAC-SHA1{Obj_Token, s_key})

7) Completing the process of identity authentication by opponent.

Next procedure has four steps. Service request and the Privilege Management through a process of mutual authentication is to go through the certification process for the service. It is from 8 to 11 steps.

8) User request access to the Service Provider for the resource.

Request_Service= EN$_{SK}${Service_ID | Obj_name | R | W | E | Optional }

9) Service Provider requests privilege information of user for prove the legitimacy of user request. The authorization information is encrypted using the session key.

User_Request=EN$_{SK}$ { Service_ID | Obj_name | ID | PWD | TS | nonce}

10) Privilege Management to validate the user's rights..

11) Privilege management transfer user's privilege information by encryption. At this time, guide to license is according to the User's privilege.

User_Privilege = EN$_{SK}${ Service_ID | Obj_name | R | W | E | Optional }

12) Service Provider transfers the results of limiting by privilege management to the user's request. At this time, you can avoid the man-in-the-middle attacks by the other party's public key encryption.

Response_Service(Resource=EN$_{SK}$ (Service_ID | Obj_result)

13) Finally, disconnect a session that means communication is terminated.

We can be seen that the course of action to provide basic security services of confidentiality, integrity, non-repudiation, such as man-in-the-middle attack. Table 3 is list of abbreviations for the ADAMS's operating procedure.

Table 3. Abbreviations Table

Abbreviations	explanation
ENC/DEC	Encryption/Decryption
SGM	Signature Generate Module.
SVM	Signature Verify Module
SMM	Session Management Module.
EDM	Encrypt & Decrypt Module
TMM	Transaction Management Module.
TGM	Token Generate Module
SigMM	Signature Management Module
EDM	Encrypt & Decrypt Module.
TMM	Transaction Management Module.
PMM	Privilege Management Module.

4. Experiment and Analysis

4.1. Experimental Scenario

In this paper, we build a book search system in order to test the proposed protocol, the user authentication protocol design and implementation. Environment of proposed system has two Linux operating system of the Book Search server. Book Search server each to each was designed have three Book Research DATABASE server. We are Book Search in a cloud computing environment use Hadoop.

Experimental scenarios are two. User's access to the system and authority was limited. Scenario 2 has all rights to the User access to the system. The order of the authority is the read, modify, download and optional.

(1) Experimental scenario 1

User A request access to the system by the Book Search Book named "Antonio Salieri". User A read, download, and print rights have to connect to the web server. User A experiments were possible to normal data research. Also, Test the fails of the experiment when DATABASE to modify the data access.

Privilege_A = { 1 | 0 | 1 | 1 } Order to read, impossible to modify, download, option to authorize. Shown in Figure 7.Shows the modification is limited privileges.

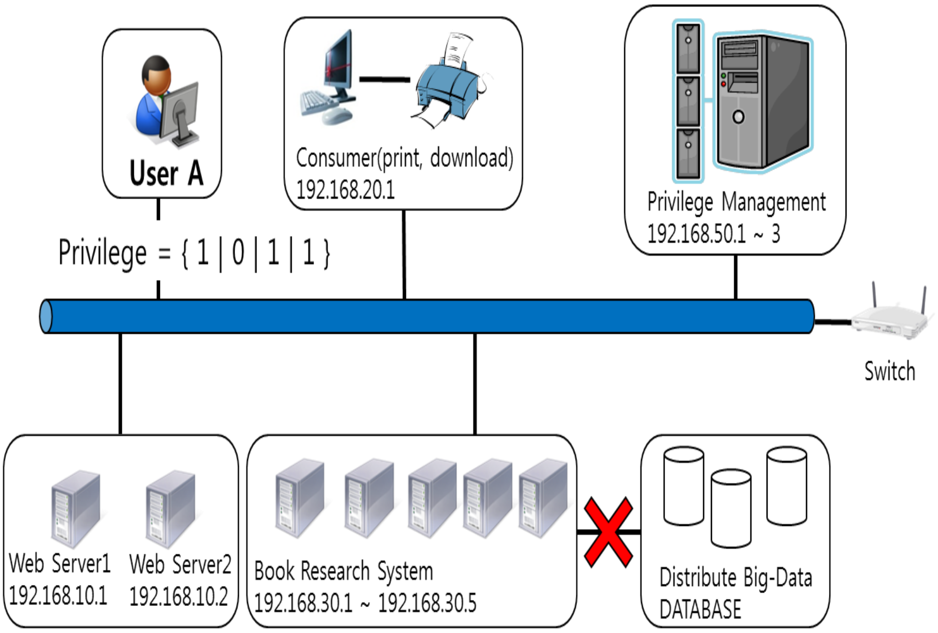


Figure 7. System Configuration of Scenario 1

(2) Experimental scenario 2

User B to read, modify, download, the option shall have the authority. Experiments was to the normal behavior when a user B with all privileges to research data. Also, Test the success of the experiment when DATABASE to access and modify data.

Privilege_B = { 1 | 1 | 1 | 1 } user B read, modify, download, the option was to authorize.

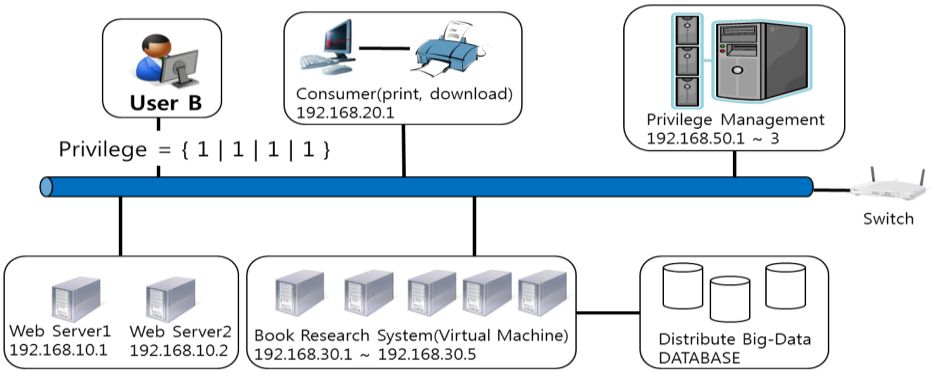
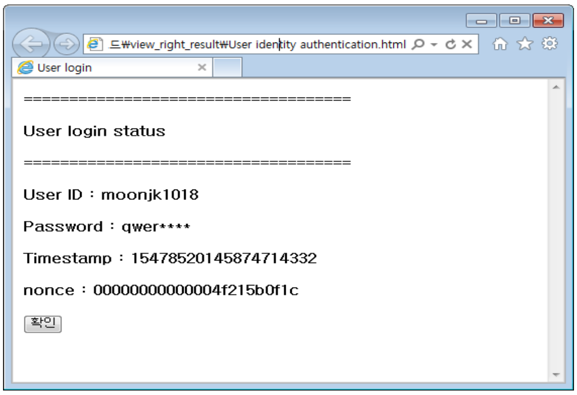


Figure 8. System Configuration of Scenario 2

4.2. The Experimental Results

(1) Experimental results of Scenario 1

This scenario, ADAMS was implemented of the user's initial identification process to connect to the web server to handle the authentication. In Fig.9, Logged in enter your user ID and password then user ID, password, timestamp and nonce value is checking the screen.



=====================================

User login status

=====================================

User ID : moonjk1018

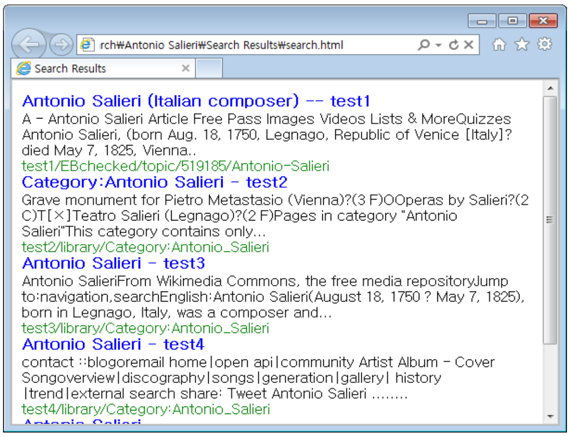
Password : qwer****

Timestamp : 15478520145874714332

nonce : 000000000000004f215b0f1c

Figure 9 Result of Identity

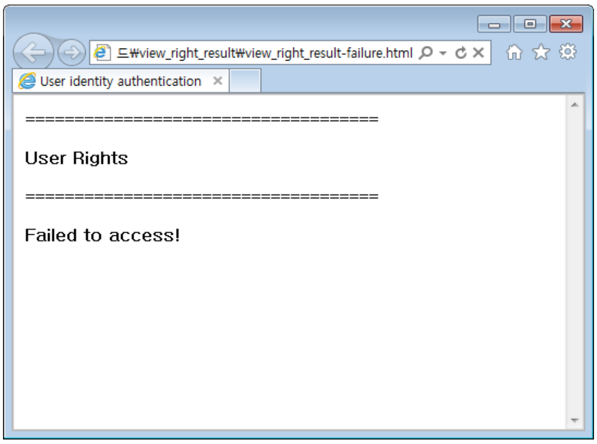
Figure 10, Log in and search for "Antonio Salieri" As a result, the search is successful screen.



Antonio Salieri (Italian composer) -- test1
A - Antonio Salieri Article Free Pass Images Videos Lists & MoreQuizzes Antonio Salieri, (born Aug. 18, 1750, Legnago, Republic of Venice [Italy]? died May 7, 1825, Vienna..
test1/EBchecked/topic/519185/Antonio-Salieri
Category:Antonio Salieri - test2
Grave monument for Pietro Metastasio (Vienna)?(3 F)OOperas by Salieri?(2 C)T[×]Teatro Salieri (Legnago)?(2 F)Pages in category "Antonio Salieri"This category contains only...
test2/library/Category:Antonio_Salieri
Antonio Salieri - test3
Antonio SalieriFrom Wikimedia Commons, the free media repositoryJump to:navigation,searchEnglish:Antonio Salieri(August 18, 1750 ? May 7, 1825), born in Legnago, Italy, was a composer and...
test3/library/Category:Antonio_Salieri
Antonio Salieri - test4
contact ::blogoremail home|open api|community Artist Album - Cover Songoverview|discography|songs|generation|gallery| history |trend|external search share: Tweet Antonio Salieri ....
test4/library/Category:Antonio_Salieri
Antonio Salieri

Figure 10. Result of Data Research

Figure 11, when access to the request for modification of the material to DATABASE, Shows that the approach does not have permission to access is restricted.

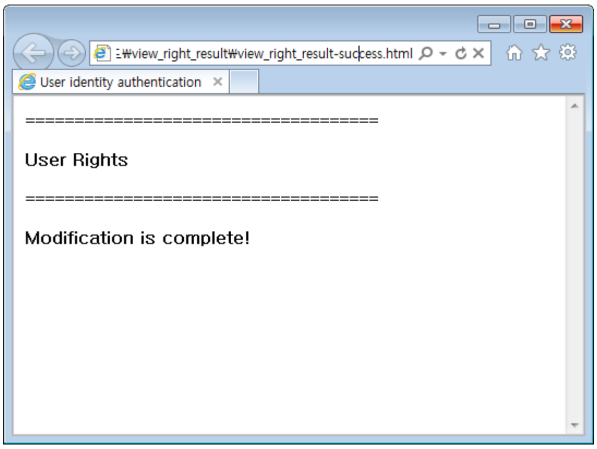

드₩view_right_result₩view_right_result-failure.html
User identity authentication

```
========================================

User Rights

========================================

Failed to access!
```

Figure 11. Result by User Authentication Failure

(2) Experimental results of Scenario 2

Scenario 2 is the same as for Scenario1 except DATABASE to modify the approach that it is possible. It shows that cannot to access if you do not have permission. It shows that success in DATABASE modification of Scenario 2 because you have to the permissions.


:₩view_right_result₩view_right_result-success.html
User identity authentication

```
========================================

User Rights

========================================

Modification is complete!
```

Figure 12. Result of Access Success

4.3. Verification

We want verify the reasonableness of our proposed schemes in this paper, by using the logic of ASVO verification one of the security protocol verification techniques. Verification goals are ASVO 0 is Activeness check the activation status. Next, ASVO 1 is Aliveness checks online status. And ASVO3 is verify the Authentication status [12].

(1) ASVO 0: Activeness

It can determine whether you have received the message X for activation protocol other party in online status. It does not confirm the identity of others.

ASVO 0 : *A believes A received X*……………………………………………………………… *(Expression 1)*

Protocol enable state is verified as a received by the X. In this paper, protocol Activity state is verified because Consumer received the token from Privilege Management.

C believes SP received token from D……. ……. ……. ……. ……. ……. ……. ……. …….
(Expression 2)
SP believes U received token from D……. ……. ……. ……. ……. ……. ……. ……. …….
(Expression 3)
U believes C received token from D ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ………. ……. ……. …….
(Expression 4)

(2) ASVO 1 : Aliveness

Protocol activity state is verified other party of online status. For Implied to the identity of the other party to make, protocol participants should be able to get the trust on the other side of the transmission and point.

ASVO 1 : *A believes B says X* ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ………. ……. ……. ……. …….
(Expression 5)

This is authentication to implied because perform protocol between A and B. In this paper, Consumer can verify to activity protocol as the Service Provider exchange the Token in online status.

C believes SP say token ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ………. ……. ……. …….
(Expression 6)
SP believes U say token ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ………. ……. ……. …….
(Expression 7)
U believes C say token ……. ……. ……. ……. ……. ……. ……. ……. ……. ……. ………. ……. ……. … ……. ……. ……. ….
(Expression 8)

(3) ASVO 2 : Authentication

We cannot be sure whether a trust for the communication between themselves and that is the other party. Therefore, Shall determine whether the certification of the other party through the key distribution.

ASVO 2 : A believes B says A ←key→ B and A believes A ←key→B ... ……. ……. …. …. ……. ….
(Expression 9)

It trust the fact that A and B share the same key, and it shows that B also recognized the fact. In this paper, Consumer believes Service Provider because consumer and service provider share the same key. And Consumer believes you because consumer and service provider share the same key.

C believes SP say C ←token→ SP and C believes C say C ←token→ SP …. ……. ……. ….
(Expression 10)
SP believes U say SP ←token→ U and SP believes SP say SP ←token→ U ……. ……. ….
(Expression 11)
U believes C say U ←token→ C and U believes U say U ←token→ C ……. … … ……. ….
(Expression 12)

ASVO verification method validation results, we were able to prove that this protocol is logically.

5. Conclusion

Cloud computing environment is growing rapidly in demand because due to ease of access and increase resource utilization. But it has many security vulnerabilities Due to the specificity of virtualization technology to provide of cloud computing environment. Recently, has been developed a fast and simple protocol OAuth to authentication structure. But yet the problem of security and privacy is implied.

This paper proposed and designed ADAMS for user authentication systems to be used in cloud environments and mobile cloud environment. ADAMS is a hybrid authentication protocol. User identity authentication was used symmetric-key approach and service authentication was used public-key approach. In the Services Certification was adding that privilege management method by change the existing OAuth protocol authentication. As shown in the operating procedures provide basic security services such as confidentiality, integrity and non-repudiation. ADAMS structure has higher security than OAuth protocol. It has simple processing procedures compared with existing authentication system.

ADAMS is integrated authentication protocol system to one integrated system configured into user identity authentication and privilege management services. We expected good retrieval system by integrating several agencies, including the ability to perform cross-certification system utilizing advanced research in progress.

References

[1] Dillon, T., Chen Wu, Chang, E., Cloud Computing: Issues and Challenges, Advanced Information Networking and Applications (AINA), IEEE International Conference on, pp.27-33, 20-23 April 2010

[2] http://oauth.net/core/1.0/

[3] http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-i-overview/

[4] http://art.tools.ietf.org/html/rfc5849

[5] Jeong-Kyung Moon, Jin-Mook Kim, Hwang-Rae Kim, Hwa-Young Jeong, Easy and Secure Authentication Method using PMI, Applied Mechanics and Materials Vol. 281, pp 86-89, 2013

[6] Jin Li, Design and Implementation for universal Privilege Management Infrastructure, Applied Mechanics and Materials Vols. 241-244, pp. 3125-3129, 2010

[7] Sang Ting, A Log Based Approach to Make Digital Forensics Easier on Cloud Computing, Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on , pp.91-94, 16-18 Jan. 2013

[8] Anton Joha, Marijn Janessen, Design Choices Underlying the Software as a Service (SaaS) Business Model from the User Perspective: Exploring the Fourth Wave of Outsourcing, Journal of Universal Computer Science, vol. 18, no. 11, 2012

[9] George Lawton, Developing Software Online with Platform-as-a-Service Technology, Computer, June 2008

[10] Jia Fu; Junchao Wang; Lu Jing; Chen Zhenghong; Mingqiong He, Research on Meteorology Indices Forecasting Framework based on Hybrid Cloud Computing Platforms, Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering Vol. 214, pp. 727-735, 2013

[11] Deqing Zoua, Wenrong Zhanga, Weizhong Qiang, Guofu Xiang, Laurence Tianruo Yang, Hai Jin, Kan Hua, Design and implementation of a trusted monitoring framework for cloud platforms, Future Generation Computer Systems, Available online 23, January 2013

[12] P. Syverson, P. van Oorschot, On Unifying Some Cryptographic Protocol Logics, inProc. of the IEEE Symposium on Research in Security and Privacy, pp.12-28, 1994

Authors

Jeong-Kyung Moon, received the MS degree in Electronic Commerce from Dankook University in 2006. And she received the PhD. Candidate in Computer science from College of Engineering / Kongju National University in 2012. She is a professor of Contract in Division of Information Technology Education, Sunmoon University currently. She’s research interests includes Cloud Computing, Information security, Network security, and Authentication.

Hwang-Rae Kim, received the BS. And MS. degrees in the Department of computer Engineering from ChungAng University in 1982 and 1991. And he received PhD. Degrees in Department of Computer Engineering from Taejeon University in 2007. He was worked from 1983 to 1994 in ETRI. Currently, he is a professor in the Department of Computer Engineering at KongJu National University, Chungnam, Korea. His research interest includes Network, Security, and Cloud Computing

Jin-Mook Kim, eceived the BS and MS degree in Computer Engineering from Paichai University in 1998 and 2000. And he received the PhD degree in Computer science from Kwangwoon University in 2006. Currently, He is a assistant professor in Division of Information Technology Education, Sunmoon University from 2008. His research interests are in the areas of Network information security, RFID, Sensor network, Cloud Computing and Social network service.