Interconnected Hybrid Clouds Using Scheduling Techniques

Dalima Parwani[1], Dr. Amit Dutta[2], Meenu Tahiliyani[1]
[1]Dept of CS, Sant Hirdaram Girls College, Bhopal (M.P.) India.
[2]Dept of CSA, BU, Bhopal (M.P.) India.

ABSTRACT

Technology is changing to embrace the cloud. Cloud Computing is simply sharing computing resources that are available through a service provider. Those resources can be storage space, use of software applications or servers. You buy more if you need more resources; you give back resources that you no longer need. Cloud computing infrastructure enables companies to cut costs; by outsourcing computations on-demand. However, clients of cloud computing services currently have no means of verifying the confidentiality & integrity of their data and computation. The paper tableaux a Publish-Subscribe model to balance the real and perceived risks with the value of adopting a cloud solution that improves the security of data over the cloud.

Keywords: technology, cloud computing, confidentiality, integrity, publish, subscribe.

I INTRODUCTION

Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud providers use virtualization technologies combined with self service abilities for computing resources via network infrastructure.

In cloud environments, several kinds of virtual machines are hosted on the same physical server as infrastructure. In cloud, costumers must only pay for what they use and have not to pay for local resources which they need to such as storage or infrastructure. Nowadays, there is having three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds which they are running applications externally by large service providers and offers some benefits over private clouds.

Private Cloud refers to internal services of a business that is not available for ordinary people. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some resources internally and has some others for public use. Also there is combination of private and public clouds that called Hybrid cloud. In this type, cloud provider has a service that has private cloud part which only accessible by certified staff and protected by firewalls from outside accessing and a public cloud environment which external users can access to it. There are three major types of service in the cloud environment: SaaS, PaaS, and IaaS [2].

In cloud, similar to every proposed technology, there are some issues which involved it and one of them is RAS factor. For having good and high performance, cloud provider must meet several management features to ensure improving RAS parameters of its service such as:

(a) Availability management
(b) Access control management
(c) Vulnerability and problem management
(d) Patch and configuration management
(e) Countermeasure
(f) Cloud system using and access monitoring.

II CLOUD SECURITY ISSUES

Innately, Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack [3]. Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward [4].

III SECURITY REQUIREMENTS FOR SECURE CLOUD COMPUTING

Information Security should cover a number of suggested themes. Cloud computing security should also be guided in this regard in order to become an effective and secure technology solution.

(a) **Identification & authentication:** In Cloud computing, depending on the type of cloud as well as the delivery model, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly. This process is targeting at verifying and validating individual cloud users by employing usernames and passwords protections to their cloud profiles.

(b) **Authorization:**Authorization is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing. Authorization is maintained by the system administrator in a Private cloud.

(c) **Confidentiality:** In Cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. It is a must when employing a Public cloud due to public clouds accessibility nature.

(d) **Integrity:** The integrity requirement lies in applying the due diligence within the cloud domain mainly when accessing data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the cloud's data should without a doubt be robustly imposed across all Cloud computing deliver models.

(e) **Non-repudiation:** Non-repudiation in Cloud computing can be obtained by applying the traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).

(f) **Availability:** Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability in cloud services and resources between the cloud provider and client.

(g) **Main problems with cloud computing**: Security problems that may exist in the cloud are so high, that even the whole IT industry has undergone a revolution; however, it is not perfect [5]. Existing security technology still cannot solve some of the problems associated with cloud security; there are so many security characteristics of the cloud it is difficult to give fully display. Security policy is needed to ensure healthy and stable development of cloud computing.

(h) **Cloud Transparency** Transparent security would entail cloud providers disclosing adequate information about their security policies, design, and practices, including disclosing relevant security measures in daily operations .Public clouds are more likely to be seen as having a greater degree of transparency as compared to the Hybrid or Private Cloud models. This is due to public cloud vendors having a "standardized" cloud offering thereby targeting a wider client base. Private clouds are usually built for specific organizations having more attention focused on offering customization and personalization cloud functionality [6].

IV OBJECTIVES & SCOPE

The methodology implemented here is based on the concept of developing an efficient framework which is base on the concept of interconnected federated cloud. The framework should be such that the various applications used in interconnected federated cloud and access of resources over this network is efficient and also the framework provides less communication overhead means during the transmission of data to the receiver no data should be loss and it consumes less power. The security against various attacks especially DOS and DDOS attacks can be detected and prevented by the framework. Since DOS attack can be significantly increased by using malicious workloads of greater complexity, which can involve a proportional increase of memory consumption or processing delay. Moreover, since both the brokers and the subscribers need to maintain internal status information in order to operate correctly, state-full attacks may be performed against them.

V METHODOLOGY

(a) If 'N' is the number of users in the network with number of local brokers and data centers.

(b) Let 'Ui' user requests for a publish service item 'Ii'.

(c) Each of the nodes contains a set of items that are being serviced at 'v'.

(d) Some of the items are not scheduled at the node 'v'.

(e) Here managers are used for the insertion of item in the serviced node 'v'.

(f) Now Manager uses the scheduling of the item sets at each serviced node 'v'.

(g) All the managers which maintains publish services is attached with the global manager.

(h) If any of the local service uses more time to access the item cached at node 'Vi', then at that local manager scheduling is done by the global Manager.

```
(a)  If 'N' of request are send from User 'Ui' to DataCenter 'Di'
(b)  If 'Ri' is the resources to be involved in the communication.
(c)  For each of 'Ri' → 'Di'
(d)  Compute power for each of the resource
(e)  $P_{T,IP} = 2.H.P_{tr1} + (H-1).P_{IP}$
(f)  If check 'Rold'==Rnew' request for new resource and new resource is same or not.
(g)  Send only 'Rold'
(h)  Else
(i)  Send Rnew
(j)  End
```

VI PUBLISH & SUBSCRIBE

```
While(true){
Tcurrent = get Raccess from VM;
foreach Resource{
//resource is unallocated
If (!Tcurrent[Resource])
For each Useri→ Resource
Allot Useri→Tcurrent
Else
WaitT→ till Resource(Alloted)
Store → Stable
If U ← Access Subscribe
U → Subscribe Command
Check Validity U
Allot Subscribe → U
End
End
```

VII PROPOSED SCHEDULING

The proposed methodology uses the combination of two scheduling techniques Shortest Job First and Priority based Scheduling. The processing can be applied for the public as well as Hybrid Cloud. The formal algorithms steps of the proposed methodology are given below:

Notation	Description
Ui	Various Users of the cloud
DCi	Data Centers
UBi	Broker of the cloud
Bi	Burst Time for the Job Ji
Ji	Sequence of Jobs
Ti	Process time
Pi	Priority of Job Ji

VIII VARIOUS NOTATIONS USED IN ALGORITHM

(a) If 'N' is the number of requests to send from 'Ui; users of the cloud 'C' with 'Bi' burst time of each of the user 'Ui' to the data Centers 'DCi' through brokers 'UBi'.

(b) If 'T1, T2, ………….Tn' is the various burst time from various users "Ui' for the request of the Jobs 'Ji'.

(c) If 'P1,P2,…………Pn' be the priority of various jobs 'Ji' for the request.

(d) Compute Priority vector for all d matrices using

(e) $A_w = \gamma_{maxw}$

(f) Make a matrix with priority vector using

a. $\Delta = [w^1 w^2 \ldots\ldots w^d]$

(g) Compute 'C' for the consistent comparison matrix.

(h) Compute PVS which is a vector included value of priority of jobs.

(i) Check the 'Ji' having highest priority from 'Pi'.

(j) Now also check the burst time 'T' of the job 'Ji' having highest priority 'Pi'.

(k) If burst time 'Ti' is very less then execute the scheduling of the job 'Ji'.

a. Otherwise the job having shortest burst time 'Ti' is executed.

IX CONCLUSIONS

The methodology implemented here can be analyzed and compare with the existing system on the basis of following factors.

(i) Communication overhead and delay.
(ii) Reliability
(iii) Delivery Time
(iv) Success Rate

(a) Expected Outcomes of the proposed work may be It may be possible to get better Adaptability & Attack Resiliency in proposed cloud architecture.
(b) Vulnerabilities assessment of the proposed secure cloud architecture will be done against DoS and DDoS or else attacks.
(c) Counter measures of the above attacks on the proposed secure cloud architecture will be done.

REFERENCES

[1] FarzadSabahi "Cloud Computing Security Threats and Responses", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp. 1-5, 2011.

[2] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at theEighth IEEE International Conference on Dependable, Autonomicand Secure Computing, Chengdu, China, 2009.

[3] N. Mead, etai, "Security quality requirements engineering (SQUARE) methodology" Technical report of Carnegie Mellon Software Engineering Institute, 2005.

[4] J. W.Rittinghouse and J. F.Ransome Cloud Computing: Implementation,Management,and Security Taylor and Francis Group, LLC,CRC Publication, 2010.

[5] Ramgovind S, Eloff MM, Smith E.The Management of Security in Cloud Computing, IEEE 2010.

[6] Bodkins J, 2008, 'Gartner: Seven cloud-computing security risks', InfoWorlds, viewed 13 March 2009.

[7] Christian Esposito, Massimo Ficco, Francesco Palmieri, Aniello Castiglione,"Interconnecting Federated Clouds by Using Publish-SubscribeService", 2013.

[8] Stefan Birrer," A Comparison of Resilient Overlay MulticastApproaches", IEEE 2007.

[9] RajkumarBuyya, Rajiv Ranjan and Rodrigo N. Calheiros," InterCloud: Utility-Oriented Federation ofCloud Computing Environments for Scaling ofApplication Services", Springer 2010.

[10] Miguel Castro, Peter Druschel, Anne-Marie Kermarrec and Antony Rowstron," SCRIBE: A large-scale and decentralizedapplication-level multicast infrastructure", IEEE 2002.

[11] ÁineMacDermott, Qi Shi, MadjidMerabti, and KashifKifayat, "Security as a Service for a Cloud Federation", PROTECT: Research Centre for Critical Infrastructure Computer Technology and Protection, 2014

[12] Joseph Latanicki, Philippe Massonet, Syed Naqvi, Benny Rochwerger andMassimo Villari, "Scalable Cloud Defenses for Detection,Analysis and Mitigation of DDoS Attacks",G. Tselentis et al. (Eds.)IOS Press, 2010.

[13] Wei Deng, Fangming Liu, Hai Jin, Bo Li and Dan Li "Harnessing Renewable Energy in Cloud Datacenters: Opportunities and Challenges" IEEE, 2014.

[14] Ahmed Q. Lawey, Taisir E. H. El-Gorashi and Jaafar M. H. Elmirghani "Distributed Energy Efficient Clouds Over Core Networks", Journal OfLightwave Technology, Ieee, 2014.

[15] Weiwen Zhang, Yonggang Wen, Kyle Guan, Dan Kilper, Haiyun Luo and Dapeng Oliver Wu "Energy Optimal Mobile Cloud Computing under Stochastic Wireless Channel", IEEE Transactions On Wireless Communications, 2013.