# Unit 4
# Data Storage and Security in Cloud

**Cloud file systems:** GFS and HDFS, BigTable, HBase and Dynamo Cloud data stores: Datastore and Simple DB, Cloud Storage-Overview, Cloud Storage Providers.

**Securing the Cloud-** General Security Advantages of Cloud-Based Solutions, Introducing Business Continuity and Disaster Recovery. Disaster Recovery- Understanding the Threats.

# System Security

- Security issue in Cloud Computing :
  - Cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security.
  - It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

# 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.

# System Security

- Important security and privacy issues :
  - **Data Protection -** To be considered protected, data from one customer must be properly segregated from that of another.
  - **Identity Management -** Every enterprise will have its own identity management system to control access to information and computing resources.
  - **Application Security -** Cloud providers should ensure that applications available as a service via the cloud are secure.
  - **Privacy -** Providers ensure that all critical data are masked and that only authorized users have access to data in its entirety.

# Security in Cloud Computing

- Cloud computing security or cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks.

- Three main factors on which planning of cloud security depends.
  - **Resources that can be moved to the cloud and test its sensitivity risk**
  - **The type of cloud is to be considered.**
  - **The risk in the deployment of the cloud depends on the types of cloud and service models.**

# Security in Cloud Computing

**1) Assessing Resources and Sensitivity Risk**

- Before moving to the cloud, organizations must identify which resources (data, applications, workloads) can be migrated and assess their sensitivity and risk level.
- Example:
- A retail company can move product inventory and marketing data to the cloud with minimal risk.
- However, customer credit card details require higher security controls, such as encryption, access controls, and compliance with PCI DSS standards.
- A healthcare provider moving patient records must follow HIPAA regulations to ensure data confidentiality and integrity.

# Security in Cloud Computing

- 2. Choosing the Right Type of Cloud
- The type of cloud deployment determines security responsibilities and access controls.
- The main cloud types are:
- Public Cloud (e.g., AWS, Azure, Google Cloud) – Managed by third-party providers, cost-effective but less control over security.-A startup can use a public cloud for hosting a website
- Private Cloud – Dedicated infrastructure, higher security but costly.-A bank prefers a private cloud to store sensitive financial data
- Hybrid Cloud – Mix of public and private, balancing cost and security.-A large enterprise might use a hybrid cloud where confidential client data is stored on a private cloud, while less sensitive workloads run on a public cloud

# Security in Cloud Computing

- 3. Risk in Cloud Deployment Based on Cloud & Service Models
- The level of security risk depends on the deployment model (public, private, hybrid, or multi-cloud) and the cloud service model chosen:
- Cloud Service Models and Risk Levels
- Infrastructure as a Service (IaaS) – Provides virtual machines, storage, and networking. Security risks: Misconfigured servers, lack of encryption, DDoS attacks.
- Platform as a Service (PaaS) – Provides frameworks for app development. Security risks: Vulnerabilities in third-party integrations, insecure APIs.
- Software as a Service (SaaS) – Delivers applications over the internet. Security risks: Data breaches, unauthorized access, phishing attacks.

# Cloud Computing Security Controls

- **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.-Multi-Factor Authentication (MFA), IAM, Firewalls,

- **Detective Controls** : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.

- **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack.

- **Deterrent/Compensatory Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.

# Cloud Computing Security Controls

- **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.-Multi-Factor Authentication (MFA), IAM, Firewalls.

- **Detective Controls** : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.

- **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack.

- **Deterrent/Compensatory Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.

# Cloud Computing Security Controls

- **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.-Multi-Factor Authentication (MFA), IAM, Firewalls.

- **Detective Controls** : It identifies and reacts to security threats and control. Some examples of  detective control software are Intrusion detection software and network security monitoring tools.

- **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack.

- **Deterrent/Compensatory Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.

# Cloud Computing Security Controls

- **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.-Multi-Factor Authentication (MFA), IAM, Firewalls.,Zero Trust Security Model

- **Detective Controls** : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools, Antivirus & Anti-malware:

- **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack., Data Backup & Disaster Recovery, **Automated Security Patching**

- **Deterrent/Compensatory Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.-**Security Awareness Training,** Legal & Compliance Policies:**ample:** A **healthcare provider** ensures compliance with **HIPAA** by **training employees** on handling patient data securely.

# Preventive Control in Cloud Computing Security

- **Hardening** - process of reducing security exposure and tightening security controls

- **Security Awareness Training** - process of providing formal cybersecurity education to your workforce

- **Security Guards** - A person employed by a public or private party to protect an organization’s assets.

- **Change Management** - The methods and manners in which a company describes and implements change within both its internal and external processes.

- **Account Disablement Policy** - A policy that defines what to do with user access accounts for employees who leave voluntarily, immediate terminations, or on a leave of absence.

# Detective Control in Cloud Computing Security

- Intrusion Detection & Prevention Systems (IDS/IPS)
- Log Monitoring-Monitors system logs, user activity, and configuration changes in real time.
- Security Information and Event Management (SIEM) Tool-(e.g., Splunk, Microsoft Sentinel).–SIEM systems collect, analyze, and correlate security logs from multiple sources to detect threats.
- Trend Analysis-identifies patterns in cyberattacks, unauthorized access, and system
- Security Audits
- Video Surveillance- Helps in investigating security incidents (e.g., unauthorized physical access).
- Motion Detection- Triggers alerts, alarms, or automatic locks when unauthorized movement is detected.

# Corrective Control in Cloud Computing Security

- **Intrusion Prevention System (IPS) -** A network security technology that monitors network traffic to detect anomalies in traffic flow. IPS security systems intercept network traffic and can quickly prevent malicious activity by dropping packets or resetting connections.

- **Backups And System Recovery -** Backups and system recovery is the process of creating and storing copies of data that can be used to protect organizations against data loss.

# Compensatory Controls in Cloud Computing Security

- alternative security measures used when primary controls are not feasible, too costly, or ineffective in a given cloud environment
- Multi-Factor Authentication (MFA)
- Time-based **One Time-Password (TOTP)** - A temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors.

- **Encryption** - Database security applications, e-mail encryption and other tools.

# Fault Tolerance

- What is fault tolerant system ?
  - Fault-tolerance is the property that enables a system to continue operating properly in the event of the failure of some of its components.
  - Graceful degradation-If its operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naively-designed system in which even a small failure can cause total breakdown.
- Four basic characteristics :
  - No single point of failure
  - Fault detection and isolation to the failing component
  - Fault containment to prevent propagation of the failure
  - Availability of reversion modes

# Fault Tolerance

- Single Point Of Failure (SPOF)
  - A part of a system which, if it fails, will stop the entire system from working.
  - The assessment of a potentially single location of failure identifies the critical components of a complex system that would provoke a total systems failure in case of malfunction.

- Preventing single point of failure
  - If a system experiences a failure, it must continue to operate without interruption during the repair process.

# Fault Tolerance

- Fault Detection and Isolation (FDI)
  - A subfield of control engineering which concerns itself with monitoring a system, identifying when a fault has occurred and pinpoint the type of fault and its location.

- Isolate failing component
  - When a failure occurs, the system must be able to isolate the failure so it does not impact other system parts.

# Fault Tolerance

- Fault Containment
  - Some failure mechanisms can cause a system to fail by propagating the failure to the rest of the system.
  - Mechanisms that isolate a rogue transmitter or failing component to protect the system are required.

- Available of reversion modes
  - System should be able to maintain some check points which can be used in managing the state changes.

# System Resilience

- Resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.

- Resiliency pertains to the system's ability to return to its original state after encountering trouble.

- In other words, if a risk event knocks a system offline, a highly resilient system will return back to work and function as planned as soon as possible.

- **Key Aspects of System Resilience:**

1. **Robustness** – The system’s ability to resist failures and operate under stress.
2. **Redundancy** – Availability of backup components or alternative pathways to maintain functionality.
3. **Fault Tolerance** – The capability to continue functioning despite component failures.
4. **Self-Healing** – Automatic detection and recovery from failures.
5. **Adaptability** – The ability to modify and improve in response to changes and evolving threats.
6. **Monitoring & Detection** – Continuous tracking of system health and early warning mechanisms.
7. **Incident Response & Recovery** – Effective strategies to restore normal operations after disruptions.

# System Resilience

- Disaster Recovery - a strategy and set of processes that ensure an organization can restore critical systems and data after an unexpected disruption, such as cyberattacks, hardware failures, natural disasters, or human errors.

- Some common strategies :
  - Backup
    - Make data off-site at regular interval
    - Replicate data to an off-site location
    - Replicate whole system
  - Preparing
    - Local mirror systems
    - Surge protector
    - Uninterruptible Power Supply (UPS)

# Disaster Recovery in Cloud

- Data is one of the most valuable assets that any company can hold. One of the best ways to store these assets is within the cloud. However, what can you do if a disaster occurs that affects your cloud data?

- Disaster recovery in cloud computing can be done through measures such as **a robust backup system** or even by using **multiple servers in different regions** to reduce the harm that a single disaster could cause.

# Disaster Recovery in Cloud

- Disaster recovery (DR) is the process that goes into preparing for and recovering from a disaster.

- This disaster could take one of a number of forms, but they all end up in the same result: **the prevention of a system from functioning as it normally does**, preventing a business from completing its daily objectives.

# Key Components of Disaster Recovery

- **1. Disaster Recovery Planning (DRP)** : A **Disaster Recovery Plan (DRP)** is a documented strategy that outlines steps to recover IT infrastructure, data, and applications.
- It typically includes:

  ✓ **Risk Assessment** – Identifying potential threats (e.g., data breaches, power failures).

  ✓ **Recovery Objectives** – Setting **RTO** (Recovery Time Objective) & **RPO** (Recovery Point Objective).

  ✓ **Backup Strategy** – Defining data backup frequency and storage locations.

  ✓ **Failover & Failback** – Switching to backup systems and restoring normal operations.

  ✓ **Testing & Drills** – Regularly testing DR procedures to ensure effectiveness.

# Key Components of Disaster Recovery

**2. Key Disaster Recovery Metrics**

- **Recovery Time Objective (RTO)**
- The **maximum acceptable downtime** before a system must be restored.
- Example: If RTO = 1 hour, the system must be recovered within 1 hour after failure.
- **Recovery Point Objective (RPO)**
- The **maximum data loss** measured in time before recovery.
- Example: If RPO = 15 minutes, backups must occur at least every 15 minutes to minimize data loss.
- **Goal**: Lower RTO & RPO = Faster and more effective disaster recovery.

# Kinds of Disasters

- **Natural disasters**: **uncontrollable environmental events**
- Causes severe damage to IT infrastructure, data centers, and cloud computing services.
- Lead to **system failures, data loss, network outages, and business disruptions**
- Rarer but not infrequent
- Earthquakes – Can destroy data centers, servers, and network connections.
- Floods & Hurricanes – Water damage to on-premise servers, power outages.
- Fires & Wildfires – Physical destruction of data centers and equipment.
- Tornadoes & Storms – Power failures, damaged fiber optic cables.
- Extreme Heat or Cold – Overheating of data centers or freezing of hardware.

# Kinds of Disasters

- **Human disasters:**
- Caused by **human errors, cyberattacks, or intentional**
- **Cyberattacks** – Ransomware, DDoS attacks, phishing, malware infections.
  - **Insider Threats** – Employees accidentally or intentionally harming systems.
  - **Terrorist Attacks** – Physical destruction of IT infrastructure.
  - **Theft** – Unauthorized access to hardware or sensitive data.
  - **Negligence & Accidental Data Deletion** – Mistaken deletion of critical files or misconfigured systems.

# Kinds of Disasters

- **Technical disasters**: Perhaps the most obvious of the three, technical disasters
- Failures in IT infrastructure, software, or networks.

◆ **Hardware Failures** – Server crashes, storage drive failures, network device malfunctions.

◆ **Software Bugs & Glitches** – Unpatched vulnerabilities, misconfigurations, OS crashes.

◆ **Cloud Outages** – AWS, Azure, or Google Cloud failures impacting multiple services.

◆ **Power Failures** – Blackouts, unstable power supply, UPS failures.

◆ **Internet & Network Failures** – ISP outages, DNS failures, bandwidth overload.

# Disaster Recovery

- In the event of a disaster, a company with disaster recovery protocols and options **can minimize the disruption to their services and reduce the overall impact on business performance**.

- Minimal service interruption means a reduced loss of revenue which, in turn, means user dissatisfaction is also minimized.

# Disaster Recovery

- Having plans for disaster in place also means your company can define its **Recovery Time Objective (RTO**) and its **Recovery Point Objective (RPO)**.

- The RTO is the **maximum acceptable delay between the interruption and continuation of the service** and the RPO is the **maximum amount of time between data recovery points.**

# Disaster Examples in Past

- A data Centre run by OVHCloud was destroyed in early 2021 by a fire. 4 datacentres destroyed.3.6 million websites were impacted, including banks, government sites, cryptocurrency exchanges, and gaming services.
- In June 2016, storm and heavy rain in Sydney battered the electrical infrastructure and caused an extensive power outage. This led to **the failure of a number of Elastic Compute Cloud instances and Elastic Block Store volumes** which hosted critical workloads for a number of large companies.
- **Major outage** in **Simple Storage Service (S3)** due to **human error**. :In February 2017 an Amazon employee was attempting to debug an issue with the billing system when they accidentally took more servers offline than they needed to.
- Google Cloud Storage Failure (2020) – A Technical Disaster: a **Google Cloud Storage failure** resulted in **permanent data loss** for some customers due to a **misconfiguration issue**

# Disaster Recovery Methods

- **Backup and restore – Simplest method,** Backing up data and restoring it is one of the easiest, cheapest and fastest ways to recover from a cloud computing disaster.
- Data is backed up regularly (daily, weekly, or real-time) and restored when needed.
- Can be stored on-premises, in the cloud, or offsite.
- Automate backups to prevent human error.
- This can be mainly used to mitigate regional disasters such as natural disasters by replicating the data and storing it in a geographically different location.

# Disaster Recovery Methods

- **Cold Site Recovery**
- A secondary location that has basic IT infrastructure but no active data or systems.
- Requires manual setup and data restoration after a disaster.
- Slow recovery, but low cost.
- Minimal Maintenance

Best Practices:

Use for non-critical systems where cost savings are a priority.

Combine with cloud backups for faster restoration.

# Disaster Recovery Methods

- **Warm Site Recovery**
- A **partially operational backup** site with some pre-installed infrastructure & data.
- Requires configuration & data restoration but is faster than a cold site.
- Compared to a **Cold Site**, a **Warm Site reduces downtime**
- Best Practices:

  ✅ Use scheduled data replication to keep it updated.

  ✅ Ideal for medium-priority applications that can afford some downtime.

# Disaster Recovery Methods

- Hot Site Recovery
- A **fully functional, real-time** duplicate of your main site.
- that runs 24/7, ensuring instant failover in case of a disaster
- Minimal downtime because it automatically takes over if the primary system fails.
- Expensive but essential for mission-critical businesses (e.g., banks, hospitals).
- Best Practices:
  ✅ Use real-time data synchronization between primary and hot sites.

# Disaster Recovery Methods

| Strategy | Cost | Recovery Speed | Best For |
|---|---|---|---|
| **Cold Site** | Low | Slow (Manual Setup) | Small businesses, cost-sensitive industries |
| **Warm Site** | Medium | Quick (Partially Ready) | Healthcare, e-commerce, retail |
| **Hot Site** | High | Instant (Fully Running) | Banking, stock markets, emergency services |

# Disaster Recovery Methods

- **Pilot Light –**
- The Pilot Light strategy is a disaster recovery (DR) approach where a minimal version of the system runs in the backup environment, ready to be scaled up when needed.
- A small, essential part of the infrastructure is always running in the DR site
- Critical data (databases, storage, configurations) is replicated continuously.
- If the primary system fails, the DR site can quickly scale up by launching additional resources.

# Disaster Recovery Methods

- **Multi-site deployment –**
- high-availability disaster recovery (DR) strategy where an application is deployed across multiple geographic locations
- Although the most expensive solution of the three, multi-site deployment provides the most comprehensive solution to regional disasters.
- These regions can be actively used or on a standby in case of disaster in a different region.-ensuring **minimal downtime and data loss**.
- Real-time data replication ensures consistency across sites.
- 1) Active-Active Deployment –**high availability** (e.g., banking, e-commerce).
- 2) Active-Passive Deployment-cost savings
- 3) Multi-Cloud Deployment –**fault tolerance**.

# Disaster Recovery Methods

- Example: Multi-Site Deployment on AWS
- Amazon Route 53 (DNS Failover) – Routes traffic to the available site.
- AWS Global Accelerator – Improves performance by directing users to the closest region.
- Multi-Region RDS & S3 Replication – Ensures real-time data synchronization.

# Disaster Recovery Methods

| Strategy | Cost | Recovery Speed | Best For |
|---|---|---|---|
| Cold Site | Low | Slow (Manual Setup) | Low-priority apps |
| Pilot Light | Medium | Faster (Scaling Needed) | Cost-sensitive businesses |
| Warm Site | Higher | Quick (Partially Running) | Medium-priority apps |
| Hot Site | Highest | Instant (Fully Running) | Mission-critical apps |
| Multi-Site | High | Instant (Zero Downtime) | Enterprise, Cloud-Native Apps |

# Security Issues in Cloud

- CC offers scalability, flexibility, and cost savings, but it also introduces security risks
  - Data Loss
  - Interference of Hackers and Insecure API’s
  - User Account Hijacking
  - Changing Service Provider
  - Lack of Skill
  - Denial of Service (DoS) attack

# Data Loss

- Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage/data breach.

- our sensitive data is in the hands of Somebody else, and we don't have full control over our database.

- So if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.
- Threat: Unauthorized access to sensitive cloud data due to weak encryption, misconfigurations, or cyberattacks
- Example: In 2019, Capital One suffered a data breach exposing 100M+ records due to a misconfigured firewall.
- 🔷 Mitigation:

✅ End-to-end encryption (in transit & at rest)
✅ Regular security audits & vulnerability assessments
✅ Strict access control policies (IAM, Zero Trust)

# Insecure API's and Interfaces

- Easiest way to communicate with Cloud is using API.
- So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain.
- Threat: Poorly secured APIs can be exploited by hackers to access cloud data and services.
- 🔹 Example: The Facebook API breach in 2018 exposed 50M user accounts due to token vulnerabilities.
- 🔹 Mitigation:
- ✅ Use OAuth, OpenID, and API gateways for authentication
- ✅ Implement rate limiting & API monitoring
- ✅ Regularly update API security patches

# User Account Hijacking & Credential Theft

- Most serious security issue in Cloud Computing.
- If somehow the Account of User or an Organization is hijacked by Hacker. Then the hacker has full authority to perform Unauthorized Activities.
- Threat: Attackers can steal login credentials through phishing or brute-force attacks.
- 🔹 Example: The 2017 Deloitte breach occurred due to an admin account without two-factor authentication (2FA).
- 🔹 Mitigation:
- ✅ Use Multi-Factor Authentication (MFA/2FA)
- ✅ Enforce strong password policies & rotation
- ✅ Monitor login anomalies with AI-based security tools

# Insider Threats

- **Threat**: Employees or contractors may **intentionally or accidentally** expose sensitive cloud data.

  🔹 **Example**: An **ex-Amazon employee** was found guilty of hacking Capital One's cloud servers.

  🔹 **Mitigation**:

  ✅ **Strict role-based access control (RBAC)**
  ✅ **Regular security training for employees**
  ✅ **Behavior analytics to detect unusual access patterns**

# Denial of Service (DoS) attack

- This type of attack occurs when the system receives too much traffic.
- Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it
- **Threat**: Hackers overload cloud servers, making them unavailable for users.
  - Example: In 2020, Amazon AWS mitigated a massive 2.3 Tbps DDoS attack, the largest ever recorded.
  - Mitigation:

✅ Use cloud-based DDoS protection (AWS Shield, Cloudflare, Azure DDoS Protection)

✅ Implement rate limiting & IP filtering

✅ Deploy auto-scaling to absorb traffic spikes

# Lack of Skill

- While working, shifting to another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn’t have skilled Employee.
- So it requires a skilled person to work with cloud Computing.
- Example: In 2017, a misconfigured AWS S3 bucket exposed millions of U.S. voter records.
- The issue was caused by human error due to a lack of cloud security knowledge.

🔷 Mitigation Strategies:

✅ Train IT teams in cloud security best practices (AWS/Azure/GCP certifications).

✅ Use automated security tools to detect misconfigurations.

✅ Regular security audits to identify weaknesses.

# Changing Service Provider

- Vendor lock In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another.

- For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they face various problem's like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that.
- Example:
- In 2020, the Google Cloud outage prevented users from accessing services like Gmail and YouTube.
- Companies relying only on Google Cloud faced business disruptions with no quick failover option.

# Cloud security

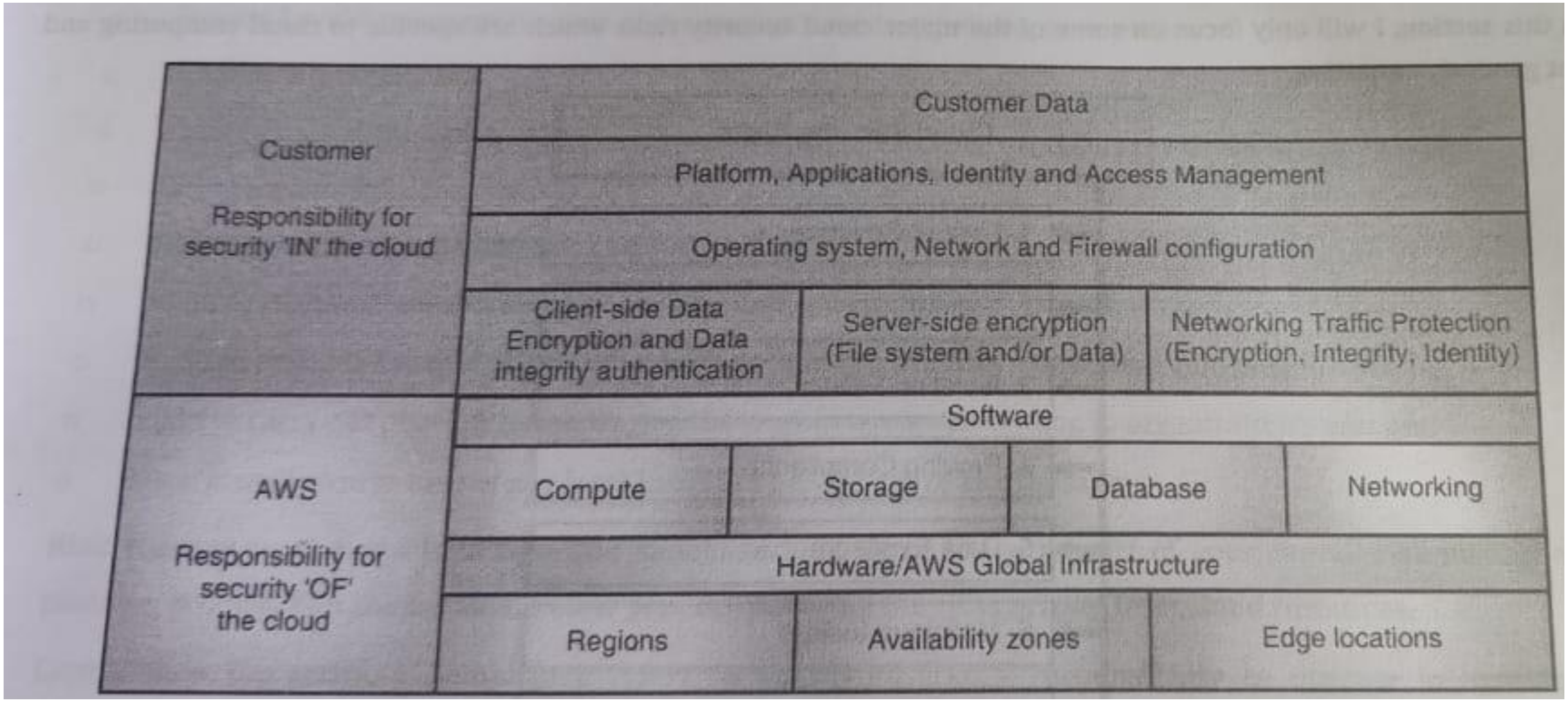
- Cloud security is a collection of procedures and technology designed to address external and internal threats to business security.
- Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats.
- Cloud security is a responsibility that is shared between the cloud provider and the customer.

# Cloud security

- responsibilities that are *always* the provider’s:safeguarding of the infrastructure itself, as well as access to, patching, and configuration of the physical hosts and the physical network on which the compute instances run and the storage and other resources reside.
- responsibilities that are *always* the customer’s: managing users and their access privileges (identity and access management), the safeguarding of cloud accounts from unauthorized access, the encryption and protection of cloud-based data assets,
- responsibilities that *vary depending on the service model*

# Cloud security

- AWS is responsible for security OF the cloud: responsible for managing and securing underlying h/w and datacentres and operations
- Customer is responsible for security IN cloud: Anything above the service software layer is customer’s responsibility
- Eg Microsoft releases security patch for windows OS.
- Its user’s responsibility to install the patch



| | | | | |
|---|---|---|---|---|
| Customer<br>Responsibility for security 'IN' the cloud | Customer Data | | | |
| | Platform, Applications, Identity and Access Management | | | |
| | Operating system, Network and Firewall configuration | | | |
| | Client-side Data Encryption and Data integrity authentication | Server-side encryption (File system and/or Data) | Networking Traffic Protection (Encryption, Integrity, Identity) | |
| AWS<br>Responsibility for security 'OF' the cloud | Software | | | |
| | Compute | Storage | Database | Networking |
| | Hardware/AWS Global Infrastructure | | | |
| | Regions | Availability zones | Edge locations | |

# Basic terms and concepts

- Assets
- Security controls
- Threat
- Vulnerability
- Risk
- Exposure
- Accountability

# Basic terms and concepts

- Assets: An asset is anything valuable that needs protection.
- Security controls: countermeasures, mechanism /action to safeguard an asset
- Threat: Potential danger that can exploit asset
- Vulnerability: A vulnerability is a weakness that a threat can exploit.
- Risk :Likehood of a harm occurring to an asset, risk can never be zero.,reduce it to acceptable level
- Exposure:refers to the damage or impact caused if a risk occurs.
- Accountability:A way to record your actions

# Basic terms and concepts

| Security Concept | Debit Card & PIN Example |
|---|---|
| Asset | Debit card and PIN |
| Security Controls | PIN authentication, encryption, fraud alerts |
| Threat | Card skimming, phishing, shoulder surfing |
| Vulnerability | Weak PIN, writing PIN on the card, using an unsecured ATM |
| Risk | High if PIN is weak or exposed, low if security measures are strong |
| Exposure | Financial loss if the card and PIN are stolen |
| Accountability | Bank secures transactions, user protects PIN,report card lost |

# General understanding of security

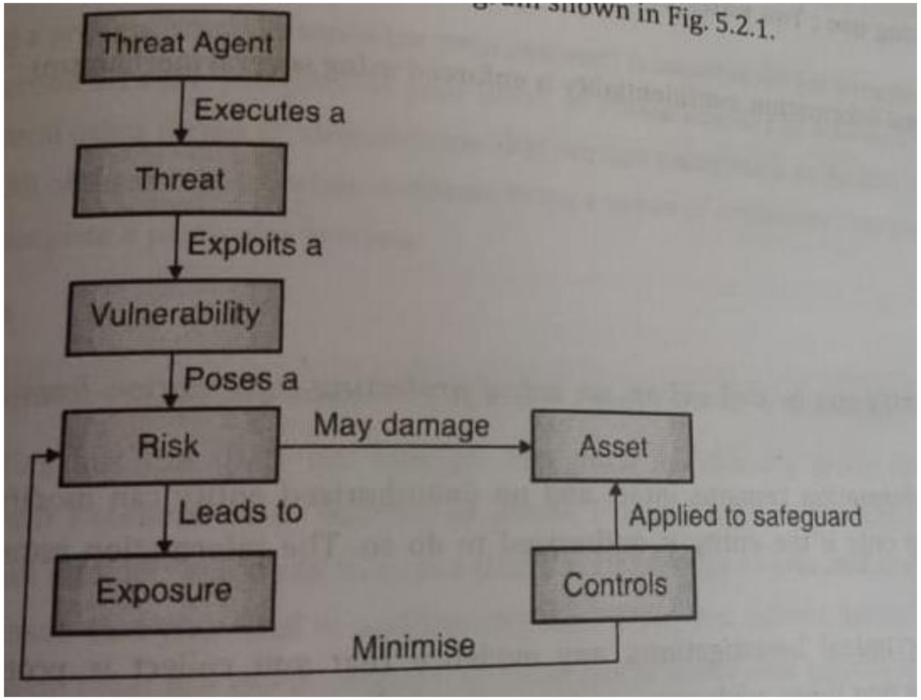
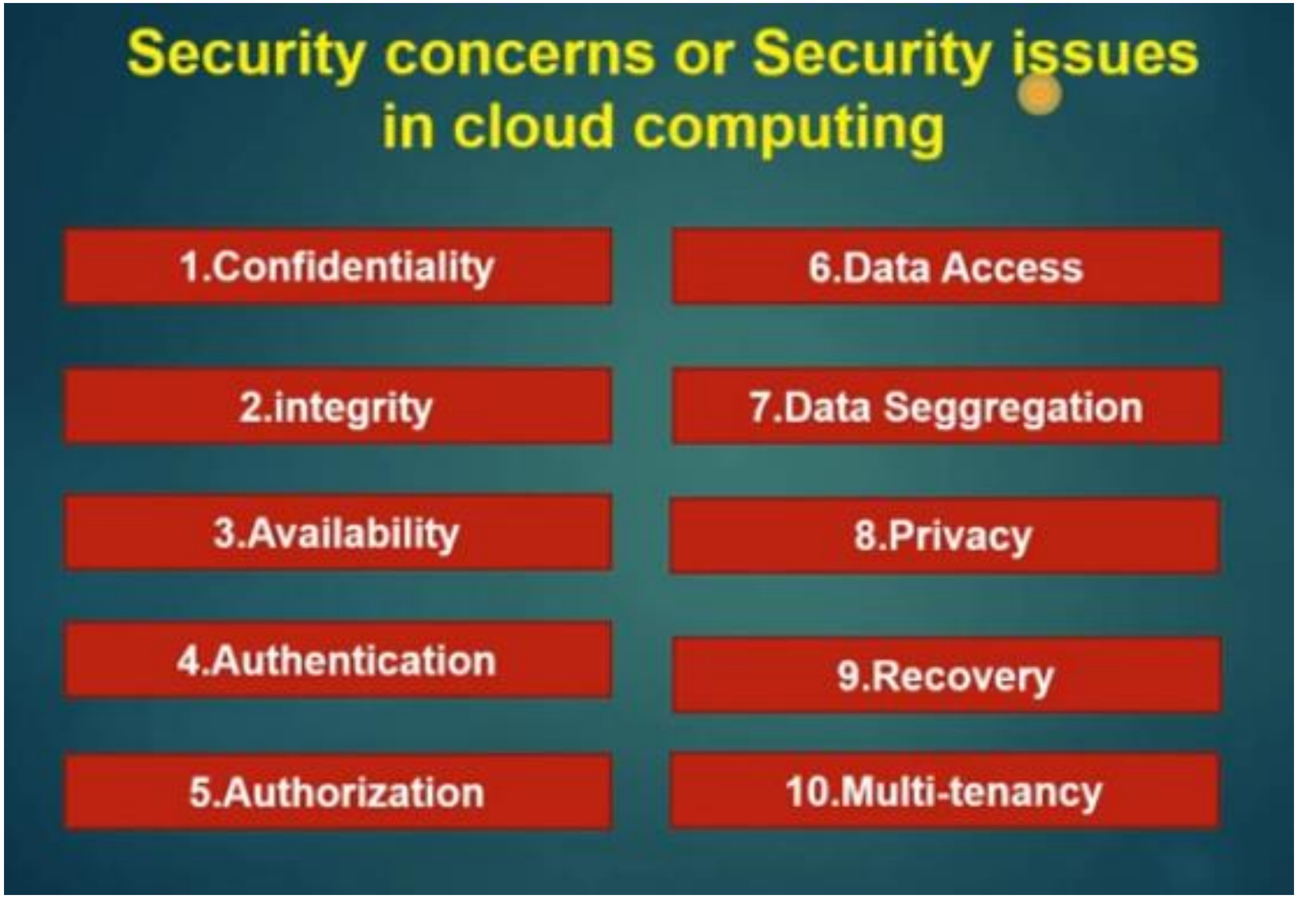


Image Source: Pravin Goyal, “Cloud Computing”, Techknowledge publication

# Security concerns



Security concerns or Security issues in cloud computing

1.Confidentiality

2.integrity

3.Availability

4.Authentication

5.Authorization

6.Data Access

7.Data Seggregation

8.Privacy

9.Recovery

10.Multi-tenancy

# Security concerns

- Confidentially,integrity and availability -3 pillars of security
- Data Confidentiality is **whether the information stored on a system is protected against unintended or unauthorized**
    - Protected at rest
    - Protected in motion
    - Protected during use
    - It can be enforced by using encryption and access control

# Security concerns

- The Data Integrity is simply termed as **no corruption in the data that can be assured with consistency and accuracy over the time**
  - Protecting information from unauthorized modification
  - Access Control & IAM
  - Hashing
  - Data Replication

- Availability: **data is accessible to users whenever needed, without disruptions**. It guarantees that **stored, processed, and transmitted data remains reachable** even in the event of failures, cyberattacks, or natural disasters.
  - Access control
  - Isolation
  - Back up
  - Disaster recovery

**redundancy, failover systems, and distributed architectures**

# Security concerns

- Data availability means that information must be available when authorized persons need it.
- Data availability is one of the biggest concerns of service providers.
- If for some reason a Cloud service is interrupted, many clients will be affected.
- Service providers contractually Undertake to ensure an availability level of 99.9%.
- In addition, the duplication of data and physical resources and their distribution on different locations increases the level of availability.
- There are many risks that could affect the availability of data in the Cloud such as storage reliability, dependence on internet connection and technical failures. Generally, data availability in Cloud is more reliable than on a traditional infrastructure as large suppliers like Google, Amazon and Microsoft are better equipped to manage these risks than a simple individual or a company.

# Security concerns

- Identification process of **recognizing and verifying a user, device, or system before granting access to cloud resources**
- Eg icard,adhar,pan,login to any account
- Authentication is the process of determining the identity of a client.
  - Biomeric,pin,OTP.SFA,MFA,
- Authoriation:Access rights
  - A way to determine what resources an entity can access
  - Voter card example
  - Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) Policy-Based Access Control (PBAC)

•**Authentication**: "Who are you?" (e.g., verifying identity with a password or biometrics).
•**Authorization**: "What are you allowed to do?" (e.g., restricting access to sensitive cloud files based on user roles)

# Security concerns

- Accountability: a way to record your actions, how securely your system is operating
  - Logging & Monitoring,IAM,
- Data access how users, applications, and systems retrieve, modify, or store data in a cloud environment.
  - Public Access
  - Private Access
  - Role-Based Access (RBAC)
  - Attribute-Based Access (ABAC)
  - Time-Based Access
  - Just-in-Time (JIT) Access

# Security concerns

- Data segregation: the process of separating certain sets of data from other data sets so that different access policies can be applied to those different data sets.
- logically or physically separating data belonging to different customers, applications, or business units within a shared cloud environment. This ensures that one customer’s data is not accessed, altered, or compromised by another customer.
- Data segregation is critical in **multi-tenant cloud environment**

# Security concerns

- **Data privacy** is another problem often associated with confidentiality.
- Privacy concerns personal information that must be hidden from unauthorized persons. The user privacy is associated with the collection, use, communication, storage and destruction of personal data.
- Encryption at Rest & in Transit
- IAM)
- Zero Trust Security Model

# Security concerns

- Data recovery in cloud security ensures that **data can be restored** in case of accidental deletion, cyberattacks, system failures, or disasters.
- Backup & Restore
- Replication
- Hot,warm cold, site recovery

# Security concerns

- Multitenancy is a cloud architecture where **multiple customers (tenants) share the same computing resources** (e.g., servers, storage, databases) while keeping their data isolated and secure.
- Best Practices for Securing Multitenancy
  - Strong Data Segregation
  - Role-Based Access Control (RBAC)
  - Activity Logging & Monitoring
  - Resource Allocation & Throttling

# THANK YOU!