ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

Security Layout of Cloud Computing Using RBAC

Ravneet Kaur, Manish Mahajan

M.Tech Student, CEC Landran, Punjab, India

Associate Professor, CEC Landran, Punjab, India

ABSTRACT: Cloud computing data centre is an efficient service provider in terms of infrastructure, software and platform. There are two major types of cloud that is Public and Private cloud. In Private cloud which is formed within the organizations. So in Private cloud data will accessible only by the authorized users and also we provide more level of security inside the organization. In the case of Public Cloud the resources should publically share to all cloud users. So here the issue is security. Although cloud server is secure enough to keep the data with its architecture but still the future cannot be predicted in terms of security. This paper describes the RBAC layout over a cloud computing platform and also this paper focuses on the security threats of the cloud network.

KEYWORDS: Cloud data centre , RBAC model , security threats, DDOS Attack;

I. INTRODUCTION

The Cloud computing is defined in the term of the virtual infrastructure which can provide shared information and communication technology services, via an internet cloud, for "multiple external users" through use of the Internet or "large-scale private networks. Cloud computing provides a user access to Information Technology (IT) services i.e., applications, servers, data storage, without requiring an understanding of the technology or even ownership of the infrastructure.[1]

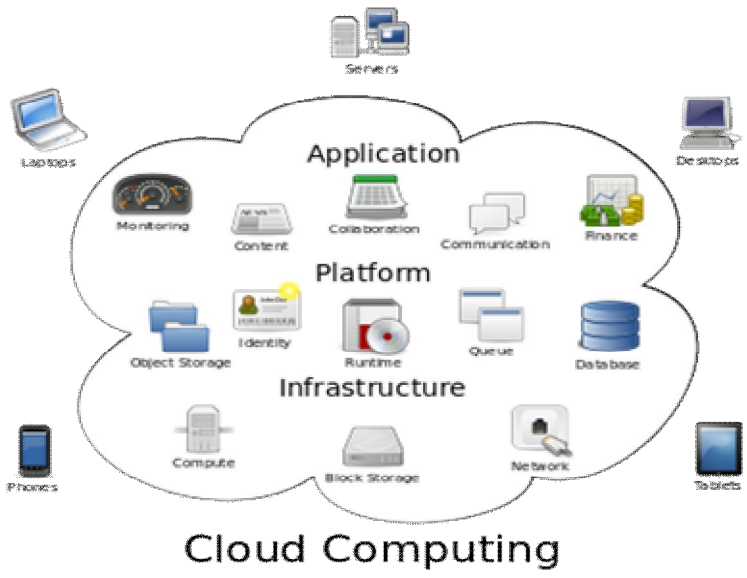

Figure 1: Over view of Cloud Computing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

II. ROLE BASED ACCESS CONTROL APPROACH(RBAC)

Role-based access control (RBAC) is a method of access to computer or network resources based on the roles of individual users within an organisation. Roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles.

Members of staff are assigned particular roles, and through those roles assignments acquire the computer permissions to perform particular functions. Since users are not assigned permission directly, but only acquire them through their role, management of individual user rights becomes a matter of assigning appropriate roles to the user's account, simplifies the common operations, such as adding a user, or changing a user's department.

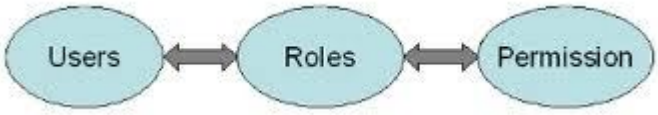

FIG 2: ROLE BASED ACCESS CONTROL

III. CLOUD COMPUTING ARCHITECTURE

3.1 Cloud Computing Deployment and Service Model are defined as:

- Software as a Service - A SAAS provider allows users access to both resources and applications. SAAS also makes it possible to have the same software on all of your devices at once by accessing it on the cloud. [2]
- Platform as a Service - A PAAS system goes a level above the Software as a Service setup. A PAAS provider gives users access to the components that they require to develop and operate applications over the internet. [2]
- Infrastructure as a Service - An IAAS deals primarily with computational infrastructure. In an IAAS agreement, the subscriber completely outsources the storage and resources,[2]

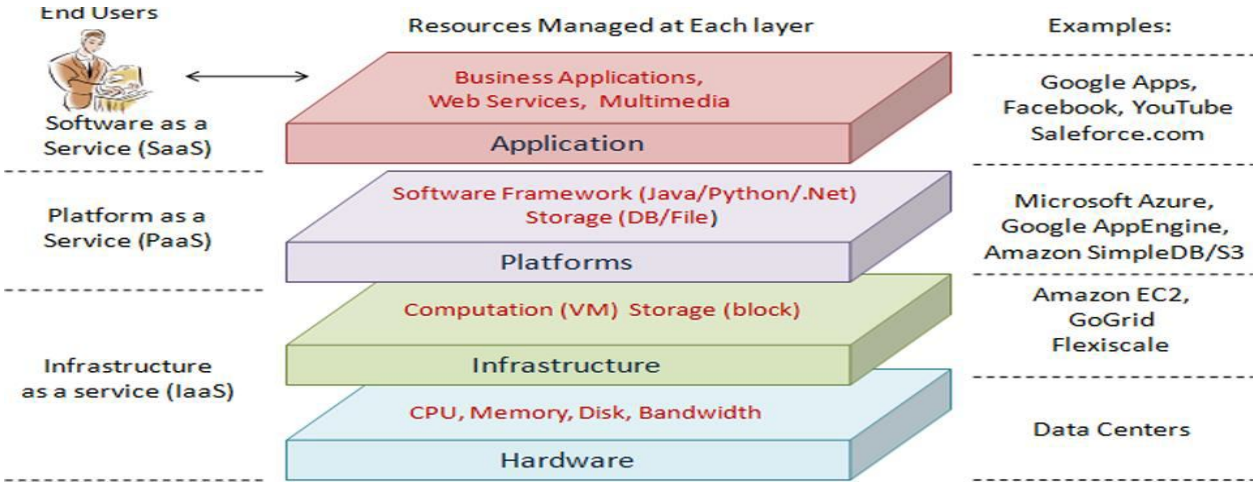

Fig. 3 Cloud Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

3.2 Multi-Tenancy in Cloud

Multitenancy has made cloud computing famous by permitting businesses continue to gain access to data and applications within a cloud environment along with the benefit of reduced costs.[3].In the multi-tenancy model, many user's data and resources are located in the same cloud, and are controlled and differentiated through the use of tagging for the unique identification of resources owned by individual user.

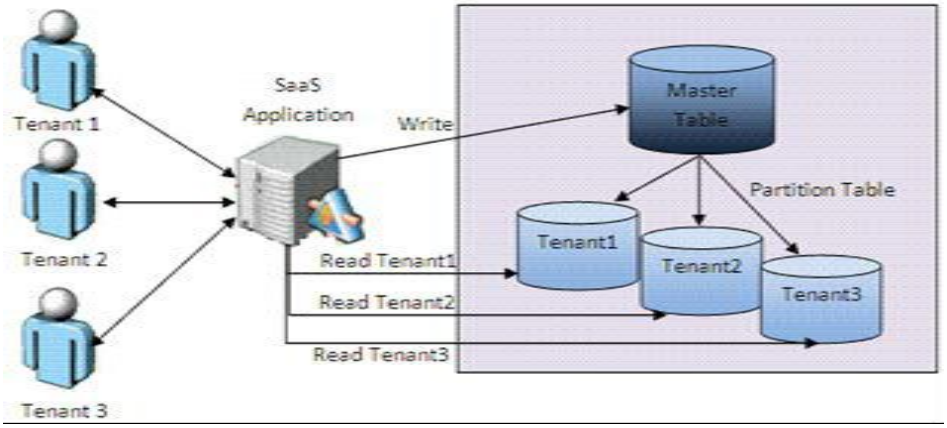

Fig.3.1: Multi-tenancy in Cloud

IV. PROPOSED WORK

Denial of service (DDOS) Attack Overview

A denial-of-service attack is defined as an explicit effort performed by attackers to prevent authorized users of an organisation to access that particular resources for which they are allowed. A distributed denial-of-service focuses multiple machines at the same time. [4]The service is stopped by flooding a large number of requests to a victim that either using some resource, or allows the attacker with unlimited access to the victim machine so he can provide loss to the user.

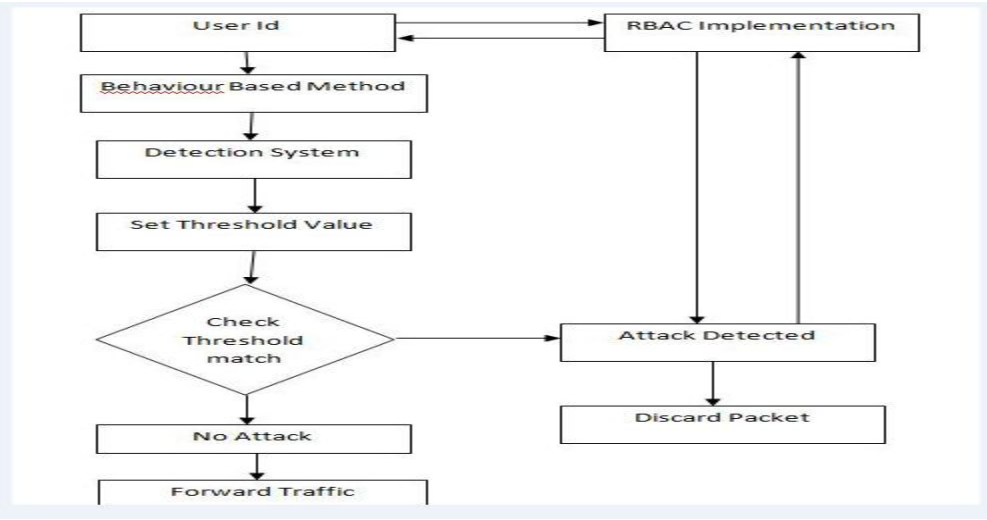

Fig 4: DDOS Attack Detection & Prevention with implementation of RBAC.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

Here we are implement duel mechanism

- User id: it shows that a request comes for process. It helps to communicates with that client.
- It is method that helps to detect the request on the basis of their behavior. It calculates all requests that sent from a client for process on server.[5] The server works on the basis of RBAC mechanism that implemented with the detection and prevention of DDOS attack.
- Now a detection system that store all the request time and manage them during process.
- Now at the server side a threshold set that checks the number of requests from the user and according to that a threshold set for prevent that attack.
- If he requests are continually sent by client at a same time then after some request it checks the threshold that decided. If user crosses the limit that decided then the attack is detected and the client that request will discard from the server. Else it shows normal behavior for the client that send request for processing.

V. CONCLUSION

Distributed Denial of Service (DDOS) attack is a major problem for any kind of server. **A lot of different mechanisms have been already implemented to prevent the DDOS attack such as third party authentication (TPA) was integrated with access control mechanism but there was problem with that mechanism because TPA was outsourced to third party that was result in higher cost and the system was totally relay on third party that effects the reliability of the system .**The proposed method deal with prevention of server from unauthorized access so that the number of request to the server decreases. It also includes one step further point in which if the DDOS attack happens then what are the chances of prevention of our data. For the same purpose, we have an integrated authentication mechanism for which a MAC number would be associated with every data which would be helpful in the identification to check whether the data which has been uploaded before has been changed or not

REFERENCES

[1]. Wei-Tek Tsai, Qihong Shao, "Role Based Access Control Using Reference Ontology in Clouds", IEEE, ISADS Tenth International Symposium on Autonomous Decentralized Systems, pp. 121-128,ISBN 978-1-61284-213-4,March 2011.
[2]. Parminder Singh,"A New Advance Efficient RBAC to Enhance the Security in Cloud Computing",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, ISSN: 2277 128X,JUNE 2013
[3] K.Venkataramana, Prof.M.Padmavathamma, "Multi-Tenant Data Storage Security In Cloud Using Data Partition Encryption Technique", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, ISSN 2229-5518,JULY2013
[4]. U. Goyal, G. Bhatti, and S. Mehmi, "A Dual Mechanism For Defeating DDOS Attacks In Cloud Computing Model", IJAIEM, Volume 2, Issue 3, ISSN 2319 – 4847, March 2013
[5]. A.M. Lonea, D.E. Popescu, H. Tianfield, "Detecting DDOS Attacks In Cloud Computing Environment". International Journal Computing Communication, ISSN 1841-9836 8(1):70-78, February 2013.