Name : Hemant Tiwari

Student Id : 2022MT93184

Stream : M. Tech. in Software Engineering

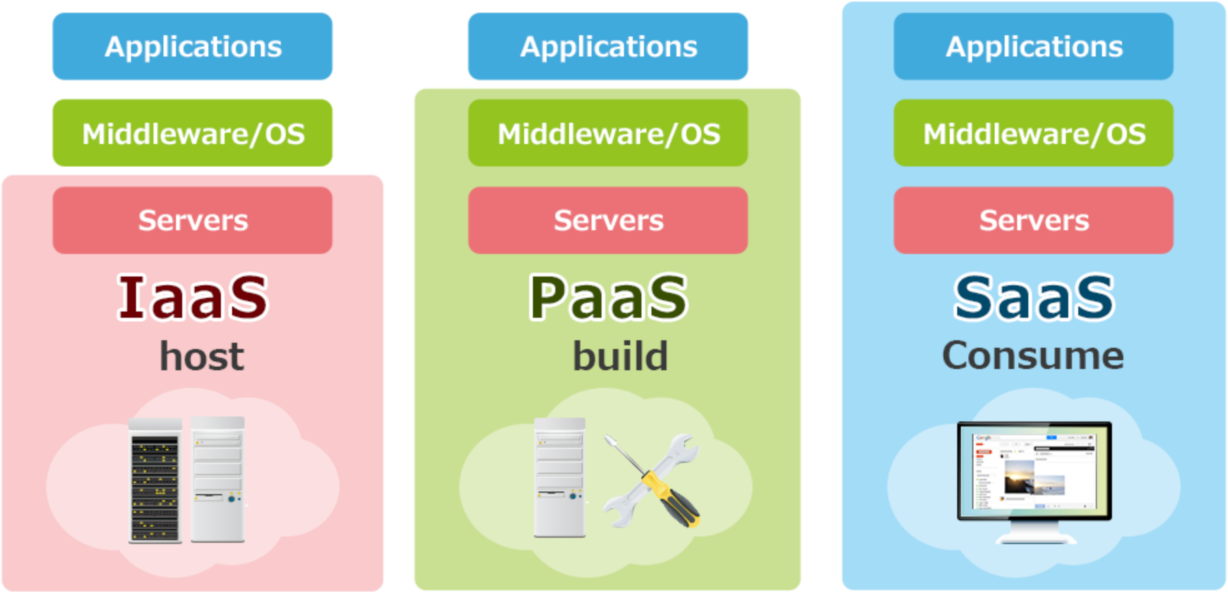
Subject : Assignment of Cloud Computing

Table of Contents

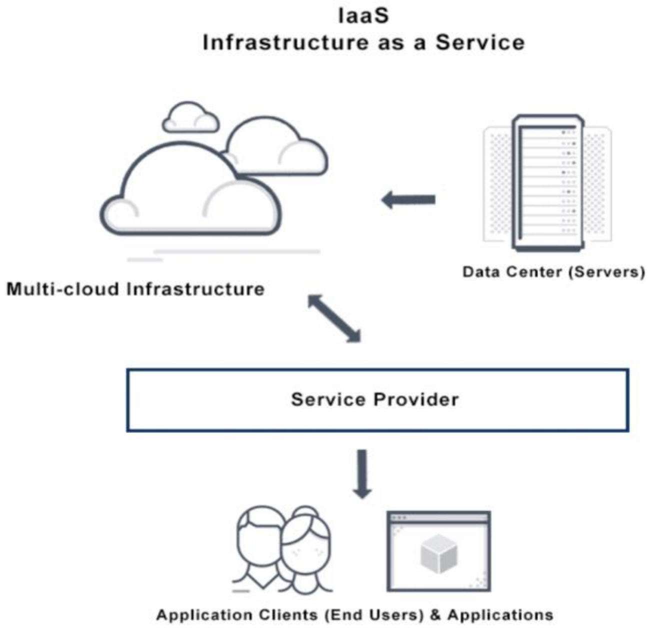
1. Which are the different layers that define cloud architecture?

Answer: There are 3 different layers of cloud computing –

1. IAAS (Infrastructure As A Service),
2. PAAS (Platform As A Service), and
3. SAAS (Software As A Service)



IAAS – Offering virtualized resources (computation, storage, and communication) on demand is known as Infrastructure As A Service (IAAS). A cloud infrastructure enables on-demand provisioning of servers running several choices of operating systems and a customized software stack. Infrastructure services are considered to be the bottom layer of cloud computing systems . The IAAS model is about providing compute and storage resources As A Service. According to NIST, IAAS is defined as: *“The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).”*


IaaS
Infrastructure as a Service
Multi-cloud Infrastructure
Data Center (Servers)
Service Provider
Application Clients (End Users) & Applications

The user of IAAS has single ownership of the hardware infrastructure allotted to him (may be a virtual machine) and can use it as if it is his own machine on a remote network and he has control over the operating system and software on it.

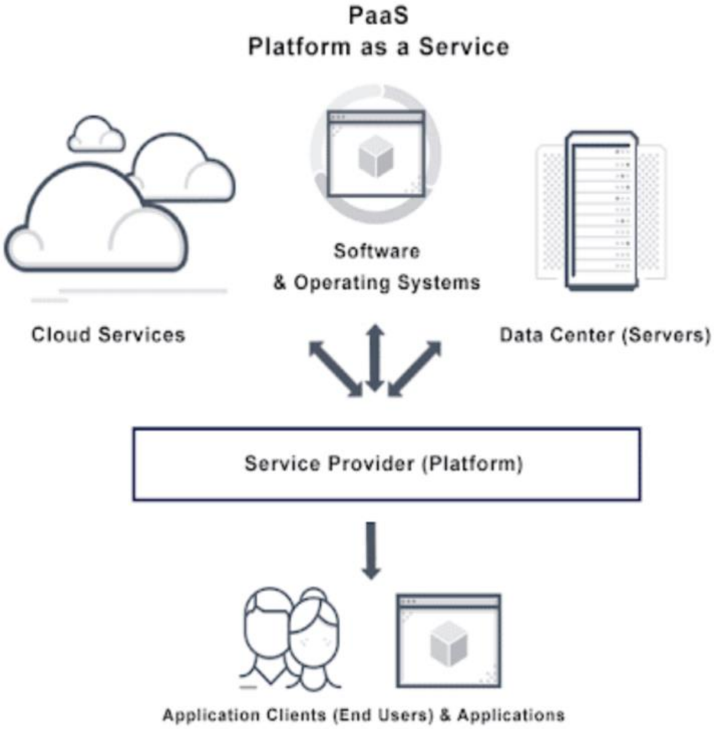
The IAAS provider has control over the actual hardware and the cloud user can request allocation of virtual resources, which are then allocated by the IAAS provider on the hardware (generally without any manual intervention). The cloud user can manage the virtual resources as desired, including installing any desired OS, software and applications. Therefore IAAS is well suited for users who want complete control over the software stack that they run; for example, the user may be using heterogeneous software platforms from different vendors, and they may not like to switch to a PAAS platform where only selected middleware is available. Well-known IAAS platforms include Amazon EC2, Rack space, and Right scale. Additionally, traditional vendors such as HP, IBM and Microsoft offer solutions that can be used to build private IAAS.

Amazon Web Services mainly offers lAAS, which in the case of its EC2 service means offering VMs with a software stack that can be customized similar to how an ordinary physical server would be customized. Users are given privileges to perform numerous activities to the server, such as: starting and stopping it, customizing it by installing software packages, attaching virtual disks to it, and configuring access permissions and firewalls rules.

PAAS : A higher level of abstraction to make a cloud easily programmable, known as Platform As A Service (PAAS). A cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory that applications will be using. In addition, multiple programming models and specialized services (e.g., data access, authentication, and payments) are offered as building blocks to new applications.

The PAAS model is to provide a system stack or platform for application deployment As A Service.

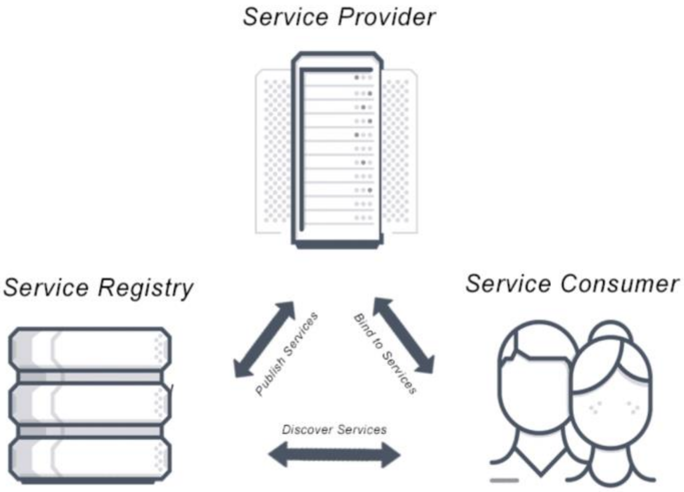
NIST defines PAAS as follows, *"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations."*



The hardware, as well as any mapping of hardware to virtual resources, such as virtual servers, is controlled by the PAAS provider. Additionally, the PAAS provider supports selected middleware, such as a database, web application server, etc. shown in the figure. The cloud user can configure and build on top of this middleware, such as define a new database table in a database. The PAAS provider maps this new table onto their cloud infrastructure. Subsequently, the cloud user can manage the database as needed, and develop applications on top of this database. PAAS platforms are well suited to those cloud users who find that the middleware they are using matches the middleware provided by one of the PAAS vendors. This enables them to focus on the application. Windows Azure, Google App Engine, and Hadoop are some well- known PAAS platforms. As in the case of IAAS, traditional vendors such as HP, IBM and Microsoft offer solutions that can be used to build private PAAS.

SAAS : Applications reside on the top of the cloud stack. Services provided by this layer can be accessed by end users through Web portals. Therefore, consumers are increasingly shifting from locally installed computer programs to on-line software services that offer the same functionally. Traditional desktop applications such as word processing and spreadsheet can now be accessed As A Service in the Web. This model of delivering applications, known as Software As A Service (SAAS), alleviates the burden of software maintenance for customers and simplifies development and testing for providers.

SAAS is about providing the complete application As A Service. SAAS has been defined by NIST as follows, *"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."*



The SAAS provider controls all the layers apart from the application. Users who log in to the SAAS service can both use the application as well as configure the application for their use. For example, users can use Salesforce.com to store their customer data. They can also configure the application, for example, requesting additional space for storage or adding additional fields to the customer data that is already being used. When configuration set- tings are changed, the SAAS infrastructure performs any management tasks needed (such as allocation of additional storage) to support the changed configuration. SAAS platforms are targeted towards users who want to use the application without any software installation (in fact, the motto of Salesforce.com, one of the prominent SAAS vendors, is “No Software”). However, for advanced usage, some small amount of programming or scripting may be necessary to customize the application for usage by the business (for example, adding additional fields to customer data). In fact, SAAS platforms like Salesforce.com allow many of these customizations to be performed without programming, but by specifying business rules that are simple enough for non-programmers to implement. Prominent SAAS applications include Salesforce.com for CRM, Google Docs for document sharing, and web email systems like Gmail, Hotmail, and Yahoo! Mail. IT vendors such as HP and IBM also sell systems that can be configured to set up SAAS in a private cloud; SAP, for example, can be used as an SAAS offering inside an enterprise.

2. What are the security aspects provided with the cloud?

Answer: Security is one of the three major factors quoted by respondents as being inhibiting factors. Verification of the security of data arises as a concern in public clouds, since the data is not being stored by the enterprise. Cloud service providers have attempted to address this problem by acquiring third-party certification.

The cloud consists of a shared infrastructure that can be rapidly configured on demand to meet business needs. At a high level, the cloud infrastructure can be partitioned into a physical infrastructure, and a virtual infrastructure. The security requirements and best practices can also similarly be divided into the requirements for physical security and those for virtual security.

The basic objectives of cloud security are to ensure the confidentiality, integrity and availability of the cloud system. Confidentiality implies that there is no unauthorized access to functions of the cloud system. Integrity requires that the cloud system be protected against tampering (e.g., against implanting of viruses that steal passwords or corruption of data). The availability requirement is that the system should not be made unavailable by, for example, a denial of service attack that puts a great deal of load on the system, preventing legitimate users from using the system. In addition, the above objectives may also be impacted by legal requirements. For example, if the system stores health-related data, certain levels of confidentiality may be legally mandated. Therefore, the cloud system should be able to support the required legal constraints.

Physical security implies that the datacentre the cloud is hosted in should be secure against physical threats. This includes not only attempts at penetration by intruders, but also protection against natural hazards and disasters such as floods, and human error such as switching off the air conditioning. To ensure physical security, a multi-layered system is required. This includes,

- A central monitoring and control centre with dedicated staff
- Monitoring for each possible physical threat, such as intrusion, or natural hazards such as floods.
- Training of the staff in response to threat situations
- Manual or automated back-up systems to help contain threats (e.g., pumps to help contain the damage from floods)

- Secure access to the facility. This requires that the various threats to the datacentre be identified, and appropriate procedures derived for handling these threats.

Virtual Security The following best practices have been found to be very useful in ensuring cloud security.

Cloud Time Service - If all systems in the datacentre are synchronized to the same clock, this is helpful both to ensure correct operation of the systems, as well as to facilitate later analysis of system logs. It is particularly important in correlating events occurring across geographically distributed systems. A common way to do this is by use of the Network Time Protocol (NTP). NTP is a protocol that synchronizes the clock on a computer to a reference source on the Internet. To protect against false reference sources, the protocol messages can be encrypted. Due to the importance of having a common timeline, there should be at least two paths to reliable time sources (such as WWV and GPS), and the time sources should be verifiable.

Identity Management - Identity management is a foundation for achieving confidentiality, integrity and availability. Some of the requirements for identity management are that:

- It should scale to the number of users typically found in a cloud system
- Due to possible heterogeneity in cloud systems, a federated identity management system that allows establishing a single identity and single sign-on across multiple different types of systems may be needed.
- The identity management system should satisfy applicable legal and policy requirements (for example, allow deleting of users across the system within a specified time period)
- Maintain historical records for possible future investigation.

Access Management - The core function of access management is to allow accesses to cloud facilities only to authorized users. However, additional requirements are to:

- Not allow unrestricted access to cloud management personnel
- Allow implementation of multi-factor authentication (e.g., use of a password together with a digital key) for very sensitive operations.

It is also good practice to:

- Disallow shared accounts, such as admin
- Implement white-listing of IP addresses for remote administrative actions.

Break-Glass Procedures - It is desirable for the access management system to allow alarmed break-glass procedures, which bypass normal security controls in emergency situations. The analogy is with breaking the glass to set off a fire alarm. Clearly, it is important to ensure that the break-glass procedure can be executed only in emergencies under controlled situations, and that the procedure triggers an alarm.

Key Management - In a cloud, with shared storage, encryption is a key technology to ensure isolation of access. The cloud infrastructure needs to provide secure facilities for the generation, assignment, revocation, and archiving of keys. It is also necessary to generate procedures for recovering from compromised keys.

Auditing - Auditing is needed for all system and network components. The audit should capture all security-related events, together with data needed to analyse the event such as the time, system on which the event occurred, and user id that initiated the event. The audit log should be centrally maintained and secure. It should be possible to sanitize or produce a stripped-down version of the audit log for sharing with cloud customers, in case their assistance is needed to analyse the logs.

Security Monitoring - This includes an infrastructure to generate alerts when a critical security event has occurred, including a cloud-wide intrusion and anomaly detection system. The intrusion detection systems may be installed both on the network as well as the host nodes. It may also be necessary to allow cloud users to implement their own intrusion and anomaly detection systems.

Security Testing - It is important to test all software for security before deployment in an isolated test bed. Patches to software should also be tested in this environment before being released into production. Additionally, security testing should be carried out on an ongoing basis to identify vulnerabilities in the cloud system. Depending upon the risk assessment, some of these tests may be carried out by third parties. There should also be a remediation process to fix identified vulnerabilities.

3. What is the requirement of virtualization platform in implementing cloud?

Answer: Virtualization is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called virtual machine. Each VM can run its own operating systems and applications as if it were in a physical machine. So It is way to run multiple operating systems on the same hardware at the same time. For e.g., Windows and Linux both can run on the same laptop at the same time.

Virtualization has enabled dealing with infrastructure that cannot be touched and is used to deploy the three major components of cloud computing that include Infrastructure As A Service (IAAS), Platform As A Service (PAAS), and Software As A Service (SAAS).

- Virtualization allows multiple operating system instances to run concurrently on a single computer.
- It is a means of separating hardware from a single operating system.
- Each “guest” OS is managed by a Virtual Machine Monitor (VMM), also known as a hypervisor.
- Because the virtualization system sits between the guest and the hardware, it can control the guests’ use of CPU, memory, and storage, even allowing a guest OS to migrate from one machine to another.
- Instead of purchasing and maintaining an entire computer for one application, each application can be given its own operating system, and all those operating systems can reside on a single piece of hardware.
- Virtualization allows an operator to control a guest operating system’s use of CPU, memory, storage, and other resources, so each guest receives only the resources that it needs.

Certain features of a cloud are essential to enable services that truly represent the cloud computing model and satisfy expectations of consumers, and cloud offerings must be

i. self-service,
ii. per-usage metered and billed,
iii. elastic, and
iv. customizable.

The feature “per-usage metered and billed” is practical only in presence of flexibility and efficiency in the back end. This efficiency is readily available in Virtualized and Machines.

4. Explain what are the different modes of software As A Service (SAAS)?

Answer: Software As A Service (SAAS) is a cloud computing model where a third-party provider offers software applications to consumers over the internet. The services are scalable and can be modified by the users as they find necessary for their business. The SAAS applications can be accessed and used by multiple consumers simultaneously. The users are reduced of the infrastructure costs and the expenses are shared among the multiple users. The main purpose is to share the data resources between multiple users while maintaining data isolation between the users. The services are delivered in two modes.

- **Simple Multi-Tenancy or Cross-Grain Multi-Tenancy:** It is a hosted service model where the users have their own resources that are independent of other users. It is not instantly scalable and users have to be content with low margins due to high competition. The advantage is it is simple and does not require any code modifications.
- **Fine Grain Multi-Tenancy:** This again involves sharing of the same database among multiple users. The data is kept separate although the computing resources are shared. It is easily scalable and offers efficiency in services.

The above described are the two different modes of software As A Service (SAAS) in which the service provider offers the software applications to the customer via the internet. SAAS applications can be effectively handled by multiple users making them the top choice for the companies using software through the cloud.

Both the SAAS modes mentioned above are known for offering the best working environment and thus companies choose them more often. If you are a budding business then going with any mode of SAAS will easily solve your problem and you will not face any issues.

5. Before going for cloud computing platform what are the essential things to be taken in concern by users?

Answer: There are five essential factors to be taken in concern by users before switching to cloud computing platform

1. **Security -** Service providers promise that they can be more secure than physical datacentres. Protection of expertise and assets is a key requirement. Cloud applications need to protect data being transferred over the net. This includes not only encryption of transmission data, but also encryption of stored data. Certificates, such as SAS 70 or ISO 27001, can be good indicators for good security measures. Customers should be aware of the physical location of their data and the available security features. This awareness facilitates a holistic security view of your cloud service provider.

2. **Adaptability -** Heterogeneous usage contexts demand a certain amount of adaptability from a cloud solution. The way of accessing a solution, the platform that is used, and the way users are dealing with the system are diverse and are constantly changing. The latest trend in usage contexts is the transition to mobile computing. People become focused on mobile technologies and have adopted its concepts (for example. app stores, always-on, location-based services, and so on) in their private life. They have the same expectations for their business life. As an IT department, it becomes important to satisfy the demand for mobile technologies. The next generation of business leaders is used to accessing every service with their smartphone and is aware of the competitive advantages of mobile computing.

3. **Integration-** Typical applications rely on data from other applications. The worst case would be to have separate data pools with unsynchronized content, which can lead to redundancy and inconsistency across applications. Data from other applications can enrich cloud services and provide comprehensive insight. In general, most services offer web services interfaces. Some do also provide a REST interface. Complex interfaces require a

tool to handle connectivity and transformation, and manage future challenges. The use of XML as a data format offers the best possibilities to make data handling comfortable.

4. **Migration -** The aspect of integration leads us to the next point: migration. What do you do, if your cloud provider goes out of business? Are you able to migrate your valuable business data to another platform or have you locked-in a particular vendor? These questions should be asked before the decision for a particular provider is made. The longer a cloud service is being used, the more important and valuable are the assets that have been developed. Common standards can help to make your resources reusable. A (potential) migration strategy sustains your possibilities to react on market changes and future innovations.
5. **Scalability -** It is not very common that providers offer information about the scalability of their solution. SAAS and PAAS offerings promise to scale automatically. IAAS offerings might provide additional tools to control scalability. In hybrid cloud environments, scalability becomes very important because the decision to provision new instances must be based on reliable data. Multi-tenancy is essential for most cloud applications to provide reasonable scalability.

6. State the list of a need of virtualization platform in implementing cloud?

Answer: Virtualization is the foundation of cloud computing. It enables creation of an intelligent layer of abstraction to hide the intricacies of the software or hardware that is underlying beneath the layer.

We can list a plethora of platforms such as VMWare that are associated with a technology to provision a private cloud and also to act as a union between private cloud and external cloud. We need to appreciate three vital attributes for creating a private cloud such as management of service level policies, cloud operating system and virtualization. Virtualization separates the back-end level and user level for creation of a seamless environment between the two.

Virtualization is used for deployment of models of cloud hosting services including Software As A Service (SAAS), Platform As A Service (PAAS), and Infrastructure As A Service (IAAS) among others.

Following are the three Important Attributes of Virtualization that Signify its Role in Cloud Computing:

- Partitioning can be used for supporting a multitude of operating systems and applications within a single physical system such as a web server.
- Isolation imparts protection to virtual machines from any events such as virus attacks or crashes in other machines. Additionally, encapsulation is also used for protection of every application to prevent it from interfering with other applications.
- Virtual machines can use encapsulation for being represented as well as stored as single files in order to facilitate their identification and presentation to other applications

Different operating systems such as Windows or Linux can be enabled for sharing same hardware with help of virtualization. It is possible to shift operating systems between different hardware even while different applications are running with help of virtualization.

Cloud computing leverages storage virtualization for creating a layer of abstraction between applications and storage platforms that are being used by these applications for storage of the data. Storage virtualization enables providers to offer storage as a commodity.

Companies can leverage virtualization layer for choosing the platform they desire without concerns of getting locked in with a particular provider.

One of the important reasons that make virtualization as a key component of cloud computing is it facilitates delivery of cloud based services. It provisions a platform that optimizes intricate resources of IT in a manner that is scalable and enables cost effectiveness as well.

Virtualization can be used for almost any component including applications, operating systems, hardware, networks, memory, and storage to name a few. Virtualization is important for cloud computing because of its ability of decoupling hardware from software.