# Decentralized Authentication Method for Accessing Pedagogical Resources in a Cloud Computing based Virtual Organization

Amadou Dahirou Gueye
Department TIC
University Alioune Diop
Bambey, Senegal
dahirou.gueye@uadb.edu.sn

Ibrahima Sanogo
Department Computer Engineering
University Cheikh Anta Diop
Dakar, Senegal
ibrahima124@gmail.com

Samuel Ouya
Department Computer Engineering
University Cheikh Anta Diop
Dakar, Senegal
samuel.ouya@gmail.com

Hamadou Saliah-Hassane
TELUQ
University of Quebec
Montreal, Canada
hamadou.saliah-hassane@teluq.ca

Claude Lishou
Laboratory LTI
University Cheikh Anta Diop
Dakar, Senegal
clishou@ucad.sn

***Abstract*—Today, more and more researchers are advocating the use of Clouds to form a virtual organization. However, the implementation of a cloud based virtual organization presents some security challenges. Generally, in the cloud, the authentication system is centralized. This represents an obstacle and contradicts the principle of virtual organizations, which requires that each member organization of the virtual organization retains control over its own authentication system. The aim of this paper is to address this issue and show the possibility of using clouds in virtual organizations while proposing a decentralized authentication system. For that purpose, we propose to include Shibboleth in clouds to decentralize users' authentication of the virtual organization. The relevance of our approach has been proved through a virtual organization where each member organization has its own Cloud infrastructure to host shared resources. Users will authenticate from their organization to access resources.**

***Keywords-Virtual Organization; Online Laboratory; Cloud Infrastructure;Decentralized authentication; Shared Resources; Shibboleth***

## I. INTRODUCTION

Cloud computing refers to computer services and resources provided on demand through internet [1]-[3]. In other words, it offers, through internet, an easy access, anywhere and on demand, to a number of configurable and shared computer resources, networks, and servers, storages, applications and services. This paradigm is ground breaking in terms of management of universities resources, and will allow for considerable budgetary gains.

Today, universities are increasingly using more cloud to form virtual organization (VO) in order to share resources. The cloud is here the basis for resource sharing virtual organization.

Some studies show the relevance of using clouds in virtual organizations [4]-[6]. Other studies, in addition to showing the utility of clouds in virtual organizations (VOs), deal with the security aspects of such VOs [6].

Our paper is concerned with the issue of authentication arising from such a VO. In general, the authentication system of a cloud system is centralized and ignores inherent authentication methods in each partner organization. This goes against the idea of VOs that promotes heterogeneity

978-1-4799-4437-8/14/$31.00 ©2014 IEEE 03-06 December 2014, Dubai, UAE
**2014 International Conference on Interactive Collaborative Learning (ICL)**

authentication methods allowing each partner to maintain its authentication system and control over its own resources.

So, in this paper, we are offering a decentralized authentication method for the cloud based VO. Since access to the cloud is mainly based on the web, and Shibboleth giving access to web applications, we propose to include Shibboleth in the clouds for solving the problem of managing the decentralized authentication system.

Considering OpenStack as a platform IaaS (Infrastructure as a Service) most used, our solution is, first to outsource authentication keystone, responsible of authentication service of OpenStack. Second, knowing that dashboard offers a friendly and intuitive GUI, we propose a method of shibbolize the dashboard service. This second method has the advantage of not disorient users who use graphical user interface.

This proposition does not reject security policies of partner organizations. It will also allow them to have access to cloud resources while maintaining their own authentication methods.

The paper is outlined as follows: section 2 deals with the state of the arts in the use of clouds in virtual organizations as well as the authentication issue. In section 3, we offer a decentralized authentication model in a cloud based virtual organization. Section 4 shows the use of Shibboleth in decentralized management. The conclusion recapitulates results and opens the door to further discussions.

## II. The use of clouds in Virtual organizations and the authentication issue

The authors in [6] show the need to make several clouds cooperate in one virtual organization for the purpose of putting together the virtual resources. This cloud based virtual organization will have the following features: dynamic, autonomous and distributed. These features bring about new challenges for a secure management of a virtual organization based on several clouds. To provide a solution to the issue, authors in [6] present a framework "CloudVO" which based on security policies and trust management techniques to provide some flexible and dynamic VO management protocols for clouds. This framework takes into account security policies of partner organizations. "CloudVO" adopts proxy and identity mapping policies. This allows the VO to face the challenges in terms of distribution, autonomy and dynamism in cloud environments.

Our paper has the same idea of making several clouds collaborate while dealing with security challenges in the components relating to authentication and access to shared resources. Our solution which consists in using Openstack along with Shibboleth as an interface, allows every partner organization to monitor its own users and authentication systems while complying with the other partners' systems. However, access to resources will be monitored by the host organization which will provide a provisional profile to the user demanding access to resources. This profile will contain the information needed for accessing the resources.

In addition, the authors in [7] deal with the evolution of online labs toward Cloud Computing. The cloud computing SaaS (Software as Service) proposed in [7] provides participants with an environment that allows for network conferencing through the BigBlueButton platform. The platform allows each guest participant to connect and start a collaborative or individual session in the lab. Also referred in [7] the use of clouds to establish a virtual organization but security aspects are not dealt with and authors call for taking care of these issues. In our paper, we demonstrate the need for a partner organization to include its resources in the cloud while proposing a method for accessing these resources.

For a wide and efficient use of the clouds, the authors in [5] propose an open cloud computing federation which covers several heterogeneous cloud computing platforms. They also propose an architecture of mobile agent based on an open federation of cloud computing which aims to ensure portability and interoperability between various clouds platforms. However, the authors have not dealt with the security aspects of such federation. In our paper, we propose a model of decentralized authentication in a federation of clouds around a virtual organization. In our previous work [8] we show the need to include clouds in VOs by proposing two models for facilitating sharing of virtual and physical cloud resources.

## III. Decentralized authentication method

In this model, we first define the concepts of origin organization and partner organization.

The origin organization manages credentials for a user. In our approach, we incorporate the concept of delegation of authentication that is to authenticate the user from its original organization.

The organization member of the VO which holds the resource as demanded by the user is called partner organization or service provider.

An origin organization may be a host organization when it holds the resource demanded. In our approach, we include clouds in VOs. Thus, a member organization wishing to share resources (virtual machines, storage, applications, database, etc.). To allow access to these resources provided within the cloud, we propose a decentralized authentication method that allows all users to authenticate in their origin organization before accessing a shared cloud infrastructure. So, the partner organization will be materialized by a cloud system which accommodates the resource. Figure 1 illustrates the authentication principle of a user that wishes to access resource owned by a VO organization member. The host organization is materialized by the cloud which accommodates the shared resources.

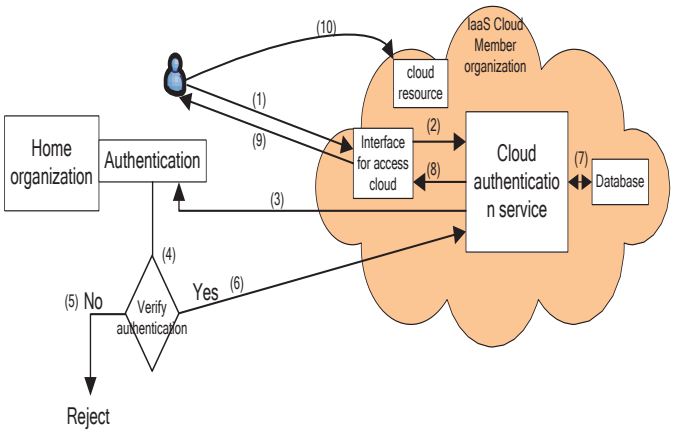


Figure 1. Authentication principle

The main resource here is the IaaS Cloud computing infrastructure. It has the following components: An interface for accessing the cloud, an internal authentication service, and a database containing the identities and attributes of the cloud users.

(1) The user submits a request for accessing a cloud resource held by a member organization. (2) The interface receives the user's request and transmits it to the cloud authentication service. (3) The authentication service gets in touch with the user's origin organization for authentication. (4) The origin organization which holds the users' identification and attributes authenticates the latter. (5) If authentication fails, the request is rejected. (6) If authentication is correct, the origin organization sends to the authentication service evidence for authenticating the user and a few attributes if necessary. (7) The authentication service creates temporary profile for the user with a session key. (8), (9). The authentication service sends to the user the session key. Then the user can pick any resource needed.

## IV. USE OF SHIBBOLETH IN DECENTRALIZED MANAGEMENT

Shibboleth is an Internet2 project designed to implement an open, standards-based protocol for securely transferring user attributes between collaborating sites [9]. It designates both a standard and a product (open source). It is a SAML extension which enriches its functionalities for a federation of entities by facilitating, for a set of partners, the setting up of important functionalities, authentication by proxy and dissemination of attributes.

Shibboleth was designed for the satisfaction of the needs of university teachers. For taking care of the issue of authentication, we include Shibboleth to allow, on the one hand, each member administrator to take care of the identity and authentication of its own users; and on the other hand, to shibbolize the interface of access to the cloud system.

The shibboleth based authentication process, based on the SAML language is illustrated in the works [9]-[11] through figure 2.

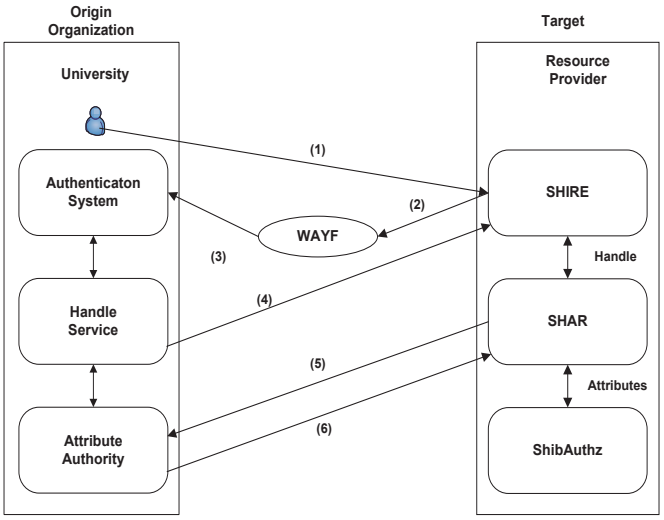


Figure 2. The basic shibboleth authentication process

This paper is partly based on the work of these authors for including shibboleth in the cloud to address the issue of decentralized management. So, we propose a decentralized monitoring model of a cloud based VO. In the model proposed, we consider a VO composed of member organizations (universities, laboratories) which collaborate for sharing virtual resources through their IaaS cloud infrastructure.

A university teacher may connect to an IaaS cloud infrastructure of a partner university to collect virtual resources for themselves or to allow their students to access these resources. For this, we implement a discovery service WAYF to redirect a user to her original organization for authentication.

See figure 3 for such scenario.

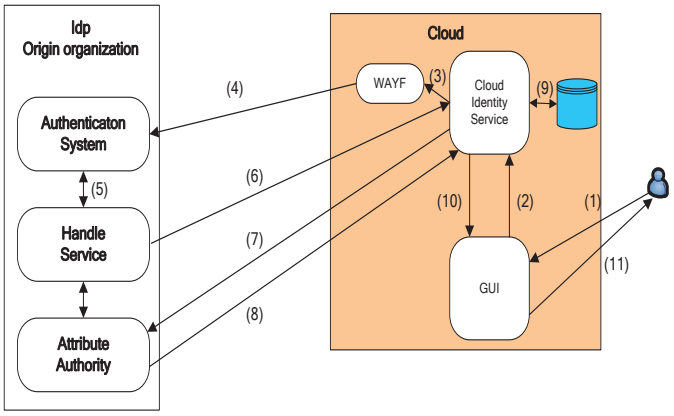


Figure 3. Integration Shibboleth in the Cloud

After showing the importance of integrating shibboleth in the clouds, we propose two methods for decentralized authentication: shibbolize keystone or shibbolize dashboard.

*A. Keystone service*

For setting up the IaaS platform, we chose Openstack. Openstack is an Open Source Project under the Apache label which allows building and administering public and private Clouds. It has a modular architecture with several components (see figure 4). Among these components, we are most concerned with keystone, responsible for authentication and monitoring of Openstack users. Figure 4 shows the relationships between various Openstack services.

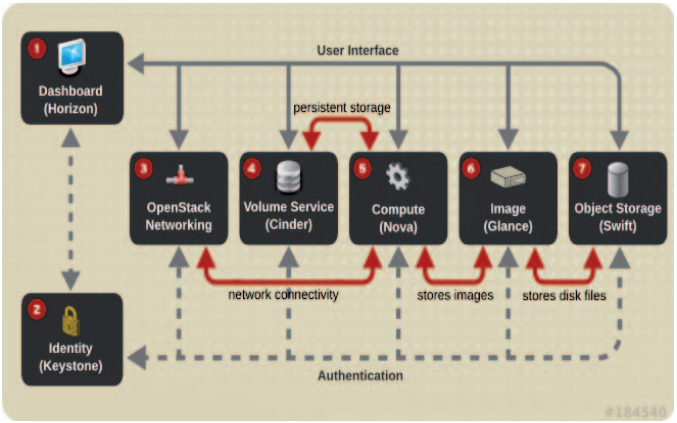


Figure 4. Relationships between various services [12]

The keystone component (Identity) is the identity service used by Openstack for authenticating and authorizing users. Every keystone service is operated by a plugged backend which allows for specific use of the service. Most of those services contain standard backends such as LDAP or SOL. Keystone is not a web application but is embedded by default in a web server called Eventlet.

However, Eventlet takes into account only base authentication systems. Ideally, partner organizations should be able to use their own traditional authentication methods such as Kerberos or public key infrastructure (PKI) for their exchanges with Openstack's keystone. In addition, Eventlet does not contain IPV6 although users need routable IP addresses for cloud based deployments. Consequently, it is recommended to replace Eventlet by an apache server which takes into account the constraints in Eventlet.

*B. Shibbolizing keystone*

To access shared resources in the cloud, external users will auto supplies through the dashboard. But before accessing the dashboard, users must authenticate keystone module, responsible for the management of authentication and authorization. After authentication, the latter grants a token that will be used for subsequent requests to other services (Nova, Neutron, Glance, Cinder, etc.). Before proposing a solution to shibbolise keystone, we are going to describe the keystone authentication process.

*1) Authentication process keystone*

It is important to remember the authentication process keystone that depending on the content of the variable REMOTE_USER offer or not a token for access to services.

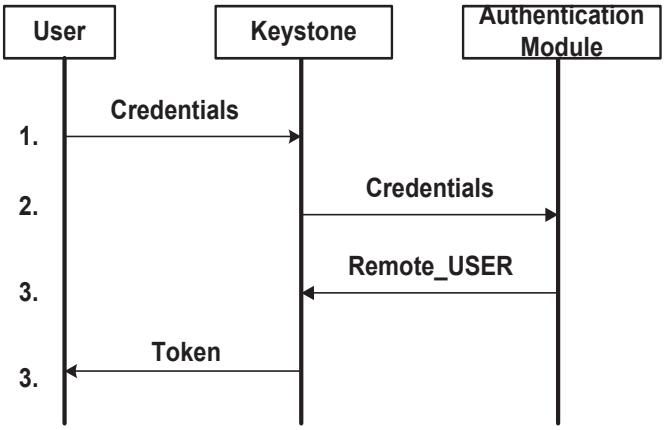


Figure 5. Authentication process keystone

Keystone retrieves the credentials of the user to send the authentication module that can be internal or external to the keystone. The authentication module authenticates the user and sends a keystone REMOTE_USER environment variable. If the variable is set, the authentication is successful except if the content of the variable is empty, the authentication was not successful.

*2) Httpd as an authentication engine*

In this case, the authentication engine is replaced by HTTPD as illustrated in Figure 7.

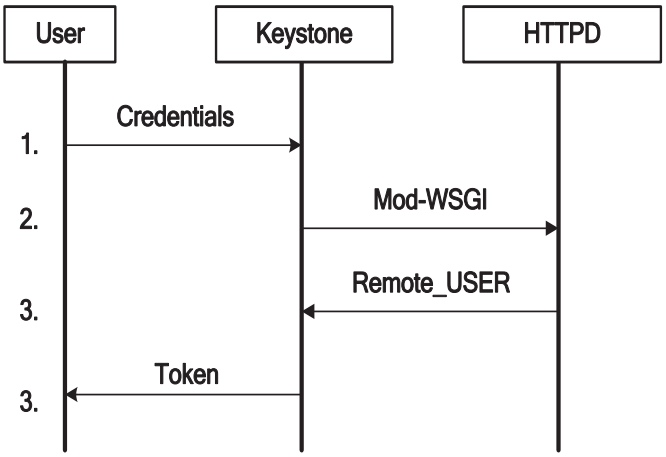


Figure 6. Apache as authentication engine

Keystone SGI incorporates a python module (the service gateway interface) that allows it to communicate with Apache WSGI module for REMOTE_USER variable information. Apache includes several authentication modules allowing him to use any information base as MySQL , LDAP, Kerberos, etc.

*3) Hosting keystone in Apache*

The keystone service manages user authentication in centralized manner, which is a major obstacle in virtual organizations. To manage the problem of centralized authentication, the authors in [13] proposed to integrate shibboleth in OpenStack to establish an identity federation inter-clouds. In our paper we have shibbolised management interface OpenStack by service keystone for each administrator can freely create instances without having to centralize authentication. Thus with shibbolisation of keystone, it becomes a keystone SP (Service Provider) integrating WAYF module to allow any user to choose the original organization for authentication. After authenticating a user of the virtual organization from its original organization, Keystone will be able to accept the external authentication system and create in its local database project for this user (for a first attempt).

For this, we propose to outsource authentication of keystone by integrating keystone in apache. A virtual site is created with apache as shibboleth authentication method. The user enters the URL of the virtual site. The latter incorporating WAYF redirects its original IDP for authentication. If authentication is successful, the REMOTE_USER variable will be informed by the IDP. Keystone accepts external authentication and assign a token to the user for access to resources.

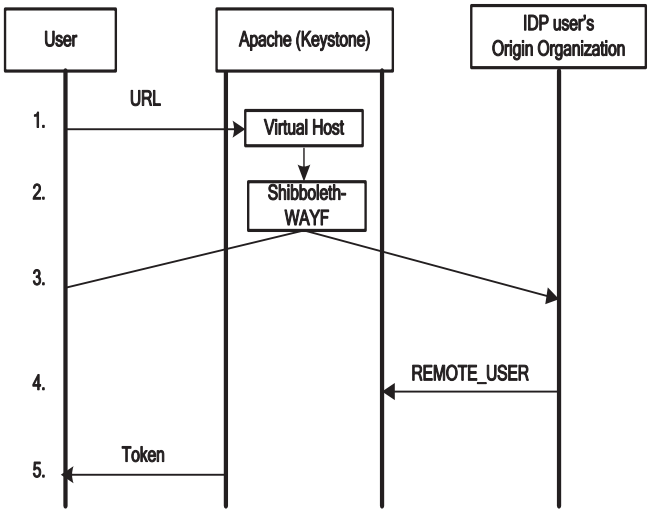


Figure 7. Hosting keystone in Apache

*C. Shibbolizing Dashboard*

The new API v3 allows keystone to receive shibboleth attributes and map with its own attributes [14]. This possibility has led us to use Apache as a front end of the dashboard. We used the shibboleth authentication module *apache lib-apache2-shib2* to redirect a user to the IDP. Once authenticated, the shibboleth attributes received are redirected via apache mod-WSGI module to Dashboard that runs Django [15], which is a Python web framework. The process is illustrated through the figure 8

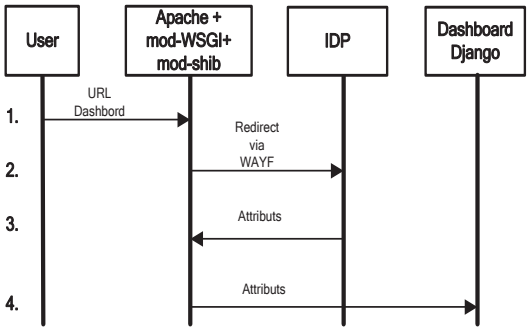


Figure 8. Shibbilize dashboard (1)

After the authentication phase shown in figure above, with version 3 of the OpenStack API, keystone receives shibbo attributes and maps them to its own attributes, which allows keystone assign a token to user via dashboard.

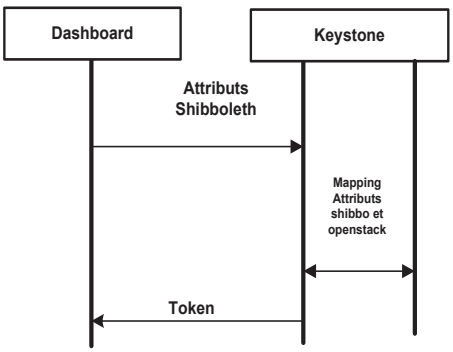


Figure 9. Shibbolize dashboard (2)

## V. ILLUSTRATION DASHBOARD

The following steps have allowed shibbolization dashboard.

Step1: Install shibb on the machine hosting apache
Step2: Configure Shibboleth
Step 3: Configure the apache server as SP

Here is an extract of the configuration file of apache that is hosted on Ubuntu 12.04.

**/etc/apache2/conf.d/shib.conf**

**<Location /secure>**
**AuthType shibboleth**

**ShibRequestSetting requireSession 1**
**require validuser**
**</Location>**

**<Location /dashboardshib>**
**AuthType shibboleth**
**ShibRequestSetting requireSession 1**
**require validuser**
**</Location>**

Etape 4: Configuring communication apache and dashboard via mod-WSGI

**/etc/apache2/conf.d/openstackdashboard.conf**

**WSGIScriptAlias /dashboardshib/usr/share/openstackdashboard/openstack_dashboard/wsgi/django.wsgi.**

To illustrate the principle of decentralized authentication, we set up our own federation of shibboleth identities with its components: Identity provider (IdP), service provider (SP) and WAYF service. The federation will put together the Senegalese public universities. So to test the functioning of our various shibboleth blocs, we tested the access to cloud interface by a VO user.
Step 1: The user will select a web navigator and type the dashboard URL: https:/servpro.sn/uvscloud/dashboard.
Step 2: A discovery service (WAYF) is displayed for the user to choose a linking body corresponding to the IdP in charge of the user authentication.

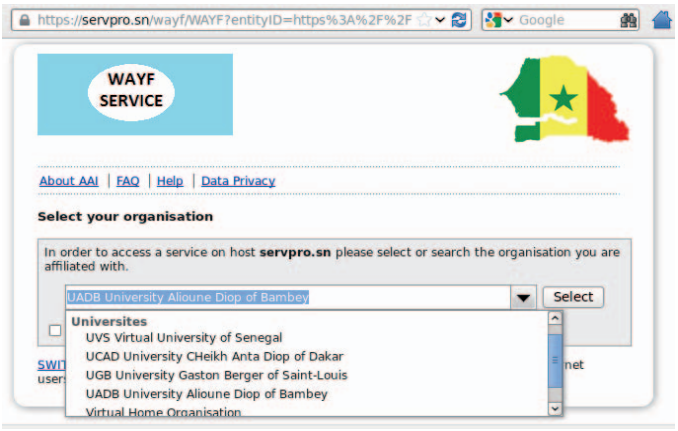


Figure 10. WAYF Service

The user selects his origin organization from the list.
Step 3: Once the selection made, which corresponds to the identity provider (IdP), the user is redirected to the authentication page provided by the IdP.
In our test the user (dahirou) fills in his connection parameters in the form.


Figure 11. Origin organization authentication

When authentication is validated the user accesses to dashboard which provides users a self-service portal to provision their own resources (e.g., networks, servers, storage, applications and services).

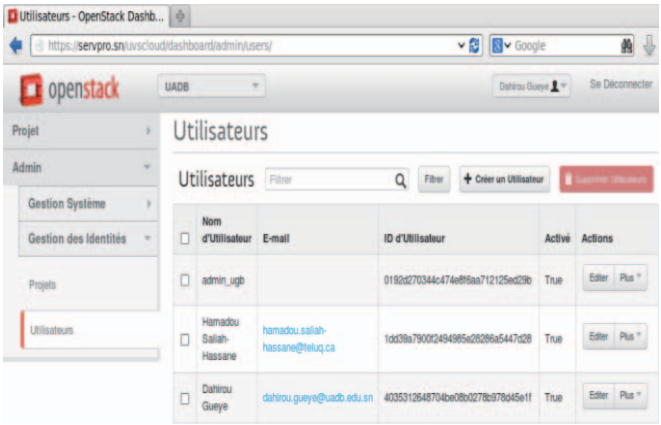


Figure 12. Access to interface dashboard

## VI. CONCLUSION

The paper first studied the relevance of clouds use in virtual organizations. Then, it raised the issue of the authentication of a cloud system used as resource for the VO and for taking care of the issue of authentication.

Based on the fact that cloud platforms are web-based and shibboleth is a product of identity federation based on the web, we propose to integrate shibboleth in OpenStack. To manage the problem of decentralized authentication in OpenStack, two methods have been proposed: shibbolize keystone or shibbolize dashboard. To shibbolize keystone, we hosted it in apache. This solution will allow users to manipulate resources from the command line or via the GUI. To shibbolize dashboard, apache is set with the front dashboard. This will

allow users to self service via the dashboard interface. Both solutions take into account the inherent authentication systems partner organizations while allowing the cloud to accept authentication methods from these organizations.

This will allow each VO manager, on his/her own, to create and manage virtual machines without having to resort to centralized authentication.

## REFERENCES


[1] K. Keahey, M. Tsugawa, A. Matsunaga, and J. Fortes, "Sky Computing," IEEE Internet Computing, vol. 13, pp. 43-51, 2009.

[2] Marinescu, Dan C. "Cloud Computing- Theory and Practice, " Elsevier Sciences & Technology Books, ISBN: 978-0-12-404627-6, 2013.

[3] Sosinsky, Barrie "Cloud Computing Bible," Published by Wiley Publishing, inc., ISBN: 978-0-470-90356-8, 2011.

[4] Razvan I. Dinita, George Wilson, Adrian Winckles, Marcian Cirstea, Aled Jones, " A Cloud-based Virtual Computing Laboratory for Teaching Computer Networks," 978-1-4673-1653-8/12, IEEE, 2012.

[5] [D] Zehua Zhang, Xuejie Zhang, "Realization of open Cloud Computing Federation Based on Mobile Agent," 978-1-4244-4738-1/09, IEEE, 2009.

[6] Jianxin Li, Bo Li, Zongxia Du, Linlin Meng, "CloudVO: Building a Secure Virtual Organization for Multiple Clouds Collaboration," 978-0-7695-4088-7/10, IEEE Computer Society, 2010.

[7] H. Saliah-Hassane, M. Saad, W. Ofosu, K. Djibo, H. Alzouma Mayaki, M. M. Dodo Amadou, "Lab@Home: Remote Laboratory Evolution in the Cloud Computing Era," Proceedings of the 118th ASEE Annual Conference, Vancouver, BC Canada, June 26-29, 2011.

[8] Gueye Amadou Dahirou, Sanogo Ibrahima, Ouya Samuel, Saliah-Hassane Hamadou, Lishou Claude, "Proposal for a Cloud Computing solution and application in a pedagogical virtual organization," 2014 Joint International Conference on Engineering Education & International Conference on Information Technology (ICEE/ICIT), Riga, Latvia, June 2-6, 2014.

[9] The Shibboleth Consortium. (2013) Shibboleth. [Online]. http://shibboleth.net

[10] Wang Ying, "Research on Multi-Level Security of Shibboleth Authentication on Mechanism," 978-0-7695-4261-4/10, Third International Symposium on Information Processing, IEEE Computer Society, 2010.

[11] Abdelmalek Benzekri, "Virtual organization security policy: specification and deployment, " VIVACE Consortium Members, 2006.

[12] https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux_OpenStack_Platform/2/html-single/Getting_Started_Guide/images/184540-OpenStack_services.png

[13] David W. Chadwick, Kristy Siu, Craig Lee, Yann Fouillat, Damien Germonville, "Adding Federated Identity Management to OpenStack, " J Grid Computing, DOI 10.1007/s10723-013-9283-2, 2014.

[14] http://people.redhat.com/tcameron/OpenStack_Meetup_21_May_2014/OpenStack_Meetup_21_May_2014.pdf

[15] https://pypi.python.org/pypi/django-dash