Security Framework for Cloud Based E-Learning System

Vikas khandelwal[1], S. Magesh[2]

[1]Student, [2]Assistant Professor,
[1]Department of Information Technology, SRM University Chennai, India
[2]Department of Information Technology, SRM University, Chennai, India
[1]vikasguptta002@gmail.com, [2]magesh.s@ktr.srmuniv.ac.in

***Abstract*—Cloud computing provides resource as a service over a network. Due to rapid growth of cloud market need how to evaluate security and performance problems that cloud computing confronts. In this paper we present Kerberos based security model for E-learning infrastructure. In the E-learning framework security and privacy will be needed. For authentication and confidentiality of the E-learning material we will use the Kerberos based authentication model. Problem is that how to connect cloud with the Kerberos based authentication model. At over E-learning infrastructure we discover the following problem (a) forwarding the Kerberos ticket (b) use Kerberos in a cloud infrastructure**

***Index Terms*— Cloud Computing, Authentication Server, Ticket Granting Server, Kerberos, E-learning System**

I. INTRODUCTION

Cloud computing environment is require security techniques due it's contains a numbered of assets such as data, user, technology, transaction.

Cloud computing provides and offer their services according to fundamental models IAAS (Infrastructure as a service) SAAS (Software as a service) PAAS (Platform as a service) where IAAS is the basic module of cloud computing [1].

Cloud computing IAAS Service model providers of IAAS provide physical or virtual machines and other resources. A hypervisor such as VMware runs the virtual machines as guest. IAAS provide resources such as a virtual-machine, raw (block) and file-based storage, firewalls, load balancers, IP addresses. IAAS cloud providers will provide these resources on demand from data center [2].

Cloud security not only focused on data transmission but also the system security and data stored in storage of cloud [].cloud gives you access of data but no way to ensuring the data.

In this paper we present the cloud based E-learning system in that E-learning system the confidently and authentication is required for transmission of data. In the E-learning system we put the E-learning material in data centers. According to the user requirement we will download file from the data center

In this research paper we present a security framework for E-learning system based on MIT Kerberos authentication protocol. The goal of use this to implement user authentication at lowest level (Database).

II. BACKGROUND AND RELATED WORK

In most currently distributed system client authentication mechanism are only till the first level of services. In the first service used to authenticate the server. All forwarding request to background service will be authenticated by the first service identity not on the behalf of user identity. So we have to trust each other completely. Normally service a username and password is required for further service access. User is able to use all the data without authentication. A security framework is proposed for that [3].

Kerberos: Kerberos is a authentication protocol to provide the network wide security services. It is an authentication system to prove user his identity without sending the data. Kerberos is used to solve the problem of mutual authentication between client and server. Main idea behind Kerberos is that to provide the mutual authentication between client and servers. A ticket granting ticket can be received by using a principle name and password. A principle name and key tab file on the server side or a smart key token from server side. The TGT will store the whole information of client/server to authenticate him/herself for using each service.

For that Kerberos support detailed workflow of the authentication mechanism of cloud based E-learning system. Kerberos using the six steps follow for the authentication mechanism.

AS Request: In the AS request we request for a session key and TGT by sending the principle and password or some authentication mechanism.

AS Response: On the bases of the principle name and password response the Session key and TGT.

TGS Request: After getting the ticket granting ticket send the request to TGS for grant the ticket for service.

TGS Response: TGS will response with a Service Ticket for granting access to the server.

Server Request: Client will send the request to the server with the service ticket and encrypted with the session key.

Service Response: service will do validation the service ticket by the help of TGS. And reply to the client with his own identity. For that we will work flow in the fig:1

As according to the OASIS paper we can deploy Kerberos as a service in the cloud. But now in this we use the Kerberos code to be use for the authentication to dynamic virtual machine instance [4].

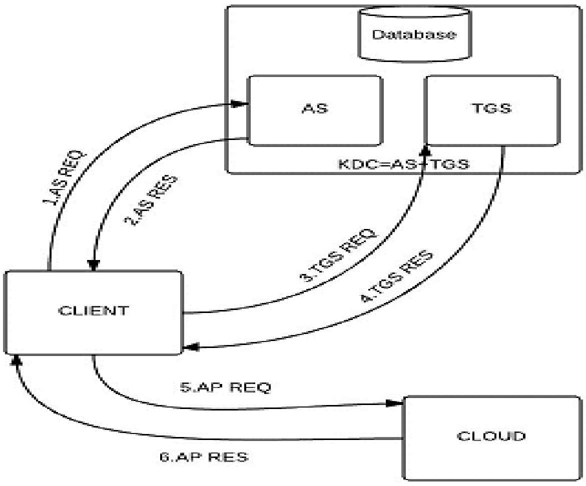

Fig 1 Kerberos Authentication Workflow

III. Concept of e-learning

In cloud based e-learning system based on request response mechanism in that data to be stored in the data centers. And according to request of cloud user with virtual machine instances we will provide the E-learning material that client will request.
In that we have to provide the security on the client and middleware cloud system side using the encrypted request and response.
So that now the security challenge will come in come in the cloud computing based e-learning system. Client will be validated.

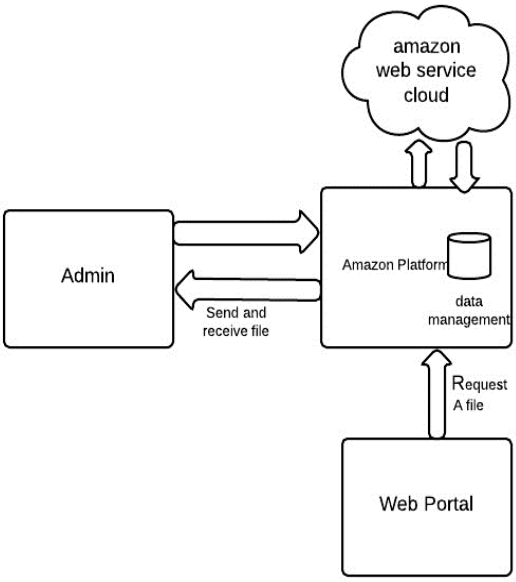

Fig 2 Cloud Based E-learning System

IV. Security concept

Within this section we present the security concept will use for single sign on concept of authentication. Every user will have to need the Kerberos user principle and other attributes.

The principles are managed by using the KDC Kerberos distribution centre. Tomcat application will be used to restrict the server with Kerberos ticket. Each server component needs an appropriate server principal (i.e. the principal has to be registered in the KDC with the DNS name of the server) in order to authenticate with Kerberos. Use client authentication as far as possible:-

To delegate the credentials to another system with Kerberos mechanism exist.
Ticket Delegation before the new service user will request a new TGT at the ticket granting service.TGT will be transmitted after the authentication at the service.
S4U2Self S4U2Proxy: is a Kerberos protocol extension from the Microsoft used to authorize service and receive user credentials without password of user for himself and other services [5].
Normally Kerberos tickets are valid for about one day. This could be a problem, especially with the code execution framework. It is possible that a calculation starts after one day because of other higher priority calculations or the calculation itself needs more

than 1 day to finish. This issue can be solved with either S4U2Self/S4U2Proxy or ticket renewing. The owner of the TGT can renew this ticket until the latest renewable time. When the renew process is started, the TGT must be valid. After that the new ticket is valid for one more day. As previously mentioned the system generated a new TGT that will be delegated to the server. The JAAS library will create the delegated TGT. The problem is that, even if the original TGT is marked renewable, the delegated TGT is not. That is the reason why it is not possible to use this mechanism to extend the ticket lifetime. We decided to increase the default lifetime of ticket to three days to solve this problem.

Each Server needs a server principal corresponding to provide the Kerberos authentication. Amazon will support the elastic IP address but each elastic IP it is not used. Each elastic IP have a cost if it is used or not. For that we will have pool of DNS at the code execution center. These DNS already registered with the principle name at the KDC. And we already generated a SSL certificate signed over test CA should be communicating over VM. To support Kerberos authentication we change the assigned DNS name (from Amazon) with our own Dynamic DNS name to a DNS from our DNS pool. The Dynamic DNS provides a DNS lookup (DNS to IP) and reverse lookup (IP to DNS).

Predefined principals will be assigned to the VM on new VM instance creation. On startup of the instance the VM has to be able to receive the server principal name and password and the SSL certificate for secure communication from the code execution controller

To be able to use the image not contain the fix IP address, DNS name and the information. So we can use image for different VM.

Step 1 the code execution controller starts a new VM-instance and sends his own server DNS name and own CA public key to the starting instance.

Step 2 code execution controller reads the IP address of the new VM instance and assigns a free DNS name of the DNS pool to the IP address and vise verse and VM itself start after the system boots up a java application worker node startup.

Step 3 then store the certificate information into the Kerberos v5 authentication configuration to the file system.

Step 4 Start the secure web service without Kerberos authentication. Then controller verifies that instance running before some minute ago. IP address same as secured one.

Step 5 if everything is ok then SSL send Tomcat private key on the SSL certificate to the VM instance. And Tomcat will be started.

Kerberos authentications and is able to authenticate itself. This workflow is one solution to inject the needed Kerberos credentials on a dynamic system (DNS).

To increase the more security we decided to use more additional features. We will add some more features to it.

On each VM instance startup and shutdown new Kerberos principal will be made. Server principal and password stored in the RAM never stored in the physical disk.

Only cloud security group will able to access the Tomcat HTTPs port from the VM instance.

V. IMPLEMENTATION & OVERVIEW

In the cloud based E-learning project very useful in big university shows in fig 3 how the E-learning system to be implanted. For the SSL certificate CA was deployed. The Kerberos distribution center will be deployed at a server with IP and DNS that is accessible from the intranet. As a local cloud Eucalyptus was deployed. The total code was executed at our security framework. All data transfers between the several different servers (components of the platform), clients, and between multiple platforms are highly secured with state of the art encryption mechanism (using 2048bit RSA keys). All web application required an authentication with Kerberos [6].

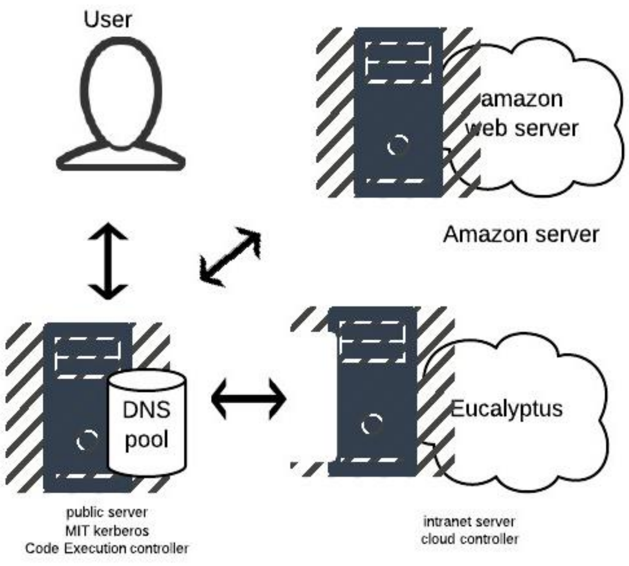

Fig 3 implementation of cloud based e-learning

VI. UNSOLVED PROBLEM

We here in this project we have the problem with the renewing of ticket that here ticket are not to be renewed. In that MIT Kerberos the ticket credential will be for three days. This duration could be a problem for very time-consuming calculations in the code execution framework and therefore it would be helpful if we could find a solution that uses the ticket renewing mechanism that Kerberos provides. Now we will try with the CAS authentication protocol for the purpose of authentication [7].

VII. CONCLUSION

In this paper we will propose Kerberos based security framework for the E-learning system. We will discuss several levels of security challenges through this paper. (a) Use client authentication to all level of system. (b) Secured cloud based analysis of e-learning system. (c) inject security credential into dynamically created VM instances. A problem with the always new instance in the VM and the DNS will be the part of the principal name and registered with KDC.

VIII. REFERENCE

[1] B.Sosinsky, *Cloud Computing Bible*, 1st ed. Wiley Publishing, 2011.
[2] "Kerberos: The Network Authentication Protocol." [Online] Available: http://web.mit.edu/kerberos
[3] "Recommended Practices for Deploying & Using Kerberos
in Mixed Environments." [Online] Available: http://www.kerberos.org/software/mixenvkerberos.pdf
[4] OASIS, "Kerberos cloud use cases," http://www.oasisopen.org/committees/download.php/38245/Kerberos-Cloud-use-cases-11june2010.pdf.
[5] "Exploring S4U Kerberos Extensions in Windows
Server2003."[Online].Available: http://msdn.microsoft.com/enus/ magazine/cc188757.aspx
[6]"JAAS Reference Guide." [Online]
Available:http://docs.oracle.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html
[7] "CAS — Jasig Community." [Online] Available: http://www.jasig.org/cas