Indian J.Sci.Res. 17(2): 489-491, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

AUTHENTICATION OF OPEN STACK – USING BIOMETRIC

[1] G. Raja Ramesh, [2] K.Vigneswara Reddy, [3] A.Ravi Kumar, [4]V.Vinod Reddy
[1,2,3,4] Department.of I.T, Sree nidhi Institute of Science & Technology, Hyderabad

Abstract- In the present world everyone is using many computer applications; from multi-national companies to a common man everyone is making use of the applications-such as to store their data in the electronic formats. In this context the Cloud Computing is the latest technology which makes the users to interact with the servers to store or retrieve data with in a fraction of seconds. Apart from data storage, Cloud Computing gives many other services like PAAS, SAAS and IAAS. With all these Cloud Computing gives a high infrastructure with low cost to all the users. As we just need not to buy the costly software or hardware, we just need to pay for using their services. Apart from so many advantages many people still think to use this Cloud Computing due to its security. As data is ever sensitive and important so it should be more secure. But still in Cloud Computing we are using the traditional "user name" and "password" for authentication, so to enhance this we came up with using Biometric with "fingerprint identification using biometrics". So we purpose a new platform using OpenStack architecture, where authentication is done by the biometric server instead of traditional "user name and password".

Keywords : Cloud Computing, OpenStack, Authentication, biometric

I. Introduction

Cloud computing is a computing paradigm, where a large pool of systems are connected in networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.

There are three service models in cloud computing namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Infrastructure as a Service (IaaS): is a form of delivering the Virtualized computing resources on demand over the cloud catering to the customer needs of compute, storage, network, etc.

Platform as a Service (PaaS): is a form of delivering a set of development tools and services as platform to simplify the development and deployment of applications over the cloud.

Software as a Service (SaaS): is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over internet on demand based on the subscription agreements.

The Deployment models of Cloud Computing, includes following models:

Private Clouds: Private clouds are solely owned and operated by single or group of organizations and made available to intended users.

Public Clouds: Public clouds are intended for all users and operated by single or group of organizations.

Hybrid Clouds: Hybrid clouds are combination of both private and public clouds.

In cloud computing, the end-users need not know the details of a specific technology while hosting their application, as the service is completely managed by the cloud service provider (CSP). Users can consume services at a rate that is set by their particular needs. This on-demand service can be provided any time. CSP takes care of all the necessary complex operations on behalf of the user. It provides the complete system which allocates the required resources for execution of user applications and management of the entire system flow. There are many benefits of cloud computing, Cost optimization among them is the frontrunner, since you pay as you go. The other benefits are increased mobility, ease of use, portability of application, etc. This means users can access information anywhere easily.

There are many open source cloud computing frameworks namely OpenStack, Eucalyptus, OpenNebula, etc to implement private clouds. Among them OpenStack is more feature rich and widely accepted and supported by the Industry.

The main aim of the paper is to discuss about current authentication and authorization of the OpenStack and to improve the security in authentication. As the existing

[1]Corresponding Author

system has tradition authentication system i.e. with "Username" and "Password" which is not so secure, so in this paper we are implementing authentication using Biometric which is more secure.

II. OpenStack

OPENSTACK is a software community which provides open source cloud computing platforms for both public and private clouds. OpenStack is an Infrastructure As A Service (IAAS) cloud computing project As smart portable devices such as: IPod, IPhone, Android Tablet, etc. are widely used, and the amount of data, especially unstructured data (such as images, audio, video, etc.) is growing sharply, traditional storage technologies are confronted with series of problems, such as high costs, complex operation and maintenance, and limited scalability. Cloud storage technology is gaining more and more attention. Cloud storage is the storage part of cloud computing, and it allows users to store their data and access them anytime anywhere via Internet.

Since its appearance in 2010, OpenStack has quickly become a popular platform for . The project emerged from a unification of the computational capability developed by NASA and the object storage system developed by RackSpace. Now combined, an extended OpenStack platform, comprising five core services is available for Linux under the Apache 2 open-source software license. The figure 1.2.1 shows the architecture of the OpenStack:

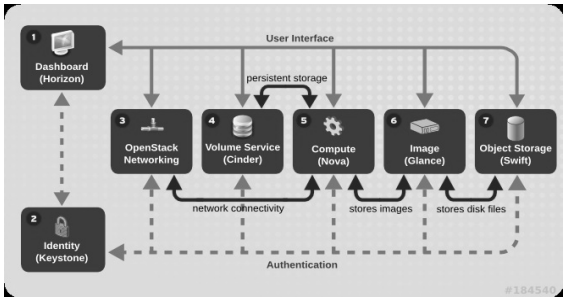


Fig 1.1: Architecture of OpenStack

Nova is a computational service that facilitates the concurrent execution of numerous virtual devices. It provides support for a wide range of hypervisors, such as KVM, QEMU. Keystone is a core identity service that provides token, policy and catalog functions via an API (Rhoton, 2013). The authentication credentials used to access any service must be unique and proprietary to each individual. Swift facilitates the storage and retrieval of files. The machine state of virtualized servers is handled within Cinder and in turn stored as an image file within Glance.

III. Current System:

Keystone is the main component which will take care of security i.e. authentication and authorization of complete OpenStack. First user should login with his/her "username" and "password". If credentials are valid then user will be issued a token. If credentials are invalid then it will show an error message as "invalid username or password". And the token will be stored in the database with user id and session time, the time restrict the user to use the OpenStack services for a specific time only.

Once the user get "Token" whenever he/she need a service such as nova, glance, swift etc. it will verify the database to check whether token is valid are not and also verify the session time. If any one doesn't match then it will through an error. The user can access any OpenStack services with the valid "token" only else it will not give any privileges to access its services. In this way the OpenStack is providing authorization to the user.

The token have complete information about user and creation time and its validity, and to which services are they allowed. It means if user created a token to access nova service, he can only access that particular service and doesn't give any permission to access other services such as glance, cinder and so on.

The token is going to generate by Keystone only, and we call it as scoped token. It's a responsibility of the Keystone to maintain both authentication and authorization. Which current system is doing with simple username and password, which is so week system.

IV. Proposed System

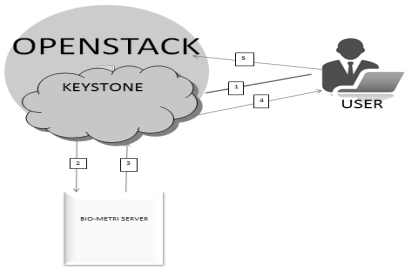
To make OpenStack more secure in this paper we are proposing a Bio Metric authentication system, which is proven as one of the best authentication system, to implement this we need to use a bio metric server, which is done as a third party service.

When a user request for OpenStack service, with username and his/her finger-print, the request should sent to the biometric server and it will do the authentication, if valid then the server will generate a token called "un scoped token", as the token is not generated by the Keystone so we call it as un scoped token. The un scoped token will have information of the user and services for what he registered and created time.

Once the Keystone gets the un scoped token, it will validate the token and will provide a scoped token so that he can access his/her services. And this scoped token will be stored in the database, and un scoped token is only used to create a scoped token.

If the credentials are invalid then the server will not generate any token and will display an error message "invalid credentials"

The following figure shows the biometric authentication process:



The above figure explain the step by step process of how authentication is done with bio metric server:

Step 1

The user will request for the OpenStack service by providing his/her user name and figure-print to the dash board, at dash board we have two options, one is for asking to get authenticate with the traditional "username and password", and the other one with the proposed system, i.e. authentication with the biometric. The user needs to give credentials using the biometric option.

Step 2

Once the keystone get the request for authentication, it will check whether the user used "username and password" or biometric authentication, if it with username and password, it will validate else it will redirect the same details to Biometric servers, where the authentication is done.

Step 3

The server will validate the user request, if the user name and the fingerprint match, then it will generate a "un scoped" token and will give back to keystone. If the credentials are invalid then it will give a "error message" and no token will be generated.

Step 4

The keystone will receive the response from the biometric server, and if it receives an error message, the same will be given to user. And if it receive a un scoped token then it will convert the un scoped token to scoped token with which user is allowed access the services for what he have a privileges.

Step 5

Once the user got authenticated he/she is allowed into the OpenStack Horizon and can able to access the services. If user got error message then user needs to try again with proper username and fingerprint.

In this way we are providing a security to the OpenStack and users can have a more trust on this system.

V. Conclusion:

With the cloud computing many software companies mainly startup companies are able to use a very high infrastructure at very low cost, more over in the present world every individual is using many applications and storing there data in the servers and retrieving them. Many social media also generating a lots of data daily, all this need to be arrange so that whenever user requested his/her data, all the information to be retrieved back. This can be possible only with the help of cloud computing. And for cloud computing security become a big issues, which made so many users to think about using cloud computing.

This paper deals with the authentication of Cloud services with the help of OpenStack, where we are authenticating the user with one the secure system i.e. fingerprint authentication. Now users can trust the OpenStack as we are proposing fingerprint authentication, where user's data can only access by him/her. Others can't even open his account without his knowledge as user need to be present to login into OpenStack

References

[1] OpenStack[online] http://www.OpenStack.org/

[2] OpenStack[online] security guide http://docs.OpenStack.org/security-guide/content/identity.html

[3] OpenStack[online] external authentication http://docs.OpenStack.org/developer/keystone/external-auth.html

[4] Madhan Kumar Srinivasan, K. Sarukesi, Paul Rodrigues,M. Saimanoj, P. Revathy, "State-of-the-art Cloud Computing Security Taxonomies – A classification of security challenges in the present cloud computing environment," ACM, Aug. 2012, pp. 470-476, DOI:10.1145/2345396.2345474.