Amity University Punjab

Introduction to Cloud Computing– [CSE-208]
Assignment - II

Submitted to:
Prof. Sanjay Gupta
Amity University, Punjab

Submitted by:
Gurmukh Singh
B. Tech CSE-A (IV-Sem)
A25305223008

1. Identify a real-world business scenario and recommend a suitable cloud deployment model.

Scenario: Online Food Delivery Platform

Business Overview:

A startup called **"TastyGo"** plans to launch an online food delivery platform that connects users with local restaurants. The platform will have a mobile app and website, support real-time order tracking, offer discounts, and manage large volumes of user data, payment info, and restaurant menus.

Business Needs:

- **Scalability:** Handle traffic spikes during meal times and festivals.
- **High availability:** 24/7 uptime with minimal downtime.
- **Cost-efficiency:** Pay-as-you-go model since the startup wants to manage expenses.
- **Security:** Protect customer data and payment info.
- **Rapid deployment:** Quickly launch updates and new features.

Recommended Cloud Deployment Model: Public Cloud

Why Public Cloud is Suitable:

- **Scalability:** Services like **AWS Elastic Beanstalk**, **Azure App Service**, or **Google App Engine** auto-scale to handle more users.
- **Cost-effective:** No upfront investment in infrastructure; pay only for resources used.
- **Quick deployment:** Developers can deploy apps and updates quickly using CI/CD pipelines.
- **Security:** Top public cloud providers offer robust security and compliance certifications.
- **Managed services:** Reduce overhead by using managed databases (e.g., Amazon RDS, Firebase), load balancers, and storage (e.g., Amazon S3).

Example Implementation:

- **Compute:** AWS EC2 or Google App Engine for running backend services.
- **Database:** Firebase Realtime DB or Amazon RDS for customer/order data.
- **Storage:** Amazon S3 for storing menu images and receipts.
- **Analytics:** Google Analytics or AWS CloudWatch for monitoring usage.
- SSL certificates, AWS Identity and Access Management (IAM), and firewall settings.

Alternative Consideration:

If the business was a large enterprise needing **complete control and data privacy**, a **Private Cloud** (like OpenStack) or **Hybrid Cloud** (mix of on-premises and cloud, like using Azure Arc) could be considered.
But for most **startups and SMEs**, **Public Cloud** is the ideal choice.

Business Scenario 2:

"**FinSure**" is a well-established bank planning to launch a **secure digital banking platform** offering services like savings accounts, loans, investment tracking, credit card management, and mobile payments. The platform is expected to serve **millions of customers**, operate **24/7**, and store **highly sensitive financial and personal data**.

The bank must comply with **strict regulatory standards**, including **data residency**, **PCI-DSS**, and **ISO 27001** compliance. The platform will also include **AI-driven financial advisory services** and **custom reports for enterprise clients**, which demand powerful computing resources but also **tight control over data and infrastructure**.

Business Requirements:

- **Maximum Security:** Sensitive data such as account details, financial transactions, and personal information must be protected with **bank-level encryption and compliance protocols**.
- **Regulatory Compliance:** Must follow **regional and international regulations** regarding data protection and financial reporting.

- **Full Control Over Infrastructure:** The organization prefers complete authority over data storage, access management, and system updates.
- **High Availability:** Services like mobile banking and card transactions must be **always accessible**.
- **Limited Public Access:** Internal banking operations and customer data shouldn't reside in a shared or public environment.

Recommended Cloud Deployment Model: Private Cloud

A **Private Cloud** is the most suitable option for FinSure because it offers **dedicated infrastructure**, full customization, and **maximum control over security and compliance**. It can be deployed **on-premises** or through **a trusted managed private cloud vendor**.

Why Private Cloud is the Best Fit:

- **High Security & Compliance:** Private cloud allows strict enforcement of **security policies**, **firewalls**, **encryption**, and **custom audit mechanisms** that public cloud options may not fully support.
- **Dedicated Resources:** Since the infrastructure is not shared, there's no risk of data leakage from other tenants — a critical requirement in financial services.
- **Compliance-Ready Environment:** Tailored setups for **regulatory frameworks** such as GDPR, PCI-DSS, RBI regulations (India), and others.
- **Custom Architecture:** The IT team can design, monitor, and update the infrastructure to suit internal security and operational protocols.
- **Predictable Performance:** As resources aren't shared with others, **latency is lower**, and performance is consistent.

Example Cloud Setup for FinSure:

cc

Component	Private Cloud Optic
Infrastructure	Hosted via VM
Database	Private SQL

Component	Private Cloud Optic
Storage	Encrypted S
Security	Custom firewa
Backup & DR	Private replicat

2. Classify different organizations based on which cloud model they should use.

1. Entertainment & Streaming Organizations → Public Cloud
Recommended Model: Public Cloud
Why:

- These organizations cater to millions of users globally.
- They require on-demand scalability to handle sudden traffic surges (e.g., new show releases).
- Public cloud offers global content delivery, low latency, and cost efficiency.

Examples:

- Netflix uses AWS to deliver streaming services to over 190 countries.
- Spotify relies on Google Cloud Platform to process real-time music data, recommendations, and analytics.
- Disney+ scales rapidly on AWS during new releases like Marvel or Star Wars shows.

2. Banking & Financial Institutions → Private Cloud
Recommended Model: Private Cloud
Why:

- Banks deal with highly sensitive data like personal, transactional, and credit card information.
- They must comply with financial regulations (e.g., PCI-DSS, RBI Guidelines).
- Private clouds give them maximum security, control, and customization options.

Examples:

- Bank of America uses a private cloud for secured financial transactions and compliance.
- JP Morgan Chase maintains internal cloud systems for real-time risk analysis and data security.
- HDFC Bank (India) uses private cloud infrastructure to support its digital banking services securely.

3. Retail & E-Commerce Companies → Hybrid Cloud
Recommended Model: Hybrid Cloud
Why:

- Retailers need to process customer data, orders, inventory, and run large-scale websites/apps.
- Hybrid cloud lets them store critical data privately while using the public cloud to manage high web traffic or sales peaks.
- It also allows integration with legacy systems while adopting modern cloud tools.

Examples:

- Walmart uses a hybrid model: private cloud for internal operations, Azure for customer-facing apps.
- Flipkart leverages a hybrid approach to run AI-based recommendations while managing supply chains securely.
- Amazon itself uses hybrid setups for combining warehouse systems and AWS.

4. Government, Research & Defence Organizations → Private or Community Cloud
Recommended Model: Private or Community Cloud
Why:

- These bodies handle classified or confidential information like national security data or scientific research.
- Private cloud offers tight control and security; community cloud allows collaboration between departments under shared rules.
- Government agencies often have regulatory restrictions on where data can be stored.

Examples:

- NASA uses the Nebula private cloud for secure and high-performance computing in space research.
- ISRO (India) uses secured infrastructure for handling space mission data, satellite communication, etc.
- EU Government Agencies use community cloud to securely share information across departments while staying compliant with GDPR.

5. Healthcare Providers → Hybrid or Community Cloud
Recommended Model: Hybrid / Community Cloud
Why:

- Healthcare systems must store electronic health records (EHRs) and patient data with privacy (HIPAA, etc.).
- Community clouds help hospitals share data securely while meeting common compliance.
- Hybrid clouds allow sensitive data to remain private while leveraging public cloud for applications, analytics, or appointment booking systems.

Examples:

- NHS UK uses a community cloud to allow hospitals to securely access and update patient records.
- Mayo Clinic (USA) partners with Google Cloud to provide AI-driven diagnostics and secure research collaboration.

- Apollo Hospitals use hybrid cloud for secure storage of patient data and running their health apps.

6. Educational Institutions & Universities → Community Cloud
Recommended Model: Community Cloud
Why:

- Universities and research institutes often collaborate across borders on shared scientific research, labs, and academic resources.
- Community cloud allows them to share infrastructure and data securely, while keeping costs low.
- It supports access control, data sharing, and joint platforms for learning and discovery.

Examples:

- CERN operates a community cloud to support research on particle physics involving institutions worldwide.
- Open Science Data Cloud (OSDC) enables researchers to store and share massive scientific datasets.
- IITs/NITs (India) use platforms provided by NIC and shared research clouds to collaborate nationally and internationally.

3. Compare and contrast different cloud deployment models based on cost, security, and scalability.

Cloud deployment models define how cloud infrastructure is structured, accessed, and managed. Choosing the right model depends on several business needs including budget, sensitivity of data, compliance requirements, and growth potential.

Public Cloud

- Operated by third-party providers like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP).
- Resources like servers and storage are shared among multiple organizations, making it very cost-efficient.

- Ideal for startups and growing businesses looking to avoid upfront infrastructure costs.
- While public cloud providers offer strong baseline security, organizations have limited control over data management, making it less suitable for sensitive information.

Private Cloud

- The cloud infrastructure is dedicated to a single organization, hosted either on-premises or through a private third-party provider.
- Offers maximum security and data privacy, making it the best option for industries dealing with confidential or regulated data such as banking, defense, or healthcare.
- Since the infrastructure is not shared, the cost of setup and maintenance is significantly higher, but control over performance and compliance is unparalleled.
- Scalability depends on the organization's own IT capabilities or hosting arrangements.

Hybrid Cloud

- Combines features of both public and private clouds, allowing businesses to store sensitive data in a secure private cloud while leveraging the public cloud for high-volume or less critical operations.
- Provides a flexible and balanced solution — organizations can optimize for cost, performance, and compliance.
- Ideal for enterprises with mixed workloads, seasonal demands, or those undergoing digital transformation.
- Highly scalable due to public cloud integration, while maintaining control over sensitive functions.

Community Cloud

- A cloud environment shared by a group of organizations that have similar security, compliance, or operational concerns (e.g., hospitals, universities, government departments).
- Infrastructure is jointly owned and managed, offering customized compliance, cost-sharing, and secure collaboration.
- More affordable than private cloud and more secure than public cloud, making it suitable for domain-specific use cases.
- Commonly used in sectors like healthcare (e.g., NHS UK), education, and scientific research consortia.

Comparison Table :

cccccc

Deployment Model	Cost

cccccc

Public Cloud	Low (Pay-as-you-go

ccccccc

Private Cloud	High (Dedicated ha

ccccccc

Hybrid Cloud	Moderate (Optimize

ccccccc

Community Cloud	Moderate (Cost sha

4. What factors influence the choice of a cloud deployment model for a business?

1. Data Sensitivity and Security Requirements

What it Means:

If a business deals with highly confidential data—like financial transactions, defence operations, patient records—it cannot risk exposing this data to the public. In such cases, businesses often prefer Private or Community Clouds.

Use Case:

- Industries like banking, healthcare, defence, and legal services prioritize data encryption, internal access control, and audit capabilities.

Real Example:

- JP Morgan Chase uses a Private Cloud to store sensitive financial data, ensuring it's not exposed to any third-party public infrastructure.
- ISRO stores satellite and mission data in its private infrastructure to ensure national security.

2. Compliance and Regulatory Requirements

What it Means:

Many industries must comply with laws such as:

- HIPAA (healthcare),
- GDPR (EU data privacy),
- PCI-DSS (financial data security), which dictate how and where data must be stored and processed.

Use Case:

- Businesses often choose Private or Community Clouds to meet specific legal compliance standards and local data residency requirements.

Real Example:

- NHS UK uses a Community Cloud to meet healthcare-specific legal frameworks and ensures all patient data remains within the UK.
- EU government agencies operate on a community cloud that respects GDPR and allows controlled data sharing across departments.

3. Budget and Cost Constraints

What it Means:

Small to medium-sized businesses or startups often lack large capital for hardware and infrastructure. They look for flexible and cost-effective solutions where they pay only for what they use.

Use Case:

- The Public Cloud is the go-to model here, offering scalability with minimal upfront investment and no maintenance responsibility.

Real Example:

- Zomato, during its early growth phase, used AWS (Public Cloud) to host their services. This allowed them to scale as demand increased without investing heavily in physical infrastructure.

4. Scalability Needs

What it Means:

Some businesses experience fluctuating workloads—for instance, during peak shopping seasons or major product launches. These businesses require infrastructure that can scale up or down instantly.

Use Case:

- Public or Hybrid Cloud offers elastic scalability, making it ideal for businesses that deal with variable demand or rapid growth.

Real Example:

- Netflix uses AWS (Public Cloud) to automatically scale during peak viewing times (e.g., global premieres) to serve millions of concurrent users without performance loss.

5. Control Over Infrastructure

What it Means:

Organizations with complex internal systems or unique hardware/software needs may require custom configurations, tight security controls, or dedicated resources.

Use Case:

- Private Cloud allows full control over the infrastructure—ideal for organizations that cannot risk using a shared environment.

Real Example:

- NASA uses a Private Cloud (Nebula) where all systems are configured to support space research, simulation, and data analysis with zero external access.

6. Nature of Workload or Application

What it Means:

Depending on whether an application is customer-facing (e.g., mobile apps, websites) or internal (e.g., payroll, CRM), the cloud deployment model may vary.

Use Case:

- Businesses may use Public Cloud for public-facing services and Private Cloud for sensitive internal operations. Hybrid Cloud combines both.

Real Example:

- Walmart hosts internal systems like inventory and HR in a Private Cloud, while using Public Cloud to manage its online store and mobile app traffic.

7. Collaboration and Shared Purpose

What it Means:

Organizations that collaborate on shared goals (like research or education) can benefit from a Community Cloud, which provides a secure and cost-effective shared environment.

Use Case:

- Multiple institutions working on joint research, academic programs, or public services can pool resources without compromising security.

Real Example:

- CERN uses a Community Cloud to enable physicists and institutions worldwide to analyse data from the Large Hadron Collider collaboratively.

8. Legacy System Integration

What it Means:

Large enterprises with old on-premise infrastructure may find it difficult to move entirely to the cloud. Instead, they gradually modernize by combining on-prem with cloud services using a Hybrid Cloud.

Use Case:

- Hybrid Cloud allows smooth transition and integration without shutting down mission-critical legacy systems.

Real Example:

- General Electric (GE) uses a Hybrid Cloud strategy to modernize its industrial operations while continuing to support existing on-site systems.

5. Identify a scenario where a community cloud would be the most suitable deployment model.

Scenario: Inter-Governmental Data Sharing

Use Case:

Several government agencies—like the **Police Department**, **Customs**, and **Tax Authorities**—need to:

- Share sensitive information (like criminal records or financial audits)
- Follow **common security policies and legal frameworks**
- Maintain **data sovereignty** (must store data within the country/region)
- **cost-effective** infrastructure shared across departments

Why Community Cloud?

- **Shared infrastructure** lowers costs for all participating agencies
- Built with **common compliance standards** (e.g., GDPR, CJIS, etc.)
- Allows **secure collaboration** without exposing data to outsiders

- Offers better **control** than public cloud but more **affordability** than private cloud

Real-World Example:
European Union (EU) Government Cloud
Several EU departments use a **Community Cloud model** for:

- Law enforcement collaboration
- Judicial and tax data sharing
- Ensuring compliance with **EU data protection regulations (GDPR)**

Managed by trusted entities, with **common governance policies**
Other Possible Use Cases:

- **Universities** sharing research data (e.g., CERN)
- **Healthcare networks** sharing patient records under common laws (e.g., NHS trusts in the UK)
- **Financial cooperatives** maintaining shared ledgers and risk assessment tools

Scenario: Collaborative Healthcare Network Using Community Cloud

Overview

In modern healthcare systems, it is essential for multiple entities—such as **hospitals, clinics, diagnostic labs, pharmacies**, and **government health departments**—to work together to provide high-quality, coordinated care. This requires **seamless, secure, and efficient sharing of data**, which includes sensitive patient records, test results, prescriptions, and treatment plans.

However, due to the **highly sensitive nature of medical data**, healthcare institutions must comply with strict regulations such as **HIPAA (Health Insurance Portability and Accountability Act)** in the United States, or **NDHM (National Digital Health Mission)** in India. This makes it difficult to use public cloud solutions where control is minimal and data is often stored in multi-tenant environments.

Why Community Cloud is Ideal for This Scenario

A **Community Cloud** is designed to support a **specific group of organizations with shared concerns** such as compliance, performance, and security. In this case, the healthcare industry benefits from a shared infrastructure that caters specifically to their needs:

1. Shared Purpose and Governance

All participating healthcare institutions have **common goals**: improving patient outcomes, reducing delays in care, and promoting health research. The cloud environment is jointly governed by these stakeholders, ensuring policies and operations align with medical standards.

2. Regulatory Compliance

A Community Cloud can be **custom-built to comply with healthcare regulations**. This ensures that **electronic health records (EHRs)** and patient information remain secure and private, while being accessible to authorized personnel only.

3. Secure and Controlled Access

Only authorized members of the healthcare community can access the cloud, making it **more secure than public cloud** models. Access control policies, encryption, and data auditing features are implemented according to the needs of the healthcare sector.

4. Cost Efficiency through Resource Sharing

Instead of each hospital maintaining its own expensive IT infrastructure, costs are **shared among all members**, reducing financial burden while still enjoying high-end cloud capabilities.

5. Real-Time Collaboration

Doctors, labs, and pharmacies can **access real-time patient data**, track medical history, and coordinate treatments more effectively, which is especially valuable during emergencies or outbreaks.

Real-World Example: NHS (National Health Service), UK

The NHS in the United Kingdom uses a **Community Cloud infrastructure** to:

- **Securely store and share patient data** between hospitals, clinics, and general practitioners.
- Ensure **compliance with the UK Data Protection Act** and healthcare regulations.
- Promote **efficiency, cost savings**, and better patient outcomes through shared digital platforms.

Additional Example: Academic Research Collaborations
A group of universities working on **climate change research** can benefit from a Community Cloud where they:

- Share large datasets like satellite imagery and weather models.
- Use common tools for analysis while keeping **research data secure and isolated** from the public.
- Reduce costs by **sharing computing power** and storage infrastructure.

Conclusion :
A **Community Cloud** is the most suitable deployment model when:

- Multiple organizations need to **collaborate on sensitive data**.
- There is a **shared interest** in security, compliance, and efficiency.
- The group wants to **balance control with cost-effectiveness**.