Introduction to Cloud computing

UNIT – I (BCSE355L)

Introduction to Cloud Computing

- Cloud computing delivers services over the Internet.

- Includes storage, servers, databases, networking, software, etc.

- You pay only for what you use.

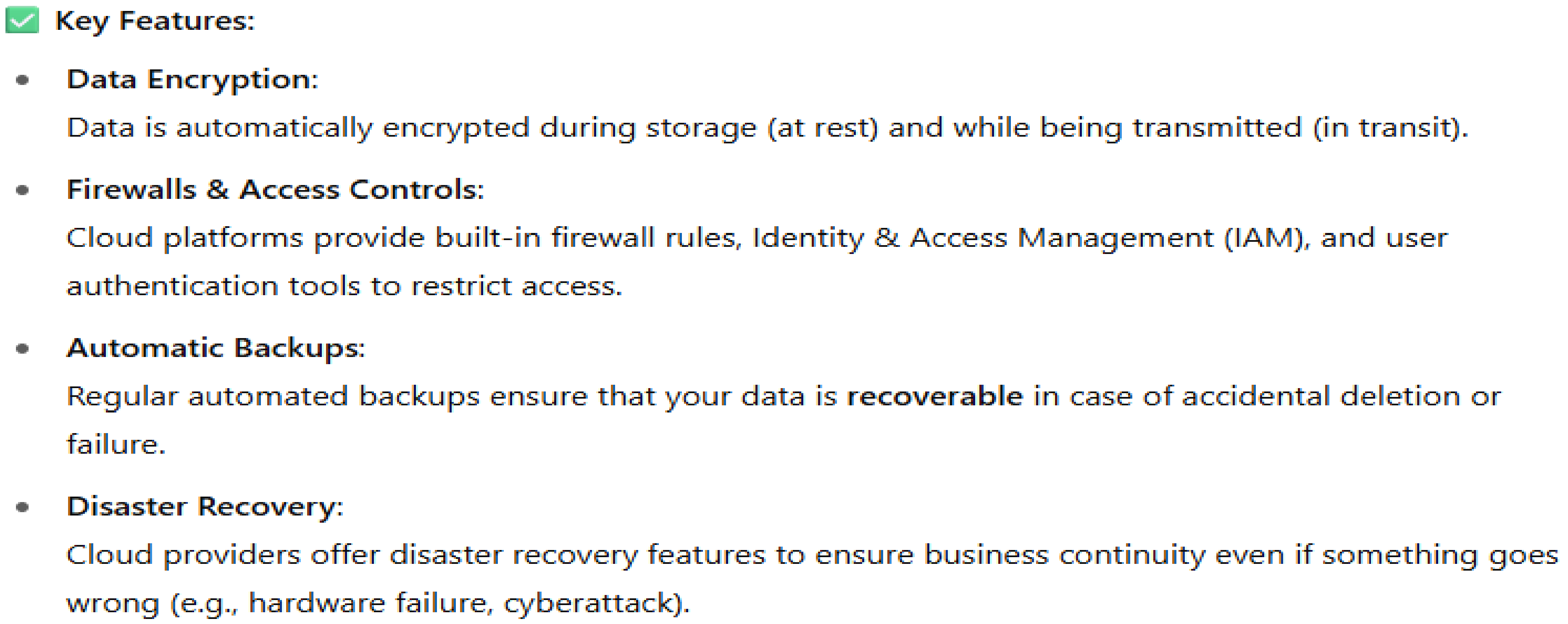
- Example: Google Drive, Dropbox.

Why Use Cloud Computing?

- Cost-Effective – No hardware investment.
- Scalability – Easily increase/decrease resources.
- On-demand Access – Available anytime, anywhere.
- Collaboration – Enables remote teamwork.
- Security & Backup – Built-in by many providers.

Security & Backup – Built-in by Many Providers

Cloud providers like AWS, Google Cloud, Azure, and others offer built-in security features and backup solutions as part of their services. This means users don’t have to set up complex security infrastructure themselves.



✅ **Key Features:**

- **Data Encryption:**
  Data is automatically encrypted during storage (at rest) and while being transmitted (in transit).
- **Firewalls & Access Controls:**
  Cloud platforms provide built-in firewall rules, Identity & Access Management (IAM), and user authentication tools to restrict access.
- **Automatic Backups:**
  Regular automated backups ensure that your data is **recoverable** in case of accidental deletion or failure.
- **Disaster Recovery:**
  Cloud providers offer disaster recovery features to ensure business continuity even if something goes wrong (e.g., hardware failure, cyberattack).

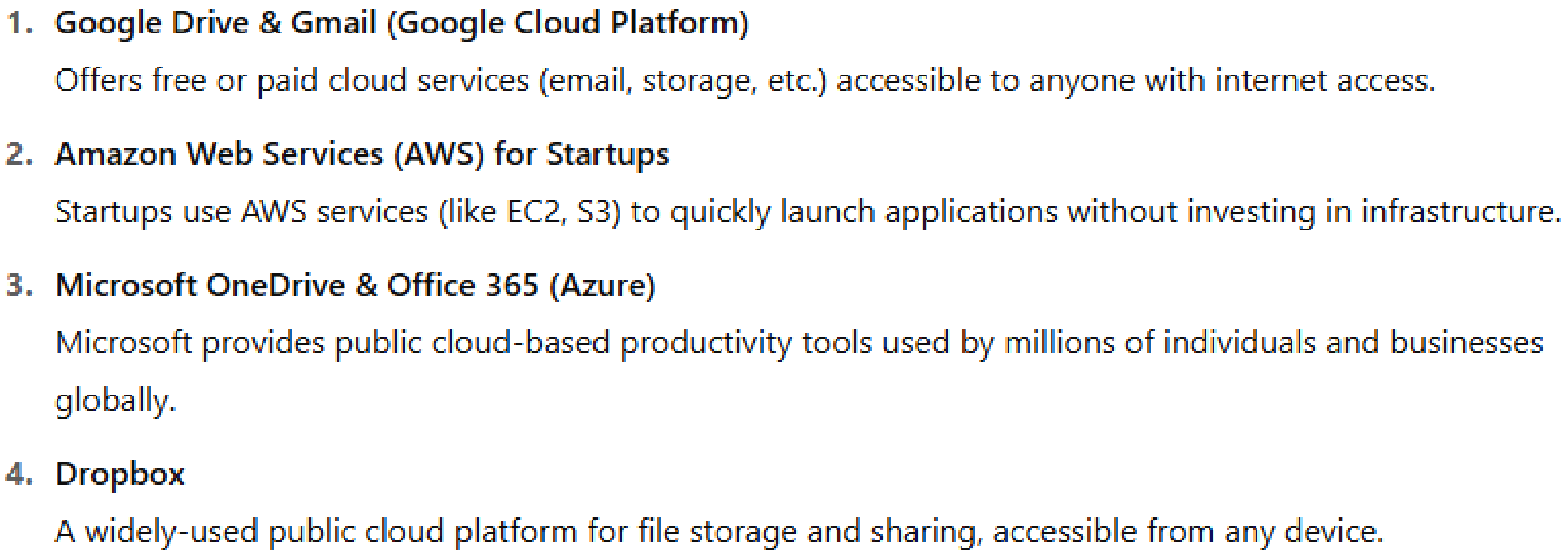
Key Characteristics

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service (Pay-as-you-go)

Types of Cloud Environments

- Public Cloud – Open to all over the Internet (AWS, GCP).
- Private Cloud – For one organization only.
- Hybrid Cloud – Combines public and private clouds.

Public Cloud – Examples



1. **Google Drive & Gmail (Google Cloud Platform)**

   Offers free or paid cloud services (email, storage, etc.) accessible to anyone with internet access.

2. **Amazon Web Services (AWS) for Startups**

   Startups use AWS services (like EC2, S3) to quickly launch applications without investing in infrastructure.

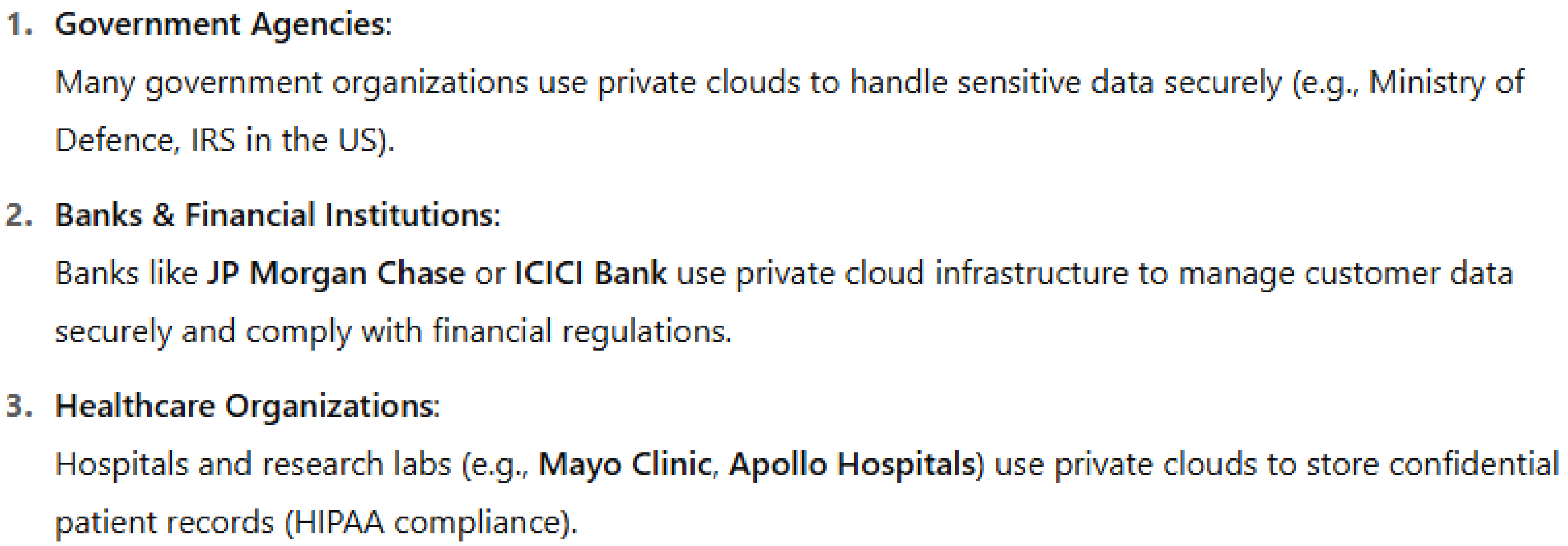
3. **Microsoft OneDrive & Office 365 (Azure)**

   Microsoft provides public cloud-based productivity tools used by millions of individuals and businesses globally.

4. **Dropbox**

   A widely-used public cloud platform for file storage and sharing, accessible from any device.

Private Cloud – Examples



1. **Government Agencies:**

   Many government organizations use private clouds to handle sensitive data securely (e.g., Ministry of Defence, IRS in the US).

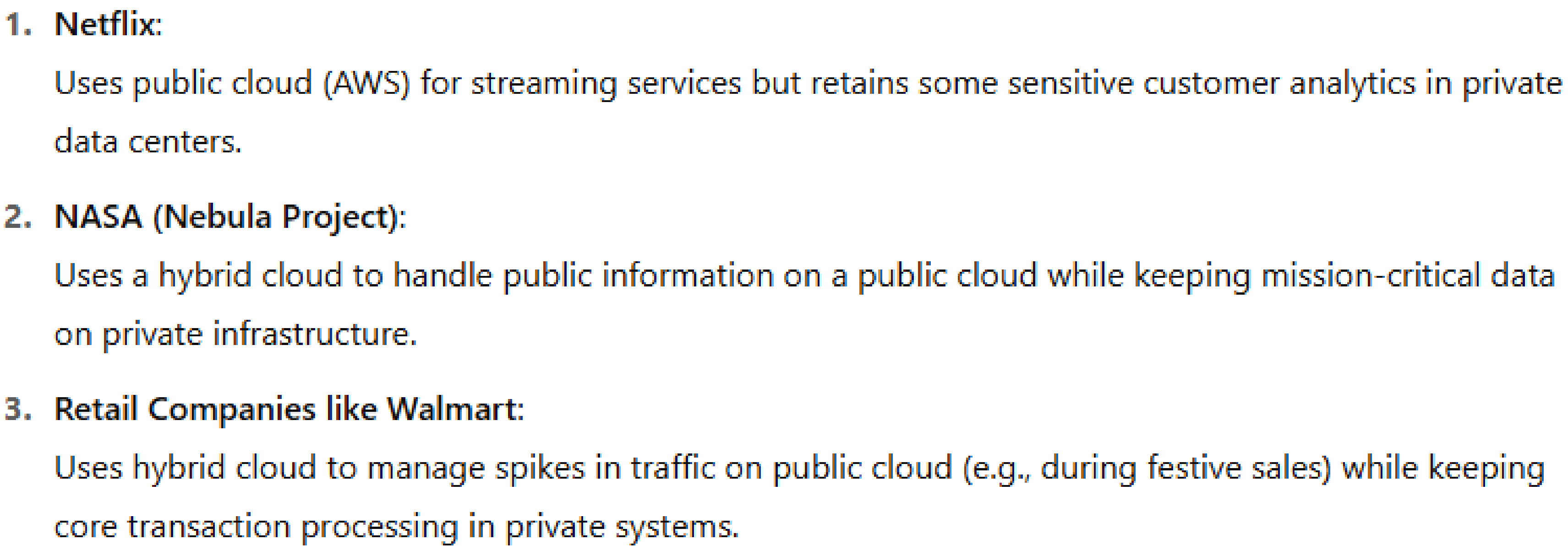
2. **Banks & Financial Institutions:**

   Banks like **JP Morgan Chase** or **ICICI Bank** use private cloud infrastructure to manage customer data securely and comply with financial regulations.

3. **Healthcare Organizations:**

   Hospitals and research labs (e.g., **Mayo Clinic**, **Apollo Hospitals**) use private clouds to store confidential patient records (HIPAA compliance).

Hybrid Cloud – Examples



1. **Netflix:**
   Uses public cloud (AWS) for streaming services but retains some sensitive customer analytics in private data centers.
2. **NASA (Nebula Project):**
   Uses a hybrid cloud to handle public information on a public cloud while keeping mission-critical data on private infrastructure.
3. **Retail Companies like Walmart:**
   Uses hybrid cloud to manage spikes in traffic on public cloud (e.g., during festive sales) while keeping core transaction processing in private systems.

Cloud Service Models

IaaS – Infrastructure (AWS EC2, Azure VM)

PaaS – Platform for development (Google App Engine)

SaaS – Software access online (Gmail, MS 365)

Applications of Cloud Computing

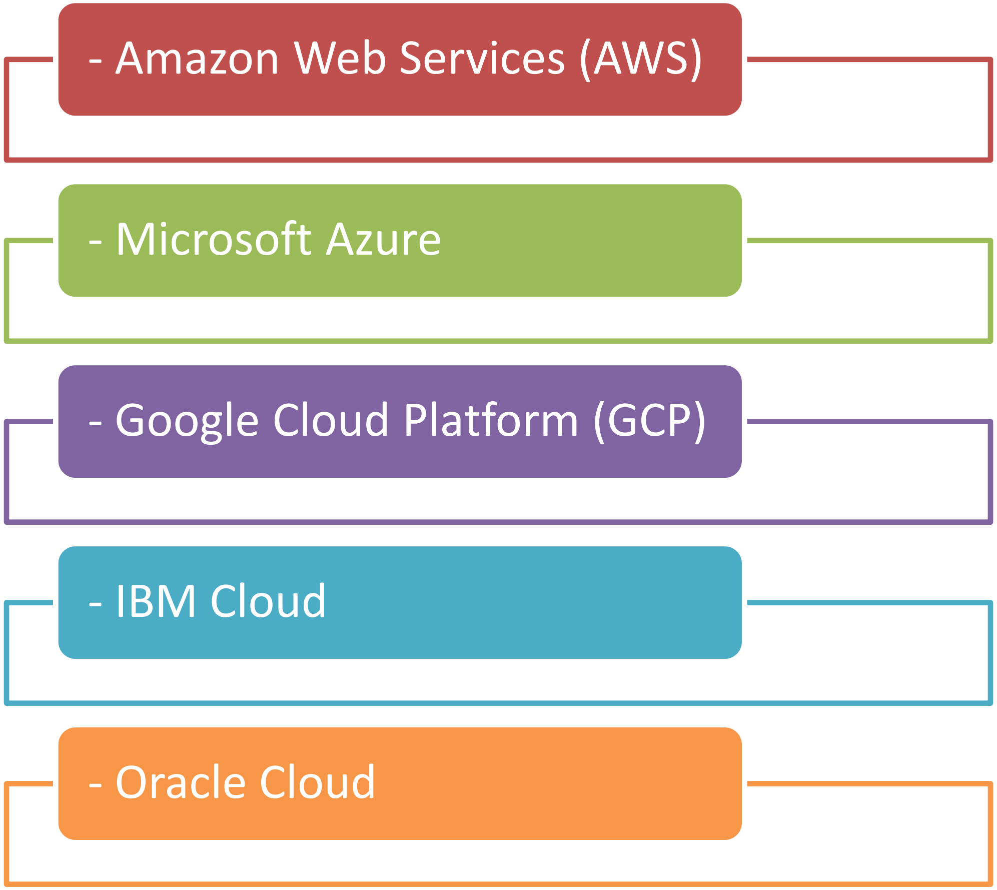
- Email Services – Gmail, Outlook

- Streaming – Netflix, YouTube

- Storage – Google Drive, Dropbox

- E-commerce – Amazon’s cloud-powered features

Cloud Providers



- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- IBM Cloud
- Oracle Cloud

Challenges in Cloud Computing

- Data Security & Privacy

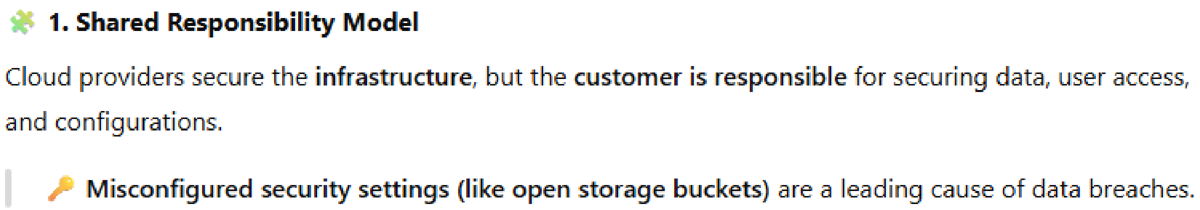
- Internet Dependency

- Compliance & Regulations

- Vendor Lock-in

- Unexpected Costs

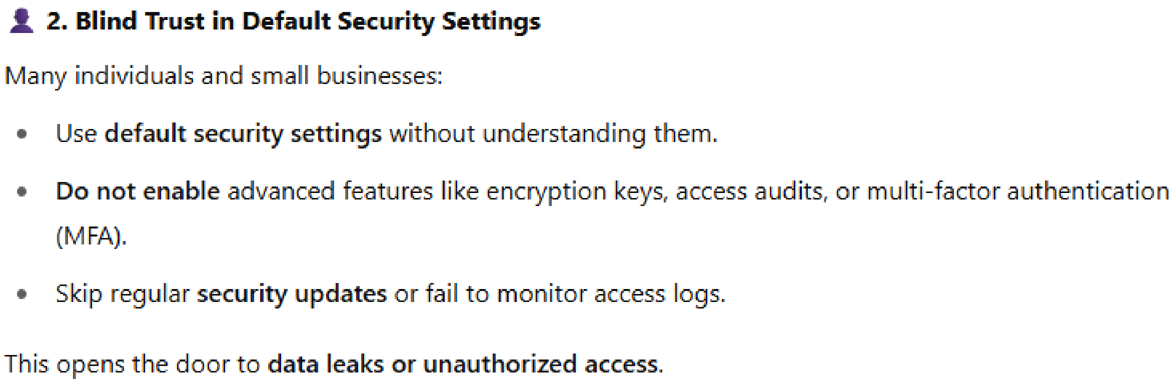
Why Data Security & Privacy is Still a Major Challenge



🧩 1. Shared Responsibility Model

Cloud providers secure the **infrastructure**, but the **customer is responsible** for securing data, user access, and configurations.

> 🔑 **Misconfigured security settings (like open storage buckets)** are a leading cause of data breaches.

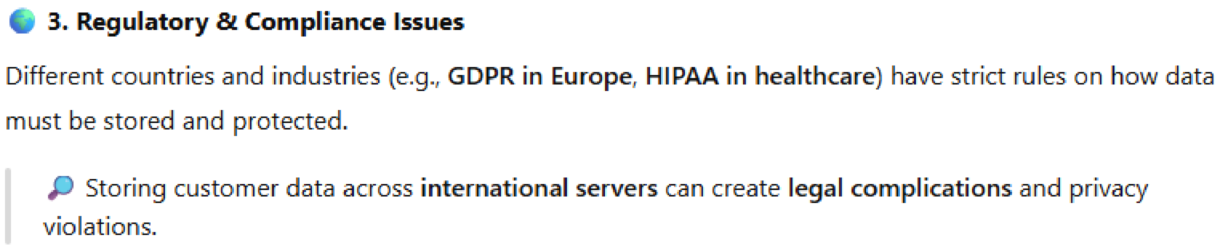


👤 2. Blind Trust in Default Security Settings

Many individuals and small businesses:

- Use **default security settings** without understanding them.
- **Do not enable** advanced features like encryption keys, access audits, or multi-factor authentication (MFA).
- Skip regular **security updates** or fail to monitor access logs.

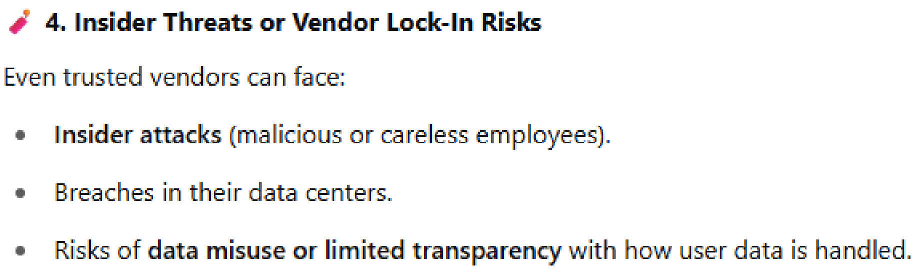
This opens the door to **data leaks or unauthorized access**.



🌍 3. Regulatory & Compliance Issues

Different countries and industries (e.g., **GDPR in Europe**, **HIPAA in healthcare**) have strict rules on how data must be stored and protected.

> 🔎 Storing customer data across **international servers** can create **legal complications** and privacy violations.



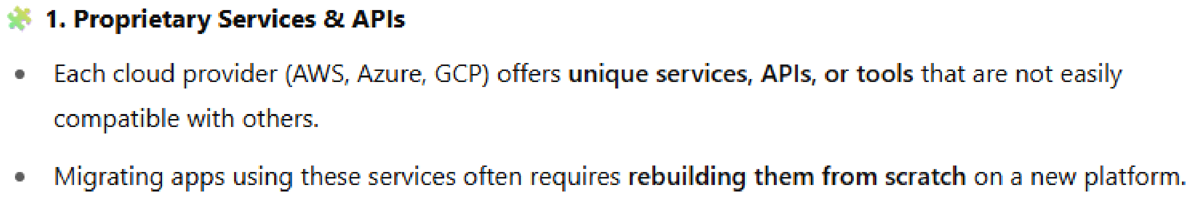
🧨 4. Insider Threats or Vendor Lock-In Risks

Even trusted vendors can face:

- **Insider attacks** (malicious or careless employees).
- Breaches in their data centers.
- Risks of **data misuse or limited transparency** with how user data is handled.

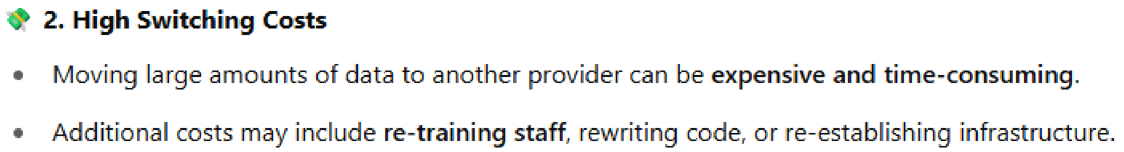
Vendor Lock-In – A Key Challenge

Vendor lock-in refers to the difficulty of switching from one cloud provider to another due to **technical incompatibility**, **cost**, or **complex integration**.



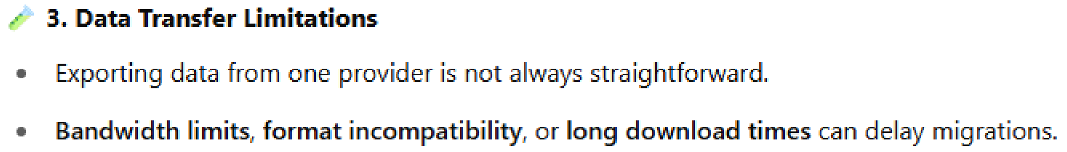
🧩 1. Proprietary Services & APIs

- Each cloud provider (AWS, Azure, GCP) offers **unique services, APIs, or tools** that are not easily compatible with others.
- Migrating apps using these services often requires **rebuilding them from scratch** on a new platform.



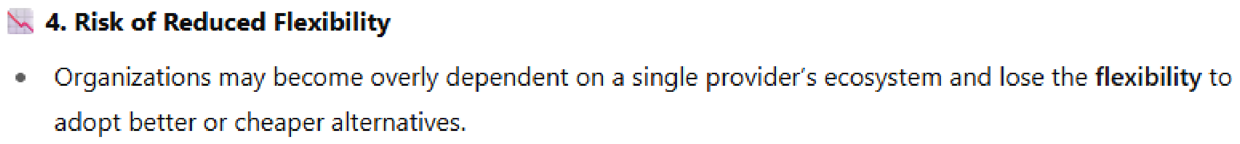
💸 2. High Switching Costs

- Moving large amounts of data to another provider can be **expensive and time-consuming**.
- Additional costs may include **re-training staff**, rewriting code, or re-establishing infrastructure.



🧪 3. Data Transfer Limitations

- Exporting data from one provider is not always straightforward.
- **Bandwidth limits**, **format incompatibility**, or **long download times** can delay migrations.



📉 4. Risk of Reduced Flexibility

- Organizations may become overly dependent on a single provider's ecosystem and lose the **flexibility** to adopt better or cheaper alternatives.

Future of Cloud Computing

- AI & MACHINE LEARNING INTEGRATION

- EDGE COMPUTING

- SERVERLESS ARCHITECTURES

- MULTI-CLOUD ENVIRONMENTS

Summary

- Cloud computing offers flexibility, scalability, and savings.

- Know the models: IaaS, PaaS, SaaS.

- Understand the environments: Public, Private, Hybrid.

- Used across education, healthcare, and e-commerce.