Cloud Deployment Models

Public Cloud

Public Cloud

Shared Cloud Infrastructure - Infrastructure is **shared among multiple organizations**.

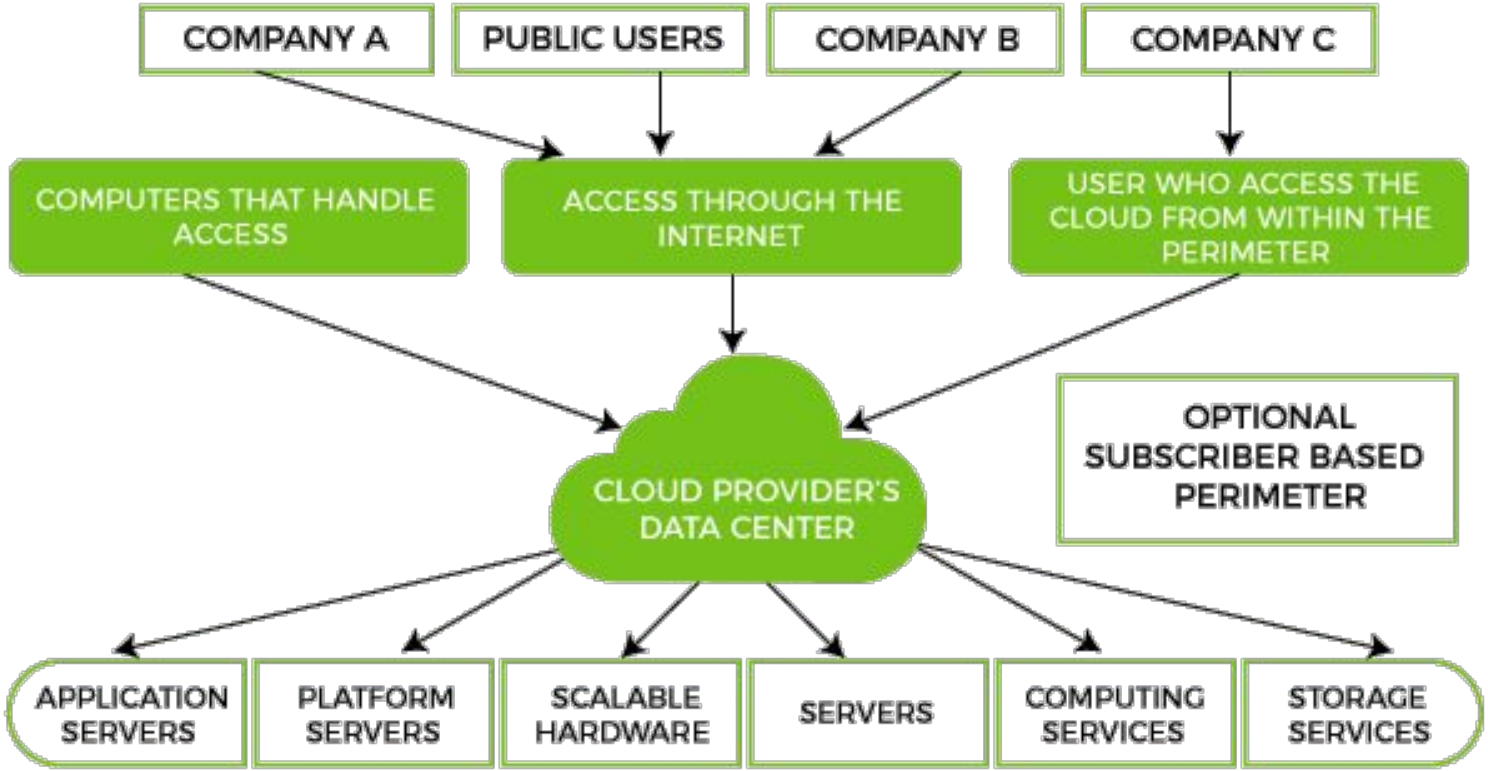
Provider-Owned & Managed - is owned, operated, and maintained by a **cloud service provider**.

Internet-Based Access - Services are accessed over the **public internet** using secure authentication.

Service Delivery Models - Offered through **IaaS, PaaS, and SaaS** service models.

Wide Adoption Across Industries - Commonly used by startups, enterprises, and public-sector organizations for a variety of workloads.

Public Cloud



Public Cloud Providers

Google Cloud

Benefits of Public Cloud

Lower Costs – Pay-as-you-go model reduces upfront investment in hardware and maintenance.

High Scalability & Flexibility – Easily scale resources up or down based on demand.

Global Accessibility – Accessible from anywhere with an internet connection.

Offer Managed Services – Cloud provider handles updates, security patches, and infrastructure maintenance.

Fast Deployment – Resources and applications can be provisioned in minutes.

Limitations of Public Cloud

Less Control – Infrastructure and security are managed by the provider.

Data Privacy Concerns – Shared environment may pose risks for sensitive data.

Ongoing Costs – Pay-as-you-go can get expensive at large scale or high usage.

Vendor Lock-in – Difficult to move workloads between providers due to proprietary services.

Performance Variability – Resource sharing with other tenants can sometimes affect speed.(rarely)

Use case: A university hosts its **public website & learning portal**

Example

- Website
- LMS

How it’s deployed

- AWS / Azure / GCP

Why public cloud fits (Design considerations)

- Low cost
- High scalability
- No sensitive data

Private Cloud

Private Cloud

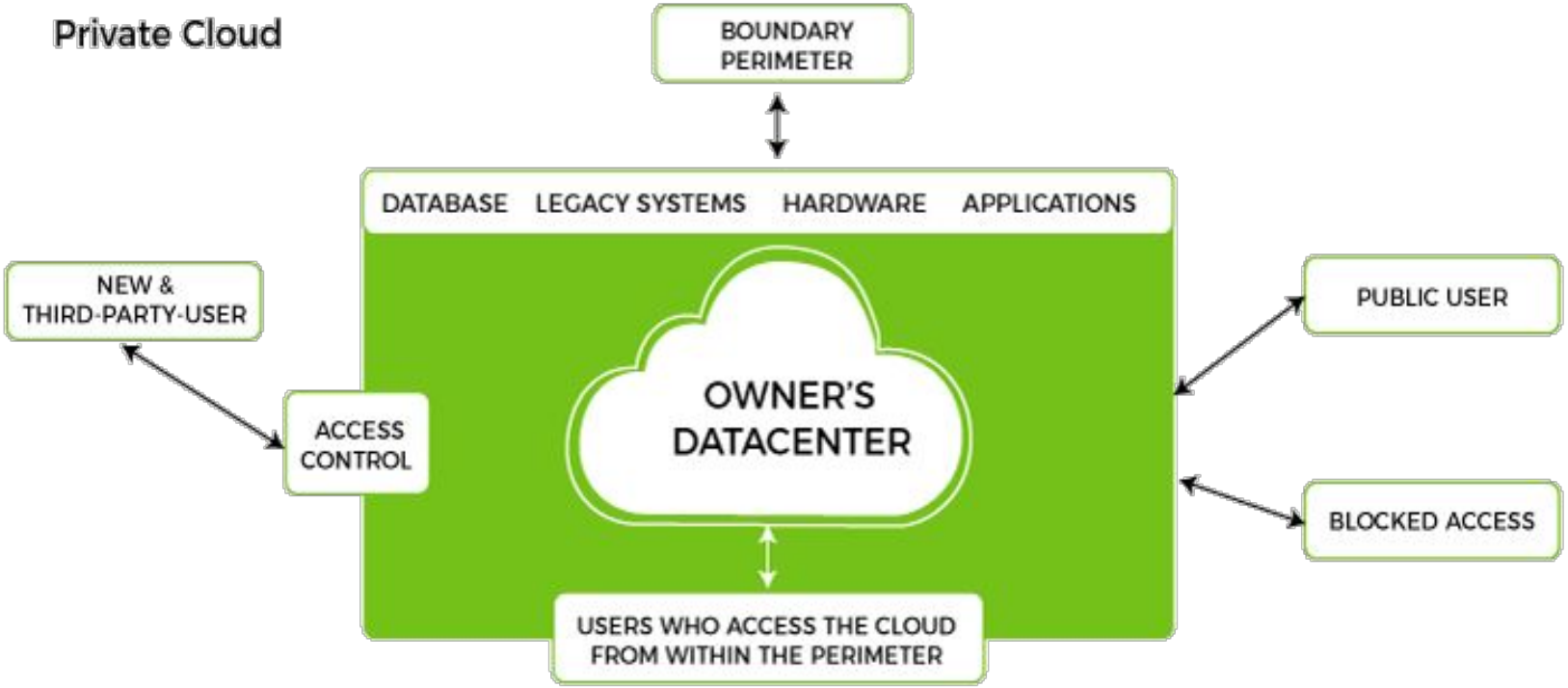
Offers **dedicated** resources(i.e single-tenant)

Hosted **on-site** or in a **service provider's data center**

Uses virtualization, automation, and self-service provisioning similar to public cloud

Better control over data, access, and policies - ideal for industries like finance, healthcare, and government.

Private Cloud



Private Cloud providers

Benefits of Private Cloud

Enhanced Security & Privacy – Data is isolated, reducing risk of breaches.

Customizable Infrastructure – Full control over hardware, software, and network configurations.

Predictable Performance – No resource sharing with other organizations ensures consistent speed and reliability.

Regulatory Compliance – Easier to meet standards like HIPAA, GDPR, or financial regulations.

Flexible Scalability – Can scale resources based on organizational needs, though within owned infrastructure limits.

Limitations of Private Cloud

Higher Costs – Expensive to build, maintain, and upgrade infrastructure.

Complex Management – Requires skilled IT teams for maintenance, updates, and security.

Limited Elasticity – Scaling is slower compared to public cloud; hardware may need to be purchased in advance.

Longer Deployment Time – Setting up private cloud can take weeks or months.

Resource Underutilization Risk – Owned resources may remain idle if demand fluctuates.

Use case : A bank runs its core banking and internal systems

Example

- Core Banking System
- Customer Transaction Processing

How it’s deployed

- On-premises private cloud
- Hosted private cloud (VMware / OpenStack)

Why Private Cloud fits (Design considerations)

- Strict security and regulatory requirements
- Full control over data and infrastructure
- Predictable and consistent performance

Community Cloud

Community Cloud

Shared Cloud Infrastructure – Resources are shared by **a group of organizations** with common goals or requirements.

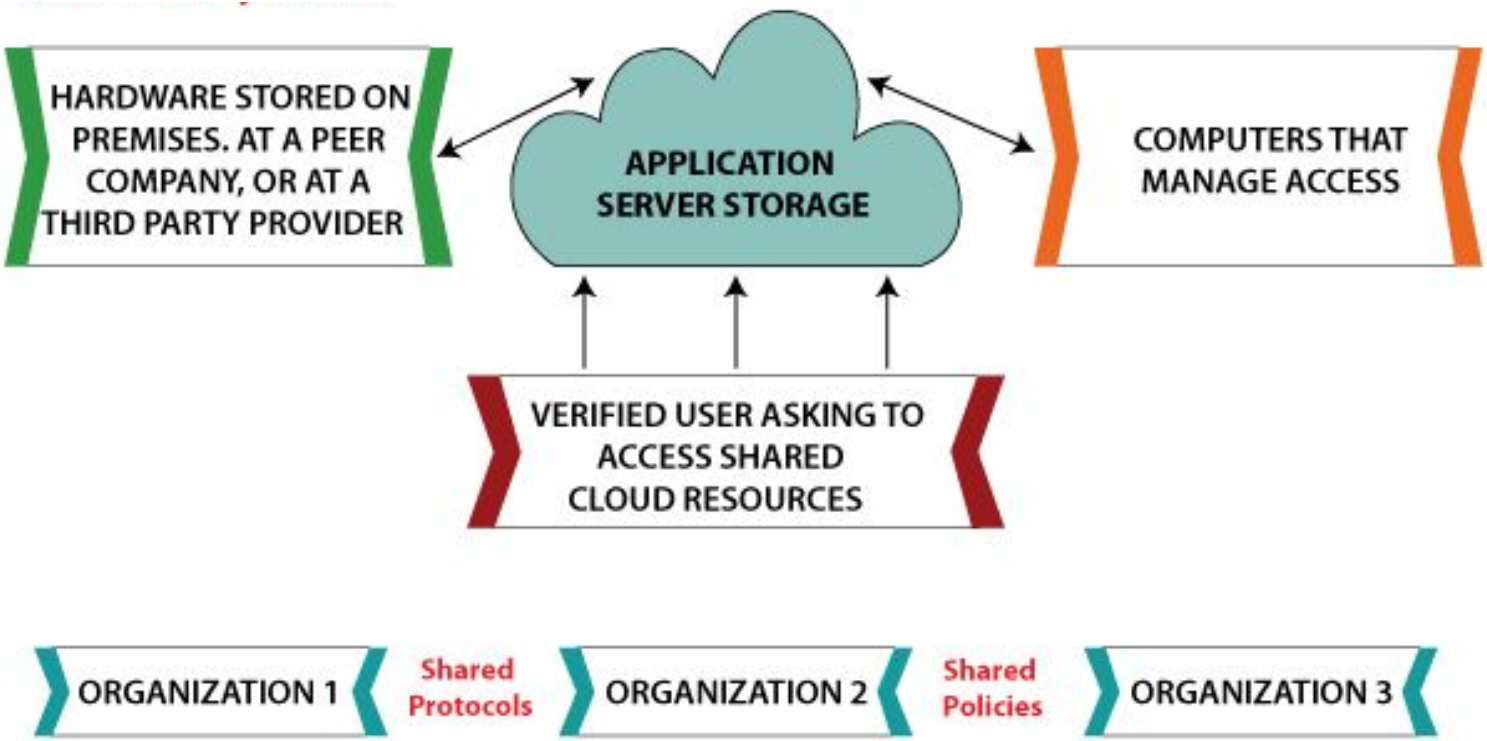
Collaborative Governance – Managed collectively by the participating organizations or a third-party provider.

Focused Use Cases – Designed for communities with **similar security, compliance, or operational needs** (e.g., healthcare, universities, government).

Cost Sharing – Expenses are distributed among the participating organizations, making it more affordable than a private cloud.

Hybrid Characteristics – Offers some **control and customization** like private cloud, but with **shared management and resources**.

Community Cloud



Community Cloud Examples

AWS GovCloud (US)

Microsoft Cloud for Healthcare

ARDC Nectar Research Cloud

salesforce community cloud

Benefits of Community Cloud

Cost Sharing – Expenses are split among the participating organizations, making it more affordable than a private cloud.

Enhanced Security & Compliance – Tailored to meet the specific regulatory and security requirements of the community.

Collaborative Innovation – Organizations can **share knowledge, tools, and best practices** within the community.

Customizable Infrastructure – Offers more control than public cloud while still leveraging shared resources.

Focused Support & Services – Cloud services are designed specifically for the community's industry or operational needs.

Limitations of Community Cloud

Limited Scalability – Resources are shared within the community, so scaling may be slower than public cloud.

Complex Governance – Requires coordination among multiple organizations, which can slow decision-making.

Higher Costs than Public Cloud – More expensive than public cloud due to shared, dedicated infrastructure.

Limited Customization – Must balance the needs of all members, so individual organizations may have restrictions.

Dependency on Community Members – Performance, updates, or policies can be affected by the actions of other members.

Use case: Multiple universities collaborate on shared research platforms

Example

- Research Data Repository
- Shared Academic Applications

How it’s deployed

- Community cloud hosted by a trusted provider
- Government or education sector cloud

Why Community Cloud fits (Design considerations)

- Shared compliance and governance needs
- Cost sharing across institutions
- Secure collaboration within a trusted community

Hybrid Cloud

Hybrid Cloud

Combination of Cloud Models - Hybrid cloud integrates **public and private (or on-premises) cloud environments**.

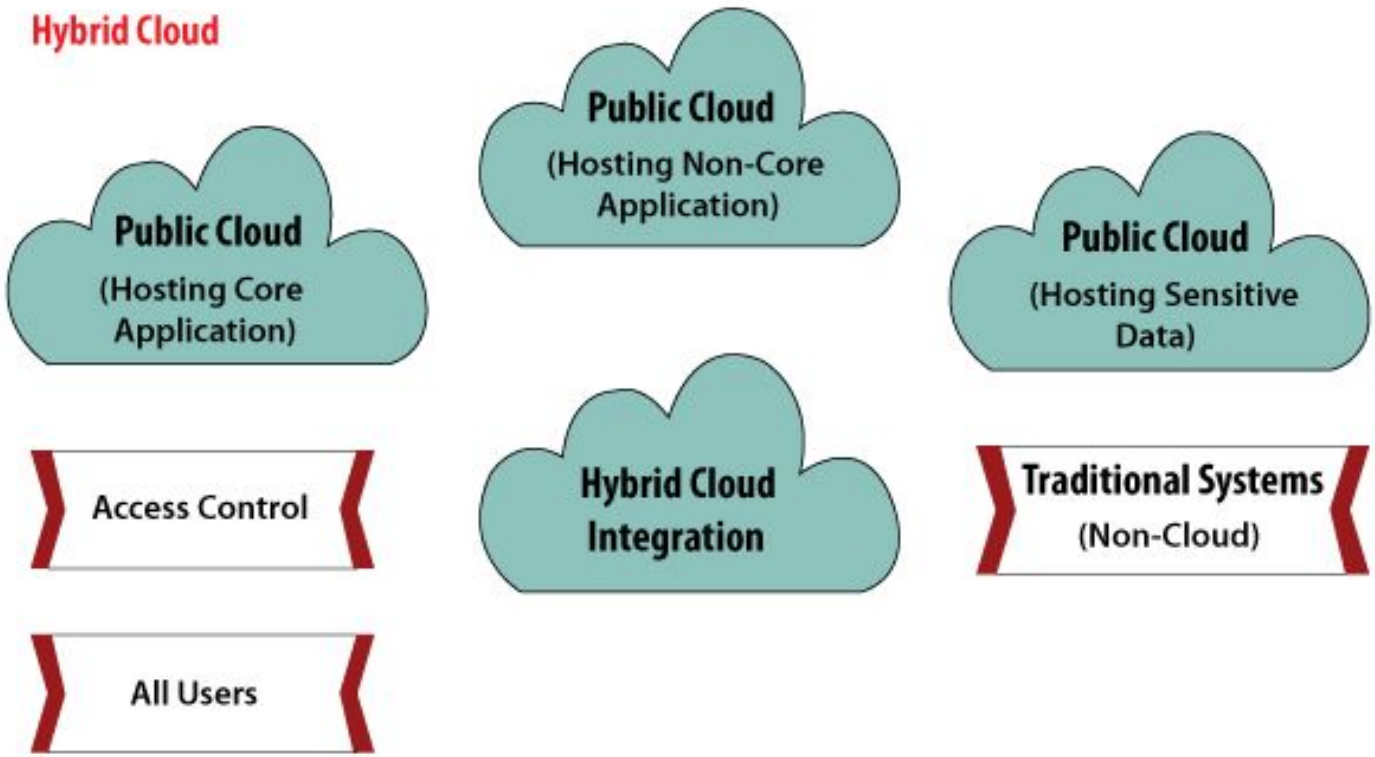
Connected Environments - Workloads and data can move between clouds through **networking and integration technologies**.

Workload Placement Flexibility - Applications can run in different environments based on **business or technical needs**.

Unified Management Approach - Uses common tools and policies to manage resources across multiple cloud platforms.

Common Enterprise Adoption - Widely used by organizations transitioning to cloud while **retaining existing systems**

Hybrid Cloud



Benefits of Hybrid Cloud

Flexibility in Workload Placement- Run sensitive or critical workloads on private cloud while using public cloud for others.

Cost Optimization - Balance fixed private infrastructure with pay-as-you-go public cloud resources.

Scalability on Demand - Use public cloud capacity to handle peak workloads without over-provisioning private resources.

Improved Security & Compliance - Keep regulated data on private environments while still leveraging public cloud services.

Smooth Cloud Adoption - Enables gradual migration to the cloud without replacing existing on-premises systems.

Limitations of Hybrid Cloud

Complex Architecture - Integrating and managing multiple environments increases design and operational complexity.

Higher Management Overhead - Requires skills, tools, and processes to operate both private and public clouds.

Security Challenges - Ensuring consistent security policies across environments can be difficult.

Network Dependency & Latency - Performance may be affected by network connectivity between cloud environments.

Increased Initial Setup Cost - Integration, tooling, and connectivity setup can be expensive at the start.

Use case: A university runs both sensitive internal systems and public digital services

Example

- Student Records & Exam Systems (Private)
- Website & Learning Management System (Public)

How it’s deployed

- On-premises / Private cloud + AWS / Azure / GCP

Why Hybrid Cloud fits (Design considerations)

- Sensitive data kept in private environment
- Public services scale easily during peak usage
- Gradual cloud adoption without replacing existing systems

Multi Cloud

Multi Cloud

Multiple Cloud Providers - Uses services from **more than one cloud provider** at the same time.

Independent Cloud Environments - Each cloud operates as a **separate environment**, not necessarily integrated.

Workload Distribution - Applications and services can be deployed across **different clouds based on need**.

Provider-Specific Services - Organizations may use **different features or services** from each provider.

Common Enterprise Strategy - Often adopted by organizations with **diverse workloads or regional requirements**.

Benefits of Multi Cloud

Avoids Vendor Lock-in - Organizations are not dependent on a single cloud provider.

Improved Resilience & Availability- Workloads can continue running if one cloud provider has an outage.

Best-of-Breed Services - Ability to choose the **best services** from different providers.

Regulatory & Regional Flexibility - Data and workloads can be placed in specific regions to meet compliance needs.

Cost Optimization Opportunities- Organizations can compare pricing and optimize workloads across providers.

Limitations of Multi Cloud

Increased Complexity - Managing multiple cloud platforms increases architectural and operational complexity.

Higher Skill Requirements - Teams must learn and maintain expertise in **multiple cloud technologies**.

Management & Tooling Challenges - Monitoring, security, and governance tools may not work consistently across providers.

Higher Operational Costs - Duplicate tools, integrations, and support contracts can increase costs.

Data Integration & Latency Issues - Moving data between clouds can introduce **latency, security, and cost challenges**.

Use case: An enterprise runs applications across multiple cloud providers to avoid dependency on a single vendor

Example

- Web Application on AWS
- Data Analytics Platform on Azure
- AI / ML Workloads on Google Cloud

How it’s deployed

- AWS + Azure + Google Cloud (separate environments)

Why Multi-Cloud fits (Design considerations)

- Avoid vendor lock-in
- Use best services from each provider
- Improve resilience and availability

Summary

Cloud Model	What It Is	Ownership	Typical Use Cases	Key Idea
Public Cloud	Shared cloud services over the internet	Cloud Provider	Websites, LMS, mobile apps, startups	Low cost & high scalability
Private Cloud	Cloud infrastructure for one organization	Single Organization	Banking systems, internal enterprise apps	Full control & security
Hybrid Cloud	Combination of public and private clouds	Shared	Sensitive + public workloads	Best of both worlds
Community Cloud	Shared by organizations with common needs	Community / Third Party	Universities, healthcare, government	Shared compliance & cost
Multi-Cloud	Multiple public cloud providers	Multiple Providers	Resilience, best services per cloud	Avoid vendor lock-in

Q&A