ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

COMPARATIVE ANALYSIS OF VARIOUS AUTHENTICATION TECHNIQUES IN CLOUD COMPUTING

Shabnam Sharma[1], Usha Mittal[2]

Dept. of CSE, Lovely Professional University, Phagwara,Punjab, India[1,2]

Abstract: Over the recent years, there is a great advancement in the field of Computer Science. Cloud Computing is the result of advancement in the existing technologies. It shares the characteristics with Autonomic Computing, Client-Server Model, Grid Computing, Mainframe Computer, Utility Computing, Peer-to-Peer and Cloud Gaming. Cloud Computing is beneficial not only for users but also for large and small organizations. Security issues are the major concern in Cloud Computing. In this paper, our focus is on the authentication techniques used for verifying the client identity to the Cloud Broker.

Keywords: Kerberos, Key Distribution Centre, Public Key Infrastructure

I. INTRODUCTION

Cloud Computing is the pool where large number of different types of resources are kept together, not physically at one place, but in such a manner, that it seems to the cloud user[1].The advantage of this computing is that the cloud user can access the resources whenever required and on pay-per-use basis. Components of Cloud Computing [2] is categorised into five categories, as described in figure.

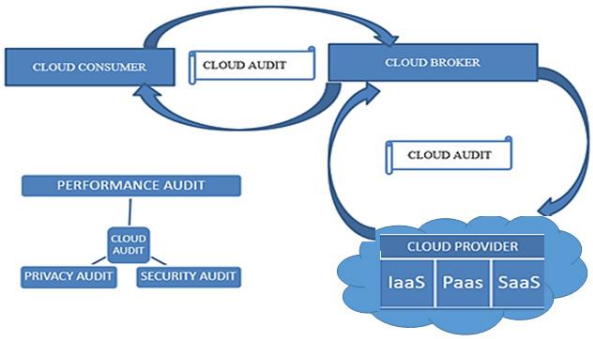

Fig 1: Cloud Computing Architecture

TABLE 1

CLOUD COMPUTING ARCHITECTURE COMPONENTS

Cloud Consumer	It can be a person or organization who wants to use service from Cloud Providers.
Cloud Provider	A person or organization who provides the services to the users.
Cloud Auditor	A party who has to verify whether cloud provider is providing the services to user according to the service level agreement or not.
Cloud Broker	It is the intermediate between cloud provider and the user.
Cloud Carrier	It is the transport media by which services are routed to intended user.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

A. Services[4]

- PaaS- In this type of service, Platform is provided to the cloud consumer as a service. For example-Operating System
- IaaS- In this type of service, infrastructure is provided to the cloud consumer as a service. For example-Storage area, server physical equipments.
- Saas- In this type of service, Software is provided to the cloud consumer as a service. For example-Microsoft Word, Notepad, Paint, or many other applications.

B. Deployment of Cloud

Deployment of cloud can be done in following ways-
*1). Public Cloud:*It means that cloud is implemented at the cloud provider site and any user can access the services from this cloud provider.
*2). Private cloud:*On-site- It means that cloud is implemented at the cloud customer site and only those users are allowed to access these services who belong to same organization as that of cloud customer.
Off-site- It means that cloud is implemented at the cloud provider site and only those users are allowed to access these services who belong to same organization as that of cloud customer.
3). Community cloud: On-site- It means that cloud is implemented at the cloud customer site and only those users are allowed to access these services who belong to same organization as that of cloud customer. Here cloud customer can be two or more organizations.

Off-site- It means that cloud is implemented at the cloud customer site and only those users are allowed to access these services who belong to same organization as that of cloud customer. Here cloud customer can be two or more organizations.
*4). Hybrid cloud:*It is the mixture of any of the above given deployments.

C. Barrier to cloud computing

- Privacy and Security
- Performance and Reliability
- Portability and Interoperability
- Data breach through fibre optical network

II. AUTHENTICATION TECHNIQUES

In this paper, we focus on the security issues of Cloud Computing, particularly on authentication techniques.[3],[5] Authentication can be done in various ways:

- Authentication using Kerberos.
- Authentication using Key Distribution Centre.
- Authentication using Public Key Infrastructure.

A. Authentication using Kerberos[7]

Kerberos is the authentication technique which is used to authenticate the clients to the server in Client-Server architecture. Cloud Computing can also be viewed as distributed Client-Server architecture, where Cloud Provider is the Server and Cloud User is the Client., which communicates by the intermediater , named as Cloud Broker. It has two main components- Ticket Granting Server and Authentication Server.

(1) C→ AS: $ID_C||P_C||ID_V$

(2) AS→ C Ticket

(3) C →V: $ID_C||$Ticket

Ticket = $E(K_v, [ID_C||AD_C||ID_V])$

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

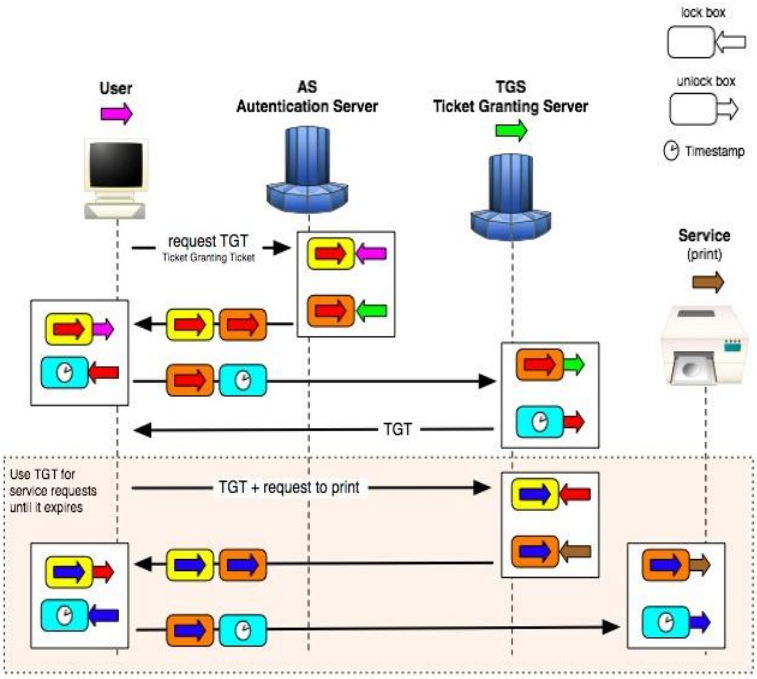

Fig 2. Kerberos

Where

C=Client
AS=Authentication Server
V=Server
ID_C=Identifier of user on C
ID_V=Identifier of Server
P_C=Password of user on C.
AD_C= Network Address of C
K_V= Secret Encryption key shared by AS and V

B. Authentication using Key Distribution Centre

A issues a request to the KDC for a session key to protect a logical connection to B. The message includes the identity of A and B and a unique identifier, N_1, for this transaction, which we refer to as a **nonce** The nonce may be a timestamp, a counter, or a random number; the minimum requirement is that it differs with each request. Also, to prevent masquerade, it should be difficult for an opponent to guess the nonce. Thus, a random number is a good choice for a nonce.

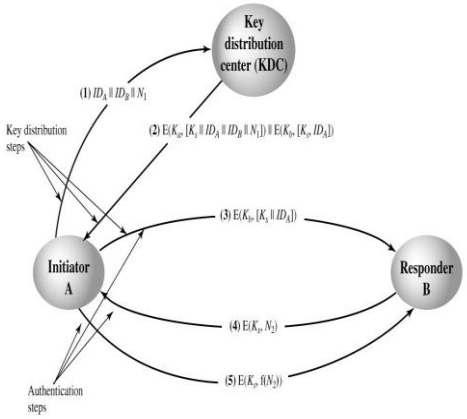

Fig 3. Key Distribution Centre

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

The KDC responds with a message encrypted using K_a Thus, A is the only one who can successfully read the message, and A knows that it originated at the KDC. The message includes two items intended for A:

- The one-time session key, K_s, to be used for the session.
- The original request message, including the nonce, to enable A to match this response with the appropriate request

Thus, A can verify that its original request was not altered before reception by the KDC and, because of the nonce, that this is not a replay of some previous request.

In addition, the message includes two items intended for B:

- The one-time session key, K_s to be used for the session
- An identifier of A (e.g., its network address), ID_A

These last two items are encrypted with K_b (the master key that the KDC shares with B). They are to be sent to B to establish the connection and prove A's identity.

A stores the session key for use in the upcoming session and forwards to B the information that originated at the KDC for B, namely, $E(K_b, [K_s \| ID_A])$. Because this information is encrypted with K_b, it is protected from eavesdropping. B now knows the session key (K_s), knows that the other party is A (from ID_A), and knows that the information originated at the KDC (because it is encrypted using K_b).

At this point, a session key has been securely delivered to A and B, and they may begin their protected exchange. However, two additional steps are desirable:

- Using the newly minted session key for encryption, B sends a nonce, N_2, to A.
- Also using K_s, A responds with $f(N_2)$, where f is a function that performs some transformation on N_2 (e.g., adding one).

C. Authentication using Public Key Infrastructure[8]

The components of PKI are listed below:

- End entity: A generic term used to denote end users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public key certificate. End entities typically consume and/or support PKI-related services.
- Certification authority (CA): The issuer of certificates and (usually) certificate revocation lists (CRLs). It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.
- Registration authority (RA): An optional component that can assume a number of administrative functions from the CA. The RA is often associated with the End Entity registration process, but can assist in a number of other areas as well.
- CRL issuer: An optional component that a CA can delegate to publish CRLs.
- Repository: A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.

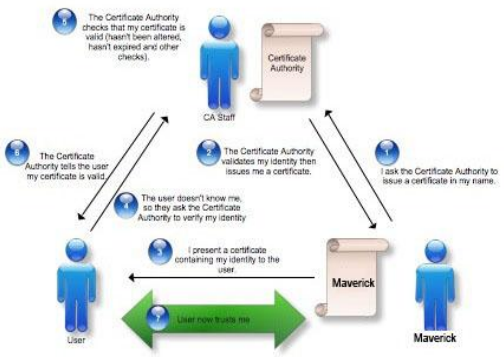

Fig 4. Public Key Infrastructure

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

III. CONCLUSION [6]

Authentication can be implemented in different types of Clouds, which can provide different types of Services, as described in following table:

TABLE 2:

IDENTIFICATION AND AUTHENTICATION

Type of Service				
		IaaS	SaaS	PaaS
Type of Cloud Deployment	Public	Yes	Yes	No
	Private	Yes	Yes	No
	Hybrid	No	Yes	No

REFERENCES

[1] http://www.uscert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf
[2] NIST SP 500-292 "Cloud Computing Reference Architecture: An Overview" publication by National Institute of Standards and Technology.
[3] "Cloud Computing Security Threats and Responses" Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference by Sabahi, F.
[4] "Cloud Computing-Concepts, Architecture and Challenges" by yashpalsinh Jadeja and Kirit Modi in Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference.
[5] "Cloud Computing: Issues and Challenges"; Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on Digital Object Identifier: 10.1109/AINA.2010.187 Publication Year: 2010, Page(s): 27 – 33 by Dillon Tharam, Wu Chen, Chang Elizabeth.
[6] "The Management of Security in Cloud Computing" in Information Security for South Africa (ISSA), 2010 by Eloff MM, Smith E
[7] "Kerberos using public key cryptography" by Farhana S. Munnee, Anirudh Jonnavitula in GMU-ECE 646 Fall 2007
[8] A comparison between traditional Public Key Infrastructures and Identity-Based Cryptography by Kenneth G. Paterson Geraint Price.
[9] Improvements on Conventional PKI Wisdom by Carl Ellison.