IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A New Approach of Multicasting in Cloud Computing

Gaurav Raj[*1], Shabnam Sharma[2]

[*1]Department Computer Science and Engineering, Punjab Technical University, Punjab, India

[2]Department Computer Science and Engineering, Lovely Professional University, Punjab, India

er.gaurav.raj@gmail.com

Abstract

Cloud Computing is the emerging and prominent technology in IT world. Rather than setting up, the infrastructure, platform and services separately for each and every IT industry, are kept collaboratively, which can be accessed by numerous users, in turn reduces the cost of setup and maintenance. Numerous organizations access the services, use the infrastructure and platform from the communal data centre's that may lie beyond the reach of the organization. Accessing the data from these data centre's necessitates secure communication. While adopting the Cloud Computing Environment, security issues are the major concern for IT industries. Moreover, authentication is required to validate the Client to the Service Broker. In this paper, we have proposed Third Party Authentication, which registers the new clients as well as authenticates the already registered clients. This paper also aims to add a new functionality at the end of Service Broker. For Service Management, we proposed Multi Client broadcast Service (MCBS), by which the Service Broker multicasts and schedule the services, in response to the same kind of service requests sent by multiple clients , under the consideration of various parameters, including network delay, bandwidth available and number of hops between client and Service Broker, service request size and cost. MCBS is integrated with service scheduling based on Round Robin, Priority scheduling.

Keywords- CBCCP, NCRP, RCCP, MCBS

Introduction

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

There are three aspects (Vogels, 2008) of the Cloud Computing-

- The resources are available to the user on demand, so the cloud users need not to worry about the provisioning.
- Cloud User can use the resources on pay-per-use basis, irrespective of the time period, even for short term basis like for a day, for few hours.
- There is no need for the commitment from cloud users, regarding their resource consumption. Small Scale industries can start with fewer requirements for hardware and software resources, but can increase the requirement with time.

Services

- 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.

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.

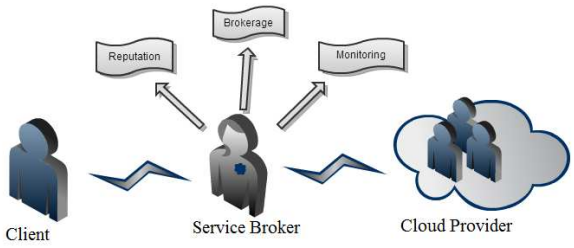

Figure 1: Architecture of Cloud Computing

- *Deployment of Cloud*

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.

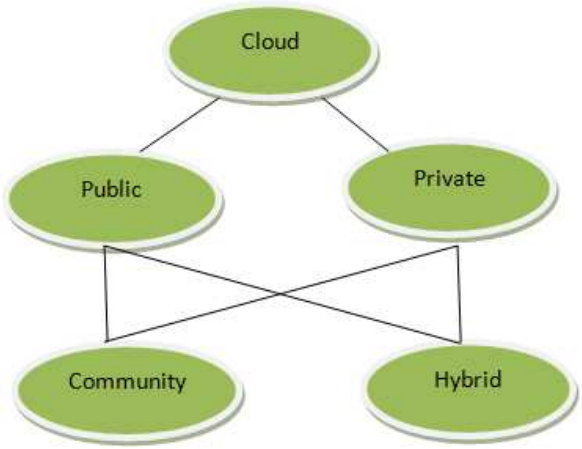

Figure 2: Deployment of Cloud

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.

- *Barrier to cloud computing*
- Privacy and Security
- Performance and Reliability
- Portability and Interoperability
- Data breach through fibre optical network.

Objectives

- To **authenticate the new clients** who want to request for the service either IaaS, PaaS or SaaS to the Cloud Provider via Service Broker. And registration of the new client is done after authentication of both client as well as service broker by third party authentication server.
- To **authenticate and validate the existing clients** who wants to access the services , for which they have already registered to the service broker. Third party will authenticate the client and service broker and provides session key for one time communication.
- To serve the requests of multiple clients at the same time, which are requesting to access the same type of service, **concept of multicast** is used.

Proposed Algorithm

A. Client-Broker-Cloud Communication Paradigm

In this paradigm, focus is on the secure communication between Client and Service Broker by implementing two hop authentication methods so that no node can join or leave the route, once the RREQ packet is formed. The need for early detection of inconsistencies like insertion and deletion of nodes on the fly are described by (Raj, 2012). This communication is classified and implemented into two steps as follows-

1. New Client Registration Paradigm (NCRP)
2. Registered Client-Cloud Paradigm (RCCP)

New Client Registration Paradigm (NCRP):

This paradigm is applicable for only new users. When a new user wants to access the services available at Cloud via Service Broker, then the following steps are carried out.

Step 1: Client will send the request message ${}_uM_b$ to Service Broker. The request includes following:

${}_uM_b=[U_{id}, ToS]$

Step 2: Service Broker will forward its own identifier and identifier of Client to Third Party Authentication, by ending the message ${}_bM_{tp}$

${}_bM_{tp}= [U_{id}, B_{id}]$

Step 3: Third Party Authentication will verify and validate both the communicating entities and respond back to the Service Broker.

Step 4: After authentication from Third Party, Service Broker will send the Service Level Agreement (SLA) to the Client.

Step 5: Client, if agrees, will respond with Yes or No to the Service Broker.

Step 6: If Client respond with "Yes" message, Service Broker will forward the Client Identifier to the Third Party Authentication, along with its own Identifier.
$D=[U_{id}, B_{id}]$

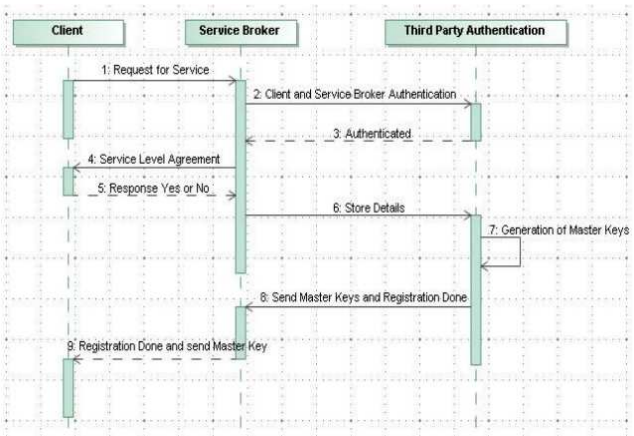

Figure 3: Sequence Diagram of New Client Registration Paradigm

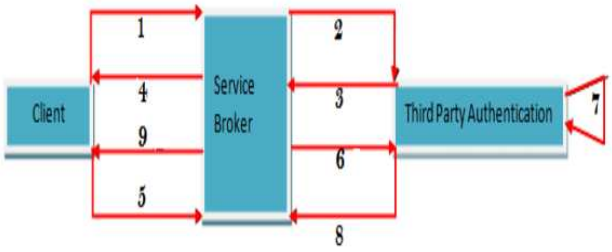

Figure 4: New Client Registration Paradigm

Step 7: Third Party Authentication will generate two Master Keys, one for Client and Other for Service Broker and store in the database repository along with their corresponding Identifiers.
$R= [U_{id}, B_{id}, MK_{Ui} , MK_{Bi}]$
Step 8: Once the records are recorded in the database, Third Party Authentication will send the acknowledgement to the Service Broker.
Step 9: Service Broker will send confirmation regarding the completion of registration to the Client.

Registered Client-Cloud Paradigm (RCCP)
This paradigm is applicable for the registered user, who wants to access the services available at Cloud. Before providing the requested services to the user, Third Party will authenticate the user. Only then the Service Broker can serve the request.
This paradigm involves following steps-
Step 1: Client will send the request to Service Broker including its identifier and master key:
$C = [MK_{Ui},U_{id}]$

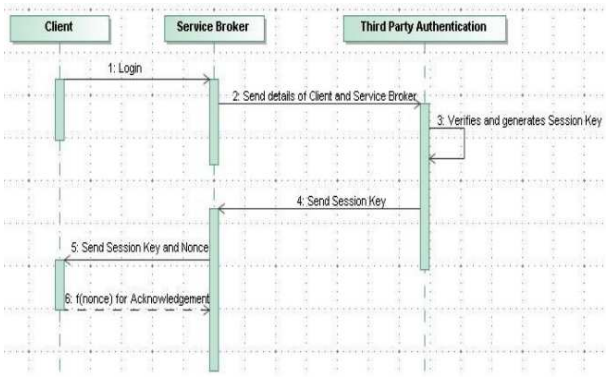

Figure 5: Sequence Diagram of Registered Client-Cloud Paradigm

Step 2: Service Broker will forward this request to Third Party Authentication for verification, along with its own identifier and master key:
$B=[C, MK_{Bi},B_{id}]$
Step 3: Third Party Authentication will verify details and generate Session Key.
Step 4: Third Party Authentication will send Session Key and identifiers of both communicating parties, to the Service Broker.
$S=[SK_{Ui},U_{id},B_{id}]$
Step 5: Service Broker will send Session Key and Nonce to Client.
$T=[SK_{Ui}, N_i]$

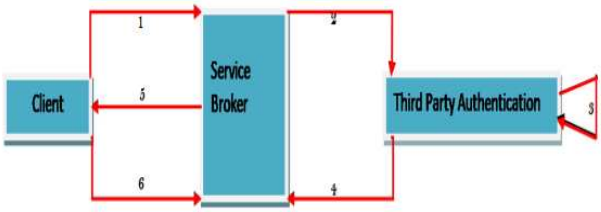

Figure 6: Registered Client-Cloud Paradigm

Step 6: Client will compute pre-decided function on Nonce and send it back to Service Broker.
$f(T)=[SK_{Ui},f(N_i)]$

B. Multi Client Broadcast Service (MCBS) Algorithm

After authentication, Service Broker will evaluate how many Clients have requested for the service at the same time and what type of service is requested by them. For handling multiple clients at a time for same type of service, we proposed this algorithm using concept of multicasting based on few reliability parameters as cost, time and space.
Algorithmic steps are as follows:

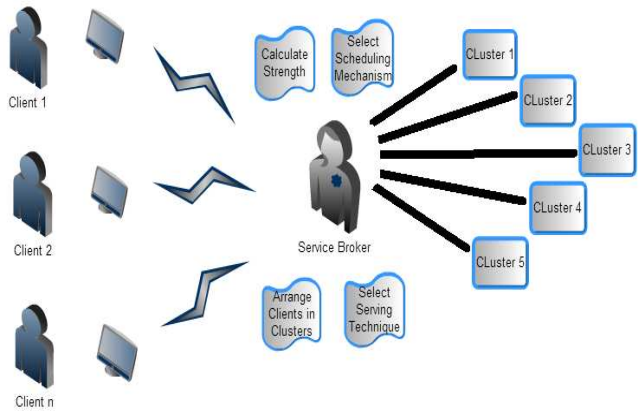

Figure 7: Multicasting Model

Step 1. If there are two or more clients who have requested for the same type of service at the same time, Service Broker will compute strength of the routes for each client asking for that service.
Strength = (Bandwidth / (Number of Hops x Network Delay))
Step 2. Create five clusters of the clients on the bases of their strength as-
Very High(VH), High(H), Medium(M), Low(L), Very Low(VL).
Step 3. For providing service to these clusters we can use different scheduling approaches as per following cases:

1. Round Robin Scheduling- In this we usually set sequence of clusters as

VH → V → M → L → VL

Multicast the service to each cluster for unit time interval.

- *Priority Scheduling*- Along with each and every cluster, priority is assigned. Arrange the clusters according to Priority and then Multicast the service to each cluster.

Step 4 : Depending upon the Serving Mechanism, Clients arranged in Clusters, are served, either unicasting is done or multicasting. Serving Mechanism depends on the number of clients who are requesting for same type of service at the same time.

Results

In this section, firstly, all clients register themselves to the service broker. Later, they login with their email id and password and verified by the service broker. Only that type of service, is offered to the client, that they have requested at registration time.
The whole scenario is shown in figures below:

Step 1: When a client registers itself to Service Broker.

Figure 9: Registration of Client 1

Step 2: Confirmation message will be shown to the user.

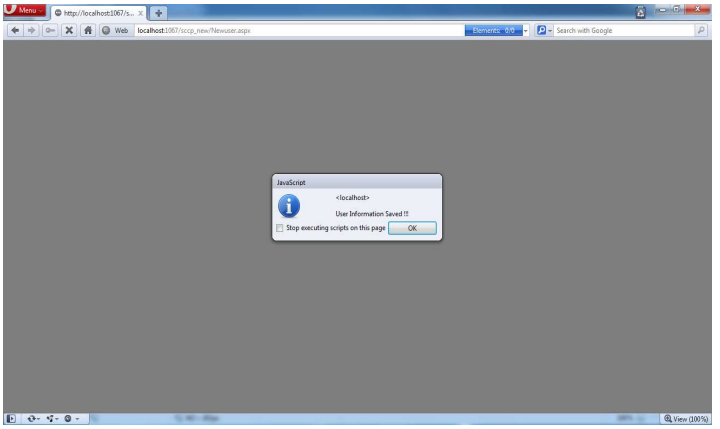

Figure 10: Client Information Saved

Step 3: Once the client data is successfully registered, he/she is provided a master key for security reasons, that can be used for authentication, whenever the clients logins next time onwards.

Figure 11: Master Key Window

Step 4: Next time onwards, each and every client must be login to access the services of Service Broker.

Client 1:

Figure 12: Login Window of Client 1

Step 5: Login will not be successful, unless the client provides the master key.

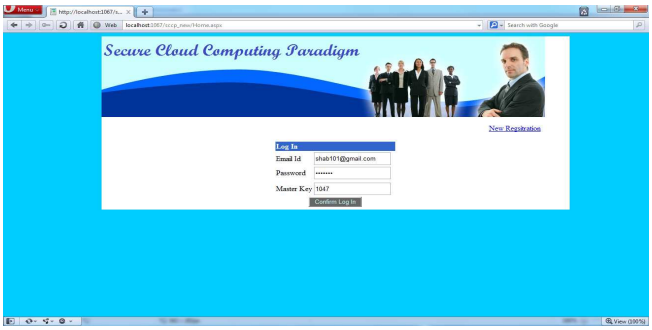

Figure 13: Authentication of Client 1

Step 6: After the successful login, the shortest route is calculated between source to destination.

Step 7: Similarly, other clients will login and shortest path is calculated.

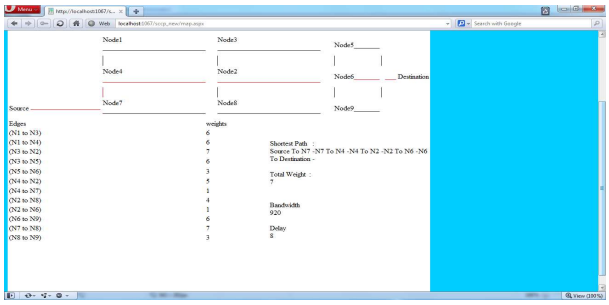

Figure 14: Shortest Route Calculation

Database Stored of all the Clients

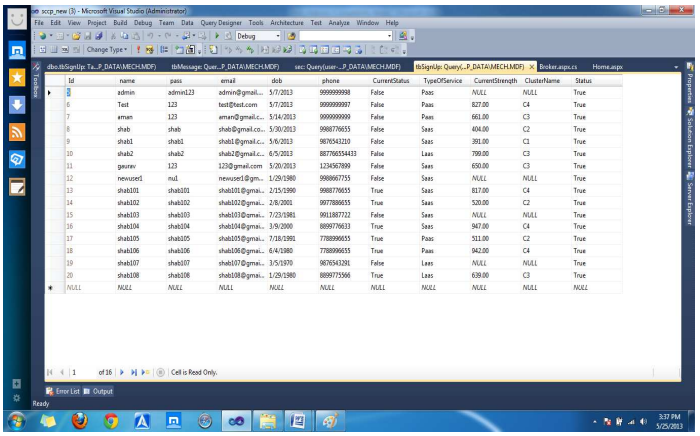

Figure 15: Registration Data of all Clients

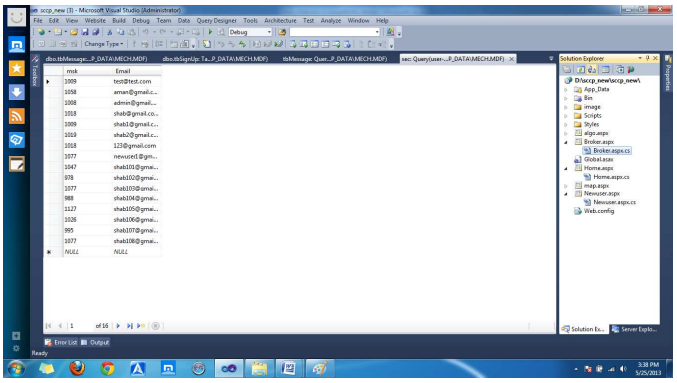

Figure 16: Table of Master Key

Step 7: Now, Service Broker will login and arrange the clients into clusters, depending upon the strength calculated.

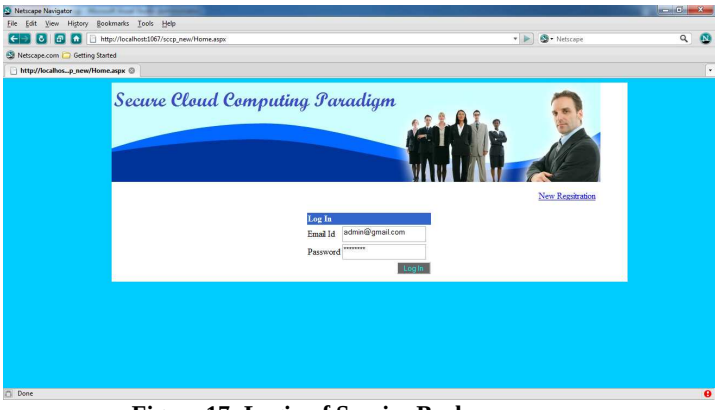

Figure 17: Login of Service Broker

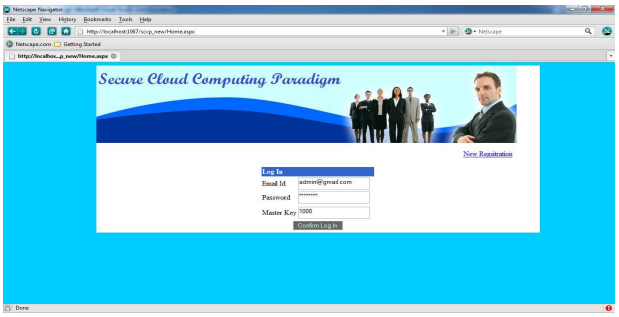

Figure 18: Authentication of Service Broker

Step 8: When Service Broker login, following window will be shown, which includes the details of clients login as well as they are also arranged into clusters.

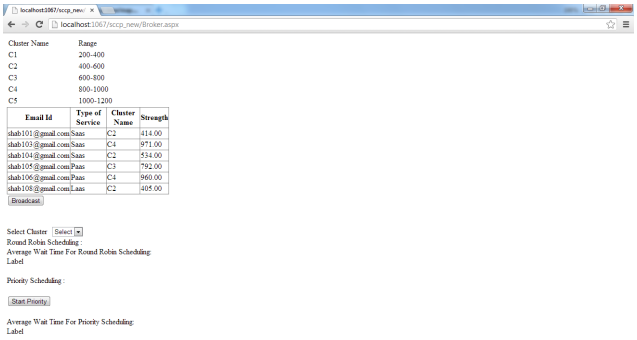

Figure 19: Main Window of Service Broker

Step 9: Depending upon the scheduling algorithm, either Round Robin or Priority based Scheduling algorithm, these clusters are served.

Step 10: If we click on Broadcast button, data is sent either using multicast or unicast, depending on the Type of Service of each Client. Unicast message will be sent if only one client from a particular cluster has requested for the service, otherwise Multicast message will be sent.

Table 2: Comparison of RR and Priority Scheduling for 6 Clients

Type of Cluster	Burst Time	Wait Time in Round Robin	Wait Time in Priority P123	Wait Time in Priority P213	Wait Time in Priority P231
Cluster 1	17	0	0	0	0
Cluster 2	23	6	5.5	6	0
Cluster 3	78	55.9	25.3	25.9	27

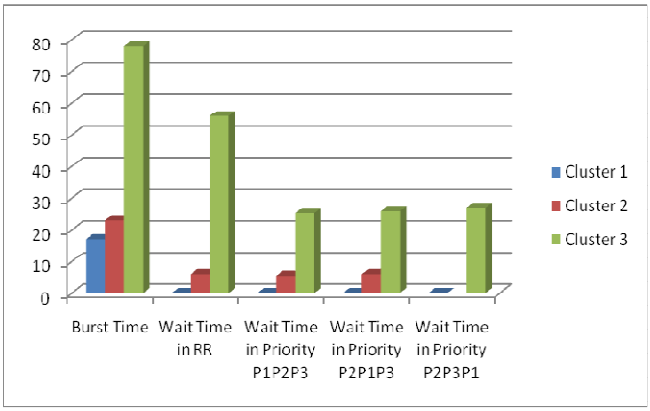

Figure 20: Performance Measurement of RR and Priority based Scheduling

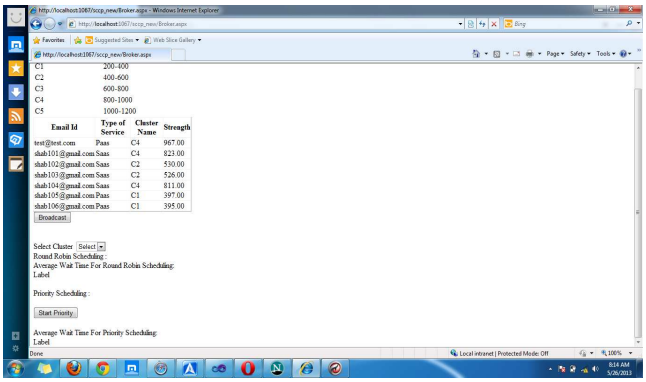

Figure 21: Main Window of Service Broker

Table 3: Comparison of RR and Priority Scheduling for 7 Clients

Type of Cluster	Burst Time	Wait Time in Round Robin	Wait Time in Priority P123	Wait Time in Priority P213	Wait Time in Priority P231
Cluster 1	45	17.5	14.2	15	15.9
Cluster 2	19	6	4.5	5	0
Cluster 3	29	11.2	7	7.5	0

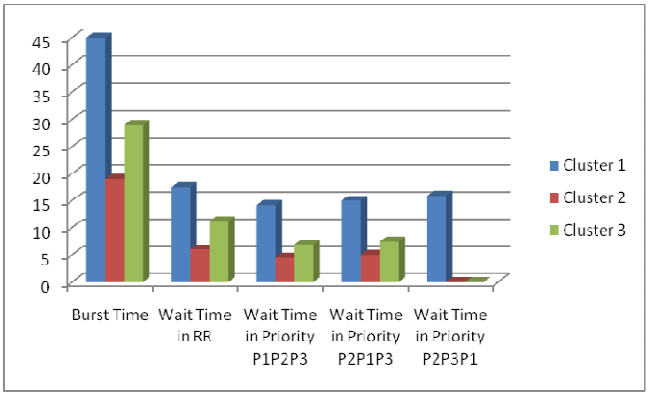

Figure 22: Performance Measurement of RR and Priority based Scheduling

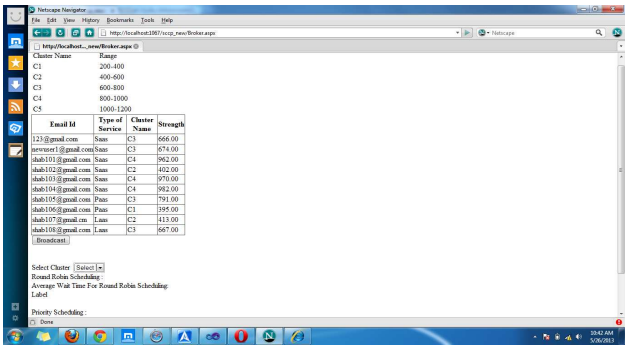

Figure 23: Main Window of Service Broker

Table 4: Comparison of RR and Priority Scheduling for 4 Clients in a Cluster

Type of Cluster	Burst Time	Wait Time in RR	Wait Time in P1213	Wait Time in P1312	Wait Time in P2321	Wait Time in P2123	Wait Time in P3132	Wait Time in P3231
Client 1	22	12	0	0	6.25	5.75	11.25	11.5
Client 2	24	14.4	11.5	17.5	17.5	0	0	6.25
Client 3	23	13.2	5.5	5.5	11.5	11.25	17.5	17.25
Client 4	25	15.6	17.5	11.5	0	17.5	5.75	0

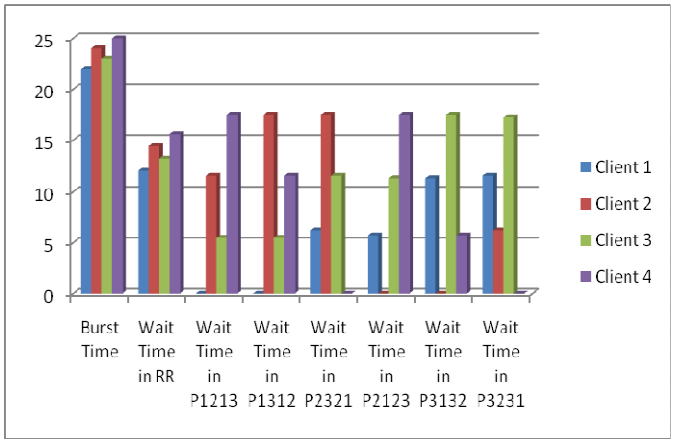

Figure 24: Performance Measurement of RR and Priority based Scheduling

Conclusion

The starting point of the paper is to provide authentication for the new clients as well as for the existing clients. Different type of authentication methods is available. Different levels of authentication are required for different type of service. Therefore, it is not possible to use same authentication algorithm for all types of applications. Even, authentication algorithms available are much complex and time consuming. So, here we have designed an algorithm of authentication, which is having least computational complexity. Next objective of the paper is to handle the requests of various clients at the same time, if they are requesting for the same type of service. So the scheme is proposed which uses the concept of Multicasting in the Cloud Computing Environment. From the results, this can be concluded that which type of scheduling mechanism is better than the other and under what circumstances.

Future Scope

A lot of work is in the process of communication in Cloud Computing. Till now, paradigm is proposed for multicasting of services, using Round Robin and Priority Scheduling algorithms. But in future, work can be carried out using other Scheduling techniques. Moreover, the problem of Congestion can occur, as the traffic in the network increases. So, the future work can be done on the above two given issues. In future, implementation of two-hop authentication algorithm will be carried out in secure reliable delivery neighborhood.

References

[1] A, D. H. (2012). Multi-level Authentication Technique for Accessing Cloud Services. *Computing, Communication and Applications.*

[2] A.Yassin, A. (2012). A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing. *IEEE 26th International Parallel and Distributed Processing Symposium Workshops.*

[3] Armbrust, M. (2009). Above the Clouds: A Berkeley View of Cloud Computing. *Electrical Engineering and Computer Sciences* .

[4] B.Meena. (2012). Cloud Computing Security Issues with Possible Solutions. *IJCST* . Behl, A. (2012). Analysis of Cloud Computing Security Issues. *IEEE.*

[5] Bhadauria, R. (2011). A Survey on Security Issues in Cloud Computing. *IEEE Communications Surveys.*

[6] Chen, N. (2010). Analysis and Improvement of User Authentication Framework for Cloud Computing. *International Journal of Innovations in Electronic Engineering and System* .

[7] Choudhury, A. J. (2011). Analysis and Improvement of User Authentication Framework for Cloud Computing. *International Journal of Innovations in Electronic Engineering and System* .

[8] F, L. (2010). Secure Virtualization for Cloud Computing. *Journal of Network Computer Application* , doi:10.1016/j.jnca.2010.06.008.

[9] Group, T. C. (2010). *Cloud Computing and Security – A Natural Match whitepaper.*

[10] Jadega, Y. (2012). Cloud Computing –Concepts , Architecture and Challenges. *Computing, Electronics and Electrical Technologies.*

[11] Jain, P. (2012). Security Issues and their Solution in Cloud Computing. *International Journal of Computing & Business Research ISSN (Online): 2229-6166* .
[12] Liu, W. (2012). Research on Cloud Computing Security Problem and Strategy. *IEEE.*
[13] Mell, P. (2011). *The NIST Definition of Cloud Computing.*
[14] Paterson, K. G. (2003). *A comparison between traditional Public Key Infrastructures and Identity-Based Cryptography.* Information Security Technical Report.
[15] Professionals, W. p. *Cloud computing :Silver Lining or Storm ahead.* IA newsletter.
[16] Raj, G. (2011). An Efficient Broker Cloud Management System. *Proceedings of the International Conference on Advances in Computing and Artificial Intelligence.* New York.
[17] Raj, G. (2012). Secure Cloud Communication for Effective Cost Management System through MSBE. *International Journal on Cloud Computing: Services and Architecture* .
[18] Rao, S. (2005). Cloud Computing-An Overview. *Journal of Theoretical and Applied Information Technology* .
[19] Revar, A. G. (2011). Securing User Authentication using Single Sign-On in Cloud Computing. *Institute of Technology.*
[20] S.Munnee, F. (2007). Kerberos using Public Key Cryptography. *GMU-ECE.*
[21] S.O., K. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks* .
[22] Sabahi, F. (2011). Cloud Computing Security Threats and Responses. *IEEE.*
[23] Saleem, R. (2011). *Cloud Computing 's Effect on Enterprises…in terms of Cost and Security.* Informatics.
[24] SeungHwan, J. (2012). Next Generation Cloud Computing Issues and Solutions. *International Journal of Control and Automation* .
[25] Shaikh, F. B. (2011). Security Threats in Cloud Computing. *6th International Conference on Internet technology and secured transactions.* Arab Emirates.
[26] Shen, Z. (2010). The Security of Cloud Computing System enabled by Trusted Computing Technology. *2nd International Conference on Signal Processing Systems.*
[27] Sivakumar, K. A. (2007). An Efficient Secure Route Discovery Protocol for DSR. *IEEE.* Technology, N. I. *NIST SP 500-292. Cloud Computing Reference Architecture: An Overview.* .
[28] Vogels. (2008). A Head in the Clouds—The Power of Infrastructure as a Service. *Workshop on Cloud Computing and in Applications* .
[29] Vouk, M. A. (2008). Cloud Computing – Issues, Research and Implementations. *Journal of Computing and Information Technology* .
[30] Wang, J. K. (2012). Data Security and Authentication in Hybrid Cloud Computing Model. *IEEE Global High Tech Congress on Electronics.*
[31] Zhang, S. (2010). Analysis and Research of Cloud Computing System Instance. *Second International Conference on Future Networks.*
[32] Zhi-hua, Z. (2012). An New Anonymous Authentication Scheme for Cloud Computing. *The 7th International Conference on Computer Science & Education.*