International Journal of Emerging Trends in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 3, Issue 2 (March-April 2016), PP.81-84

Activation of Kerberos on Cloud

Prof. Mrs. Nikita Hatwar[1] ,Anuja Dhakite[2], Komal Tadse[3]
[123]*(Department of Information Technology, Priyadarshini College of Engineering, Nagpur/RTMNU, India)*

Abstract: - Kerberos is an authentication protocol which provides security to cloud. Today's world is so much dependent on Internet. Without internet the world would stop. We upload, we download and share ‘n’ number of things, but it is not safe. This project is a system that can be incorporated in any site or social media network as everything today has a cloud to support it. We focus to verify and validate i.e., authenticate an user who wants and wills to make use and get served by a cloud or any site that makes use of cloud for storage and different services. As we live on this planet, it is our duty that we protect it and save it from getting extinct, so that the future generation doesn’t face any kind of undesired and unsolved disaster. Thus, mixing both the concepts we have tried to make software that saves paper, time, and also conducts examination. Security and authentication will be based on secret key technology where every host on the network has its own secret key. The software deals with different aspects of java that helps us in designing an interface so friendly and understanding for user.

Keywords: - Cloud, Kerberos, Key Distribution Center, Ticket Granting Server, Ticket

I. INTRODUCTION

A Cloud is an independent mass storage accessible over the internet. It is the database which also provides processing end to any electronic computing device. It gives rapid resource flexibility. As cloud computing is a great help and vital source to manage and store data, it creates new and challenging security threats just before user outsourced data.

Assume a cloud data storage service has three different entities, a cloud user, who desires to store huge data files in the cloud; a third-party, which has information and facility to keep record of the data stored and which have faith to access the cloud storage service consistency on behalf of the user request, and a cloud server, which is handled by the cloud service provider and provide data storage service. The dominant problem with cloud computation is its access control mechanism for ensuring security information and overall system security. For controlling an assortment of time-sensitive actions frequent cloud utilities such as workflow management and the operations with real-time databases, the characteristics of access control are needed so as to be improved with the most favorable and efficient temporal conditions. In this paper work and the developed system, the system optimization has been aggravated by the prerequisite of a decidedly vigorous and efficient access control scheme that could congregate and can assuage the protection concerns in cloud environment with enhanced trust intensity for abundant cloud based applications and numerous service segments.

Kerberos is a commonly used authentication service on the Internet. Developed at the MIT's Project Athena, Kerberos is named for the three-headed dog who, according to Greek mythology, guards the entrance of Hades (rather than the exit, for some reason!).Kerberos, an authentication protocol works on the ticket granting mechanism and the authenticator. In this paper we propose an authentication model for cloud based on the Kerberos v5 protocol to provide single sign-in and to prevent against different attacks in the access control system of the cloud and benefit by filtering against unauthorized access to the cloud server and to reduce the burden, computation and memory usage of cloud against authentication checks for each client. It acts as a trust third party between cloud servers and clients to allow secure access to cloud services.

II. PROBLEM STATEMENT

In enterprise systems, a pressing issue is the lack of an efficient, generic application-level model that supports unified access control frameworks for client-to system interactions. Traditional security models are not capable of addressing some of the new challenges posed by modern enterprise systems. One of the problems is that most of the existing security models are influenced by the subject operation object paradigm. A typical feature of the paradigm is that permissions are forwarded in state of the accessible permission to certain participants or beneficiary in particular access modes. Such kinds of type of permission representation have made the security management of enterprise systems more complicated because of the heterogeneous characteristics of the resources being available in authentication. Therefore, they are not appropriate for sustaining an integrated access control architecture that takes into consideration of diverse resources from numerous domains

Traditional security models are not capable of addressing some of the new challenges posed by modern enterprise systems. One of the problems is that most of the existing security models are influenced by the subject operation object paradigm. A typical feature of the paradigm is that permissions are forwarded in state of the accessible permission to certain participants or beneficiary in particular access modes. Such kinds of type of permission representation have made the security management of enterprise systems more complicated because of the heterogeneous characteristics of the resources being available in authentication.

In a cloud, a variety of security policies are specified to ensure data confidentiality and integrity. A security system is required to provide more precise authorization services to satisfy both authentication and security requirements of the cloud.

III. ALGORITHMS AND KEY GENERATION

This system incorporates an encryption technique and an algorithm namely Caesar Cipher and Advanced Encryption Standard. Both the keys are generated dynamically by the particular which is encrypting a message or a request.

The total number of characters present in the string which is the result of concatenation of the username and password of the client who is logging in. Thus, the key for Caesar cipher is generated. The key generation for the encryption of the plain text is generated by generating a random number.

The keys after encryption are concatenated in the sequence of their encryption and send for the further processing of request to use the cloud services.

IV. WORKING

Kerberos employs the client/server architecture and provides user-to-server authentication than host-to-host authentication. In this system, security and authentication will be based on secret key technology where every host on the network generates a key for the next user to decrypt the cipher text. It would really be unmanageable if each host had to know the keys of all other hosts so a trusted, secure host somewhere on the network, known as a Key Distribution Center (KDC), is established which knows the keys for all of the hosts (or at least some hosts within a particular area of the network, called as a realm). In this way, when a new node is brought online, only the KDC and the new node need to be configured with the node's key. The exchange of key is done through the same media

In Kerberos protocol we are using total two servers: Key Distribution center and ticket granting server along with Cloud.

User, Client— By user, we mean a human being who uses a program or service. A client also uses something. A client may be person or computer program.

Key, Private Key, Password—Kerberos uses private key encryption. Each Kerberos principal is assigned a large number, its private key, known only to that principal and Kerberos. In the case of a user, the private key is the result of a one-way function applied to the user's password. We use key as shorthand for private key.

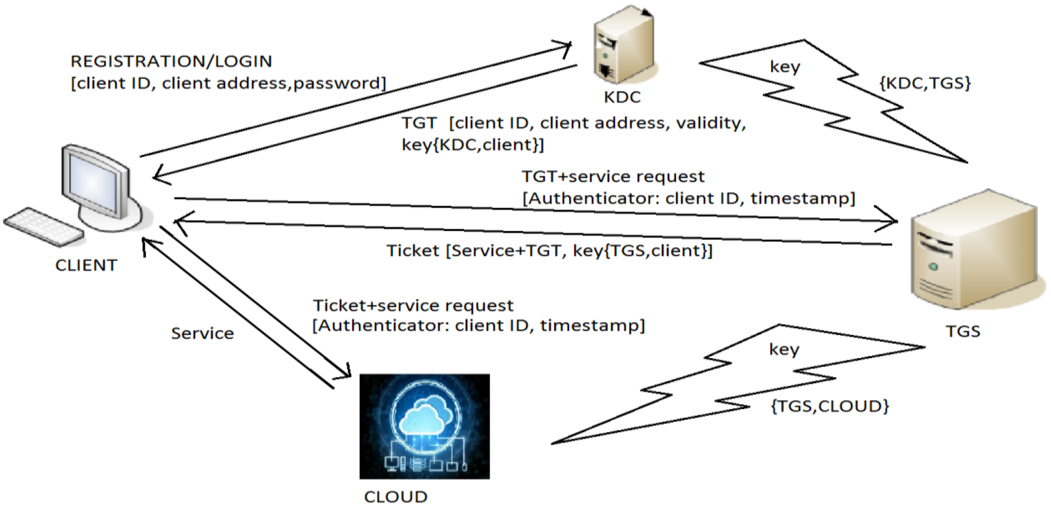
Realms—A network that uses Kerberos, composed of one or more servers called KDCs and a potentially large number of clients. In other words Realms is a user-defined administrative boundary.

Key Distribution Center (KDC)—KDC is the heart of the Kerberos realm. It provides Kerberos authentication services by issuing encrypted tickets that require secret keys to decode. KDC handles the distribution of keys and tickets

Ticket Granting Server (TGS)— TGS issues service tickets to clients upon request.

Ticket Granting Ticket(TGT)— Issued by the Authentication Server (A.S.), the TGT is encrypted in the user's password which is known only to the user and KDC.

Authenticator— Authenticator is used along with the ticket to prove that the client presenting a ticket is really the one it claims to be.


REGISTRATION/LOGIN
[client ID, client address,password]
KDC
key
{KDC,TGS}
TGT [client ID, client address, validity, key{KDC,client}]
TGT+service request
[Authenticator: client ID, timestamp]
Ticket [Service+TGT, key{TGS,client}]
CLIENT
TGS
Ticket+service request
[Authenticator: client ID, timestamp]
Service
key
{TGS,CLOUD}
CLOUD

V. CONCLUSION

Security in the present scenario has become a more rational issue either it may be in the REAL WORLD or in the CYBER WORLD. In real world as opposed to the cyber world an attack is often preceded by information gathering. In the cyber world the ―Opponents are referred to as intruders, eavesdroppers, hackers, hijacker etc. Adding Kerberos to a network can increase the overall security available to the users and administrators of that network. Remote sessions can be securely authenticated and encrypted Kerberos is a verification protocol that gives the security for system. Kerberos provides distributed authentication service that allows a process running on behalf of a principal to prove its identity to verifiers without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal.

REFERENCES

[1] S.V. Baghel , D.P. Theng "A Survey for Secure Communication of Cloud Third Party Authentication" 2 nd international conference on electronics and communication system (ICECS 2015) pp 51.53

[2] Subash .C. Patel , R S Singh , S. Jaiswal "Secure and Privacy Enchanced Authentication Framework for Cloud Computing " International Conference on electronics and communication system (ICES 2015)

[3] Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transaction onParallel and Distributed System, vol. 22, no. 5, pp. 847 – 859,2011.

[4] Gourkhede , M.H ; Theng, D.P, " Analysing Security and Privacy Management for Cloud Computing Environment " Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on ,vol .,pp 677,680,7-9 April 2014

[5] C .Wang , Sherman S.M. Chow, Q. Wang, K .Ren and W. Lou, "Privacy – Preserving Public Auditing for secure cloud storage", IEEE Transaction on computer 1, vol .62, no.2, pp 362-375, February 2013

[6] Gourkhede , M.H; Theng , D.P., " Preserving Privacy and Illegal Content Distribution for Cloud Environment ," International Journal of Computing and Technology (IJCT), 2014,vol., no1 , issue 3, pp.142,148, may 2014

[7] A.Mohta, Lalit Kumar Awasti,]"Cloud Data Security while using Third Party Auditor", InternationalJournal of Scientific & Engineering Research, Volume 3,Issue 6, ISSN 2229-8 June 2012.