Assignment 1

Explain cloud computing and how it differs from on prem environment

CLOUD COMPUTING

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

In 2011, the National Institute of Standards and Technology (NIST) identified five "essential characteristics" for cloud systems. Below are the exact definitions according to NIST:

* **On-demand self-service:** "A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider."
* **Broad network access:** "Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)."
* **Resource pooling:** " The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand."
* **Rapid elasticity:** "Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time."
* **Measured service:** "Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

**Challenges and limitations**

One of the main challenges of cloud computing, in comparison to more traditional on-premises computing, is data security and privacy. Cloud users entrust their sensitive data to third-party providers, who may not have adequate measures to protect it from unauthorized access, breaches, or leaks. Cloud users also face compliance risks if they have to adhere to certain regulations or standards regarding data protection, such as GDPR or HIPAA.

Another challenge of cloud computing is reduced visibility and control. Cloud users may not have full insight into how their cloud resources are managed, configured, or optimized by their providers. They may also have limited ability to customize or modify their cloud services according to their specific needs or preferences. Complete understanding of all technology may be impossible, especially given the scale, complexity, and deliberate opacity of contemporary systems; however, there is a need for understanding complex technologies and their interconnections to have power and agency within them. The metaphor of the cloud can be seen as problematic as cloud computing retains the aura of something noumenal and numinous; it is something experienced without precisely understanding what it is or how it works.

Additionally, cloud migration is a significant challenge. This process involves transferring data, applications, or workloads from one cloud environment to another, or from on-premises infrastructure to the cloud. Cloud migration can be complicated, time-consuming, and expensive, particularly when there are compatibility issues between different cloud platforms or architectures. If not carefully planned and executed, cloud migration can lead to downtime, reduced performance, or even data loss.

**Implementation challenges**

Applications hosted in the cloud are susceptible to the fallacies of distributed computing, a series of misconceptions that can lead to significant issues in software development and deployment.

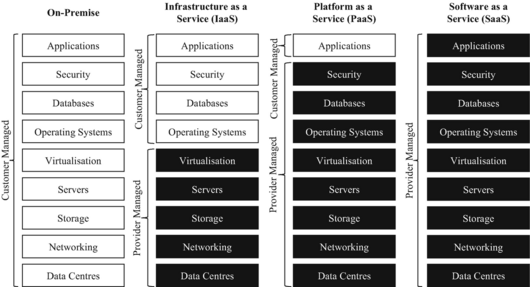
**Cloud cost overruns**

In a report by Gartner, a survey of 200 IT leaders revealed that 69% experienced budget overruns in their organizations' cloud expenditures during 2023. Conversely, 31% of IT leaders whose organizations stayed within budget attributed their success to accurate forecasting and budgeting, proactive monitoring of spending, and effective optimization.

**Service Level Agreements**

Typically, cloud providers' Service Level Agreements (SLAs) do not encompass all forms of service interruptions. Exclusions typically include planned maintenance, downtime resulting from external factors such as network issues, human errors, like misconfigurations, natural disasters, force majeure events, or security breaches. Typically, customers bear the responsibility of monitoring SLA compliance and must file claims for any unmet SLAs within a designated timeframe. Customers should be aware of how deviations from SLAs are calculated, as these parameters may vary by service. These requirements can place a considerable burden on customers. Additionally, SLA percentages and conditions can differ across various services within the same provider, with some services lacking any SLA altogether. In cases of service interruptions due to hardware failures in the cloud provider, the company typically does not offer monetary compensation. Instead, eligible users may receive credits as outlined in the corresponding SLA.

**Comparison of on-premise, IaaS, PaaS, and SaaS**



The National Institute of Standards and Technology recognized three cloud service models in 2011: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).  The International Organization for Standardization (ISO) later identified additional models in 2023, including "Network as a Service", "Communications as a Service", "Compute as a Service", and "Data Storage as a Service".

**Infrastructure as a service (IaaS)**

Infrastructure as a service (IaaS) refers to online services that provide high-level APIs used to abstract various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup, etc. A hypervisor runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. Linux containers run in isolated partitions of a single Linux kernel running directly on the physical hardware. Linux c groups and namespaces are the underlying Linux kernel technologies used to isolate, secure and manage the containers. The use of containers offers higher performance than virtualization because there is no hypervisor overhead. IaaS clouds often offer additional resources such as a virtual-machine disk-image library, raw block storage, file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles.

The NIST's definition of cloud computing describes IaaS as "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, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."

IaaS-cloud providers supply these resources on-demand from their large pools of equipment installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks). To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the number of resources allocated and consumed.

**Platform as a service (PaaS)**

The NIST's definition of cloud computing defines Platform as a Service as:

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, 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 configuration settings for the application-hosting environment.

PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including an operating system, programming-language execution environment, database, and the web server. Application developers develop and run their software on a cloud platform instead of directly buying and managing the underlying hardware and software layers. With some PaaS, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually.

Some integration and data management providers also use specialized applications of PaaS as delivery models for data. Examples include **iPaaS (Integration Platform as a Service)** and **PaaS (Data Platform as a Service)**. iPaaS enables customers to develop, execute and govern integration flows. Under the iPaaS integration model, customers drive the development and deployment of integrations without installing or managing any hardware or middleware. PaaS delivers integration—and data-management—products as a fully managed service. Under the PaaS model, the PaaS provider, not the customer, manages the development and execution of programs by building data applications for the customer. PaaS users access data through data-visualization tools.

**Software as a service (SaaS)**

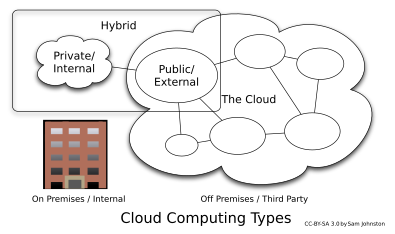
The NIST's definition of cloud computing defines Software as a Service as:

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 either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. 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.

In the software as a service (SaaS) model, users gain access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee. In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications differ from other applications in their scalability—which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user, who sees only a single access-point. To accommodate a large number of cloud users, cloud applications can be *multitenant*, meaning that any machine may serve more than one cloud-user organization.

The pricing model for SaaS applications is typically a monthly or yearly flat fee per user, so prices become scalable and adjustable if users are added or removed at any point. It may also be free. Proponents claim that SaaS gives a business the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider. This enables the business to reallocate IT operations costs away from hardware/software spending and from personnel expenses, towards meeting other goals. In addition, with applications hosted centrally, updates can be released without the need for users to install new software. One drawback of SaaS comes with storing the users' data on the cloud provider's server. As a result, there could be unauthorized access to the data. Examples of applications offered as SaaS are games and productivity software like Google Docs and Office Online. SaaS applications may be integrated with cloud storage or File hosting services, which is the case with Google Docs being integrated with Google Drive, and Office Online being integrated with OneDrive.

**Deployment models**

[](https://en.wikipedia.org/wiki/File:Cloud_computing_types.svg)Cloud computing types

The deployment of services to the cloud is referred to as cloud migration.

Reverse cloud migration, also known as cloud repatriation, refers to moving cloud-based workloads back to on-premises infrastructures including enterprise data centers, colocation providers, and managed service providers. Cloud repatriation occurs due to security concerns, costs, performance issues, compatibility problems, and uptime concerns.

**Private**

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third party, and hosted either internally or externally. Undertaking a private cloud project requires significant engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. It can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities. Self-run [data centers](https://en.wikipedia.org/wiki/Data_center) are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

**Public**

Cloud services are considered "public" when they are delivered over the public Internet, and they may be offered as a paid subscription, or free of charge. Architecturally, there are few differences between public- and private-cloud services, but security concerns increase substantially when services (applications, storage, and other resources) are shared by multiple customers. Most public-cloud providers offer direct-connection services that allow customers to securely link their legacy data centers to their cloud-resident applications.

Several factors like the functionality of the solutions, cost, integrational and organizational aspects as well as safety & security are influencing the decision of enterprises and organizations to choose a public cloud or on-premises solution.

**Hybrid** cloud is a composition of a public cloud and a private environment, such as a private cloud or on-premises resources, that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Gartner defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it cannot be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

Varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.

Another example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity needs that cannot be met by the private cloud. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds. Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization pays for extra compute resources only when they are needed. Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands.

**On Premise vs. Cloud**

Simply put, the difference between on-premise vs cloud software is the location. On-premise software is installed and runs on a company's own hardware infrastructure, and is hosted locally, whereas cloud software is stored and managed on the provider's servers, and accessed through a web browser or other interface.

Cloud computing differs from on-premises software in one critical way. A company hosts everything in-house in an on-premise environment, while in a cloud environment, a third-party provider hosts all that for you. This allows companies to pay on an as-needed basis and effectively scale up or down depending on overall usage, user requirements, and the growth of a company.

A cloud-based server utilizes virtual technology to host a company’s applications offsite. There are no capital expenses, data can be backed up regularly, and companies only have to pay for the resources they use. For those organizations that plan aggressive expansion on a global basis, the cloud has even greater appeal because it allows you to connect with customers, partners, and other businesses anywhere with minimal effort.

Additionally, cloud computing features nearly instant provisioning because everything is already configured. Thus, any new software that is integrated into your environment is ready to use immediately once a company has subscribed. With instant provisioning, any time spent on installation and configuration is eliminated and users are able to access the application right away.

**Key Differences of On-Premise vs. Cloud**

As outlined above, there are a number of fundamental differences between an on-premises and a cloud environment. Which path is the correct one for your enterprise depends entirely on your needs and what it is you’re looking for in a solution.

**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 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, 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.

**Hybrid Cloud Solutions**

While the debate of the pros and cons of an on-premises environment pitted against a cloud computing environment is a real one, and one that many enterprises are having within their offices right now, there is another model that offers the best of both worlds.

A hybrid cloud solution is a solution that features an element of different types of IT deployment models, ranging from on premises to private cloud and public cloud. A hybrid cloud infrastructure depends on the availability of a public cloud platform from a trusted third-party provider, a private cloud constructed either on premises or through a hosted private cloud provider, and effective WAN connectivity between both of those environments.

**Cleo Integration Cloud**

Regardless of what kind of environment you are looking for, whether that’s to add a software-as-a-service (SaaS) solution to address a specific business need, move processes and data into a cloud integration platform, or whether you are a SaaS organization that thrives on delivering faster responses to customer requests, you rely on integration to make your data flows work.

Every successful company needs a scalable infrastructure that can support any-to-any hybrid integration, data transformation, fast and secure file transfer, and end-to-end visibility of all the data that flows their dynamic ecosystems. Cleo Integration Cloud enables enterprises to accelerate ground-to-cloud and cloud-to-cloud integration processes to easily integrate applications, and storage and business platforms, to connect all your data, no matter what it is, and wherever you want it, be it on premises or in the cloud.

**Assignment 2**

**Advantages of on premises infrastructure**

**Total control and ownership**

The first benefit is the most obvious - total ownership of your data and the data center it is stored in just feels safer and makes good business sense. Owning an on-prem data centre allows businesses to continue to guzzle their data, while enjoying complete control over that data, the infrastructure and its data centre operations. This freedom allows companies to configure their own hardware, their software and networks according to their specific needs and not having to deal with third-party providers saves time.

**Data security and privacy**

With a new cyber attack making the headlines every week, data centres have security at the front of their minds and are doing everything they can to ensure that their data is protected, internally and externally.

Through on-prem data centres, all data - from the sensitive to the mundane - is kept within the businesses own systems. The risks linked to data breaches and unauthorised access are reduced and kept in line with that businesses own security protocols and privacy measures.

**Regulatory compliance**

Following on from security, some businesses have strict regulations for data privacy and location based on the geographic location that they operate in. For data centres with facilities across the world, these rules may change. Through using on-prem infrastructure, it can be easier to comply with differing local regulations.

For some industries, like healthcare, there are tight rules for data privacy and storage. By using on-prem data centres, it is easier to follow these regulations and ensure that sensitive data is stored and processed in accordance with legal requirements.

**Physical control**

On the back of data security, many companies just feel more comfortable having physical control over their data centre - and everything inside of it. On-prem data centres offer that peace of mind over the full physical control of both hardware and facilities, allowing companies to directly manage their physical security, environmental conditions and maintenance. In addition, when any problems arise, instead of waiting by the phone for a call back, you can walk straight over to see the data centre and get to work fixing any problems.

**Lower long-term costs**

The infrastructure costs of a data centre include cabling, equipment and the connectivity costs of the network infrastructure. As well as internet security, there are costs to cover the physical security of the building. Additional costs go into the power and the cooling of the centre and a company may wish to invest in sustainable initiatives to lower their emissions.

While upfront costs are high, in the long run, this can be the less expensive option, over using the cloud. Data centres can avoid ongoing service fees and the total cost of ownership will be met over time.

**Existing investments**

In a similar vein, many data centres organizations have already invested in their on-prem infrastructure. While they may see the glittering benefits of cloud computing, such as external providers managing flexible scaling and cybersecurity, if a company has already made their investments in on-prem infrastructure, there will be a strong focus on maximising their return in this.

However, when the company reaches their data peak, they will have to expand their existing infrastructure or look into hybrid solutions, which will require additional investments.

**Legacy applications**

On-prem data centre legacy applications refer to software systems that have been in use for quite a long time across an organisation. These are usually based on older technologies and architectures. Such applications may have been acquired from third-party vendors or even developed internally. Regardless of their age, such legacy applications are a critical part of an organisation's operations. These applications may not be easily moved over to the cloud and simply perform better in an on-prem environment.

**Network dependence**

On-prem network dependence relates to the reliance of a data centre’s IT infrastructure on its local network for:

* Components which rely on the network to communicate with each other and exchange data.
* Applications, databases and other resources which are hosted in the on-prem data centre through the local network and used by employees.
* Data transfer within the on-premises infrastructure, such as backups and synchronisation between servers.

**Customization and performance**

What makes one data centre unique from another? For data centres with special policies on-prem facilities can be customised for that businesses specific needs. For example, the Sagrada Familia in Barcelona, attracts three million visitors a year. The increase in online traffic and data-driven solutions from tourists means that the site requires a data centre structure with a high degree of reliability and flexibility. It was these challenges that led the Sagrada Familia to invest in its own on-prem, tailor-made data centre.

“The reason why we added a data centre to the site was, mainly, to gain the capacity to manage a big amount of data, which required us to avoid the latency as a factor of risk in the efficiency and availability of services such as video surveillance, design, engineering and ticketing,” Fernando Villa, the CIO of the Sagrada Familia, told Mobile magazine.

**Edge computing**

In contrast to traditional cloud computing, which centralises data processing in remote data centres, edge computing distributes computing resources closer to the data sources, or "edges" of the network. This then offers several advantages, including:

* Reduced latency - edge computing processes data locally, which is critical for real-time applications like autonomous vehicles or industrial automation.
* As data is processed locally, edge computing reduces the amount of data that needs to be transmitted to centralised data centres, saving bandwidth.
* As with some of the benefits outlined earlier, edge computing provides organisations with complete control over their on-premises data centres, from security to maintenance to compliance with local regulations.

On-prem data centres provide controlled environments which are centralised and offer high-capacity for computing and data storage. Edge computing brings computational power closer to the data source, which creates an IT infrastructure that is both sturdy and stable.

**Assignment 4**

**List and describe other cloud service model**

**"Backend" as a service (BaaS)**

In the "backend" as a service (m) model, also known as "mobile backend as a service" (MBaaS), web app and mobile app developers are provided with a way to link their applications to cloud storage and cloud computing services with application programming interfaces (APIs) exposed to their applications and custom software development kits (SDKs). Services include user management, push notifications, integration with social networking services and more. This is a relatively recent model in cloud computing, with most BaaS startups dating from 2011 or later but trends indicate that these services are gaining significant mainstream traction with enterprise consumers.

**Serverless computing and Function-as-a-Service (FaaS)**

"Serverless computing is a cloud service category in which the customer can use different cloud capabilities types without the customer having to provision, deploy and manage either hardware or software resources, other than providing customer application code or providing customer data. Serverless computing represents a form of virtualized computing." according to ISO.  Function as a service is a form of serverless computing.