IEN: - **Batch: -**

Name of the Student: - **Div.: -**

Date of Performance: -

Course Outcome: - L 605.1:

EXPERIMENT NO.: - 01

Aim: Study of NIST (National Institute of Standard & Technology) model of Cloud Computing .

(Understand deployment models , Service models, Advantages of Cloud Computing)

System Software/ Instruments/ Equipment's Requirements: -

Theory/ Working Principle:

The term **Cloud** refers to a **Network** or **Internet.** In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN.

Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

What is Cloud Computing?

Cloud Computing refers to **manipulating, configuring,** and **accessing** the hardware and software resources remotely. It offers online data storage(Google drive), infrastructure, and application (facebook,DTE,.

Cloud computing offers **platform independency,** as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications **mobile** and **collaborative.**

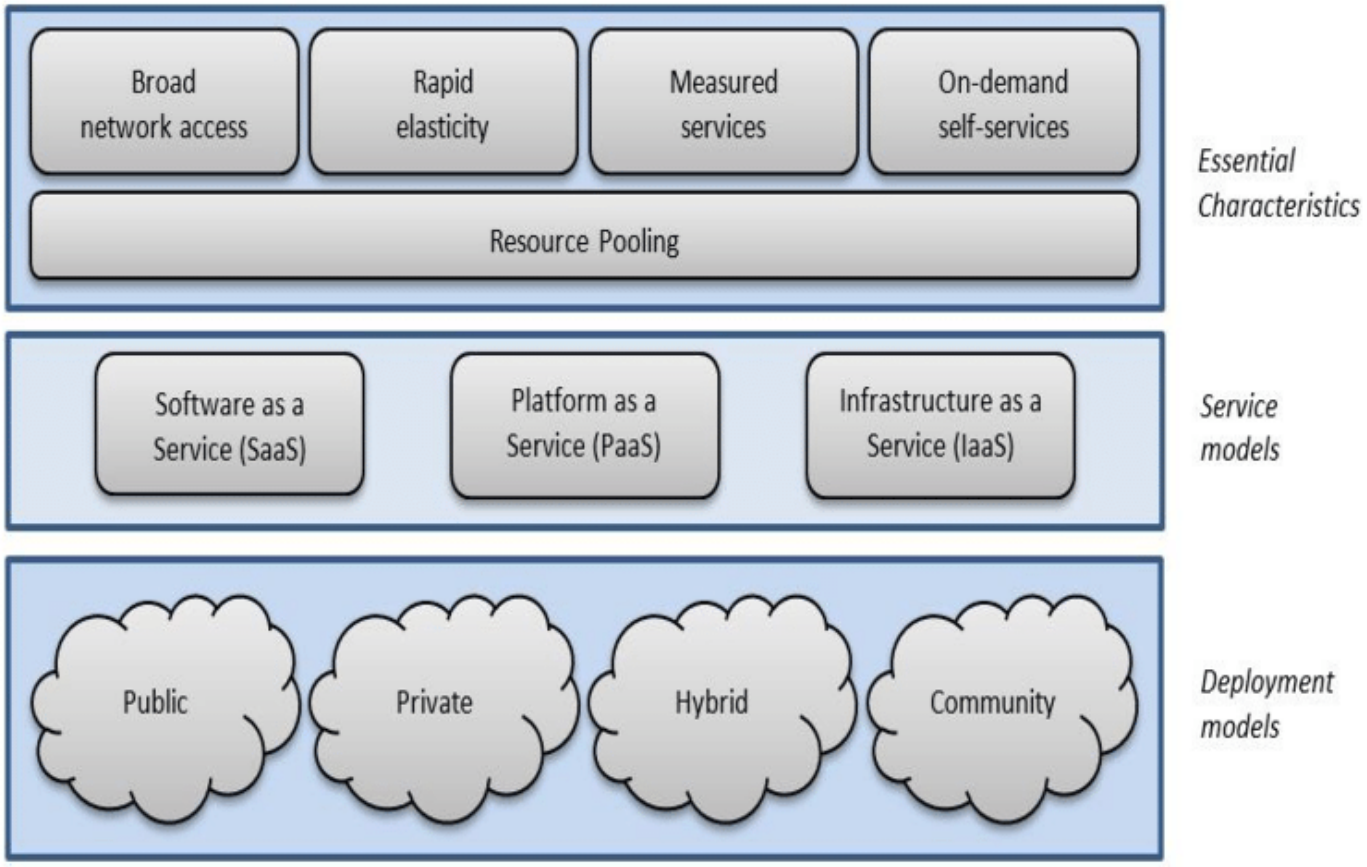
Features of cloud

On demand self service (24 X 7) – This feature enables the consumer in using the services as and when required without any interaction with the provider.

Resource pooling – This feature allows the service provider to provide its services through a multi tenant model. Resources, both virtual as well as physical, are assigned or reassigned as per the demands of the consumer.

Measured service – In this feature, the aspects of cloud service are monitored as well as controlled by the service provider. This helps in billing, resource optimization, access control and capacity planning.

Rapid Elasticity – Cloud computing has the ability of scaling the resources both ways as per the need and for the consumers, cloud is infinite and one can buy the computing power as per the need.



NIST MODEL

Types of cloud

PUBLIC CLOUD

The **public cloud** allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.

Example : Amazon Web Service, Microsoft Azure.

PRIVATE CLOUD

The **private cloud** allows systems and services to be accessible within an organization. It is more secured because of its private nature.

Example: College facilities

COMMUNITY CLOUD

The **community cloud** allows systems and services to be accessible by a group of organizations.

Example: facebook

HYBRID CLOUD

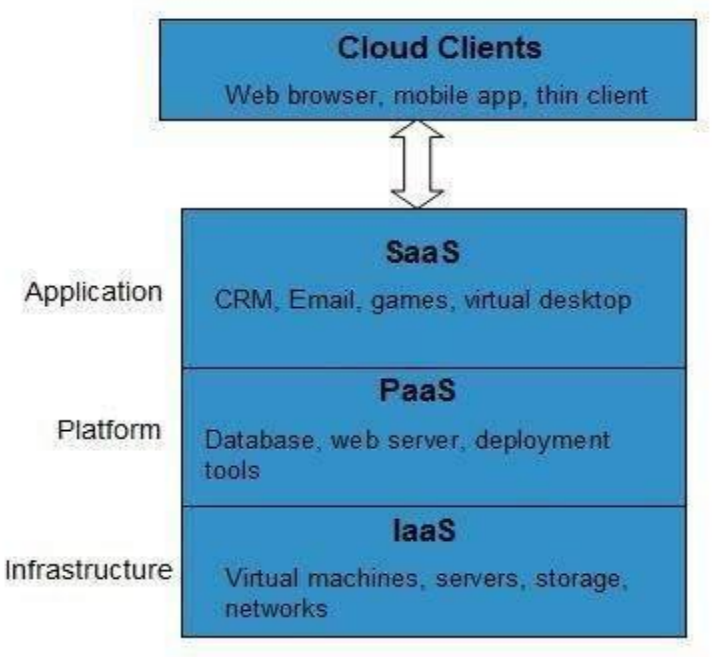
The **hybrid cloud** is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Infrastructure-as-a-Service (IaaS) is the most basic level of service. Each of the service models inherit the security and management mechanism from the underlying model, as shown in the following diagram:



Architecture of Cloud

INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

Eg- Amazon EC2

PLATFORM-AS-A-SERVICE (PAAS)

PaaS provides the runtime environment for applications, development and deployment tools, etc.

E.g.- Azure

SOFTWARE-AS-A-SERVICE (SAAS)

SaaS model allows to use software applications as a service to end-users.

E.g.- Owncloud, Amazon S3

What is Cloud Cube Model – 4 Dimensions & Cloud Layers

Cloud Cube Model, designed and developed by Jericho forum. Which helps to categorize the cloud network based on the four-dimensional factor:

1.Internal/External (Physical Loacation of Data)

2. Proprietary/Open(Ownership)

3. De-Perimeterized/Perimeterized(Security Range)

4.Insourced/Outsourced.

What is Cloud Cube Model?

Cloud Cube model, helps to categorize the cloud network based on the four-dimensional factor. Their main focus is to protect and secure the cloud network. This cloud cube model helps to select cloud formation for secure collaboration.

This model helps IT managers, organizations, and business leaders by providing the secure and protected network.

Security is an important concern for cloud customers and most of the cloud providers understand it. The customer should also keep in mind, the selected cloud formation meets the regulatory and location requirements.

They should also keep in mind that if cloud providers stop providing the services, where else they can move. There are three service models, which include:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

In addition, there are four deployment models such as:

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

These models are very flexible Agile and responsible. They are user-friendly and provide many benefits to the customers.

How to Secure Data in the Cloud Cube Model?

There are some steps and points to keep in mind before securing your data in a cloud cube model:

- Step 1

The classification of the data, the customer should know what rules must be applied to protect it.

- Step 2

It should be ensured, the data exist only in specific trust levels.

- Step 3

It should check that what regulatory compliance and restrictions are applicable. For example, the data should stay in a particular boundary and whether it has to stay in the safe harbour or not.

After the data is classified and is ready to put in the required zone, the assigned person is in a position to decide the following factors-

- The data and processes, which are to be moved in the cloud.
- At what level the user wants to operate in the cloud. It can be infrastructure, platform, software, or platform as a service.
- The cloud formations, which are mostly compatible as per the requirement.
- The level of operation in the cloud can be different as per the requirement.

After that, there are forms of cloud and the user can store the data which is mostly compatible with the company.

Dimensions of Cloud Cube Model

Cloud Cube model has four dimensions to categorized cloud formations:

- Internal/External (Physical Loacation of Data)
- Proprietary/Open(Ownership)
- De-Perimeterized/Perimeterized(Security Range)

- Insourced/Outsourced.

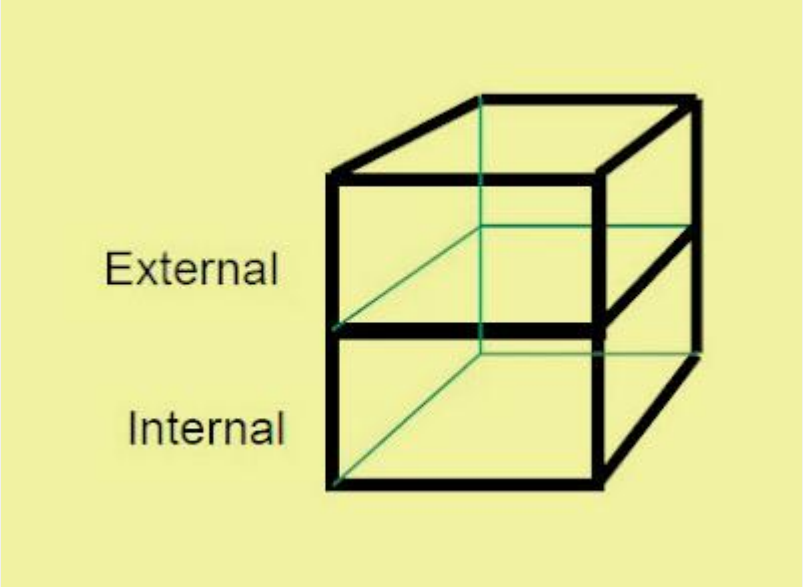
i. Internal/External (Physical Location of Data)

First type of cloud formation is Internal and External

Internal:- Resources are hosted in your own physical Boundaries

External :- Resource are hosted outside your Physical Boundaries

Here, the data which is stored using a private cloud deployment will be considered internal and data outside the cloud will be considered external.



Cloud Cube Model – External/Internal

ii. Proprietary/Open (Ownership)

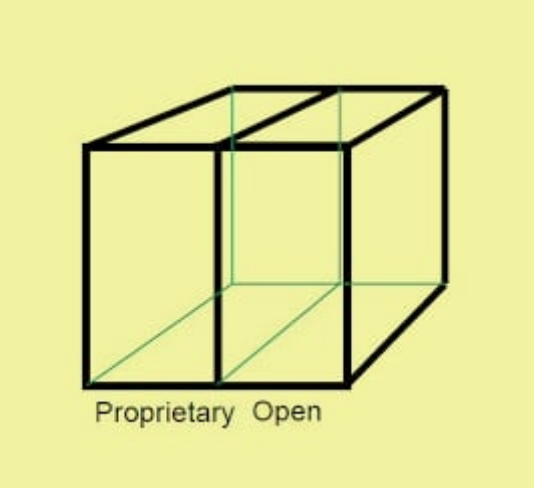
The second type of cloud formation is proprietary and open.

proprietary or open dimension states about the state of ownership of the cloud technology and interfaces.

It also tells the degree of **interoperability,** while enabling data transportability between the system and other cloud forms.

The **proprietary dimension** means, that the organization providing the service is securing and protecting the data under their ownership.

The **open dimension** is using a technology in which there are more suppliers. Moreover, the user is not constrained in being able to share the data and collaborate with selected partners using the open technology.



Cloud Cube Model – Proprietary/Open

iii. De-Perimeterized/Perimeterized(Security Range)

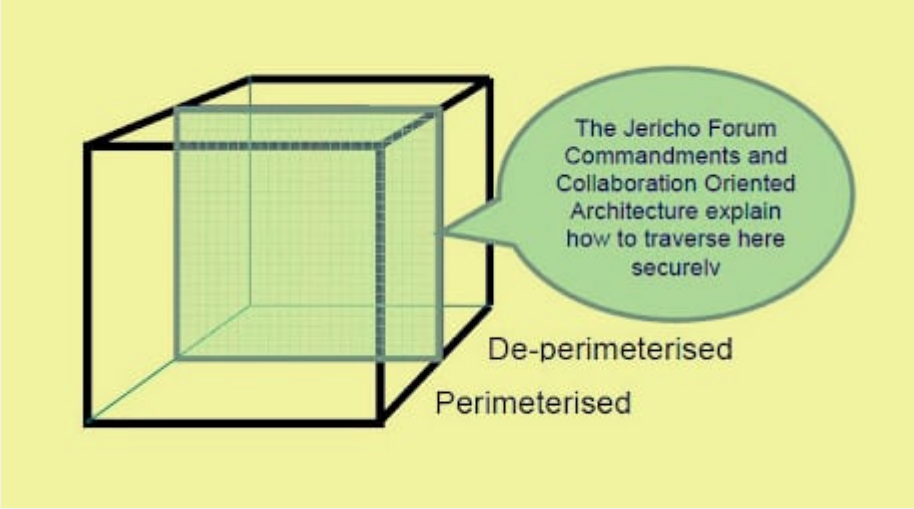
The third type of cloud formation is De-perimeterized and Perimeterized.

The Perimeterised and De-perimeterized dimension tells us whether you are operating inside your traditional it mindset or outside it.

Perimeterized dimension means, continuing to operate within the traditional it boundary, orphan signaled by network firewalls.(Is inside Traditional IT boundaries)

With the help of VPN and operation of the virtual server in your own IP domain, the user can extend the organizations perimeter into external Cloud Computing domain. This means that the user is making use of the own services to control access.

De-perimeterized dimension means the system perimeter is architected on the principles outlined in the Jericho forums commandments. In De-perimeterized dimension, the data will be encapsulated with metadata and mechanisms, which will further help to protect the data and limit the inappropriate usage.(Is outside Traditional IT boundaries)



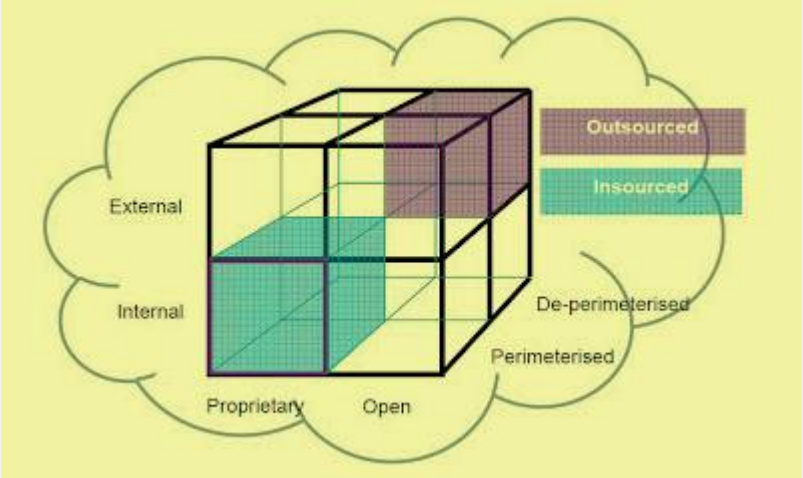
Cloud Cube Model – De-Perimeterized/Perimeterized

iv. Insourced/Outsourced

The Insourced and outsourced dimensions have two states in each of the eight cloud forms. In the *outsourced dimension* the services provided by the third party, whereas in the *insourced dimension* the services provided by the own staff under the control.

In this few organizations that are traditional bandwidth software or hardware, providers will run fluently on becoming cloud service providers.

The organizations which are seeking to procedure cloud services must have the ability to set legally binding collaboration agreement. In this, an organization should ensure that data is deleted from the service provider's Infrastructure.



Insourced/Outsourced Dimension

Questions For Cloud Cube Model

The Jericho forum states that there are three key questions, which a customer should ask their Cloud Computing supplier. So, that they must be aware that the data is secure and protected. The three questions are-

Q 1. Wherein the cloud cube model is the cloud supplier operating while providing the services?

Q 2. How will the clouds suppliers get a surety when the customer is using services in a cloud from that has maintained the features as per the expectations?

Q 3. How can a customer ensure that the data which is stored in the cloud services will be available at the time of mishappenings such as bankruptcy or change in business direction?

Summary of Cloud Cube Model

One of the *major factors in the cloud cube model is encryption and key management*, which provides the confidentiality and integrity of the model. *Strong encryption* provides the data (lost or stolen). This model helps to select cloud formation for security corporations.

Moreover, it benefits its managers and business tycoons by providing a secure and safe environment. The main aim of designing a cloud cube model is to let the users know that the traditional notion of network rangers and its boundary with network firewall is no longer applicable in cloud computing.

Conclusion:

Experiment Rubric:

Evaluation Criteria	Marks	Signature of Instructor with Date
Lab Performance		
Topic Knowledge		
Task Conclusion		
Attainment Level (Out of 3)		