Third Party Authentication Process in CBCCP for Services Management using MSBE and MCBS

Shabnam Sharma [1], Gaurav Raj[2] , Dr. Dheerendra Singh[3]
[1] M. Tech., Computer Science Department, Lovely Professional University
Punjab, India, [2]PhD Scholar, Computer Science Department, Punjab Technical University
Punjab, India, [3]Professor and Head of CSE Department , SUSCET, Tangori, India
[1]shabnamsharma09@gmail.com, [2]er.gaurav.raj@gmail.com, [3]hodcse@suscolleges.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 centres that may lie beyond the reach of the organization. Accessing the data from these data centres 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 RR, Priority and Priority based RR scheduling.**

Keyword- CBCCP, MSBE, NCRP, RCCP, SRDN, Service Scheduling,

I. INTRODUCTION

It is defined as the large distributed environment where infrastructure, applications, storage area and other physical media is provided to the user, in the form of service, either directly or through cloud broker[9].The Cloud Computing architecture includes Cloud Consumers(Client), Cloud Coordinator, Cloud Carrier, Cloud Auditor and Cloud Broker (Service Broker) as its five major actors[5] .

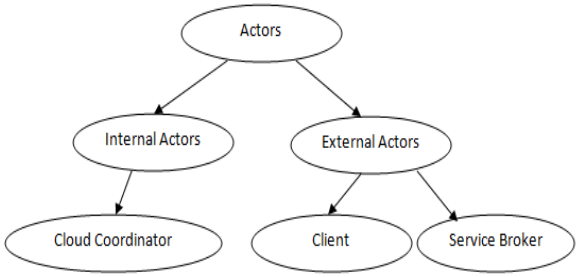

Fig 1: Internal and External Actors

These actors are categorized into two categories, one is of Internal Actors and other is External Actors. Client and Service Broker are said to be External while Cloud Coordinator is considered as Internal Actors. Cloud Carrier works as communication channel between client, broker and cloud to deliver services. Due to unsecure communication channel (cloud carrier)[7], Cloud Audit is most important part for handling security, privacy and performance. Client is the stakeholder in the Cloud Computing environment. Cloud Consumer is such an entity, which can be a person or an organization, asking for services dealing with Service Broker who will do all negotiation and provide the service from Cloud Provider. Client and Cloud Coordinator must be agreed upon Service Level Agreement (SLA), which specifies the technical performance requirements. Cloud Auditor is a part of Service Broker who is accountable for auditing of SLA. Cloud Auditor verifies whether Cloud Coordinator and Client is satisfying the technical performance requirements of SLA. Cloud Coordinator is responsible for the service deployment, service orchestration, cloud services management, security and privacy. Cloud Coordinator provides services to the Client using dedicated Virtual Machines, Data centres and Servers. Service Broker acts as middleman between Client and Cloud Coordinator using Cloud Carrier [4]. The major responsibilities of Service Broker are as follows:

1. Service intermediation,
2. Service aggregation,
3. Service arbitrage.

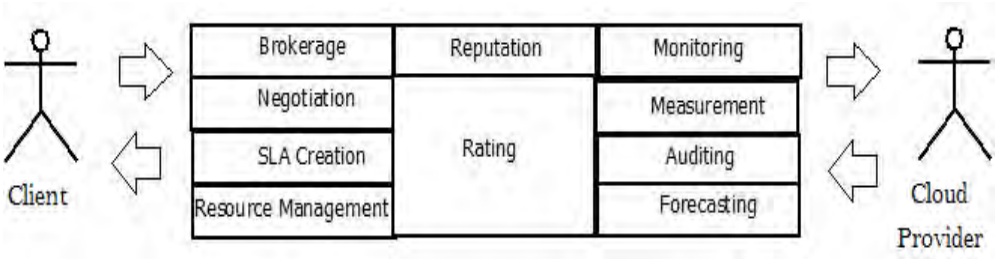

Fig 2: Referral Model of Cloud Computing

II. Service and Deployment

Cloud computing basically provides three types of services, i.e. Software as a service, Infrastructure as a service and Platform as a service [2]. The cloud application which delivers the SaaS, holds the potential to eliminate the need of installation of application software on the end user system. PaaS includes all platform required by Cloud Consumer. Client need not to worry about the acquisition of hardware and software. While providing, IaaS, Cloud Consumer need not to buy servers for the storage of large amount of data, for example, in case of organization. For the deployment of services, NIST has described three types of models, i.e. Public, Private, Community or Hybrid.[3] In the Public Cloud, resources are made available to general public. The Private Cloud is accessible only to a particular organization. It can be implemented either on-site or off-site. On the other hand, Community Cloud serves numerous Cloud Consumers who belong to different organizations. These organizations can access the same Cloud for the services. Hybrid Cloud is a combination of two or more cloud models [7][8].

III. Proposed Architecture

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 in [1].

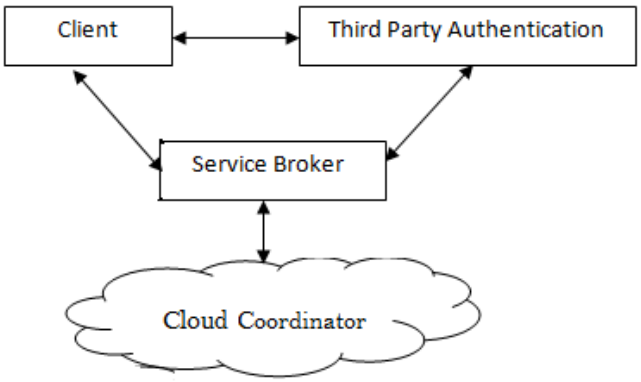

Fig 3: Proposed Architecture of Cloud Computing

In Cloud Computing, Client communicates first with Service broker, which in turn communicates with Cloud Provider. In this paper, strong user authentication framework is designed[6], where Third party authenticates the user and restricts the illegal access to the services provided by Cloud Coordinator via Service Broker[10].

This communication is classified and implemented into two steps as follows-

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

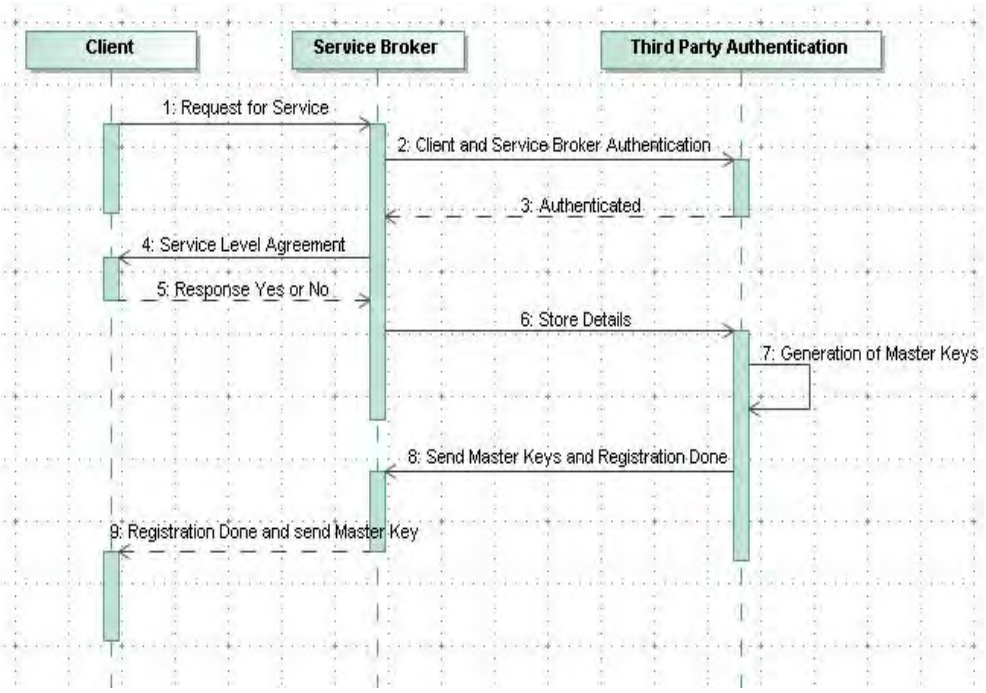

Fig 4: New Client Registration Paradigm

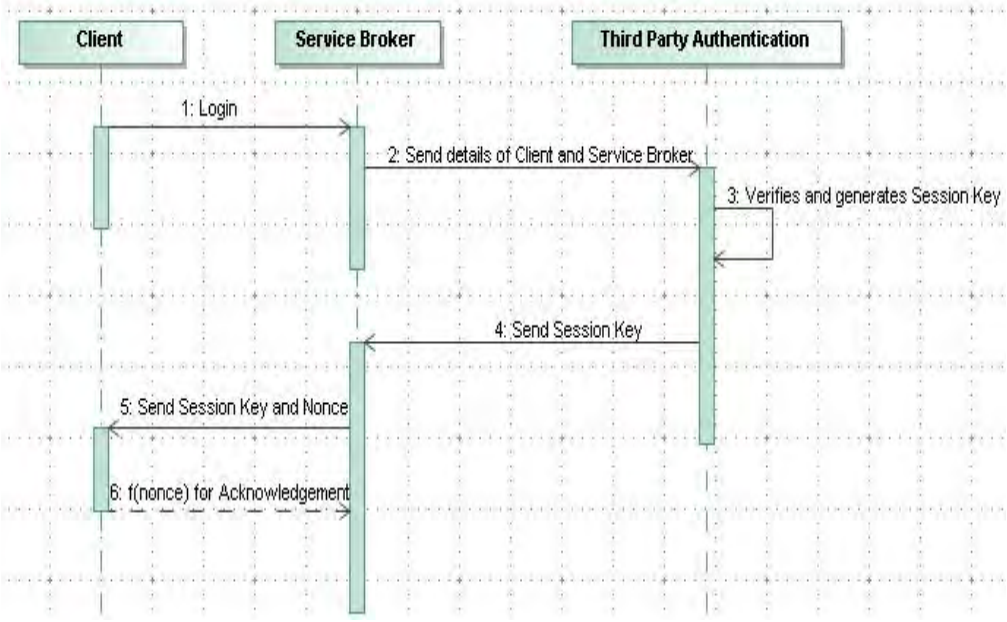

Fig 5: Registered Client-Cloud Paradigm

1) 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:

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

Step 2: Service Broker will forward its own identifier and identifier of Client to Third Party Authentication, by sending 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.

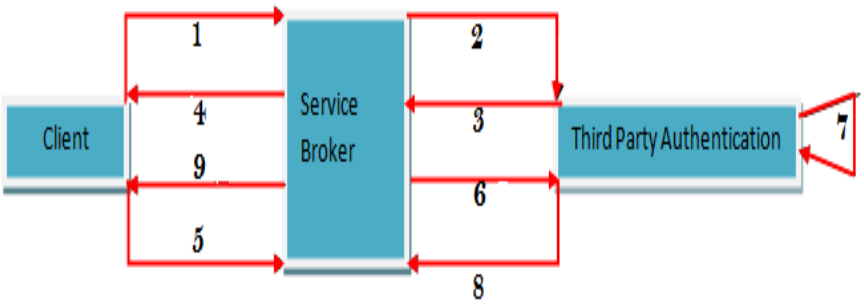

Fig 6: New Client Registration Paradigm

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.

$$D=[U_{id}, B_{id}]$$

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.

TABLE 1. ABBREVIATIONS USED IN ALGORITHM

Abbreviation	Meaning
U_{id}	Identifier of Client
B_{id}	Identifier of Service Broker
MK_{Ui}	Master Key of Client
MK_{Bi}	Master Key of Service Broker
SK_{Ui}	Session Key of Client
ToS	Type of Service

2) 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:

$$C = [MK_{Ui},U_{id}]$$

Step 2: Service Broker will forward this request to Third Party Authentication for verification, along with its own identifier and master key:

$$B=[C, MK_{Bi},B_{id}]$$

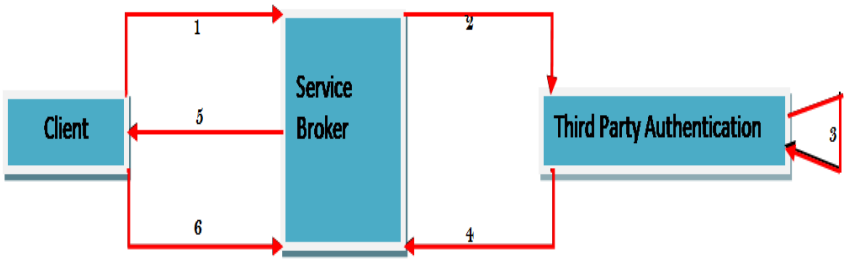

Fig 7: Registered Client-Cloud Paradigm

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:

$$T=[SK_{Ui,}\ N_i]$$

Step 6: Client will compute pre-decided function on Nonce and send it back to Service Broker.

$$f(T)=[SK_{Ui},f(N_i)]$$

3)- Multi-Source Broadcast Encryption with SRDN :

In this, we are implementing Multi-Source Broadcast Encryption (MSBE) scheme along with Secure Reliable Delivery Neighborhood (SRDN) for two hop authentication [3]. For secure communication between Client and Service Broker, identification of nodes is necessary which lies in RDN. Such nodes are provided with the secret key. If Client "A" wants to access the services offered by Service Broker "B", it will assign the secret key K_A to all nodes which are present in RDN. No transmissions are carried out by those intermediate nodes which are not the part of RDN. Such nodes are said to be "revoked nodes". In the Multi-Source Broadcast Encryption (MSBE) scheme, the Key Distribution Centre (KDC) selects "N" number of secret keys and a one-way function denoted by F() and a cryptographic hash function denoted by h(). The one- way function F (A) = $\{A_1, A_2, A_3, \ldots\ldots A_m\}$ determines the collection of secret keys assigned to Client "A". Client "A" is assigned m decryption secrets denoted by S_A and k encryption secrets denoted by G_A

$$S_A= \{ K_{A1}, K_{A2}, K_{A3}, \ldots\ldots.. K_{Am} \}$$

$$G_A=\{ K_j^A = h(K_j \| A) \}, \text{ where } 1<=j<=k$$

Suppose U is the set of all the nodes which are having encryption and decryption secret keys and let N_A U, is the subset of revoked nodes. T_A is the encrypted broadcast secret key with the subset of its encrypted secret keys G'_A G_A is conveyed to all nodes by the Client "A" in its RDN. Only those encryption secrets are chosen which are uniquely determined by specific indices and guarantees the following-

1. No revoked node is allowed to access the encryption secrets.
2. Except revoked nodes, all other nodes must have access to at least one of the encryption secrets in G_A. These nodes are represented by U/N_A.

To broadcast the secret key to all the nodes in U/N_A, Client "A" will form a broadcast message.

$$B_A=[N_A \| \{ G'_A(K_A) \} \| h(N_A, G'_A(K_A), T_A)]$$

4)- Secure Route Discovery Protocol (SRDP)

1. Client will create a Route Request (RREQ) to communicate with Service Broker which consists of various fields, as given below:

   $$[Client_{Addr}, Client_{Seq}, Broadcast_{id}, Broker_{Addr}, Max\_Hop, Hop\_Count, Path\_Cost]$$

   The values of first four fields do not change from Client to Service Broker, but last two fields will keep on changing, until it reaches Service Broker.
2. Client will broadcast the M_A to only those nodes which are present in SRDN.
3. If the intermediate node has already received the RREQ , then it will simply discard it, otherwise the updations are carried out in Hop_Count and Path_Cost fields.
4. Path_Cost is dependent on the Bandwidth available and Network delay:

   $$[Path\_Cost=Path\_Cost +\alpha.Number\_of\_hops +\beta .Avl\_BW +\gamma.Net\_Delay]$$
5. Every intermediate node rebroadcasts the RREQ and updates its routing table.

6. When the Service Broker receives the first RREQ , it will go into Wait_All state. Service Broker will remain in this state, until it receives the RREQ from all other intermediate nodes.
7. Once the RREQ are collected at Service Broker, it selects the RREQ with the smallest cost value.
8. Now the Service Broker will send the RREP to Client over reverse path of that RREQ which is having smallest cost value.
9. Both parties (Client and Service Broker) can communicate now over this selected route.

RREQ Packet

Client will broadcast the RREQ to find out the route to Service Broker. Client will create a RREQ with following fields-

$$M= [Client_{Addr} || Client_{Seq} || Broadcast_{id} || Broker_{Addr} || Max\_Hop || Hop\_Count || Path\_Cost]$$

$$RREQ_0 = [Client_{Addr} || Client_{Seq} || Broadcast_{id} || Hop\_Count || Path\_Cost || K_{CB}(M || M_0 || h_0)]$$

Where

$$h_0 = h(M ,K_{SD}),\ h_1=h(h_0),\ M_0= h(M,h_1,T_S)$$

K_{CB} is the secret shared between Client and Service Broker. M_0 denotes the Hashed Message Authentication Code for the authentication by the Service Broker and h_0 denotes the HMAC for the authentication by two-hop nodes. The fields of RREQ are secured by encrypting using secret key of Client. The immediate next node, say "A", decrypts the received RREQ and broadcast the RREQ by modifying the Client address (actually next hop address), its sequence number, HMAC designed for authentication of Service Broker, HMAC designed for authentication by two hop nodes.

$$RREQ_1 = [A_{Addr} || A_{Seq} || Broadcast_{id} || Hop\_Count || Path\_Cost || K_{AB}(M || A || M_0 || M_1 || h_1)]$$

Where

$$h_2=h(h_1),\ M_1= h(M,A,h_2,T_A)$$

The node, say "B", which is two hops away from the Client, decrypts the RREQ packet received from the previous node "A". Node "B" then verifies whether HMAC h_1 sent by previous node "A" is consistent with the HMAC M_0 forwarded by Client. After verification, node "B" truncates the HMAC M_0 and appends a new HMAC, say M_2, which is used for the authentication by next two hops. Now node "B" forward the following RREQ packet.

$$RREQ_1 = [B_{Addr} || B_{Seq} || Broadcast_{id} || Hop\_Count || Path\_Cost || K_{BB}(M || A(,B) || M_1 || M_2 || h_2)]$$

Where

$$h_3=h(h_2),\ M_2= h(M,(A,B),h_3,T_B)$$

If there are multiple clients who wants to communicate with Service Broker at the same time, then multiple RREQ are generated by several clients individually.

RREP Packet

When the Service Broker receives the RREQ from the Client, RREQ contains the per hop HMAC code represented by h_i, where i represents the number of intermediate nodes between Client and Service Broker. Service Broker then verifies the consistency of h_0 with h_i. Service Broker can easily verify it by using the secret shared between Client and Service Broker. Service Broker send the RREP packet back to the Client, including following fields.

$$M = [Client_{Addr} || Client_{SeqNo} || Service\_Broker_{Addr} || Service\_Broker_{SeqNo} || (A,B, \ldots , W,X, Y, Z)]$$

$$RREP_0 = [Service\_Broker_{Addr} || Service\_Broker_{SeqNo} || K_D([M || q_0 || M_{DY}])]$$

$$M_{DY}= h(M, q1,K_{DY})$$

Where

$$q_1= h(q_0)$$

The RREP packets generated at the node Z and node Y are:

$$RREP_1 = [Z_{Addr} || Z_{SeqNo} || K_Z([M || q1 || MDY|| M_{ZX}])]$$

$$M_{ZX}= h(M, q2,K_{ZX})$$

Where

$$q2= h(q1)$$

$$RREP_2 = [Y_{Addr}|| Y_{SeqNo} || K_Y([M || q2 || M_{ZX} || M_{YW}])$$

$$M_{YW}= h(M, q3,K_{YW})$$

Where q3= h(q2)

5)- 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 handeling 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:

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)) (1)

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).

3. For providing service to these clusters we can use different scheduling approaches as per following cases

   I) *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.

   II) Priority Scheduling- Calculate the priority factor(P_f) for each cluster based on service request size(SR_S) and cost(C) can be set as per following cases-

   i) $P_f = SR_S \text{ X } C$

   ii) $P_f = 1 /(SR_S \text{ X } C)$

   iii) $P_f = C / SR_S$

   iv) $P_f = SR_S / C$

   Arrange the clusters according to P_f and then Multicast the service to each cluster

   III) Priority based Round Robin Scheduling- Calculate the priority factor(P_f) for each cluster based on service request size(SR_S) and cost(C) can be set as per following cases-

   i) $P_f = SR_S \text{ X } C$

   ii) $P_f = 1 /(SR_S \text{ X } C)$

   iii) $P_f = C / SR_S$

   iv) $P_f = SR_S / C$

   Arrange the clusters according to P_f and then Multicast the service to each cluster for unit time interval

IV. CONCLUSION

In this paper, we have proposed the concept of multicasting at the end of the Service Broker. Strength of the route is calculated by considering Bandwidth available, number of intermediate nodes and network delay. We have proposed MCBS algorithm which will help broker to deal with clustering of client request and scheduling of services based on RR, Priority and Priority base RR scheduling algorithms. We are implementing and checking the efficiency of these proposed Algorithms. The problem of congestion is yet to be considered while doing multicasting. Moreover, this proposed algorithm can be implemented in different environments like MANET and VANET. Our future we would analyze the impact of other parameters like throughput, efficiency, reliability on the proposed algorithm which can be considered for the calculation of strength , priority and the path cost.

REFERENCES

[1] Raj Gaurav, “An Efficient Broker Cloud Management System” ACAI '11 Proceedings of the International Conference on Advances in Computing and Artificial Intelligence ACM New York, NY,USA ©2011 ISBN: 978-1-4503-0635-5.

[2] Raj Gaurav, Kaur kamaljit, “Secure Cloud Communication for Effective Cost Management System Through MSBE”, International Journal on Cloud Computing: Services and Architecture, June 2012, Vol. 2, No. 3, ISSN: 2231 - 5853[Online]; 2231 - 6663 [Print]

[3] Buyya R., Ranjan R., Calheiros R.N. “Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities" ; High Performance Computing and Simulation, 2009. HPCS '09. International Conference on Digital Object Identifier: 10.1109/HPC-SIM. 2009.5192685 Publication Year: 2009 , Page(s): 1 – 11.

[4] Kulasekaran A. Sivakumar and Mahalingam Ramkumar, “An Efficient Secure Route Discovery Protocol for DSR”, Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE.

[5] Yashpalsinh Jadeja and Kirit Modi“Cloud Computing-Concepts, Architecture and Challenges”, Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference.

[6] “NIST Cloud Computing Reference Architecture” Services , 2011 IEEE World Congress.

[7] Amlan Jyoti Choudhary, Pardeep Kumar, Mangal Sain, Hyotaek Lim and Jae-Lee, “A Strong User Authentication Framework for Cloud Computing”,Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific

[8] Dillon Tharam, Wu Chen, Chang Elizabeth, “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.
[9] Yashpalsinh Jadeja, Kirit Modi, “Cloud Computing - Concepts, Architecture and Challenges” in 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].
[10] Srinivas Rao, Nageswara rao and E Kusuma Kumari, “Cloud Computing-An Overview” in Journal of Theoretical and Applied Information Technology.
[11] Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee, “A Strong User Authentication Framework for Cloud Computing” in 2011 IEEE Asia -Pacific Services Computing Conference.