Simulation implementation using cloud sim library for the visualization into the multiple servers in cloud computing

Author:
Sunny H. Bhadlawala
M.Tech, B.E., MCP, MCTS,

***Abstract*— In the world of information technology or any fields have a some limitations and challenges but how to resolve that is the challenge for the researcher, here I have trying to resolve some limitations for the cloud computing.**

The main objective of the research goal is to explore key strategic issues related to the adoption of cloud computing based on the resources such as Servers, Processing units for the computing processes for on demand using multi-cloud strategies.

***Keywords*—cloud computing, multi-cloud computing, cryptography, Security, Authentication, Protocols.**

I. INTRODUCTION

TRUST AND CHALLENGES IN CLOUD COMPUTING ADOPTION

Cloud computing adoption is faced with a number of challenges, these challenges are security challenges, legal and compliance challenges and organizational challenges.

Linked to all these challenges is the issue of trust between clients and vendors because cloud computing calls organizations to trust vendors with the management of their IT resources and important about data. Trust is a critical factor when adopting the cloud computing.

This research will focus specifically on identifying the challenges and facing the organizations issues.

The reality of security is tied to the probability of different risks and how it will effect to the originations.

Security is also a feeling in that it is based on the psychological reactions to both the risks and the countermeasures.

Therefore, Cloud computing needs to appeal to both the feelings of the potential customers and address the reality of the risks associated with cloud computing in a way that customers will feel safe and secure to use cloud computing.

That is the ability of cloud computing to appeal to both the feelings of potential customers and the reality of the security risks of cloud computing in a way that customers will feel safe and secure to use it.

In order to build trust, cloud computing trust models need to be able to address the different challenges that are raised by cloud computing.

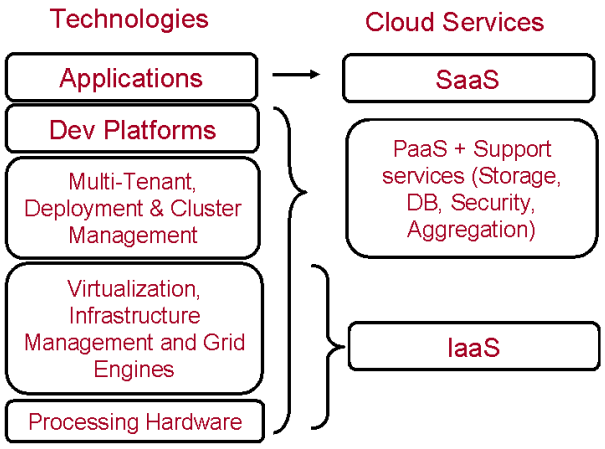
This address should be as holistic as possible covering the different aspects of cloud computing. This means the trust model should address the different challenges raised in the different deployment and delivery models and provide a way for both customers and service providers to evaluate the trust level offered.

A number of models exist that try to address the challenge in building trust between customer and cloud service providers.

TECHNOLOGIES AND CLOUD ENVIRONMENTS

Here we have to understand that, however the term when we are talking about cloud computing it one type of encompasses a different variety of services and latest technologies should need-based services are a different type of antonyms models also have different communication models.

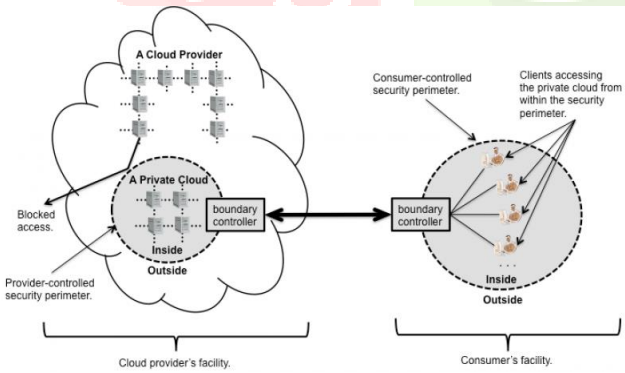
The technologies and cloud environments are describes into different cloud systems and it can be categories into the various significant scenarios, the scenario or issues related cloud in such as scalable and cloud characteristic.



There is considerable uncertainty about cloud computing, notably the difference between on-demand, demand (IaaS, basic service as a service) between cloud-based services (software such as SaaS, service software) and computer infrastructure.

As per described in the NIST definition, the cloud is a collection of connected resources more specifically known as multi-cloud which can allow accessing computing resources that cloud users can be accessed over a network.

Therefore, the provider assumes responsibility for enforcing the vendor-implemented security and preventing the blending of to achieve a suitable separation power for the subscriber. There may be compromises, for example, the VLAN, VPN, separate network segments, the type of network, and Clusters. This type of scenario which allows clients to be separated into an off-premise cloud.



The Outsourced Private Cloud Computing.

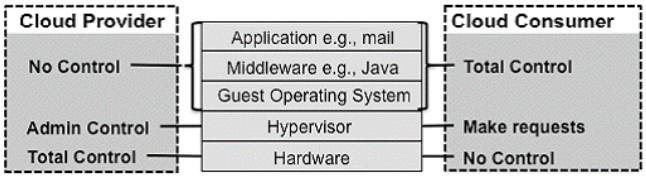
In addition, general criteria for the outsourced private scenario can apply and this also allows a paged privacy scenario to provide more detailed evidence of unanimity. When outsourcing private scenarios, participants need to be able to provide a unique protection and network to build reliable communication links. Although network dependency does not seem avoidable, in this scenario the impact on network dependency can be improved at a negotiated price.

Outsourced locations are not visible to customers in general, the outsourced private cloud needs to manage the resources of hardware and migrate to cloud-workloads between machines without bothering customers and having deliberately to migrate. When outsourced, the Private Cloud provides the scenario, which controls the workload and locations partially in part, to the subscribers and the organization. Can you assume that the provider should keep the security area with faithfulness and implement, confusion to be coordinated with the participants?

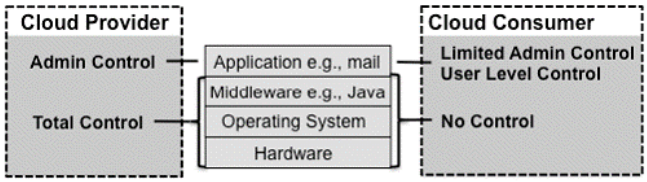
The dependence on the working mechanisms that can be selected for implementing perimeters and the subscriber's based on the different physical location, for example the cluster dies from network segments and the resources that the outsourced from private cloud is assigned to the customers which I do not know.

HOW TO CONTROL RESOURCES IN A CLOUD BY PROVIDER AND USER.

The cloud computing resource controls and key functionality are characterized by the provider and users.



The Cloud Computing Control by the Both Parties in PaaS.
Control: The safely first and for data deleting or disconnecting a network no further action has been taken to reverse the intention of the subscriber (eg, a request by a subscriber for his data should delete and undermined by the user should requested replica).



The Cloud Computing Control by the Both Parties in SaaS.

Visibility: To track the details for the participant's and it's accessible to the servers. Visibility have should in large and own access controls subscribers can calculate resources. This is achieved by breaking down the physical barrier inherent in isolated systems, automating the management of the group of the systems as a single entity.

Cloud Computing can also be described as ultimately virtualized system and a natural evolution of data centers which offer automated systems management. Enterprises need to consider the benefits, drawbacks and the effects of cloud computing on their organizations and usage practices, to make a decision about the adoption and use.

II. PREVIOUSPAPERS STUDY

After previous research, the cloud considered maintaining and calculating user-based resources when servicing third-party external storage and computer systems. This shows that instead of storing the memory on computer memory or the external hard drive as a USB device, the client stores it as an increasingly internet-provided database that can provide the connection. Between the user's computer and the data stores. Resources in the cloud must be configured to work in parallel in this case.

The various uses of computing should be diverse since they can run on a cloud and also use the concept of virtualization. In this earlier study, users connect to the cloud and access their demand-based data and resources. In general, IT resources on the structure are "pay as you go" with multi-tenants. When talking about cloud services like AmazonEC2, Google App Engine, etc., they provide a lot of infrastructures.

We have found that the proposed framework works ensure the overall security of the data during use or deployment or communicate with the users with the users.

The cloud computing mechanism must be multi-faceted when it comes to communicating information or data to different users and provides stability according to the model proposed above and it divided into the following phases.

- The first part is channel transfer and
- The second is based on the authentication information and the data must be stored on the cloud servers.

PREVIOUS RESEARCH STUDY CONCEPT

Here, previous research has described implementation based on the algorithms and mathematical implementation. The details description is described based on the proposed model as mentioned in the based paper.

CO-OPERATE DATA SECURITY IN CALCULATION OF THE CLOUD

The proposed framework has been structured to ensure complete data security throughout the cloud computing process, whether in the cloud or in transit. Therefore, several available mechanisms and techniques are used to protect critical information from unauthorized parties. The proposed framework is divided into two phases.

The first phase deals with the process of transferring and securely storing data in the cloud and the second phase will focus on data recovery from the cloud, demonstrating the generation of data access requests, dual authentication, digital signature verification, and integrity, providing the authorized user with data on the passage of all security mechanisms.

HOW ALGORITHM WORK AND IMPLEMENT

1. Input: Data, protection section, D [] array of n integer size.

   Where D [ ] array consisting of C, I, A, SR, R of n integer size.

2. Output: Categorized data for corresponding section.
3. For i=1 to n

   C [i] = Value of Confidentiality.

   I [i] = Value of Integrity.

   A [i] = Value of Availability.

   Calculate SR [i] = (C[i] + (1/A[i])*10+I[i])/2

4. For j=1 to 10

   For i=1 to n

   IF SR[i] == 1||2||3 then

   S[i] = 3

   IF SR[i] == 4||5||6 then

   S[i] = 2

   IF SR[i] == 8||9||10 then

   S[i] = 1

In the above algorithm, the main task of the owner is to categorize the data based on cryptographic parameters over: C, I, and A. Here, D [] represents the data and the user must specify the values of C, I, and A. After applying the proposed formula as stated above, the sensitivity value (SR) is calculated.

III. PROPOSEDAPPROACH

In the world of information technology or any fields have some limitations and challenges but how to resolve that is the challenge for the researcher, here we are trying to resolve some limitations for the cloud computing. The main objective of the research goal is to explore key strategic issues related to the adoption of cloud computing based on the resources such as Servers, Processing units for the computing processes for on demand.

Cloud computing has become a household name and is often used to refer to different technologies, services, and concepts. In addition, it is associated with virtualized infrastructure or on-demand hardware needs, utility computing, outsourcing, platform and software as a service,

and many other things that are now at work which is centre of various computer industries. Here, the cloud is another type of parallel and distributed system that consists of a collection of interconnected and virtualized computers that are dynamically deployed and presented as one or more unified IT resources based on service level agreements and established through negotiation the service provider and the consumers.

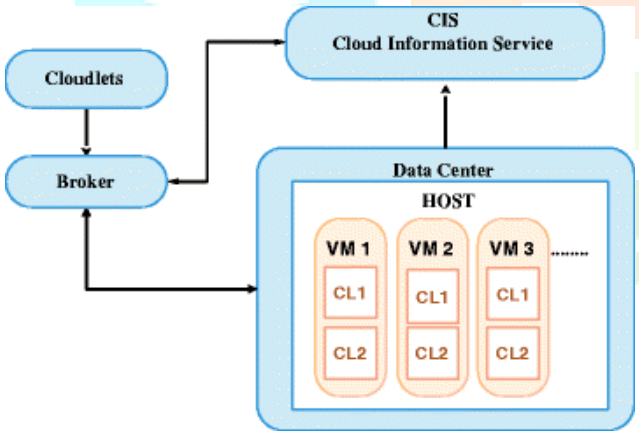
Cloud computing is a model that provides the user with ubiquitous, convenient and on-demand network access and a common pool of configurable computing resources such as networks, servers, storage, applications and services, and more. With a minimum of administrative effort or interaction with the service provider.

Dividing encrypted data is allowed and data storage is enabled.

Here, the initialization can be started with the two parameters, which have two groups based on the channel:

EXECUTIONS EXPERIMENTS

It makes it possible to study the assignment of policies and VM migrations, which makes its use very useful to many researchers.



The Cloudsim Execution Approach.

1. Data centres (DC): the resource provider—includes one or more hosts.

2. Host: the physical machine that allocates one or more VMs.

3. Virtual machine (VM): machines on which the cloudlet will be executed.

4. Cloud Information Service (CIS): responsible for registering all resources of data centres.

5. Broker: when a agent has the DC characteristics, and it will submit VMs to the specific host in the specific DC then allocate the cloudlets-tasks should to specific VMs. in last the agent will destroy the free VMs after complete execution of all the cloudlets.

6. Cloudlets: Into the CloudSim, the cloudlets should are all tasks and applications that should executed on VMs.

Each different type exercitation of simulation in CloudSim for that follows the basic steps in java code from configuration to simulation. These are as follows:

1. Setting the number of users for a current simulation.
2. Initializing the simulation by instantiating the common variables (current time, trace flag, number of users).
3. Creating CIS instance.
4. Creating data centre instance and then registering it with CIS.
5. Creating physical machines (hosts) with their characteristics.
6. Creating data centre broker instance.
7. Creating VMs with their characteristics.
8. Submitting VMs to data centre broker.
9. Creating cloudlets and specifying their characteristics.
10. Submitting cloudlets to data centre broker.
11. Sending a call to start the simulation once there is an event to be executed.
12. Sending a call to stop the simulation once there is no event to be executed.
13. Printing the results of the simulation.

CIS records all data centre resources before they are used, with each data centre containing one or more hosts. Each host assigns one or more virtual machines that run cloudlets, while the broker is responsible for sending cloudlets to specific data centres. Power consumption in CloudSim is described by a linear relationship between power consumption and CPU utilization.

Therefore, CloudSim offers several performance models such as Power Model Sqrt, Linear Power Model, Power Model Square, and Power Model Cubic, all based on the linear relationship between power consumption and CPU utilization. Despite its advantages, CloudSim still has its limitations, such as the lack of a graphical interface. CloudSim is unable to produce results in a graphical format.

ALGORITHM IMPLEMENATION & RESULT

The below research implementation has been done first one is on multi-cloud and second one is on replication as described below.

6.1.1. THE MULTI CLOUD COMPUTING ALGORITHM IMPLEMENTATION STEPS

1. First step: Initialize the CloudSim library
   1.1. Number of users
   1.2. Calendar
   1.3. Trace flag
2. Second step: Create Datacentres Resources
   2.1. Create a Power Datacentre:

1. We need to create a list to store our machine

2. A Machine contains one or more PEs or CPUs/Cores.

In this example, it will have only one core.

3. Create PEs and add these into a list. Need to store Pe id and MIPS Rating

4. Create Host with its id and list of PEs and add them to the

List of machines
Host memory: 2048 (MB)
Host storage: 1000000kb
Band width: 10000kb

5. Create a Datacentre Characteristics object that stores the properties of a data centre: architecture, OS, list of Machines, allocation policy: time- or space-shared, time

Zone.
System architecture: x86
Operating system: Linux
Virtual machine: Xen
Time zone this resource located: 10.0

6. Finally, we need to create a Network Datacentre object.

3. Third step: Create Broker
4. Fourth step: Broker set link to datacentres
5. Fifth step: Create one Cloudlet
   5.1. Submit virtual machine list to the broker
6. Sixth step: Starts the simulation
7. Seven step: Print the results

THE MULTI CLOUD COMPUTING SIMULATION RESULT

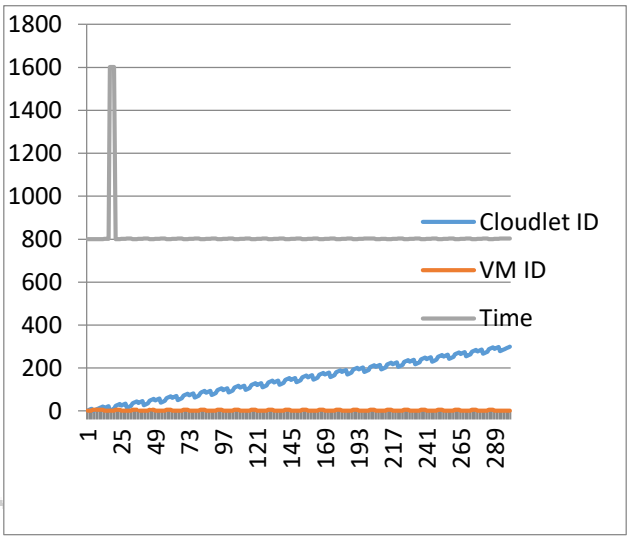
Below figure shows the multi cloud simulation of users (app0...99) they are utilizing the same data centre with their resource like virtual machine etc. this results is the simulation produced by CloudSim.

```
app89
app90
app91
app92
app93
app94
app95
app96
app97
app98
app99

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID    Time    Start Time    Finish Time
     1         SUCCESS          2            1       800        0           800
     4         SUCCESS          2            1       800        0           800
     7         SUCCESS          2            1       800        0           800
    10         SUCCESS          2            1       800        0           800
     0         SUCCESS          2            6       800        0           800
     3         SUCCESS          2            6       800        0           800
     6         SUCCESS          2            6       800        0           800
     9         SUCCESS          2            6       800        0           800
    12         SUCCESS          2            6       800      800          1600
    15         SUCCESS          2            6       800      800          1600
    18         SUCCESS          2            6       800      800          1600
    21         SUCCESS          2            6       800      800          1600
    13         SUCCESS          2            1       801      800          1601
    16         SUCCESS          2            1       801      800          1601
    19         SUCCESS          2            1       801      800          1601
    22         SUCCESS          2            1       801      800          1601
     2         SUCCESS          2            2      1601        0          1601
     5         SUCCESS          2            2      1601        0          1601
     8         SUCCESS          2            2      1601        0          1601
    11         SUCCESS          2            2      1601        0          1601
    24         SUCCESS          2            6       800     1600          2400
    27         SUCCESS          2            6       800     1600          2400
    30         SUCCESS          2            6       800     1600          2400
    33         SUCCESS          2            6       800     1600          2400
    25         SUCCESS          2            1       801     1601          2402
```

The Multi-Cloud Computing Simulation Result.

Here in a fig the cloudlet response time on that we can conclude the when number of cloudlet required the cloud server the server of the multi cloud should consuming time as demand is increasing with the limit virtual machine.



The Cloudlet Response Time for the Multi-Cloud Computing.

IV. CONCLUSION

This study examined two important topics in cloud computing. First, we implemented a proposed structure based on the problem of establishing a multi-cloud link sharing mechanism and transferring the same copy of data to another cloud-based server resource that consumers share as needed.

The second is the multi-cloud. In this study, we implemented a proposed structure to replicate servers and their data for or as needed.

This is a very important day when a large number of servers are needed and you have access to a number of resources that may not be available on the same site or server.

And based on the cloud computing structure, it is also available on demand without wasting much time and at some point, it can be moved to the site or site (known as a

replica). Availability because resources and backup are needed.

Although this study is successful in answering the main research question and bringing new knowledge to professionals and the scientific community, it is important to highlight the limitations that have limited the research process and the limited results.

Time, budget, geographic scope, data protection and the small number of companies that have already implemented cloud computing have shaped the level of detail of these research findings.

However, consistency with applied research methods adds credibility and enriches the knowledge and knowledge generated in this study.

V. SUGGESTION & FUTURE POTENTIALS

For future potentials, this search, when creating a replica, should create all the data for the information the user should create on a different server. This research is limit to configured same resources.

Other future potentials are that this research is also possible with the merger of various multi-cloud networks.

In this search for future potential, power adaptation to Green Cloud Computing concepts can be used.

VI. REFERENCES

[1]. Z. Mahmood, "Data location and security issues in cloud computing," in Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on, pp. 49–54, IEEE, 2011.

[2]. Ronald Petrlic, Christoph Sorge, "Privacy-Preserving DRM for Cloud Computing", 26th International Conference on Advanced Information Networking and Applications Workshops-2012.

[3]. Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013

[4]. Nancy J. King, V.T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud", computer law & security review28(2012)308e319

[5]. Abhishek Mohta ,Ravi Kant Sahu,Lalit Kumar Awasthi, "Robust Data Security for Cloud while using Third Party Auditor",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 2, February 2012

[6]. Ronnie D. Caytiles and Sunguk Lee, "Security Considerations for Public Mobile Cloud Computing ", international Journal of Advanced Science and Technology Vol. 44, July, 2012

[7]. Kangchan Lee, "Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012

[8]. Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, "Towards secure mobile cloud computing: A survey", Contents lists available at SciVerseScienceDirect Future Generation Computer Systems

[9]. Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Cloud Computing Date of Publication: April-June 2012 Volume: 5 , Issue: 2

[10]. M. K. F. H. Judith Hurwitz, Robin Bloor, "Cloud computing for dummies," http://www.dummies.com/how-to/content/ cloud-computing-standards-organizations.html.

[11]. J. Han, W. Susilo, and Y. Mu, "Identity-based data storage in cloud computing," Future Generation Computer Systems, vol. 29, no. 3, pp. 673–681, 2013.

[12]. L. M. Kaufman, "Data security in the world of cloud computing," Security & Privacy, IEEE, vol. 7, no. 4, pp. 61–64, 2009.

[13]. C. Cachin, I. Keidar, and A. Shraer, "Trusting the cloud," AcmSigact News, vol. 40, no. 2, pp. 81–86, 2009.

[14]. P. Kumar and H. S. Arri, "Data location in cloud computing," International Journal for Science and Emerging Technologies with Latest Trends, vol. 5, no. 1, pp. 24–27, 2013.