Assignment -1

1. What problems were we facing before cloud came into existence?

The problems faced before cloud came into existence are

Data and Security, Cost Effective, Easy Portability, Flexibility, High-Dependence on Network.

1. What is Cloud?

Cloud is providing the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical servers.

1. Comparison between on-premises servers and Cloud?

**Deployment**

**On Premises:**In an on-premises environment, resources are deployed in-house and within an enterprise’s IT infrastructure. An enterprise is responsible for maintaining the solution and all its related processes.

**Cloud:**While there are different forms of cloud computing (such as public cloud, private cloud, and a hybrid cloud), in a public cloud computing environment, resources are hosted on the premises of the service provider but enterprises are able to access those resources and use as much as they want at any given time.

**Cost**

**On Premises:**For enterprises that deploy software on premise, they are responsible for the ongoing costs of the server hardware, power consumption, and space.

**Cloud:**Enterprises that elect to use a cloud computing model only need to pay for the resources that they use, with none of the maintenance and upkeep costs, and the price adjusts up or down depending on how much is consumed.

**Control**

**On Premises:**In an on-premises environment, enterprises retain all their data and are fully in control of what happens to it, for better or worse. Companies in highly regulated industries with extra privacy concerns are more likely to hesitate to leap into the cloud before others because of this reason.

**Cloud:**In a cloud computing environment, the question of ownership of data is one that many companies – and vendors for that matter, have struggled with. Data and encryption keys reside within your third-party provider, so if the unexpected happens and there is downtime, you maybe be unable to access that data.

**Security**

**On Premises:** Companies that have extra sensitive information, such as government and [banking industries](https://www.cleo.com/blog/financial-technology-trends) must have a certain level of security and privacy that an on-premises environment provides. Despite the promise of the cloud, security is the primary concern for many industries, so an on-premises environment, despite some of its drawbacks and price tag, make more sense.

**Cloud:**Security concerns remain the number one barrier to cloud computing deployment. There have been many publicized cloud breaches, and IT departments around the world are concerned. From personal information of employees such as login credentials to a loss of intellectual property, the security threats are real.

**Compliance**

**On Premises:**Many companies these days operate under some form of [regulatory control](https://www.cleo.com/blog/california-consumer-privacy-act), regardless of the industry. Perhaps the most common one is the Health Insurance Portability and Accountability Act (HIPAA) for private health information, but there are many others, including the Family Educational Rights and Privacy Act (FERPA), which contains detailed student records, and other government and industry regulations. For companies that are subject to such regulations, it is imperative that they remain compliant and know where their data is at all times.

**Cloud:**Enterprises that do choose a cloud computing model must do their due diligence and ensure that their third-party provider is up to code and in fact compliant with all of the different regulatory mandates within their industry. Sensitive data must be secured, and customers, partners, and employees must have their privacy ensured.

1. What are the different types of cloud based on service models? Explain

Software as a Service (SaaS): -

Software as a service (SaaS) replaces the traditional on-device software with software that is licensed on a subscription basis. It is centrally hosted in the cloud. Most SaaS applications can be accessed directly from a web browser without any downloads or installations required. However, some SaaS applications require plugins.

Platform as a Service (PaaS): -

Platform as a Service (PaaS) allows organizations to build, run and manage applications without the IT infrastructure. This makes it easier and faster to develop, test and deploy applications. Developers can focus on writing code and create applications without worrying about time-consuming IT infrastructure activities such as provisioning servers, storage, and backup. PaaS brings more value to cloud. It can reduce your management overhead and lower your costs. PaaS also makes it easier for you to innovate and scale your services on demand.

Infrastructure as a Service (IaaS): -

Infrastructure as a Service (IaaS) is a self-service model for managing remote data center infrastructures. IaaS provides virtualized computing resources over the Internet hosted by a third party such as Amazon Web Services, Microsoft Azure, or Google. Instead of an organization purchasing hardware, companies purchase IaaS based on a consumption model. It is like buying electricity. You only pay for what you use. This model enables companies to add, delete or reconfigure IT infrastructure on-demand. Many IT organizations rely on IaaS because they are more familiar with IaaS, especially if they have years of experience with virtual environments or strict security and regulatory requirements that can only be met through IaaS.

1. What are the different types of cloud based on deployment models? Explain

Public Cloud: -

Public clouds are available to the general public, and data are created and stored on third-party servers. Server infrastructure belongs to service providers that manage it and administer pool resources, Provider companies offer resources as a service both free of charge or on a pay-per-use basis via the Internet. Users can scale resources as required.

Private Cloud: -

As opposed to a public cloud that is available to the general public, only one specific company owns a private cloud and also called an internal or corporate model. The server can be hosted externally or on the premises of the owner company. Regardless of their physical location, these infrastructures are maintained on a designated private network and use software and hardware that are intended for use only by the owner company. A clearly defined scope of people have access to the information kept in a private repository, which prevents the general public from using it.

Community Cloud: -

A community deployment model largely resembles the private one; the only difference is the set of users. Whereas only one company owns the private cloud server, several organizations with similar backgrounds share the infrastructure and related resources of a community cloud. If all the participating organizations have uniform security, privacy and performance requirements, this multi-tenant data center architecture helps these companies enhance their efficiency, as in the case of joint projects. A centralized cloud facilitates project development, management and implementation. The costs are shared by all users.

Hybrid Cloud: -

As is usually the case with any hybrid phenomenon, a hybrid cloud encompasses the best features of the abovementioned deployment models (public, private and community). It allows companies to mix and match the facets of the three types that best suit their requirements. As an example, a company can balance its load by locating mission-critical workloads on a secure private cloud and deploying less sensitive ones to a public one. The hybrid cloud deployment model not only safeguards and controls strategically important assets but does so in a cost- and resource-effective way. In addition, this approach facilitates data and application portability.

1. AWS history. Explain

**2006:** AWS (Amazon Web Services) was officially launched.

**2007:** In 2007, over 180,000 developers had signed up for the AWS.

**2010:** In 2010, amazon.com retail web services were moved to the AWS, i.e., amazon.com is now running on AWS.

**2011:** AWS suffered from some major problems. Some parts of volume of EBS (Elastic Block Store) were stuck and unable to read and write requests. It took two days for the problem to get resolved.

**2012:** AWS hosted a first customer event known as reinvent conference. First reinvent conference occurred in which new products were launched. In AWS, another major problem occurred that affects many popular sites such as Pinterest, Reddit, and Foursquare.

**2013:** In 2013, certifications were launched. AWS started a certifications program for software engineers who had expertise in cloud computing.

**2014:** AWS committed to achieve 100% renewable energy usage for its global footprint.

**2015:** AWS breaks its revenue and reaches to $6 Billion USD per annum. The revenue was growing 90% every year.

**2016:** By 2016, revenue doubled and reached $13Billion USD per annum.

**2017:** In 2017, AWS re: invent releases a host of Artificial Intelligence Services due to which revenue of AWS doubled and reached $27 Billion USD per annum.

**2018:** In 2018, AWS launched a Machine Learning Speciality Certs. It heavily focussed on automating Artificial Intelligence and Machine learning.