CLOUD COMPUTING

Dr. D Muhammad Noorul Mubarak

Head, Department of Computer Science,

University of Kerala

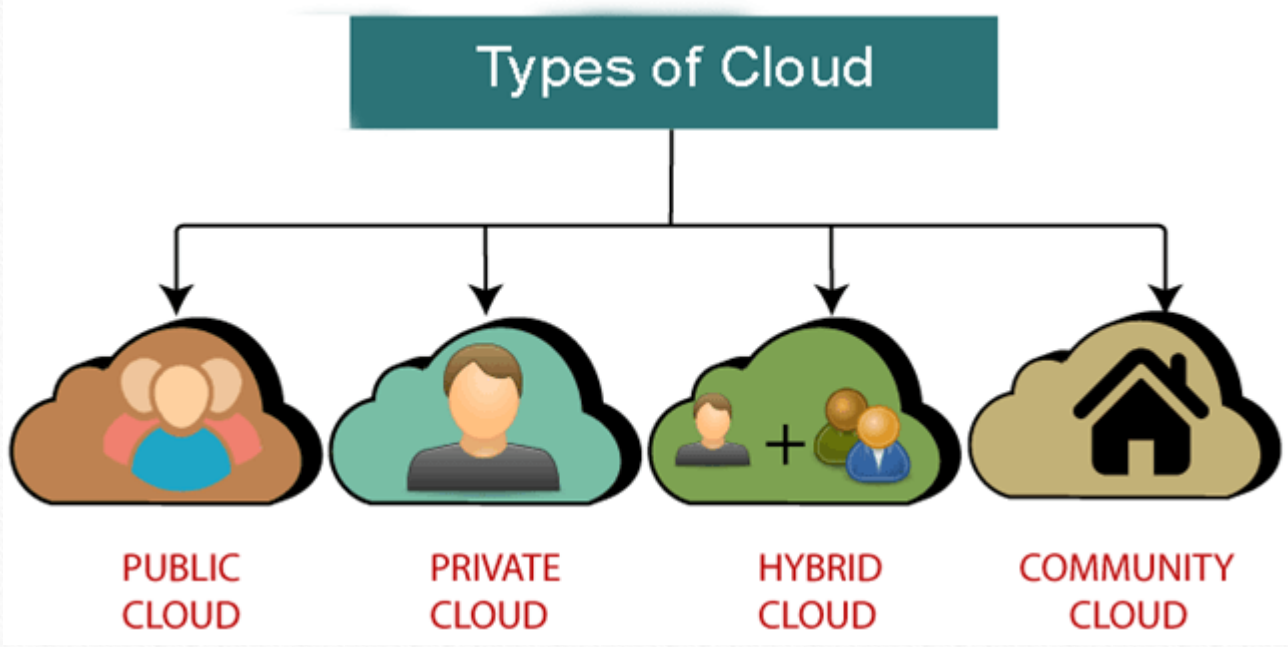
Module III

Cloud Security

- Cloud security, also known as cloud computing security, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data.
- These measures ensure user and device authentication, data and resource access control, and data privacy protection.
- They also support regulatory data compliance.
- Cloud security is employed in cloud environments to protect a company's data from distributed denial of service (DDoS) attacks, malware, hackers, and unauthorized user access or use.
- **Security** in cloud computing is a major concern.
- Data in cloud should be stored in encrypted form.
- To restrict client from accessing the shared data directly, proxy and brokerage services should be employed.

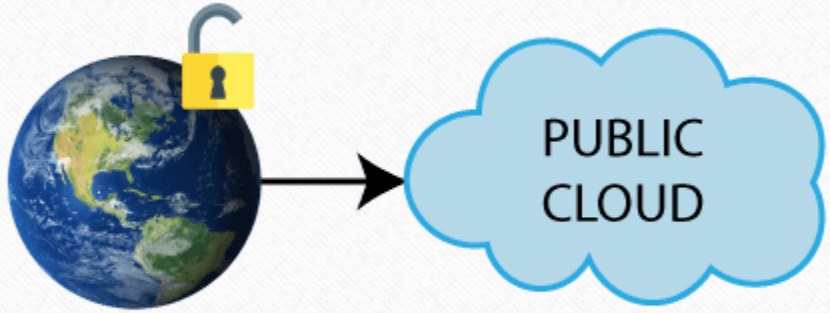
Cloud Computing Environment

- There are 4 main types of cloud computing: private clouds, public clouds, hybrid clouds, and Community:



Public Cloud

- Public cloud is open to all to store and access information via the Internet using the pay-per-usage method.
- In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP).
- Example: Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.



IBM

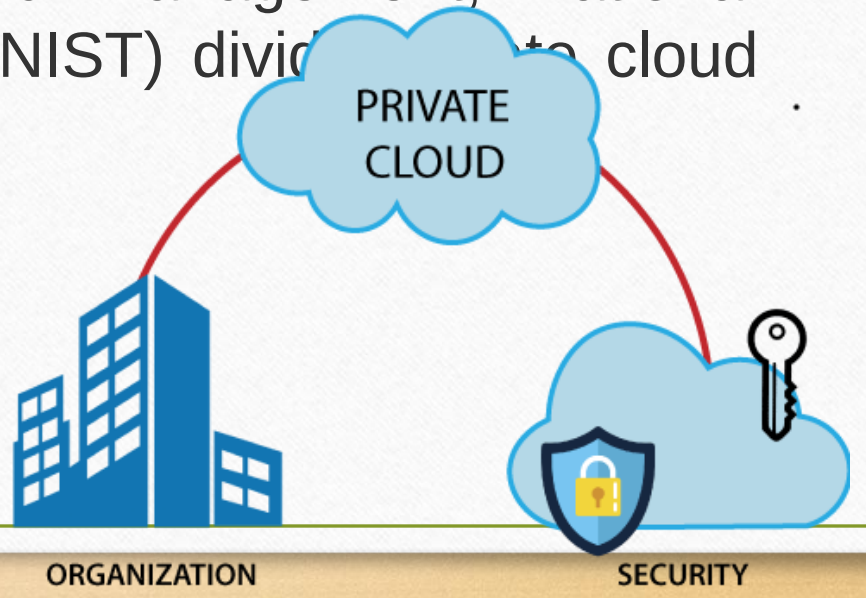
amazon

vmware

Google

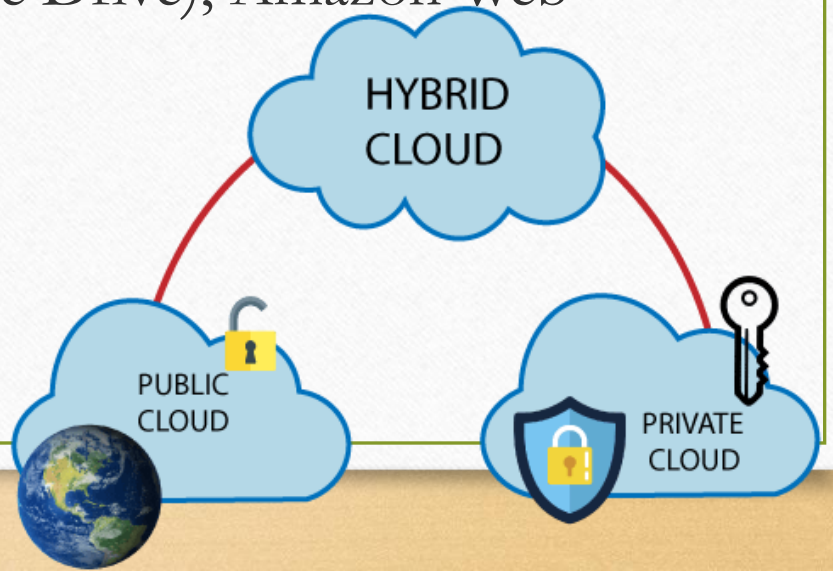
Private Cloud

- Private cloud is also known as an **internal cloud** or **corporate cloud**.
- It is used by organizations to build and manage their own data centers internally or by the third party.
- It can be deployed using Opensource tools such as Openstack and Eucalyptus. Based on the location and management, National Institute of Standards and Technology (NIST) divi cloud into the following two parts-
- On-premise private cloud
- Outsourced private cloud



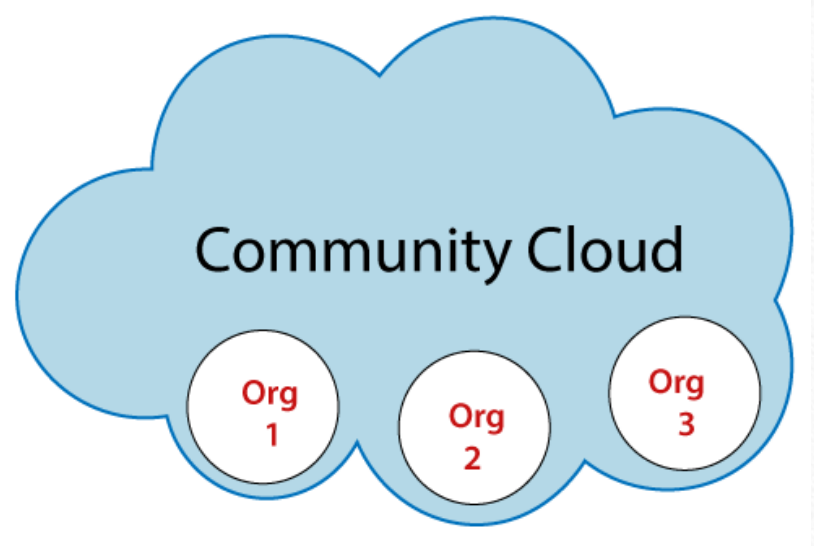
Hybrid Cloud

- Hybrid Cloud is a combination of the public cloud and the private cloud. we can say: Hybrid Cloud = Public Cloud + Private Cloud
- Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users.
- **Example:** Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services.



Community Cloud

- Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community.
- It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.
- **Example:** Health Care community cloud



Cloud Security Vs Traditional IT Security

Cloud security	Traditional IT Security
Quick scalable	Slow scaling
Efficient resource utilization	Lower efficiency
Usage-based cost	Higher cost
Third-party data centres	In-house data centres
Reduced time to market	Longer time to market
Low upfront infrastructure	High Upfronts costs

Cloud Issues and Challenges

- It becomes more challenging when adopting modern cloud approaches Like: **automated cloud integration**, and **continuous deployment (CI/CD)** methods, distributed serverless architecture, and short-term assets for tasks such as a service and container.
- Some of the advanced cloud-native security challenge and many layers of risk faced by today's cloud-oriented organizations are below:

1. **Enlarged Surface:** Public cloud environments have become a large and highly attractive surface for hackers and disrupt workloads and data in the cloud. Malware, zero-day, account acquisition and many malicious threats have become day-to-day more dangerous.

Cloud Issues and Challenges

2. **Lack of visibility and tracking**: Cloud providers have complete control over the infrastructure layer and cannot expose it to their customers in the IaaS model. The lack of visibility and control is further enhanced in the SaaS cloud models. Cloud customers are often unable to identify their cloud assets or visualize their cloud environments effectively.

3. **Ever-changing workload**: Cloud assets are dynamically demoted at scale and velocity. Traditional security tools implement protection policies in a flexible and dynamic environment with an ever-changing and short-term workload.

4. **DevOps, DevSecOps and Automation**: Organizations are adopting an automated DevOps. CI/CD culture that ensures the appropriate security controls are identified and embeddedin the development cycle in code and templates. Security-related changes implemented *after* the workload is deployed to production can weaken the organization's security posture and lengthen the time to market.

Cloud Issues and Challenges

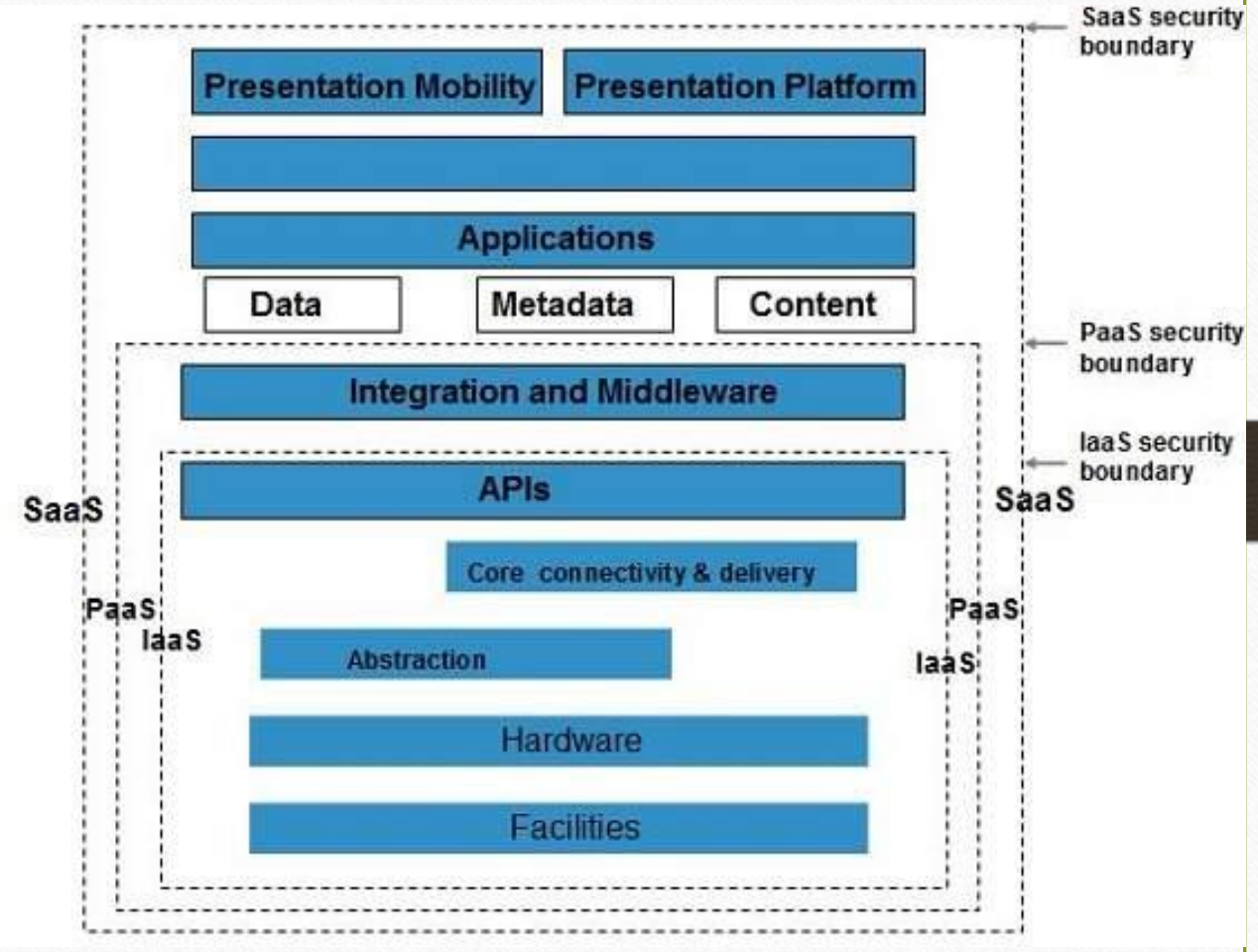
5. Granular privileges and critical management: At the application level, configured keys and privileges expose the session to security risks. Often cloud user roles are loosely configured, providing broad privileges beyond therequirement. An example is allowing untrained users or users to delete or write databases with no business to delete or add database assets.

6. Complex environment: These days the methods and tools work seamlessly on public cloud providers, private cloud providers, and on-premises manage persistent security in hybrid and multi-cloud environments-it including geographic Branch office edge security for formally distributed organizations.

7. Cloud Compliance and Governance: All the leading cloud providers have known themselves best, such as **PCI 3.2, NIST 800-53, HIPAA** and **GDPR**. It gives the poor visibility and dynamics of cloud environments. The compliance audit process becomes close to mission impossible unless the devices are used to receive compliance checks and issue real-time alerts.

Security Boundaries of Cloud

- A particular service model defines the boundary between the responsibilities of service provider and customer. **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the **CSA stack model:**



Security Boundaries of Cloud

- Key Points to CSA Model
  - IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.
  - Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.
  - IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
  - IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
  - This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
  - Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.

Cloud Provider Lock-in

- Cloud lock-in (also known as vendor lock-in or data lock-in) occurs when transitioning data, products, or services to another vendor's platform is difficult and costly, making customers more dependent (locked-in) on a single cloud storage solution.
- Some vendors, like AWS, lock-in customers by charging excessive transfer fees to move data out of their cloud, and other cloud companies lock-in customers by limiting their products' integration potential with other vendor products.

Cloud Infrastructure Security

- Cloud infrastructure security is the practice of securing resources deployed in a cloud environment and supporting systems.
- Public cloud infrastructure is, in many ways, more vulnerable than on-premises infrastructure because it can easily be exposed to public networks, and is not located behind a secure network perimeter.
- However, in a private or hybrid cloud, security is still a challenge, as there are multiple security concerns due to the highly automated nature of the environment, and numerous integration points with public cloud systems.
- Cloud environments are dynamic, with short-lived resources created and terminated many times per day. This means each of these building blocks must be secured in an automated and systematic manner.

Cloud Infrastructure Security

- **Public Cloud Security**
  - Securing workloads and data, fully complying with relevant compliance standards, and ensuring all activity is logged to enable auditing.
  - Ensuring cloud configurations remain secure, and any new resources on the cloud are similarly secured, using automated tools such as a Cloud Security Posture Management (CSPM) platform.
  - Understanding which service level agreements (SLA), supplied by your cloud provider, deliver relevant services and monitoring.
  - If you use services, machine images, container images, or other software from third-party providers, performing due diligence on their security measures and replacing providers if they are insufficient.

Cloud Infrastructure Security

- **Private Cloud Security**
  - Use cloud native monitoring tools to gain visibility over any anomalous behavior in your running workloads.
  - Monitor privileged accounts and resources for suspicious activity to detect insider threats. Malicious users or compromised accounts can have severe consequences in a private cloud, because of the ease at which resources can be automated.
  - Ensure complete isolation between virtual machines, containers, and host operating systems, to ensure that compromise of a VM or container does not allow compromise of the entire host.
  - Virtual machines should have dedicated NICs or VLANs, and hosts should communicate over the network using a separate network interface.
  - Plan ahead and prepare for hybrid cloud by putting security measures in place to ensure that you can securely integrate with public cloud services

Cloud Infrastructure Security

- **Hybrid Cloud Security**
  - Ensure public cloud systems are secured using all the best practices.
  - Private cloud systems should follow private cloud security best practices, as well as traditional network security measures for the local data center.
  - Avoid separate security strategies and tools in each environment—adopt a single security framework that can provide controls across the hybrid environment.
  - Identify all integration points between environments, treat them as high-risk components and ensure they are secured.

Cloud Infrastructure Security

- **Securing 7 Key Components of Your Cloud Infrastructure**
  - **Accounts**
  - **Services**
  - **Hypervisors**
  - **Storage**
  - **Databases**
  - **Networks**
  - **Kubernetes**

Data Security

- Cloud data security is the combination of technology solutions, policies, and procedures that you implement to protect cloud-based applications and systems, along with the associated data and user access.
- The core principles of information security and data governance is CIA:
  - **Confidentiality:** protecting the data from unauthorized access and disclosure
  - **Integrity:** safeguard the data from unauthorized modification so it can be trusted
  - **Availability:** ensuring the data is fully available and accessible when it's needed

Data Security

- Since all the data is transferred using Internet, data security is of major concern in the cloud.
- Here are key mechanisms for protecting data.
  - Access Control
  - Auditing
  - Authentication
  - Authorization
- All of the service models should incorporate security mechanism operating in all above-mentioned areas.

Data Security

- Data security in the cloud starts with identity governance. You need a comprehensive, consolidated view of data access across your on-premises and cloud platforms and workloads. Identity governance provides:
  - **Visibility**—the lack of visibility results in ineffective access control, increasing both your risks and costs.
  - **Federated access**—this eliminates manual maintenance of separate identities by leveraging your Active Directory or other system of record.
  - **Monitoring**—you need a way to determine if the access to cloud data is authorized and appropriate.

Data Security

- Data Security Recommendations:
  - **Deploy encryption.** Ensure that sensitive and critical data, such as PII and intellectual property, is encrypted both in transit and at rest. Not all vendors offer encryption, and you should consider implementing a third-party encryption solution for added protection.
  - **Back up the data.** While vendors have their own backup procedures, it's essential to back up your cloud data locally as well. Keep at least three copies, store them on at least two different media, and keep at least one backup offsite (in the case of the cloud, the offsite backup could be the one executed by the vendor).
  - **Implement identity and access management (IAM).** Your IAM technology and policies ensure that the right people have appropriate access to data, and this framework needs to encompass your cloud environment. Besides identity governance, IAM components include access management (such as single sign-on, or SSO) and privileged access management.
  - **Manage your password policies.** Poor password hygiene is frequently the cause of data breaches and other security incidents. Use password management solutions to make it simple for your employees and other end users to maintain secure password practices.
  - **Adopt multi-factor authentication (MFA).** In addition to using secure password practices, MFA is a good way to mitigate the risk of compromised credentials. It creates an extra hurdle that threat actors must overcome as they try to gain entry to your cloud accounts.

Storage Security

- **Brokered Cloud Storage Access** is an approach for isolating storage in the cloud. In this approach, two services are created:
  - A broker with full access to storage but no access to client.
  - A proxy with no access to storage but access to both client and broker.

Storage Security

- Working Of Brokered Cloud Storage Access System
- When the client issues request to access data:
  - The client data request goes to the external service interface of proxy.
  - The proxy forwards the request to the broker.
  - The broker requests the data from cloud storage system.
  - The cloud storage system returns the data to the broker.
  - The broker returns the data to proxy.
  - Finally the proxy sends the data to the client.