International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

SINGLE SIGN-ON AUTHENTICATION FOR MULTIPLE CLOUDS IN CLOUD COMPUTING

[1]Pushpendra Singh, [2]Nitin Rathod
[1]Research Scholar, Indore Institute of Science and Technology, Indore, M.P, India
[2]Assistant Professor, Indore Institute of Science and Technology, Indore, M.P, India
Department of Computer Science & Engineering.
[1]pusp1991@gmail.com

ABSTRACT:

The information and data security concerns still need to network security and confidentiality fully addressed. Cloud allows customers to avoid hardware and software, flexibility, and investment cooperation with others, and to take advantage of sophisticated services. However, security is a big problem, especially for cloud customers Access control; Subscriber management and access profiles Services provided by public cloud environments. In this article Cloud model are proposing a certification Kerberos V5 protocol to provide single sign-on and to prevent DDOS attacks against the access control system. This filtering model can benefit against unauthorized access and the calculation load and memory usage to reduce each client authentication check against the clouds. It acts as trust between cloud servers and to allow third parties to customers secure access to cloud services. In this paper, we will discuss some of the work related to cloud security access control Issues and attacks then we will discuss the proposed architecture.
Keywords: Cloud computing security, Data security, Open Key Framework (PKI), Kerberos as an administration, Administration Level Assertion (SLA).

1. INTRODUCTION

Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture, as shown in fig.. The services offered through cloud computing usually include IT services referred as to SaaS (Software-as-a-Service) which is shown on top of the stack. SaaS allows users to run applications remotely from the cloud[1][2].

Infrastructure-as-a-Service (IaaS) refers to computing resources as a service. This includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access.The data-Storage-as-a-service (dSaaS) provides storage that the consumer is used including bandwidth requirements for the storage.

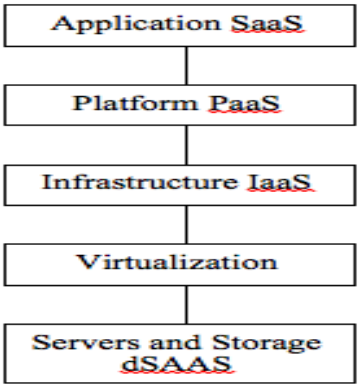

Figure1. Layered architecture of cloud computing

An example of platform-as-aService (Paas) cloud computing is shown in fig. the PaaS provides integrated development environment (IDE) including data security[3], backup and recovery, application hosting and scalable architecture.

.

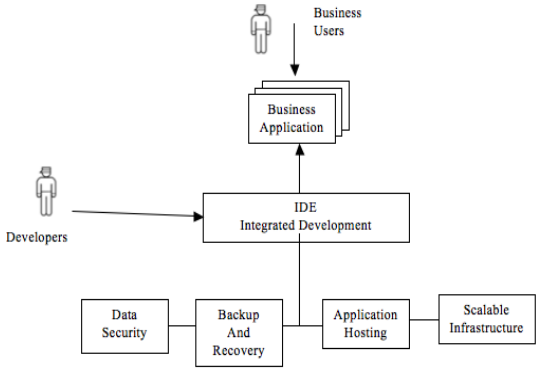

Figure 2. The concept of Platform-as-a-Service.

Figure 2 illustrates another types of cloud service, where the application runs on the client; however it accesses useful function and services provided in the cloud. An example of this type of cloud services on the desktop is apple's iTunes[4][5].

.

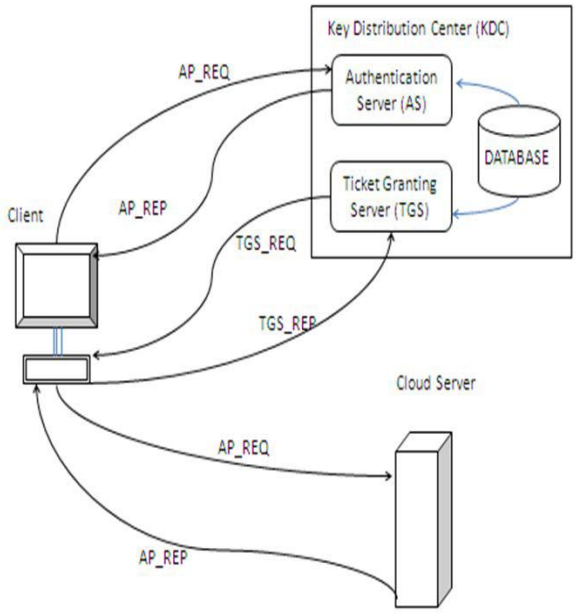

Figure 3. Kerberos authentication System

2. RELATED WORK

This is matter of fact that in any research activity the exploration and deep study of existing approaches plays a significant role, therefore consideration this factor in mind the author of this thesis has performed a deep rooted survey for the role based access control mechanism

and specially the access control approaches to be employed for cloud environment [4]. The study made on existing systems provides the well-defined and crisp knowledge about the strength as well as the weakness of the existing approaches and thus the new optimum system can be built. The literature survey conducted for role based access control and its allied processes has been given in this section, as follows:

Lan Zhou et al [6] addressed trusted administration and enforcement of role-based access control policies on data stored in the cloud. Role-based access control (RBAC) simplifies the management of access control policies by creating two mappings; roles to permissions and clients to roles. Recently crypto-based RBAC (C-RBAC) schemes have been developed which combine cryptographic techniques and access control to secured data in an outsourced environment [7]. In such schemes, data is encrypted before outsourcing it and the cipher text data is stored in the untrusted cloud. Those clients who satisfy the role-based access control policies can only decrypt this cipher text. However such schemes assume the existence of a trusted administrator managing all the clients and roles in the system. Such an assumption is not realistic in large-scale systems as it is impractical for a single administrator to manage the entire system.

Though administrative models for RBAC systems have been proposed decentralize the administration tasks associated with the roles, these administrative models cannot be used in the C RBAC schemes, as the administrative policies cannot be enforced in an untrusted distributed cloud environment.

In this paper, the researchers proposed a trusted administrative model ADC-RBAC to manage and enforce role-based access policies for C-RBAC schemes in large-scale cloud systems. The ADC-RBAC model uses cryptographic techniques to ensure that the administrative tasks such as client, permission and role management are performed only by authorized administrative roles. Their proposed model uses role based encryption techniques to ensure that only administrators who have the permissions to manage a role can add/revoke clients to/from the role and owner- can verify that a role is created by qualified administrators before giving out their data. We show how the proposed model can be used in an untrusted cloud while guaranteeing its security using cryptographic and trusted access control enforcement techniques [8][9].

3. EXISTING SYSTEM:

The major problem with cloud computing to ensure the security of your access control system Information and overall system security. To control an assortment of time-sensitive tasks constantly cloudy and utilities such as workflow management Real-time database, the operating characteristics[3], So as to access control needs to be improved with the friendly and efficient temporary reduction. In the structure of the paper work and develop systems System optimization has been growing vigorous and efficient use of a certain condition control plan that can collect and remove Security concerns in the cloud environment abundant faith intensity extended to cloud-based applications and service segments.
Kerberos authentication protocol tickets authenticator. This leads to a discussion of two authentication Protocol: An initial certification Kerberos client (in the suit), and a potential consumer and a mutual authentication protocol for a potential manufacturer of network service. In this paper we propose an authentication model Kerberos v5 protocol to provide cloud-based Single sign-on and to prevent against DDOS attacks Access control system and the benefits by filtering against unauthorized access and to reduce the burden, against the

cloud computing and memory usage authentication checks for each client[10][11]. It serves as a trust between cloud servers and to allow third parties to customers secure access to cloud services.

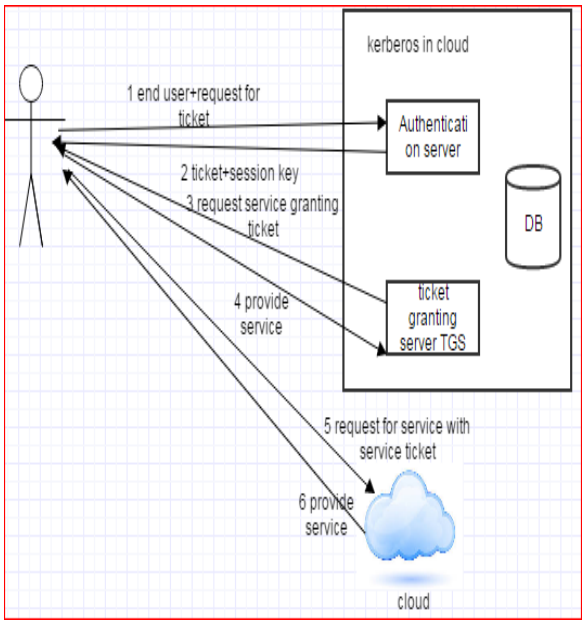

Figure 4. Kerberos in existing system

4. PROPOSED SYSTEM

The main Aim of this model is for the authentication clients before access to the service and to find the source of the attack DDOS. Check your client name and password just is not enough for the cloud computing environment, such as distributed and shared. Kerberos is a network authentication protocol and provides a single sign-on facility to clients as well. Kerberos was one of the first single sign-on solutions proposed in the literature and implemented as a network service. It is formally described as a network authentication system, initially designed for providing single sign-on to network services.

A Kerberos "realm" infrastructure is composed by an Authentication Server, a Ticket Granting Server and a set of service providers. The Authentication Server is responsible for verifying the user's identity while the Ticket Granting Server generates tickets for authenticated users.

A) AS Exchange: to obtain TGT 1. AS_REQ – {cloud customer name, expiration time, tgs cloud service name, ...} 2. AS_REP – {$S_{A, KDC,}$ expiration time, tgs cloud service name ...}. K_A + {$S_{A, KDC,}$ expiration time, cloud customer name ...}. K_{KDC}.
(B) Ticket Granting Sever Exchange: to obtain Server Granting Ticket 3. TGS_REQ – {timestamp, checksum ...}. $S_{A, KDC}$ + { $S_{A,KDC,}$ expiration time , cloud

e-ISSN: 2394-8299
p-ISSN: 2394-8280

customer name, ...}. $K_{KDC.}$ + cloud service name + expiration time 4. TGS_REP – {$S_{A,B}$, cloud service name, expiration time, ...}.$S_{A, KDC}$ + {$S_{A, B}$,cloud customer name, expiration time,...}. K_B
(C) Customer/Server Authentication Exchange: to obtain Cloud Service 5. CS_REQ – {timestamp, checksum ...}.$S_{A,B}$ + {$S_{A,B}$, cloud customer name, expiration time, ...}. K_B 6. CS_REP – {timestamp}.$S_{A,B}$

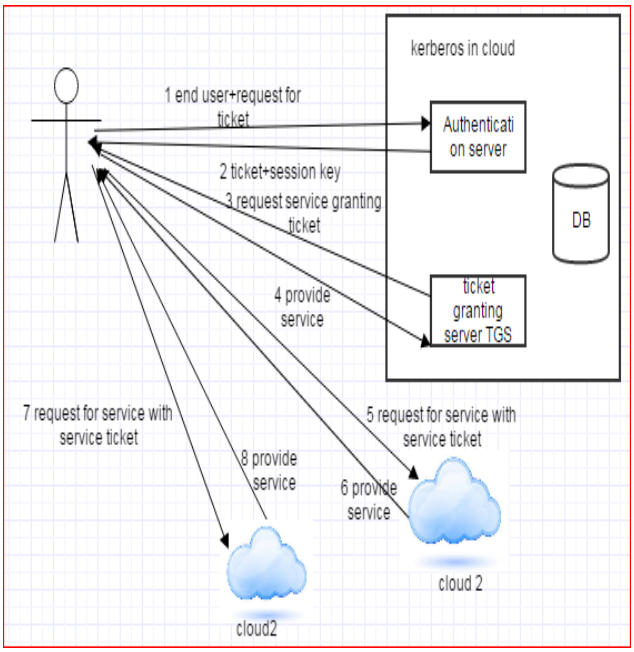

Figure 5. Kerberos system using multiple clouds

The service providers are simply networked servers that authenticated users are allowed to access. The two servers act together as an identity provider, handing the user an authentication ticket that he can use to sign-on to the relying service providers. In fact, the sign-on process in Kerberos is extremely complex, requiring several interactions between the user and the servers (which can be combined into an identity provider). Although it provides a nice practical single Sign-on solution, Kerberos infrastructure management is extremely complex, being prone to several mistakes that may severely compromise security. Both the identity provider (composed by the Kerberos servers) and all the service providers must be tightly time synchronized.

These rules out the utilization of Kerberos as a single sign-on framework for distributed applications that may reside in the internet or the cloud. Furthermore, Kerberos relies solely on unproven symmetric encryption mechanisms to authenticate users and maintain session state. It may also be possible to impersonate users and steal authentication tickets through simple network based attacks.

We will implement proposed System using openshift cloud. With help of openshift we create public cloud.in our project we will used following tools

- Openshift cloud
- JBoss
- MYSQL
- PhpmyAdmin

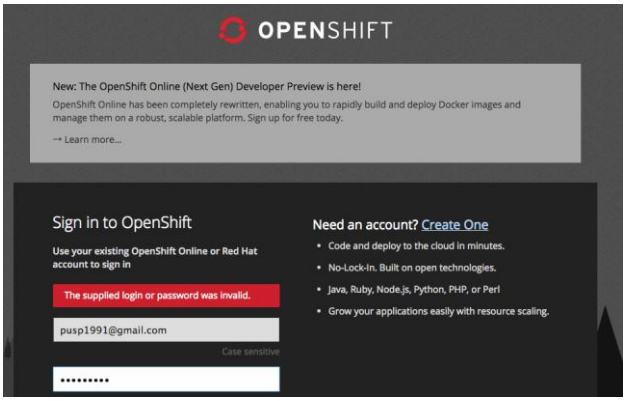

Figure 6. Openshift cloud Dashboard

5.CONCLUSION

In this paper we have drawn Kerberos with role-based access control authentication we also introduced the framework for cloud applications access control security, the problem affecting cloud environment, which essentially is easier for customers according to their own safety to protect resources and access control requirements. As proposed specification module provides a policy framework for Cloud customers to define their resource access control RBAC policy format using the Kerberos authorization server component stores and generates RBAC access control decisions based on the policy file Also we are a certification framework to provide cloud-based Kerberos V5 protocol Single sign-on and to prevent against DDOS attacks Access control system. Although floating profit against unauthorized access and to reduce the burden, against the cloud computing and memory usage authentication checks for each client. It serves as a trust between cloud servers and to allow third parties to customers secure access to cloud services.

REFERENCES

[1]. Yaser Fuad Al-Dubai & Dr. Khamitkar S. D, "Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control", Global Journals Inc. 2014.

[2].YaserFuad Al-Dubai and Dr. Khamitkar S.D, "A PROPOSED MODEL FOR DATA STORAGE SECURITY IN CLOUDCOMPUTING USING KERBEROS AUTHENTICATION SERVICE", ISSN 0976 – 6367(Print) ISSN 0976 – 6375(Online) Volume 4, Issue 6, November - December (2013), pp. 62-69.

[3]. ANIESH KRISHNA K, BALAGOPALAN A S, "AUTHENTICATION MODEL FOR CLOUD COMPUTING USINGSINGLE SIGN-ON", Proceedings of 10th IRF International Conference, 04th October-2014, Bengaluru, India, ISBN: 978-93-84209-56-8.

[4]. Raja Shree S., "Secure Substantiation in Cloud Computing Environment", International Journal of Modern Engineering Research (IJMER) 2014.

[5]. Abhishek P, Mayank Kumar, **"**A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module **",**Volume 3, Issue 4, April 2013.

[6]. Mehdi Hojabri, "Ensuring data storage security in cloud computing with effect of Kerberos", International Journal of Engineering Research & Technology (IJERT) 2012.

[7]. Y. Shashank Rao, Dr. N. Chandra Sekhar Reddy, **"**Kerberos as a Service in Cloud Computing Security Issues", International Journal of Science and Research (IJSR) 2014.

[8]. Er. Abhijeet, Mr. Praveen Tripathi, Er.Anuja Priyam and Er.Vivek Kumar, "Implementation of Public Key Cryptography in Kerberos with Prevention of Security Attacks", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 248 - 253, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[9]. Sujay Pawar and Prof. Mrs. U. M. Patil, "A Survey on Secured Data Outsourcing in Cloud Computing", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 70 - 76, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[10]. Abhishek Pandey, R.M.Tugnayat and A.K.Tiwari, "Data Security Framework for Cloud Computing Networks", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 1, 2013, pp. 178 - 181, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[11]. A.Madhuri and T.V.Nagaraju, "Reliable Security in Cloud Computing Environment" International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 4, Issue 2, 2013, pp. 23 - 30, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.