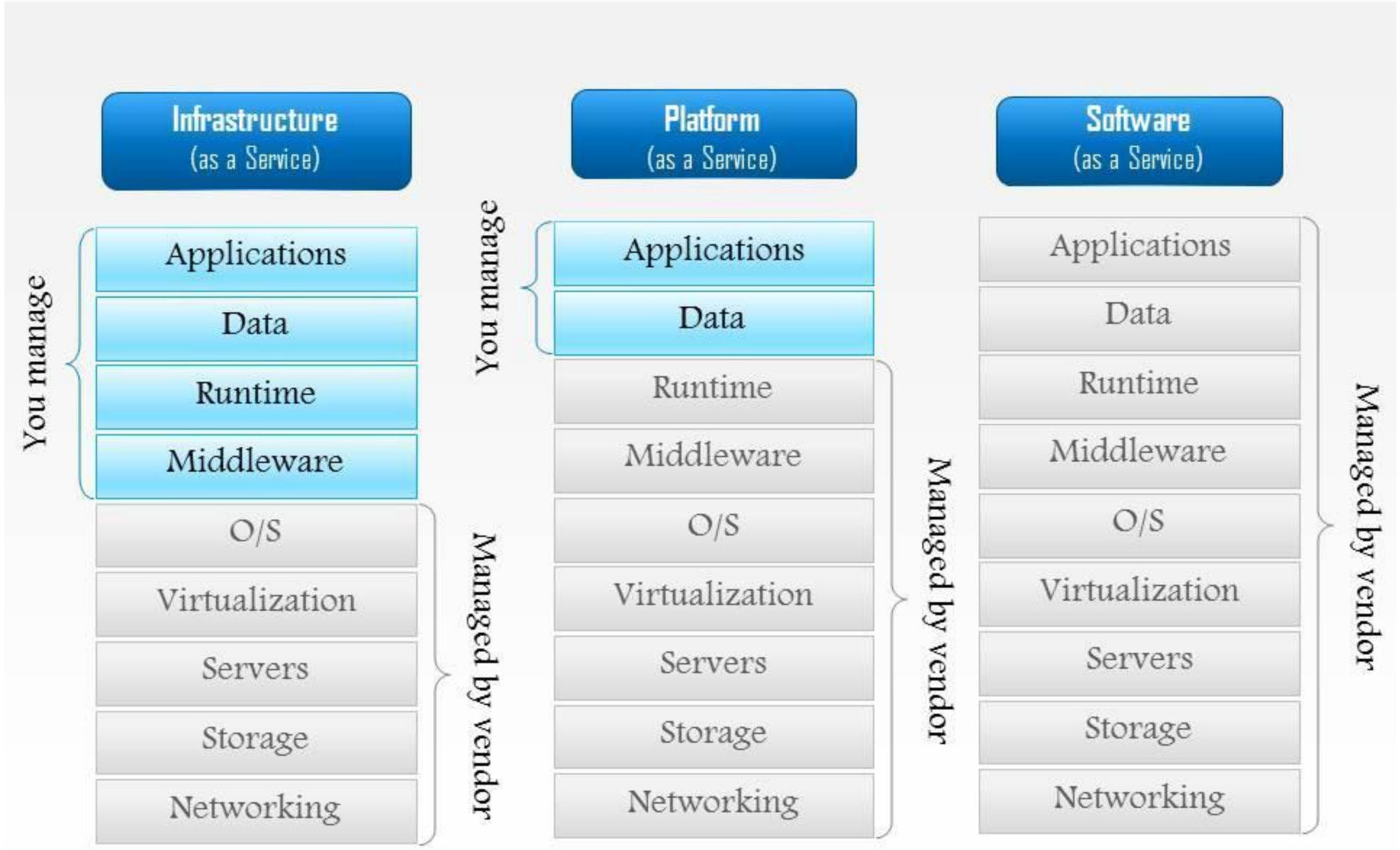
Cloud Computing Service Models

Chapter_2

Overview of Service Models

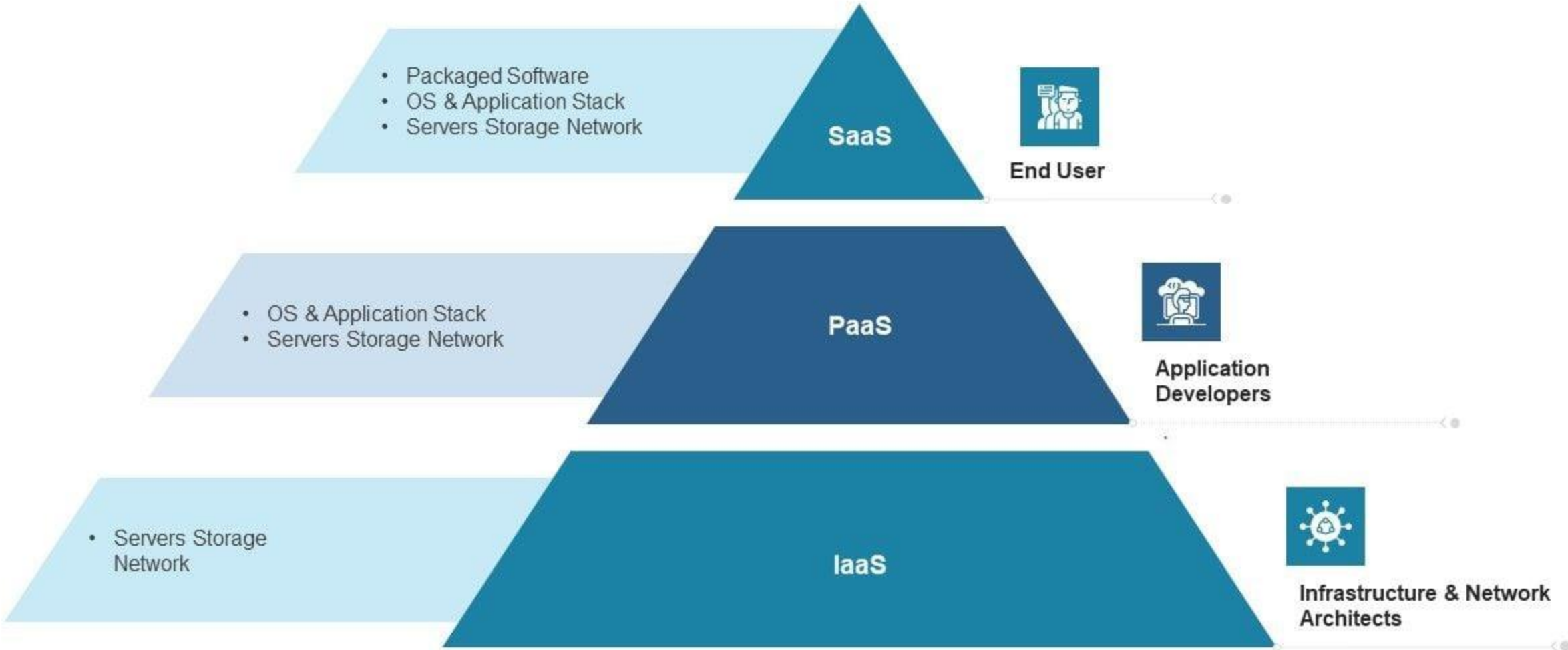
- Cloud computing provides three main service models:
- **Platform as a Service (PaaS)**
- **Software as a Service (SaaS)**
- **Infrastructure as a Service (IaaS)**
- These models cater to different business needs, from application development to ready-to-use software.

Cloud Service Models



Standard Cloud Service Models

This slide depicts the standard cloud service models, namely software as a service, platform as a service, and infrastructure as a service.



Platform as a Service (PaaS)

- **What is PaaS?**
- A platform for building, deploying, and managing applications without managing infrastructure.
- **Features**:
- Pre-configured tools for developers.
- Scalability and integration with databases.
- **Examples**:
- Google App Engine
- Microsoft Azure App Service
- **Use Case**:
- A startup uses PaaS to focus on app development instead of infrastructure setup.

Platform as a Service (PaaS)

- **Advantages**:
- Reduces time for development with pre-configured tools.
- Simplifies app deployment and testing.
- Scales automatically with application demand.
- **Disadvantages**:
- Limited control over the underlying infrastructure.
- Dependency on the provider for updates and maintenance.
- Potential risk of vendor lock-in.

Platform as a Service (PaaS)

- **When to Use**:
  - When developing or deploying applications quickly without managing servers.
- **How to Use**:
  - Choose a PaaS provider (e.g., Google App Engine) and deploy your application code.
- **Where to Use**:
  - Ideal for startups, developers, and small businesses needing rapid deployment.

Software as a Service (SaaS)

- **What is SaaS?**
- Ready-to-use applications accessible via the internet.
- **Features**:
- No installation or maintenance.
- Access from any device.
- **Examples**:
- Google Workspace (e.g., Gmail, Google Docs)
- Salesforce
- **Use Case**:
  A company collaborates on documents using Google Docs, eliminating the need for software installation.

Software as a Service (SaaS)

- **Advantages**:
- Ready-to-use with no installation or maintenance required.
- Accessible from any device with an internet connection.
- Subscription-based, reducing upfront costs.
- **Disadvantages**:
- Limited customization options.
- Reliance on the provider for uptime and security.
- Data portability can be a challenge.

Software as a Service (SaaS)

- **When to Use**:
- For businesses or individuals needing simple, accessible software tools.
- **How to Use**:
- Log in to a SaaS application (e.g., Google Workspace) and start using its features.
- **Where to Use**:
- Collaboration tools for teams (e.g., Google Docs), CRM software (e.g., Salesforce), or email management.

Infrastructure as a Service (IaaS)

- **What is IaaS?**
- Virtualized infrastructure like servers, storage, and networking available online.
- **Features**:
- Full control over resources.
- Pay-as-you-go pricing.
- **Examples**:
- Amazon EC2 (AWS)
- Azure Virtual Machines
- **Use Case**:
  An e-commerce business hosts its website on AWS EC2 for flexibility and scalability.

Infrastructure as a Service (IaaS)

- **Advantages**:
- Complete control over virtualized resources.
- Flexible scaling based on usage.
- Pay-as-you-go model avoids large upfront investments.
- **Disadvantages**:
- Requires technical expertise to configure and manage.
- Potential for high costs if not managed effectively.
- Complexity in handling security and compliance.

Infrastructure as a Service (IaaS)

- **When to Use**:
  - For businesses needing full control over their IT infrastructure.
- **How to Use**:
  - Provision virtual machines or storage resources via providers like AWS or Azure.
- **Where to Use**:
  - Hosting websites, running enterprise applications, or managing large-scale data processing.

Service Model	Control Level	Target Users	Examples	Benefits
PaaS	Medium	Developers	Google App Engine, Azure App Service	Simplifies app development.
SaaS	Low	End Users	Gmail, Salesforce	Easy to use; no maintenance needed.
IaaS	High	IT Administrators	AWS EC2, Azure Virtual Machines	Complete control over infrastructure.

Aspect	Platform as a Service (PaaS)	Software as a Service (SaaS)	Infrastructure as a Service (IaaS)
Definition	Provides a platform for developing and deploying applications without managing infrastructure.	Offers ready-to-use applications over the internet.	Delivers virtualized computing resources like servers, storage, and networking.
Control Level	Medium – Control over applications, limited access to infrastructure.	Low – No control over infrastructure or applications.	High – Full control over virtual machines and resources.
Target Users	Developers, startups, and businesses building applications.	End users needing easy-to-use applications.	IT administrators and businesses managing custom infrastructure.
Examples	Google App Engine, Microsoft Azure App Service.	Google Workspace (Docs, Gmail), Salesforce.	Amazon EC2, Microsoft Azure Virtual Machines.

Deployment Models

Cloud Deployment Models

- Cloud deployment models define **how cloud services are made available** and **who has access** to the infrastructure and services.
- Each model offers a different level of **control, security, and management**.

Public Cloud Computing

- Public cloud is a deployment model where **cloud infrastructure is provisioned for open use by the general public**, owned and managed by a third-party cloud provider (e.g., AWS, Microsoft Azure, Google Cloud), and delivered over the internet.

Architecture of Public Cloud

- The **public cloud architecture** is typically multi-tenant, meaning resources are shared across different users and organizations. It includes:

1. **Data Centers**: Physical infrastructure managed by the provider.
2. **Virtualization Layer**: Allows physical hardware to be divided into virtual machines.
3. **Service Layer**: Offers services like IaaS, PaaS, and SaaS.
4. **Management Interface**: Provides dashboards, APIs, and CLI tools for users.
5. **Security Layer**: Includes authentication, encryption, compliance policies.
6. **Network Layer**: Enables internet-based access to cloud services.

Key Characteristics

- **On-demand self-service**: Provision computing resources like VMs or storage without human interaction.
- **Broad network access**: Services are accessible from anywhere over the internet.
- **Resource pooling**: Multiple users share resources dynamically.
- **Rapid elasticity**: Resources can be scaled up/down automatically.
- **Measured service**: Pay-as-you-go billing based on usage metrics.

Advantages of Public Cloud

Feature	Description
Cost Efficiency	No need for purchasing and maintaining hardware; pay-per-use pricing.
Scalability	Instantly scale resources up or down based on demand.
High Availability	Redundant systems and global data centers ensure uptime and reliability.
Accessibility	Access from any device with internet, enabling remote work and collaboration.
Reduced Time to Market	Rapid deployment of applications without worrying about infrastructure setup.

Disadvantages and Challenges

Challenge	Description
Security Risks	Shared infrastructure can pose risks if not properly secured.
Compliance Issues	Not all providers comply with regional laws (e.g., GDPR, HIPAA).
Limited Control	Users have limited control over infrastructure and customization.
Vendor Lock-in	Migration to another provider can be costly and technically complex.
Performance Variability	Multi-tenant environment may lead to unpredictable performance.

Use Cases of Public Cloud

Use Case	Description
Web Hosting	Hosting websites and web applications (e.g., blogs, e-commerce).
Development and Testing	Quickly spin up dev/test environments.
Big Data Analytics	Analyze massive datasets with tools like Google BigQuery or AWS Athena.
Backup and Disaster Recovery	Store backups securely and restore quickly during outages.
Machine Learning	Use managed ML services (e.g., Azure ML, AWS SageMaker) without setup.
Content Delivery	Distribute content globally via CDNs like AWS CloudFront or Azure CDN.

Examples of Public Cloud Providers

Provider	Key Services
Amazon Web Services (AWS)	EC2 (VMs), S3 (storage), Lambda (serverless), RDS (DB), SageMaker (ML)
Microsoft Azure	Azure VMs, Blob Storage, Azure Functions, Cosmos DB, Azure ML
Google Cloud Platform (GCP)	Compute Engine, Cloud Storage, BigQuery, Vertex AI
IBM Cloud	Watson AI, Kubernetes, DevOps tools
Oracle Cloud Infrastructure (OCI)	Autonomous DB, Compute, Object Storage

Security in Public Cloud

- While public clouds are inherently multi-tenant, most major providers implement **enterprise-grade security**:
- **Data Encryption** (at rest and in transit)
- **IAM (Identity & Access Management)**
- **DDoS Protection**
- **Compliance Certifications** (e.g., ISO 27001, SOC 2, PCI-DSS)
- **Audit Logs and Monitoring Tools**

When to Use Public Cloud?

- Use public cloud when:
- You want to minimize capital expenditure.
- You need to scale rapidly.
- Your workloads are not heavily regulated.
- You want faster time-to-market.

Private Cloud

- A **private cloud** is a cloud infrastructure that is provisioned for **exclusive use by a single organization**, comprising multiple consumers (e.g., business units).
- It may be owned, managed, and operated by the organization itself or a third party and may exist **on-premises or off-premises**.

Architecture of Private Cloud

- Private cloud architectures are typically built using **virtualization and orchestration platforms** that provide services similar to public clouds but within a controlled environment.

Key Architectural Layers:

1.Infrastructure Layer:

1. Physical servers, storage systems, and networking components hosted on-premise or in private data centers.

2.Virtualization Layer:

1. Hypervisors (e.g., VMware ESXi, KVM, Hyper-V) abstract hardware resources into virtual machines.

3.Cloud Management Platform (CMP):

1. Tools like OpenStack, VMware vCloud Suite, or Microsoft Azure Stack for orchestrating cloud services.

4.Service Layer:

1. IaaS, PaaS, and sometimes SaaS offered internally for various departments.

5.Security & Compliance:

1. Integrated firewalls, identity management (e.g., LDAP, Active Directory), and auditing.

Key Characteristics of Private Cloud

Characteristic	Description
Exclusive Access	Only accessible to a single organization.
Customizable Architecture	Infrastructure tailored to specific business or compliance needs.
High Security	Greater control over data, firewalls, and identity management.
In-House or Outsourced Management	Can be managed by internal IT teams or outsourced providers.
Support for Legacy Systems	Easier to integrate with existing enterprise systems and databases.

Advantages of Private Cloud

Benefit	Explanation
Enhanced Security & Privacy	Isolated resources reduce exposure and improve data protection.
Greater Control	Complete control over configurations, policies, and governance.
Compliance-Ready	Easier to comply with regulations (HIPAA, GDPR, etc.).
Customizable Performance	Infrastructure can be optimized for specific workloads.
Predictable Costs	Fixed cost model for infrastructure and maintenance.

Limitations of Private Cloud

Limitation	Explanation
High Capital Cost	Requires significant upfront investment in hardware and software.
Maintenance Overhead	Ongoing responsibility for infrastructure updates, patches, and scaling.
Limited Scalability	Less elastic than public cloud; hardware must be scaled manually.
Requires Skilled IT Staff	Complex to set up, manage, and secure without in-house expertise.

Use Cases of Private Cloud

Use Case	Description
Banking & Finance	For data-sensitive applications requiring tight compliance (e.g., PCI-DSS).
Healthcare Sector	To store and process patient records securely (e.g., HIPAA compliance).
Government & Defense	Where data sovereignty and national security are critical.
Large Enterprises	For managing internal apps like ERP, HRM, CRM with control and integration.
Research Institutions	Hosting compute-intensive workloads in a secure, collaborative setting.

Security in Private Cloud

- Security is a major strength of private cloud systems. Key security measures include:
- **Dedicated firewalls**
- **Role-based access control (RBAC)**
- **Data encryption at rest and in transit**
- **Intrusion Detection Systems (IDS)**
- **Regular security auditing and vulnerability scanning**

Private Cloud Technologies & Tools

Tool/Platform	Description
VMware vSphere/vCloud	Enterprise-grade private cloud solution with robust virtualization tools.
OpenStack	Open-source cloud platform to build scalable private clouds.
Microsoft Azure Stack	Extends Azure services into on-premise environments.
Nutanix	Hyperconverged infrastructure for private cloud.
Red Hat OpenShift	For container-based (Kubernetes) private cloud environments.

Examples

Organization	Private Cloud Implementation Description
Bank of America	Uses a private cloud built on VMware for secure financial operations.
NASA	Built Nebula (private cloud) for internal research and development needs.
Walmart	Operates its own private cloud to manage e-commerce infrastructure.

Hybrid Cloud Computing

- A **hybrid cloud** is a cloud infrastructure that is a **composition of two or more distinct cloud infrastructures** (private, public, or community) that **remain unique entities** but are **bound together by standardized or proprietary technology** that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Architecture of Hybrid Cloud

- Hybrid cloud architectures are designed to allow **seamless integration between on-premise/private cloud infrastructure and public cloud services**.

Key Components:

Layer	Description
Private Cloud	On-premises or hosted infrastructure controlled by the organization.
Public Cloud	Third-party services like AWS, Azure, or Google Cloud.
Hybrid Integration Platform	Middleware or APIs for connecting apps and services across both environments (e.g., Azure Arc, Anthos, AWS Outposts).
Security and Governance Layer	Unified identity, compliance, and access management systems.
Orchestration Layer	Tools to automate workload movement, provisioning, and monitoring (e.g., Terraform, Kubernetes).

Key Characteristics

Characteristic	Description
Interoperability	Ability to move workloads across private and public clouds.
Data Portability	Sync and replicate data securely across environments.
Elasticity	Use public cloud for demand spikes (cloud bursting).
Centralized Management	Single pane of glass to manage and monitor hybrid environments.
Secure Communication	Encrypted channels (e.g., VPNs, dedicated lines) to link cloud services.

Advantages

Advantage	Description
Flexibility	Run sensitive workloads in private cloud and less critical ones in public.
Cost Optimization	Only scale into public cloud during peak demand, reducing overall cost.
Disaster Recovery	Public cloud can serve as backup or failover system.
Faster Innovation	Developers can test apps in public cloud and deploy in private.
Compliance & Control	Maintain data sovereignty while still leveraging public cloud scalability.

Challenges

Challenge	Explanation
Complex Setup	Requires integration of different platforms and networks.
Security Management	Must maintain consistent security policies across environments.
Latency Issues	Data transfer between clouds may introduce latency.
Data Synchronization	Keeping data consistent across platforms is non-trivial.
Vendor Lock-in	Proprietary APIs can restrict flexibility.

Common Use Cases

Use Case	Description
Cloud Bursting	Temporarily scale to public cloud when private resources are exhausted.
Backup & Disaster Recovery	Use public cloud for cost-effective backup and restore options.
Regulatory Workloads	Keep regulated data in private cloud; use public cloud for analytics.
Dev/Test Environments	Build and test apps in public cloud, deploy in secure private cloud.
Edge Computing	Combine edge devices with public cloud for real-time processing.

Examples

Organization	Use of Hybrid Cloud
Netflix	Uses AWS for streaming and a private cloud for backend ops.
NASA	Combines OpenStack-based private cloud with Amazon GovCloud.
General Electric (GE)	Uses Predix (private cloud) integrated with Microsoft Azure.
Walmart	Hybrid architecture with its own cloud platform + public cloud.

Technologies & Tools Enabling Hybrid Cloud

Tool/Service	Function
AWS Outposts	Brings AWS services to on-premise data centers.
Azure Arc	Manage on-premise and multicloud resources from Azure.
Google Anthos	Unified platform to manage apps across on-prem, GCP, and other clouds.
VMware Cloud Foundation	Hybrid cloud platform integrating vSphere, vSAN, and NSX.
IBM Cloud Satellite	Secure cloud services anywhere: edge, on-prem, or public cloud.

Security in Hybrid Cloud

- Security in hybrid environments must be **consistent and centrally managed**. Key approaches include:
- Unified identity & access control (e.g., SSO, LDAP).
- Zero Trust Network Architecture.
- End-to-end encryption.
- Centralized logging and monitoring (e.g., SIEM).
- Continuous compliance auditing.

Community Cloud Computing

- A **community cloud** is a cloud infrastructure that is **shared by several organizations** and supports a **specific community** that has **shared concerns** (e.g., mission, security requirements, policy, compliance considerations).
- It may be **managed by the organizations** or a **third party**, and it may exist **on-premises or off-premises**.

Architecture of Community Cloud

- A community cloud's architecture is **similar to private cloud** but **shared among multiple trusted organizations** that agree on common policies and objectives.

Key Components:

Layer	Description
Infrastructure Layer	Physical or virtual servers shared among community members.
Virtualization Layer	Hypervisors manage multi-tenant isolation (e.g., VMware, KVM).
Cloud Management	Centralized tools for provisioning, orchestration, and resource governance.
Security & Compliance	Controls tailored to meet regulatory or sector-specific standards.
Governance Layer	Defines policies for usage, billing, access rights, and audit logging.

Deployment Models:

- **Internally Hosted** (e.g., a consortium of universities managing their own infrastructure)
- **Third-Party Hosted** (e.g., a cloud vendor hosting on behalf of the community)

Key Characteristics

Feature	Description
Shared Purpose	Built for organizations with common missions or needs (e.g., government, healthcare).
Collaborative Ownership	Joint investment, usage, and decision-making.
Customized Policies	Policies are aligned with specific community goals.
High Trust Environment	Participants usually have pre-established trust or legal agreements.
Sector-Specific Optimization	Optimized for particular domains like education, research, or healthcare.

Challenges

Challenge	Explanation
Governance Complexity	Requires coordination between multiple stakeholders.
Dispute Resolution	Conflicts over policies or billing may arise.
Limited Scalability	May not scale as flexibly as public clouds.
Long Setup Time	Establishing trust, agreements, and infrastructure takes time.
Cost vs. Value	If not enough members, it might become cost-ineffective.

Use Cases of Community Cloud

Sector	Use Case
Government Agencies	Inter-departmental cloud to share applications, citizen data, security tools.
Healthcare Institutions	Shared cloud to manage patient data, comply with HIPAA.
Educational Consortia	Universities pooling resources for research, learning management, data centers.
Banking & Finance	Shared infrastructure to ensure consistent fraud detection and KYC systems.
Research Labs	Shared environment for data-intensive simulations and AI models.

Examples

Organization/Consortium	Description
OpenStack-based Community Clouds	Used by European academic and research institutions (e.g., CERN, GÉANT).
NJEDge.Net (USA)	A consortium cloud for higher education and government in New Jersey.
GovCloud (U.S.)	A special community cloud setup by AWS for U.S. government agencies.
HealthShare NSW	Australian shared health cloud infrastructure for public health organizations.

Security in Community Cloud

- Security measures are implemented to serve multiple but aligned organizations:
- **Federated Identity Management** (e.g., SAML, OAuth)
- **Data Encryption** (at rest and in transit)
- **Auditing and Compliance Logging**
- **Role-Based Access Control (RBAC)**
- **Shared Risk Management Policies**

Cloud Deployment Models with Nepal-Specific Examples

Cloud Model	Real-Time Example in Nepal	Domain	Deployment & Purpose
Public Cloud	**eSewa, Khalti using AWS/Azure**	Digital Payments & Fintech	eSewa and Khalti use public cloud providers (AWS, Azure) to host their applications, ensuring scalability and availability across Nepal. They use public cloud for payment gateways, digital wallets, and mobile apps.
Private Cloud	**Nepal Rastra Bank (NRB) Private Data Center**	Central Banking & Regulation	NRB maintains its private cloud infrastructure to host sensitive financial data, regulatory applications, and interbank settlement systems to ensure data sovereignty and comply with financial security standards.
Hybrid Cloud	**Nepal Telecom (NTC) - Private Cloud + Google Cloud for disaster recovery**	Telecommunications	Nepal Telecom operates private cloud infrastructure for core operations but uses Google Cloud for disaster recovery and backup services. This ensures business continuity while keeping critical data on-premises.
Community Cloud	**National Education Network (MoEST + Tribhuvan University collaboration)**	Education & Research	MoEST (Ministry of Education, Science & Technology) collaborates with Tribhuvan University and other institutions to create a community cloud for shared learning management systems (LMS), research data repositories, and academic collaboration platforms.

Nepal-Specific Scenarios for Each Cloud Model

Model	Scenario in Nepal	Example Use
Public Cloud	Small startups and e-commerce sites in Nepal (Daraz Nepal, Foodmandu) use public clouds like AWS to manage customer data, e-commerce apps, and logistics.	
Private Cloud	Large banks (Nabil Bank, NIC Asia) operate private cloud environments for sensitive financial transactions, ensuring compliance with NRB regulations.	
Hybrid Cloud	Hospitals like **Grande International Hospital** may use on-premises servers for Electronic Health Records (EHR) while utilizing public cloud services for telemedicine platforms.	
Community Cloud	Government agencies like **Department of Hydrology and Meteorology (DHM)** and universities could share infrastructure to collaborate on climate research, disaster management, and GIS data sharing.	