

Internet of Things

Assignment - 4

① Private Cloud.

Private cloud provides computing services within the organizations. Private network and selected other users.

→ In this cloud model all the hardware, software, datacenter, employees, infrastructure, etc. etc. - are maintained, monitored and installed by the organization.

→ This particular deployment model can be chosen whenever confidentiality matters the most.

→ A private cloud is like a single tenant in which the network is handled by the in-house team. here data of single enterprise stored.

→ It supports activity performed over the private network or internet.

→ Scalability is limited, reliability is high.

→ It is expensive and loves devoted servers.

→ The performance is high in a private cloud.

Public Cloud

→ The cloud resources are owned and managed by a third party cloud service provider.

→ Pay as per usage approach makes it most cost effective model.

→ It is like multi-tenant in which the network is managed by your service provider.

→ Here data of several enterprises is stored.

→ It supports activity performed over the public network or Internet.

→ The scalability is high & reliability is moderate.

→ The security depends on service provider.

→ Performance is low to medium.

→ It covers the shared servers.

Advantages & disadvantages of public cloud deployment

Advantages :-

1. Cost effective, faster delivery, cost reduction.

2. Inexpensive model, no need to invest in setting up the infrastructure and maintenance.

3. Less technical skill required.

4. Customer support team can be reached on demand.

5. Easily scaled up or scaled down based on requirements.

→ High reliability - availability of network against failures.

Disadvantages :-

→ Security and privacy issues are major challenges.

→ Less flexibility and controls.

② Challenges of IoT with cloud:-

1. Privacy and security :-

Security is a major concern in the field of IoT. Valuable and confidential data goes into cloud, outside the firewall. The moment the firewall is crossed, this data becomes hackable. There is a possibility that this data could be monitored without informing user.

Solutions:-

- Periodic monitoring of network activities.
- Select private cloud if data is confidential.
- To reduce risk of being exposed, use recognized activities of antivirus solutions.
- Before signing the contract with a cloud service provider, it is necessary to read & understand regulations involved in services being provided.

2. Bandwidth Cost

It is one of challenges because of continuous data transferring from IoT devices and great losses.

→ IoT is all about data and huge investment in storage is needed.

→ cloud computing is preferred for storage and processing in IoT.

→ small-scale IoT application demanding lesser resources. But if application is data concentrated, then investment in band width would be considerable.

3. Migrations and Portability → when data to be moved or migrate from the cloud, we have to take care of following:-

→ How easy & safe is it to move data?

→ what is strategy to migrate data to the cloud?

→ will it be easy to select a

out of the cloud and take data

back to the infrastructure?

→ How much would it cost?

→ would there be support offered
to migrate smoothly to another

Cloud Service provider?

→ All these challenges are doubled
with IoT as the data comes
from the various sensory nodes
at a very high speed.

↳ Availability, Reliability and Robustness

→ Continuous monitoring and reading
of the data need tools having
continuous (cloud service availability
is about IoT).

→ In downtime, it would miss
critical data so reliability of process
has to be monitored.

→ The process should be robust
towards handling data at
different rates.

* Data could be flooded or stored at any time, in the both situations, it should be handled effortlessly.

5. Costing:

It is main advantages of cloud, is that it can scale up with rising demand while it is scalable and flexible, an organisation should plan its budget carefully.

6. Wrong Selection

without having clear vision & planning it may lead to unnecessary cost.

7. Data ownership:

* The data stored by user on the cloud is owned by the user.

* This means that the data is under the ownership of person who generates it.

* However, when opting for cloud storage, the data is under custody of service provider.

→ Then, it appears that service provider owns the dataset generated with IOT → which it comes to IoT, data is generated at multiple points and ownership could lie with multiple Participating Parties.

→ Hence in IOT the ownership related challenges are multiplied.

4. Expertise :-

→ The use of cloud with IOT requires a specific skill set. The cloud platform gets updated every now and then and so experts have to constantly upgrade themselves.

→ When IOT and cloud comes together then it will be more challenging.

→ To understand sensors and at a same time, to be updated on cloud development is a challenging task.

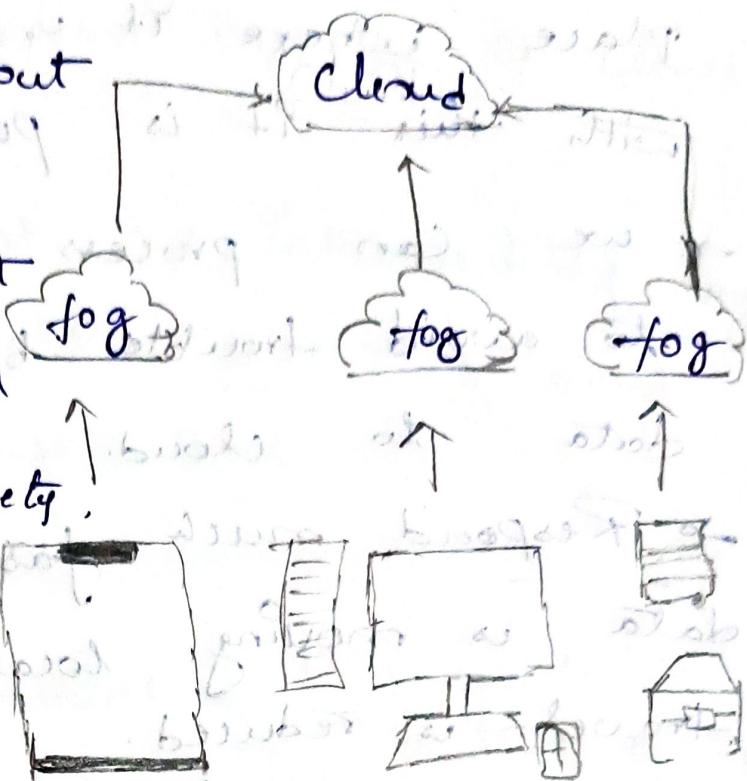
③ Fog Computing

IoT is all about the data.

The factors that affect data are all

the four V's - Variety,

Velocity, Velocity & Volume.



- + All IoT applications require instant analysis and action.
- + Most of time, the action would be connective in nature, it would be business critical.
- + In case, the data volume is high and it reaches cloud after some delay. So we may lost the opportunity to use the data.
- + In such cases, fog computing serves the solution.

- The most sensitive data could be analysed in the area closer to the place where it is generated. With this it is possible.
- we can process data locally and to avoid trouble by not sending data to cloud.
- Respond much faster because of data is moving locally so data travel is reduced.
- It will process data in milliseconds.
- Required data will be sent to cloud.
- After analysis data stored is pushed on to the cloud.
- Sensors/devices generate data transmit through bus very close to the data source.
- There nodes in middle layer are capable of handling the data.

- This requires minimum power & lesser resources.
- All data need not go to cloud at instant.
- Fog is just an intermediary layer for faster data processing and faster response time.

Advantages.

- Minimal amount of data sent to the cloud.
- Reduced bandwidth consumption.
- Reduced data latency.
- Improved data security when limited data goes to cloud. It is easier to protect it.
- Immediate processing of data in real time.

④ Service models of cloud computing:

Cloud is preferred more than expected as, it is affordably effective and efficient for data.

1. Software - as - a - service (SaaS) :-

Complete software applications as a service is provided to the user. It makes the software available over the Internet it refers to, software that is deployed on a hosted service and is accessible via Internet.

SaaS Applications such as CRM applications, helpdesk applications, HR Solutions.

Characteristics:-

- Available on demand.
- The Software is maintained by vendor or rather than where they are running and hence making it cost effective.
- The license to software may be subscription based or usage based and it is billed on recurring basis.

- Scaled up or down on demand.
- Automatically upgraded or updated
- SaaS offers are running the same version of the software.

2. Platform - as - a - service (PaaS)
 Development tools, APIs, libraries etc. will be provided by cloud service providers. Users have to build, manage & maintain the applications. It offers runtime environment.

It has a feature of Point-and-click tools that enables non-developers to create web applications. com platform is example of PaaS

Characteristics:

- PaaS offers a browser-based development environment. It allows developers to create a database and edit application code either via API or point-and-click tools.

- PaaS Provide built-in security, scalability and web service interface.
- PaaS also provides web services interfaces that allow us to connect applications outside the platform.

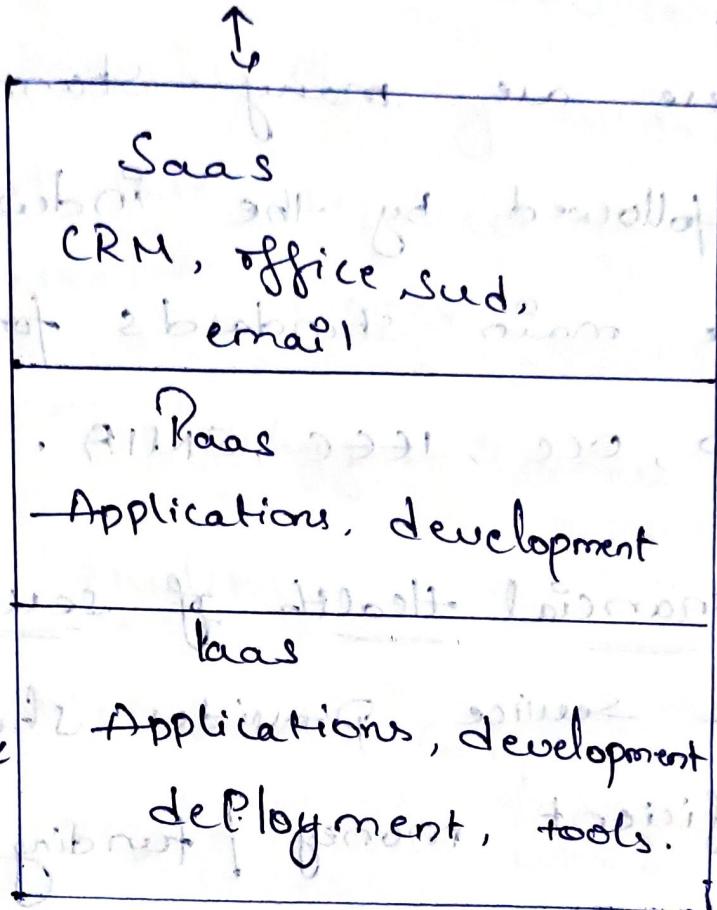
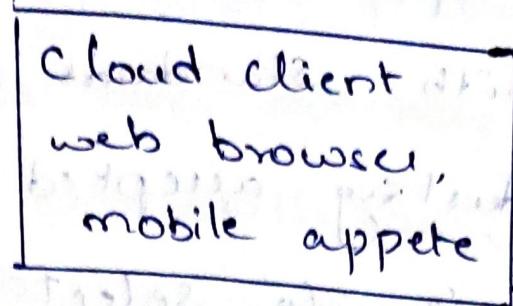
3. Infrastructure - as - a - Service (IaaS) :-

The entire infrastructure will be provided as support. The service is mostly provided as virtual machines (VMs), where the user need not worry about infrastructure at all and they manage the machines. They select the OS and underlying applications. PAAS as you use it with IaaS approach, you can choose VMs over physical machines.

Characteristics :-

- VMs with Pre-installed software
- VMs with Pre-installed OS
- On demand availability of resources.

* the computing resources can be easily scaled up and down.



⑤ Selecting cloud service providers:

There are many parameters and considerations to select the cloud service provider.

1) Certification and standards compliance:

When a product ad here to

Standards that are accepted widely
it is considered as a reliable product.
Similarly, CSPs are also expected to
comply with standards. This compliance
with industry accepted standards is
first criteria to select CSP. Though
there are many standards framed
& followed by the industry, some of
the main standards for cloud are
ISO, OCE, IEEE, SNIA.

2. Financial Health of service providers:

The Service Providers should hold
sufficient money / funding to operate
for a long period. If Service Provider
has a healthy financial status and
history of sustenance, then it is
most unlikely to shut down.

3. Business and Technology strength:-

Having the technical expertise to

sustain and adapt to a clients requirements is a key factor in selecting a CSP. Having just technical skill and strength does not help, the CSP needs business skills as well to sustain. Business skills (includes) growth Planning, financial Planning and other factors that are required to sustain in the market. Hence,

Sustenance = Technology + Business skills

4. Compliance Audit:-

The CSP must validate compliance with the clients requirements, which should be done through a proper third

Party audit. This will enable transparency & Perfect validation.

5. Service level Agreements:-

Service level agreements (SLAs) provide details and information about the services provided and related

Value that a customer gets out of them. They serve as a contract between two parties, they define terms and conditions and also legal aspects of the contract and relationship between two parties.

6. Reporting / Tracking :-

The service provider should be capable of issuing a comprehensive performance report, which also highlights the shortfalls. This will enable the customer to understand the complete situation.

7. Costing and Billing :-

The costing and billing should be transparent and should provide the complete details of the usage. Also, it is expected to be automated with details of complete resource utilization.

should not come as a shock to a customer to see a bill with a huge amount mentioned, without having clarity on the breakup. This means billing should be transparent & for the usage only.

8. Maintenance Monitoring and Upgrade:-

It should be easy and less expensive to migrate to the CPS's environment.

Also, when there is an upgrade, it should be done with care. Any

maintenance should be easy & affordable.

In short, it should be easier to

install, manage, maintain and upgrade.

This upgrade includes: migration from

Private to Public to hybrid cloud, if needed.

9. Support:-

Help and assistance should be provided when required. support should be available based on agreements and a dedicated resource may be needed.

based on complexity of problem also
onsite support may be needed when
Clarifications cannot be offered over
Phone. Thus, Support is major deciding
factor.

10. Security:

There should be defined Policies about
Security that should also be shared
with customer. This includes everything
from access restrictions to customer
data. The data should be safe in
case of a breakdown / failure. The
recovery & Backup options should
be sound. All these require audit
which should be carried out by a
third Party. Security is the prime
concern and cannot be ignored.
Evaluation should start from this
Point.

⑥ Deployment models of Cloud Computing:-
There are three deployment models.

1. Private cloud deployment :-

This is one of the best models, where the data generated is safeguarded without any flaw. This particular deployment model can be opted whenever confidentiality matters the most. This model can be chosen wherever and whenever the IP needs to be protected. When this model is chosen, the complete control of everything is well within the organization for which the deployment is carried out.

The cloud services are typically in the data centres provided by the organization. Hence, everything has to be taken care of by the organization. That owns this deployment. This

model demands that hardware, software, data center, personnel, infrastructure etc.

Cloud deployment models

Private cloud Public cloud Hybrid cloud

be maintained, monitored and installed by the organisation, which makes this model expensive. It offers organisation complete flexibility in terms of deciding & managing the resources:-

- Advantages :-
- Data Security is Paramount in this model & is ensured
- This model is seen as a flexible model compared to others

Disadvantages :-

- Could prove expensive

- Maintenance, Periodic upgradation, etc could be difficult.
- Policies and other related things are to be framed carefully to make sure that the data is safe.

2. Public Cloud deployment:-

This is meant for general public or a large group. The cloud service provider owns all resources, which include hardware infrastructure & software. Cloud service providers will take care of all resources management. Installation, maintenance, Upgradation and monitoring everything comes under the purview of the Service Provider.

Access to this cloud service happens via the Internet. Pay-and-use approach makes it easier for cloud service consumer. Moreover you will get 24x7 customer support for technical & other

related clarifications when you opt for this model.

Advantages :-

→ It is simple where user needs to pay for what he has used. It is also known as Pay - as - You System.

→ You do not need to invest in setting up the hardware or infrastructure when it comes to this approach.

→ Customer support team can be reached on demand and team should try to resolve the challenges.

→ It can be easily scaled up or scaled down based on requirements.

Disadvantages :-

→ Data is not within the walls of the organisation of user.

→ Securing the data while ensuring privacy.

3. Hybrid Cloud deployment :-

As the name suggests, this deployment is a mix of both private and public cloud deployment. In this, the resources offered and managed are both in house and organisation third Party based. Hence and service providers both have control and stake. This offers flexibility to decide what is to be owned by organisation and what can be secured to a great extent. But even then the data is not 100% safe.

Advantages :-

- Both organisations & third Party come together.
- Not as expensive as private cloud deployment.
- flexible and controlled access can be given.

Disadvantages:-

- The service being opted for is shared with other users. Hence, there is higher chance that data may be unsafe.
- The data could be vulnerable to attacks as well.