Cloud Authentication Using Kerberos

Ms. Moonmoon Karmakar, Ms.Pooja Choudhari ,Ms.Disha Mainani moonmoonkarmakar @gmail.com, choudharypooja196@gmail.com ,disha.mainani@gmail.com
Jhulelal Institute Technology

***Abstract** - Cloud computing is a recently developed technology for complex systems with large-scale services sharing among multiple users. Therefore, authentication and integration of both users and services is a significant issue for the trust and security of the cloud computing. SSL Authentication Protocol (SAP), once applied in cloud computing, will become so complicated that users will undergo a heavily loaded point both in computation and communication.*

This paper, based on private cloud computing, projects the authentication aspect and authoring user as well as providing integrity and high security using a protocol kerberos version 4.

Such applications of our model with great security and scalability is suited to the massive scale private cloud computing.

Keywords-Cloud,kerberos,Encryption,Wamp, phpVirtualBox

I. INTRODUCTION

Modern , systems provide service to multiple users and require the ability to accurately identify the user making a request. The identity of a user is verified by checking a password typed during login in traditional systems; the system records the identity and uses this identity to determine what operations are to be performed. Authentication is the process of verifying the user's identity. It is the verification of the identity of a user who generated some data, and of the integrity of the data. It is the process of identifying an individual, usually based on a password and username. Most of the cloud services do not provide anonymity of the users. Cloud provider can track the users easily, so privacy and

authenticity are two critical aspects of security. A user authentication is needed to use cloud computing services .

II. AUTHENTICATION TECHNIQUES:

1)*Password based authentication*: In this authentication method user’s identity is verified by password typed during login. This method is not suitable for computer networks as password can be used by eavesdroppers.

2)*Assertion based authentication*: Password based authentication is inconvenient as users do not want to enter a password each time they login to access a network service which has led to the use of even weaker authentication technique i.e. authentication by assertion. In this technique application assert the identity of the user and the server believes it. This technique is even weaker than password based as it can be easily thwarted by modifying the application. While most uses of authentication by assertion require that a connection originate from a "trusted" network address, addresses are themselves simply assertions on many networks.

3)*Cryptography based authentication*: When using cryptography based authentication an attacker listening to the network gains no information that would enable it to falsely claim another’s identity. It is a stronger authentication method. The most common example of cryptographic based authentication is **Kerberos.**

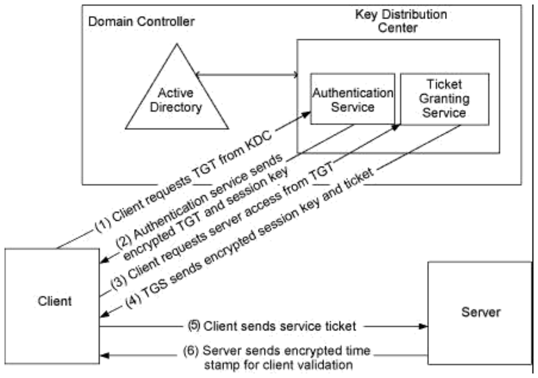
III. PROPOSED SYSTEM:

Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network;to prove their identity to one another in a secure manner.

Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity.

The Kerberos protocol messages are secured against replay attacks and eavesdropping.

Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.
Kerberos uses UDP port 88 by default.


Domain Controller
Key Distribution Center
Active Directory
Authentication Service
Ticket Granting Service
(1) Client requests TGT from KDC
(2) Authentication service sends encrypted TGT and session key
(3) Client requests server access from TGT
(4) TGS sends encrypted session key and ticket
Client
Server
(5) Client sends service ticket
(6) Server sends encrypted time stamp for client validation

The client at every login authenticates itself to the Authentication Server (AS) which forwards the user-id to a Key distribution center (KDC).

The Key distribution center then issues a Ticket Granting Ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the workstation of user.

This is done infrequently, typically at user login; the TGT remains valid until and unless it expires,though may be transparently renewed by the user's session manager while they are logged in to the system.

When the client needs to communicate with another node, the client sends the TGT to the Ticket Granting Service (TGS), which is usually shared by the same host as the KDC. After that verifying the TGT whether it is valid and the user is permitted to access the requested service, the TGS thus issues a Ticket and some session keys, which are then returned to the client.

Then the ticket is sent by the client to the service server (SS) along with its service request. The message of the user ID is sent by client to the AS requesting services on behalf of the user.

The AS then generates secret key by hashing the password of the user found at the database (ex.Active Directory of Windows Server)

The AS checks to see if the client is in its database. If it is available , the AS sends back the following two messages to the client:

Message A:- the Client/TGS Session Key encrypted using the secret key of the client/user.

Message B:-the Ticket-Granting-Ticket (which includes the client ID, client network address, ticket validity period, and the client/TGS session key) encrypted using the secret key of the TGS.

As soon as the client receives messages A and B, it attempts to decrypt message A with the secret key generated from the password entered by the user.

If in case the user entered password does not match the password in the AS database, the client's secret key will be different and thus unable to decrypt message A.

With a valid password and secret key the client decrypts message A to retrieve the Client/TGS Session Key. This is the session key that is used for further communications with the TGS.

When requesting services, the client sends the following two messages to the TGS:

Message C: It is Composed of the TGT from message B and the ID of the requested service.

Message D: Authenticator (which is composed of the client ID and the timestamp), encrypted using the Client/TGS Session Key.

Upon receiving message C and also message D, the TGS retrieves message B out of message C. It then decrypts the message B using the TGS secret key. This gives it the "client/TGS session key".

Using this key, the TGS decrypts message D (Authenticator) and sends the following two messages to the client:

Message E: Client-to-server ticket (which includes the client ID, client network address, validity period and Client/Server Session Key) encrypted using the service's secret key.

Message F: The Server/client Session Key encrypted with the Client/TGS Session Key.

Upon receiving message E and message F from TGS, the client has enough information to authenticate itself to Service Server. The client connects to the SS and sends the following two messages:

Message E from the previous step (the client-to-server ticket, encrypted using service's secret key).

Message G: a new Authenticator, including the client ID, timestamp and is encrypted using Client/Server Session Key. Service Server decrypts ticket using its own secret key to retrieve the Client/Server Session Key. Using the sessions key,

SS then decrypts Authenticator and sends the following message to the client to confirm its true identity and willingness to serve the client.

Message H: timestamp found in client's Authenticator plus 1, encrypted using the Client/Server Session Key.

The client decrypts the confirmation using the Client/Server Session Key and checks whether the timestamp is correctly updated.

If so, then the client can trust the server and can start issuing service requests to the server.The server provides the requested services to the client.

Previously,if the user wanted to use the same application software from different computer system,he had to manually install it over all the system which proved to be a tedious job when the number of system exceeded. For this purpose cloud computing serves best as a solution.

Users in the Cloud Computing environment have to complete the user authentication process required by the service provider whenever they use new Cloud service. Generally a user registers with offering personal information and a service provider provides a user's own ID (identification) . In this paper, we are using a three way security to authenticate the user to access the private cloud thus ensuring high level of security.

If user wants to access all the softwares and applications installed on the server system,the user first has to register his system to the server and then the user logs in to the system.The user can access the softwares and application thereafter from the service server by using the registered user system using his browser.

The tools that are needed is as follow :

Oracle VM box : Oracle VM VirtualBox is a virtualization software package. **PhpVirtualBox** is an open source, AJAX implementation of the **VirtualBox** user interface written in **PHP**. As a modern web interface, it allows you to access and control remote VirtualBox instances. **WAMP** refers to a software stack consisting of the operating system Microsoft Windows, the Apache web server, The MySQL database and one of PHP, Perl or Python programming languages. Also Mysql is used for connecting the database

IV. CONCLUSION:

In this paper, cloud authentication using Kerberos, was proposed and the features of this proposal are as follows: Three level security wall is used for authenticating the valid user. User has to go through those levels of authentication to login and access the cloud. So, user authentication using Protocol Kerberos, authenticates the user securely maintaining high integrity.

REFERENCES

http://en.m.wikipedia.org/wiki/Kerberos_(protocol)

http://en.m.wikipedia.org/wiki/Cloud_computing

http://en.m.wikipedia.org/wiki/Cloud_computing_security

Hyosik Ahn,Hyokyun Chang, Changbok Jang, Euiin Choi*,"User Authentication Platform using Provisioning in Cloud Computing Environment",Dept. Of Computer Engineering, Hannam University, Daejeon, Korea

[2]Kevin Hamlen, The University of Texas at Dallas, USA Murat Kantarcioglu, The University of Texas at Dallas, USA,Latifur Khan, The University of Texas at Dallas, USA,Bhavani Thuraisingham, The University of Texas at Dallas, USA, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39 -51, April-June 2010

[3]B.Clifford Neuman and Theodore Ts'o,"Keberos:An authentication service for computer networks",IEEE Communication Magazine september 1994

[4]V.Krishna Reddy,Dr.L.S.S. Reddy,"Security Architecture of Cloud Computing",International Journal of Engineering Science and Technology (IJEST)