



The Shirpur Education Society's

R. C. Patel College of Engineering & Polytechnic, Shirpur

Department of Computer Engineering



Course Title: Cloud Computing (CLC)

Course Code: 315325

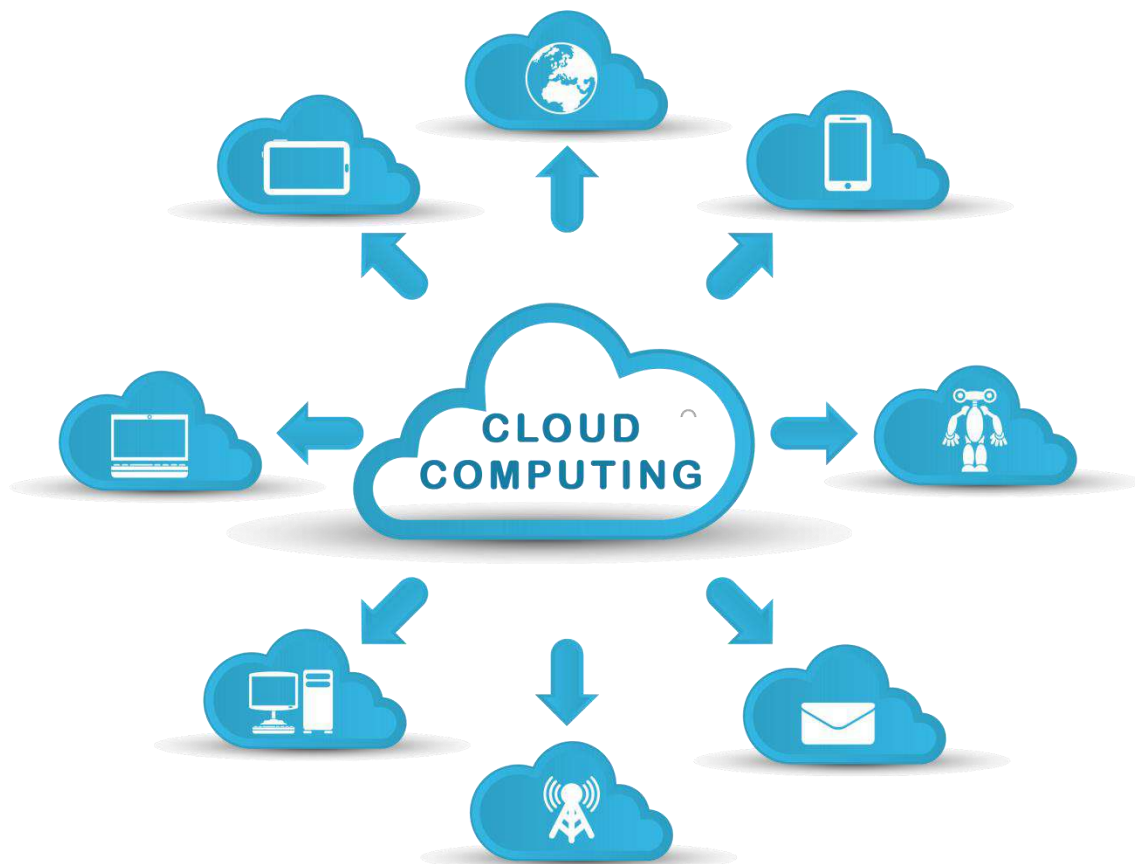
Programme Name: Computer Engineering / Computer Science & Engineering / Computer Technology/ Computer Software Technology/Computer Hardware & Maintenance/ Computer Science & Information Technology.

Semester: Fifth

Unit – IV: Security in Cloud Computing

Total Marks: 14

Prepared By: Prof. S. S. Teli



Unit-4: Security in Cloud Computing.

CO4: Apply Security in cloud computing.

Total marks :- 14. Remember Level - 02 marks
Understanding - 06 marks.
Application - 06 marks.

* Introduction :-

- Security in cloud computing :-

- Cloud computing allows users & organization to store data, run application, and access computing resources through the internet.

- Since data and services are stored on ~~malware~~ remote server, they may face threats, such as unauthorized access, data leakage, malware, hacking, account hijacking.

- Cloud Security refers to the technologies, policies, procedures, and security controls used to protect cloud based:

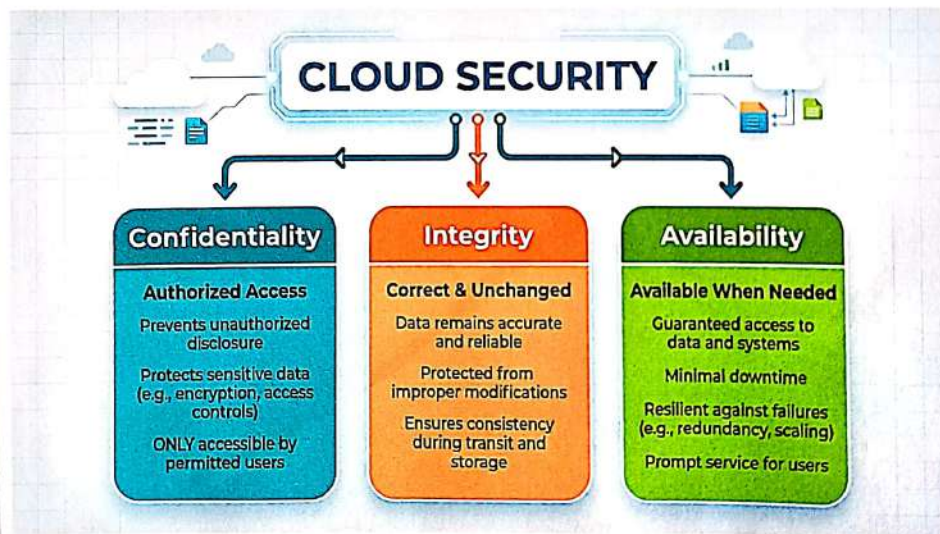
- Data
- Application
- Infrastructure
- Networks
- User Accounts.

- Objective of Cloud Security:

a) Confidentiality :- Data should be accessed only by authorized user.

b) Integrity :- Data should not be modified or destroyed without authorization

c) Availability :- Data & cloud services should be available when required.



- Security Planning in cloud computing :-

- Factors to consider while planning cloud security.
- Before Implementing cloud security, an organization should consider :-

a) Type & sensitivity of data :

Identify which data is confidential, important & sensitive.

b) Type of cloud deployment model :

Public, Private, Hybrid or Community.

c) Type of cloud service model

IaaS, PaaS, SaaS

d) Possible security risk.

Identify threats

e) Access Requirement :

Decide who can access which cloud resources.

f) Backup & recovery requirements

Plan for data backup & disaster recovery.

- Types of cloud security controls.

a) Deterrent Control:

- Deterrent Control are designed to block nefarious attack (malicious) on cloud system.

eg:- warning messages,
Security policies.

b) Preventive Control:

- Preventive Control make the system resilient to attack by eliminating vulnerabilities.

eg:- Firewall, Authentication.

c) Detective Control:-

- It identifies and reacts to security threats & control.

eg:- Intrusion Detection Software
Network Security monitoring
tools.

d) Corrective Control:

- Reduce damage & restore system

eg:- Backup & Recovery.

4.1 Cloud security Concepts :-

- a) multi-tenancy
- b) Virtualization
- c) Data Outsourcing & Trust management
- d) Metadata Security.

a) multi-Tenancy :-

- It is a fundamental cloud model where a single physical or virtual infrastructure is shared among multiple users (Tenants)

- Each tenant's data and resources are logically isolated but physically shared.

- example :- cloud provider may provide the same physical server to

- College A

- College B

- Company C

- Although hardware is shared

- Each organization data should remain isolated.

- Security Concerns/Risks :-

i) Data isolation Risk (Data leakage between tenants)

Multi-Tenancy Architecture

System Design

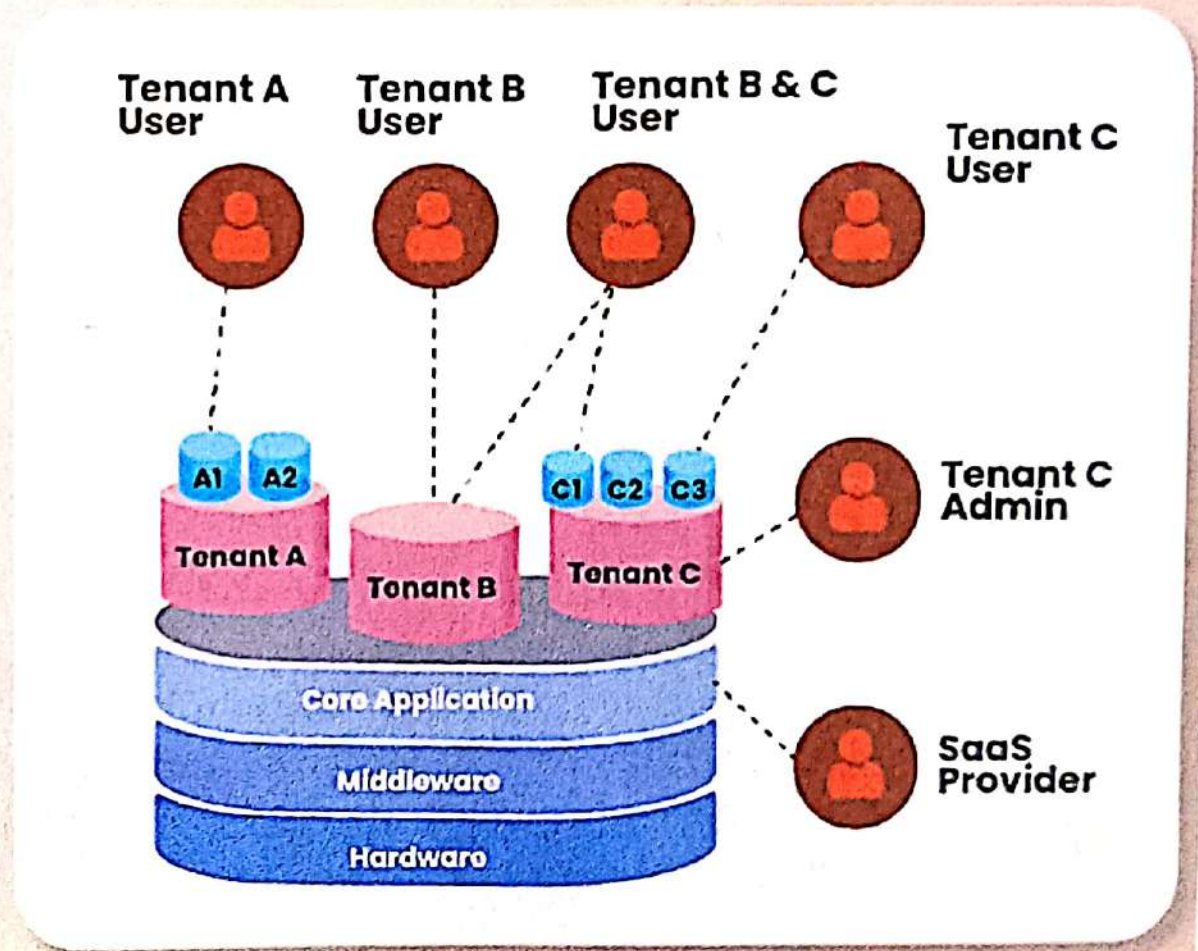


Fig:- Multi-Tenancy.

ii) Unauthorized Cross-tenants access.

iii) Resource Contention -

Malicious tenants may consume more resources, affecting other.

iv) Side channel Attack :-

(Resource

Attacker may infer sensitive data by analyzing shared CPU

v) Noisy Neighbour Problem

One tenant's heavy workload degrades other performance.

- Security mechanism / Measures :-

i) Strict Access-Control Policies to enforce tenant isolation

ii) Virtual Private Cloud for logical isolation

iii) Encryption of tenant data

iv) Tenant specific monitoring & auditing

v) Sandboxing & containerization to minimize cross-tenant attacks.

b) Virtualization :-

- Virtualization is the backbone of cloud computing.

- It enabling multiple virtual machine to run on a single physical server through a hypervisor.

- It provides scalability & efficient resource utilization

- Security Concerns / Risks :-

- i) Hypervisor attacks: if compromised, attackers can control all hosted VM.

- ii) VM Escape:

- malicious code inside a VM breaks isolation to access other VM's or host system.

- iii) VM Sprawl :-

- Rapid growth of unmanaged VMs increase attack surface.

- iv) Insecure VM images :-

- VM images can leak sensitive data

- v) Data leakage during VM migration

- Security measures / mechanisms :-

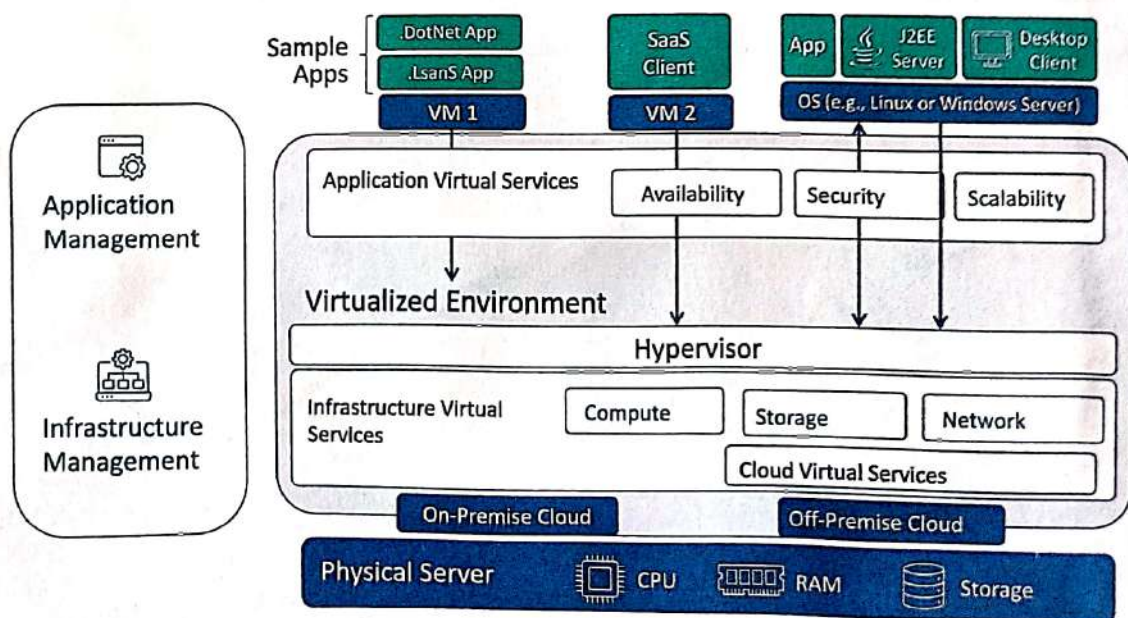
i) Hardened Hypervisor with minimal attack surface.

ii) Regular patching & updates of virtualization software.

iii) Network Segmentation between VMs to prevent lateral movement.

iv) VM introspection tools to monitor activities within VMs.

v) Secure VM migration protocols to prevent interception during live migration.



c) Data outsourcing & Trust management

- In cloud computing, data is stored & processed on third party servers, i.e. outsourced to cloud service provider.
- Since the user does not have complete physical control over the data.
- So trust is important (Confidentiality, integrity, & availability).
- Security concerns / Risks :-

i) Loss of data control :-

- Users cannot directly manage or monitor their outsourced data.

ii) Data Breaches :

- providers may mishandle or leak sensitive data.

iii) Data Integrity :

- Corruption by malicious insiders or attackers.

iv) Legal / Compliance issues :-

- Data stored across borders may face regulatory challenges.

- Security measures / mechanism :-

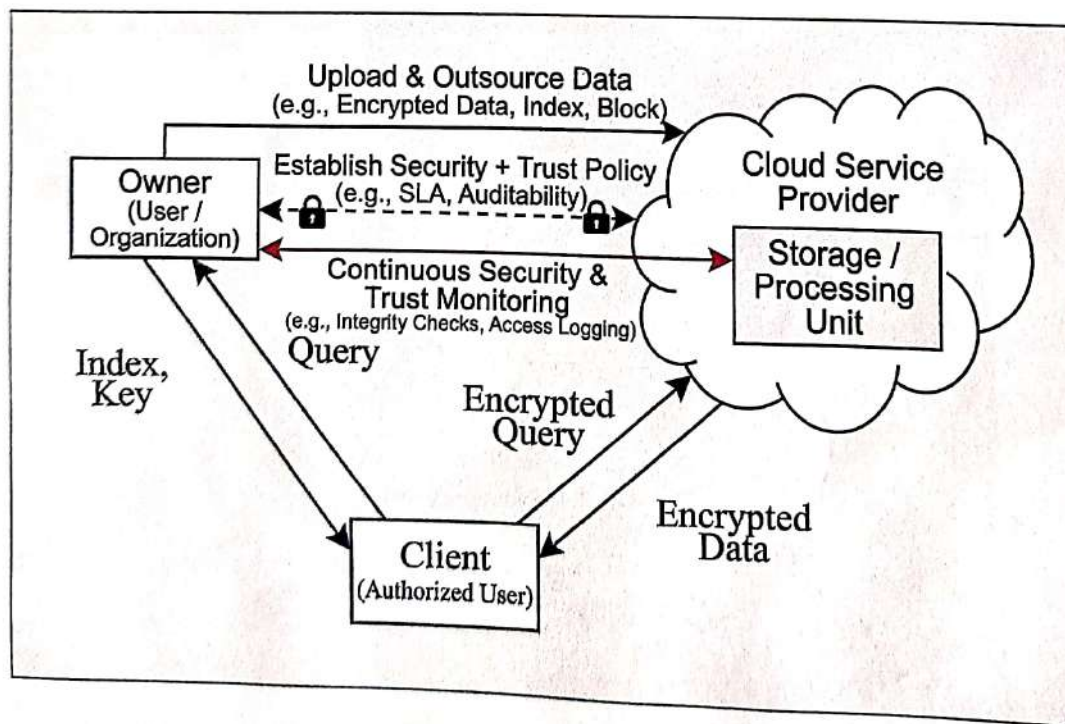
i) Data Encryption (Before upload)

ii) Attribute based access control.

iii) Third party auditing for verifying provider compliance.

iv) Blockchain Based Trust Framework for transparent transaction

v) Service Level Agreements (SLA) with well defined rules.



D) Metadata Security :-

- metadata is data about data
- Such as file names, Timestamps, location info, ownership, and access patterns in cloud system.
- Metadata plays a key role in storage, indexing & retrieval.
- A file may be encrypted, but metadata itself may contain sensitive information.
- Security Concerns/Risk.

i) Sensitive information leakage:

- Metadata may reveal usage patterns, identity.

ii) Inference Attacks:

- Attacker can analyze metadata to derive confidential info.

iii) Unauthorized Access:

- If metadata is not protected, attackers can manipulate.

iv) Big data Exposure:

- Cloud providers handling massive metadata may leak information.

- Security mechanisms :-

i) metadata Encryption to hide sensitive attributes.

ii) Access control & role based restriction.

iii) Secure logging & auditing.

iv) Differential Privacy techniques.

4.2 Cloud Risk (Concept, Types)

- Cloud Risk refers to the possibility of loss, damage, unauthorized access, service failure, or legal problems associated with cloud data, application, and services.
- It affects on:
 - Confidentiality.
 - Integrity.
 - Availability.
 - Privacy.
 - Business operations.
- Types of Cloud Risk:-

a) Policy & Organizational Risk:-

- It arises from governance gap, undefined operational roles, inadequate employee training, & rigid vendor relationship rather than technical flaws in the software.

i) Lack of proper cloud security policy

- An organization may not have clear rules regarding cloud usage & security.

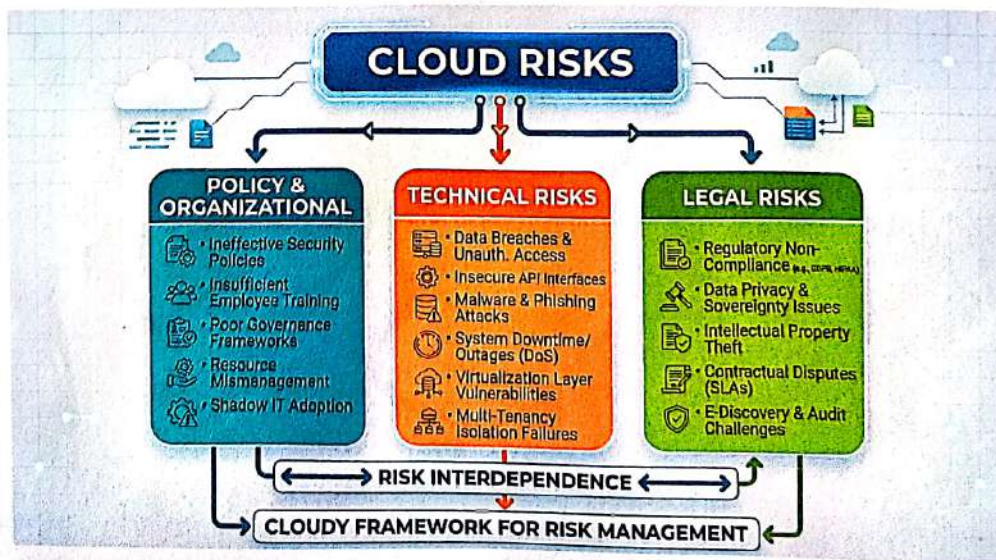
ii) Lack of Skilled Employees :-
- Employees may not have sufficient knowledge of cloud security.

iii) Vendor Lock-in :-
- organization becomes dependent on a particular cloud provider.

iv) Poor Governance :-
- Unclear responsibilities can lead to security problems.

v) Lack of Backup & Disaster Recovery Planning :-
- Failure to plan recovery may result in data loss.

vi) Poor Security Awareness :-
- Employees may fall victim to phishing or weak passwords.



b) Technical Risks :-

- Technical risks arise from hardware or software vulnerabilities, system mis-configurations, insecure interfaces, and failures in cloud infrastructure.

i) Cloud Misconfiguration :-

- Incorrect security setting that expose sensitive data.

ii) Insecure APIs & Interfaces :-

- weakly authenticated or unencrypted application programming interfaces (API) that attackers exploit to breach cloud services.

iii) Insufficient Multi Tenancy Isolation :-

- Failure to logically separated shared physical hardware
- Cross Tenant data leakage
- side channel attacks.

iv) Weak Access Control & Identity management :-

- Lack of multi factor authentication
- Poor key management.

v) Data Breach and Account Hijacking.

- Theft of sensitive records.
- Administrative login through brute-force attacks.

vi) Denial of Service (DOS/DDoS)

- High volume traffic floods targeting cloud endpoints.

vii) Lack of Continuous Automation & monitoring.

- Not available automated posture tool.
- eg:- CSPM Tool.

c) Legal Risks :-

- It involves compliance failures, contractual liabilities that arise when storing or processing data.

i) Data ownership & custodianship :-

- Lack of clarity in service contracts regarding who legally owns.

ii) Data location & Jurisdictional Conflicts.

- Cloud data distributed across multiple global data centers.
- Conflicts occur which law apply.

iii) Regulatory Non-compliance :-

- failure to meet mandatory regional & industry data protection framework.

- Due to this heavy financial penalties.

iv) Data Privacy Violations :-

- Personal information must be protected.

- Processing user data without proper legal consent.

v) Service Legal Agreement Gaps :-

- contract that fail to clearly outline

- An unclear SLA may create dispute regarding responsibility.

vi) Intellectual Property Risks :-

- cloud storage & sharing may create ownership or copyright issues.

4.3 : Data Security :-

- Data security refers to the protection of data against unauthorized access, misuse, corruption, or loss.
- Data security focuses on Content-Centric protection (Protecting the data itself rather than just the network perimeter.)
- Technologies for Data security :-

i) Database outsourcing & Query Integrity :-

- Cloud storage is essentially a form of database outsourcing, where data is stored on third party servers.
- Ensuring that queries & data retrieval remain accurate and trustworthy, without tampering or unauthorized modifications.

ii) Data Integrity in Untrustworthy Storage :-

- major problem in cloud adoption is data loss or corruption.
- To overcome this, technologies use cryptographic hash functions and proof of retrievability checks to verify that stored data is ~~an~~ unaltered and complete.

iii) Web Application Based Security:-

- Data in the cloud is often accessed via web application & browsers.
- So securing web interface become critical.
- Protects the cloud browsers and API interface against common web attacks.
such as
- Such as SQL Injection, Cross side scripting (XSS), Session hijacking.
- web security has an even higher importance than in traditional IT.

iv) multimedia Data Security:-

- The rise of high speed networks and large bandwidth connections.
- A significant amount of multimedia data (Audio, video, image) is stored in the cloud.
- multimedia requires specialized security techniques due to its size, format.
- Security requirements include encryption, digital watermarking, and access control mechanisms.

v) Data masking Technology:-

- Sensitive data can be masked or anonymized when transmitted through gateways to external cloud.
- This ensures that Confidential elements are hidden from unauthorized users.

vi) Secure Logic migration & Execution:-

- Confidential data is first assigned a security level.
- Such data can then be processed in an in-house sandbox through a secure gateway.
- Unauthorized applications or processes are blocked from accessing.

vii) Data Traceability Technology:-

- Traceability ensures that all data movements are logged & monitored.
- Log record the flow of data in/out.
- In this it enables auditing, accountability, and forensic analysis in case of security incidents.

• Data security Risk management

- Risk management is a structured, cyclical process designed to protect the CIA Triad (Confidentiality, Integrity, Availability) of organization assets.

Step:-

i) Identification of Risks :-

- Creating an inventory of critical information assets such as customer data, Employee record, Financial information, Cloud stored business application

- Identify Threats & Vulnerabilities:

- Threats:-

- External (Hacker, ransomware, phishing, DDoS)
- Internal (Insider misuse, human error)

- Vulnerabilities :-

- weak or reused passwords,
- outdated software,
- Unsecured wireless network,
- Lack of encryption
- Misconfigured cloud storage.

ii) Risk Assessment :-

a) Likelihood Analysis :-

- Estimating how probable a threat is to occur.

b) Impact Analysis :-

- measuring the severity of potential damage.

c) Prioritization :-

- Risk are ranked using qualitative methods (low, medium, high).

iii) Risk mitigation strategies :-

- organization can adopt one or more approach to deal with risk.

a) Risk Avoidance :-

- Completely eliminating high risk activities.

eg:- not store credit card details.

b) Risk Reduction :-

- Implement safeguards like,
 - Firewall
 - Encryption
 - Intrusion detection
 - multi factor authentication.

c) Risk Transfer :-

- Shifting Risk responsibility to third parties
- eg:- Outsourcing to manage security.
- Buying Cyber insurance.

d) Risk Acceptance :-

- Accepting minor risks that are less costly to tolerate than mitigate.

iv) Implementation of security controls :-

a) Preventive Controls :-

- It measures that stop incidents before they occur.
- Strong access control
- Encryption network firewall.

b) Detective Control :-

- Identify and alert when incident happen.
- Log monitoring
- Audit
- Anomaly Detection tools.

c) Corrective Controls :-

- Automated data backup,
- Patch management
- Disaster recovery execution.

V} Continuous monitoring & Review :-

- Risk mng is a continuous process.
- It tracked & re-evaluated regularly.
 - Threat Intelligence
 - Audits & Compliance checks
 - Policy updates

4.4: Digital Identity & Access management (IAM)

- Identity & access management (IAM) is a security framework that defines and manages - digital identities
 - User Roles
 - Access privileges
- Based on all this only authorized user perform approved action.

i) Authentication vs. Access management.

- Authentication :- (who are you?)
 - Verifies the actual identity of a user or system.
 - something you know :- Passwords, username.
 - something you have :- Physical token, smartphone (OTP)

- Something you are :- Biometric Auth.

• Access management :- (What can you do?)

- It refers to what a user can see & do after logging in.

- Example :- Verified identity does not mean unlimited access.

- Provide specific access to specific person.

ii) The 3 factors of Authentication :-

• Something you know

• Something you have

• Something you are

iii) Importance of IAM in cloud.

- Identity is the new perimeter :-

• Because cloud services are accessed from anywhere & any device over the internet.

- Prevent Credential Based attacks.

- Stop unauthorized access.

• Password leak

• Phishing.



- Centralized Auditing :-

- Tracks user activity & access, logs for regulatory compliance.

45: Content Level Security: Pros & cons, feature of security as a cloud services

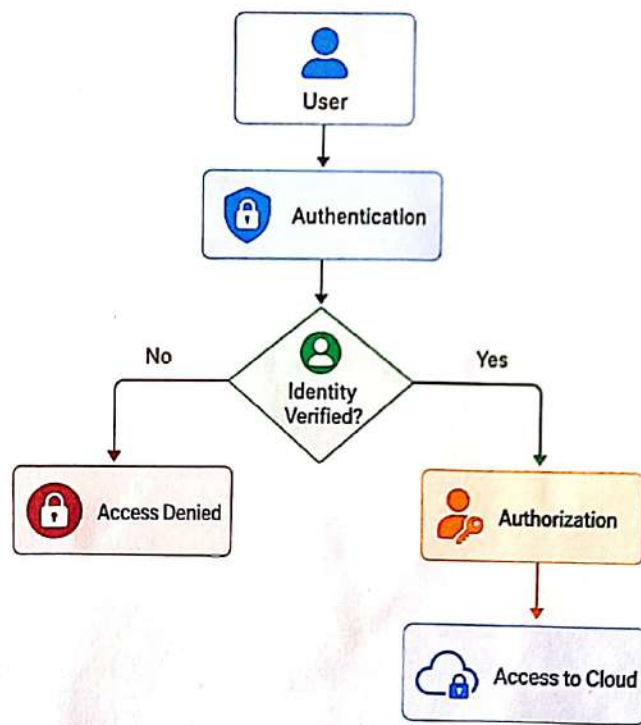


Fig. Authentication & Authorization

4.5 Content Level Security:- (Asset Based Security.)

- Security features are embedded directly into the content rather than the network or device.

(Diagram on next 2 Page)

- Advantages (Pros):-

a) Granular Access Control.

- It Restrict specific action like who can view, edit, print, email, or share.
- Using this it prevents unauthorized access & sensitive data handle by authorized person.

b) Data Protection Across Location

- Information remains protected even if it is moved to a remote location or accessed via mobile device.

c) Time Limited Access:

- Time based restriction
- Content can automatically expire after set period.

d) Reduce Risk of Data Breaches:

- By securing the content directly, organization minimize the risk that lost or stolen devices, unauthorized cloud storage.

e) Regulatory Compliance :-

- All sensitive information is handled according to compliance rules.

f) Protection Beyond Traditional Firewall.

- If attacker bypass network security but still data is protected.
- Because data encrypted or access controlled by content level security.

- Disadvantages (cons) :-

1. Complex Implementation :-

- Content level security can be technically complex, required detail policy, encryption setup, and integration with existing system.

2. Performance Overhead :-

- Continuous encryption, authentication checks, and access tracking can slow down system performance.

3. Employee Training

3. Integration challenges :-

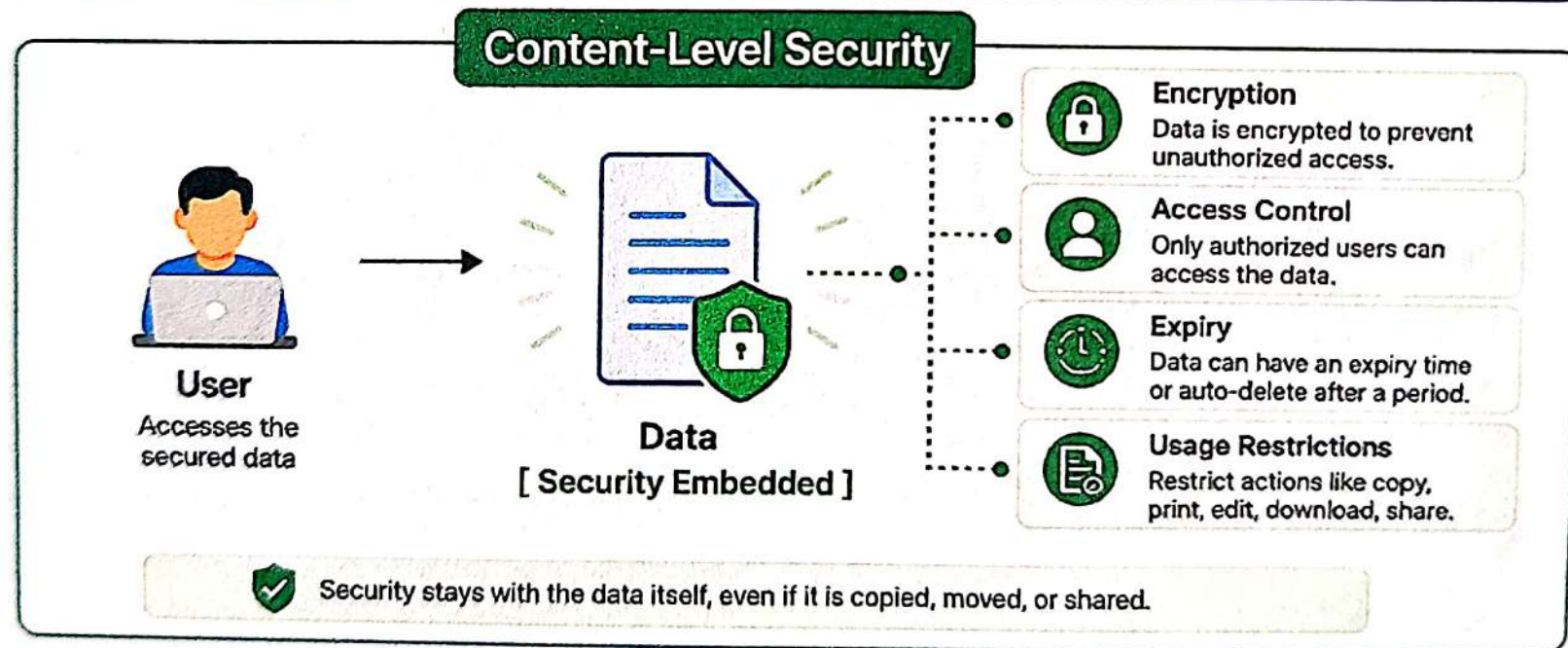
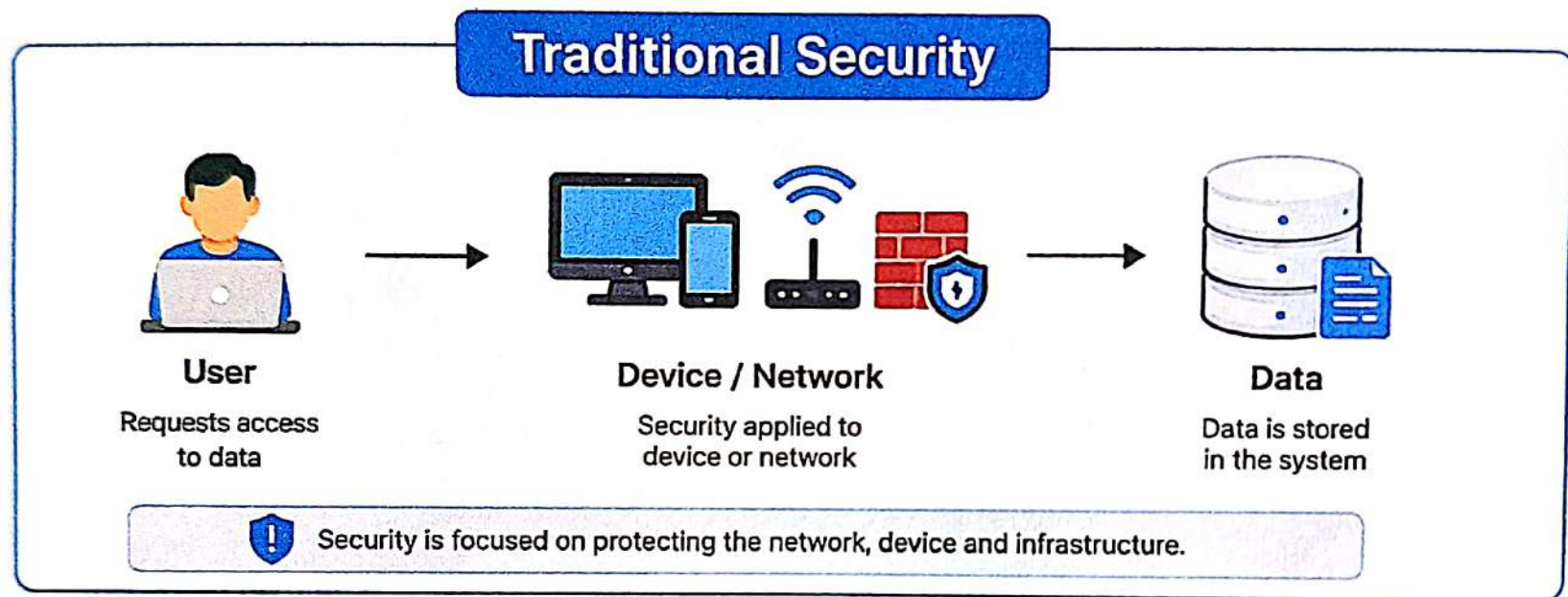
- It integrates seamlessly with legacy application, cloud services,

--	--	--	--

- or mobile platforms can be difficult.

4. Maintenance Costs :-

- maintaining, updating and auditing content level security policies require continuous effort, resources.



Fig!- Content Level Security.

- Security as a cloud Service :- (SECaaS)

- Security as a service is a cloud based model in which security services are provided to users through the Internet by third party provider.

• Features of Security as a cloud Services :-

1) Centralized Policy management :-

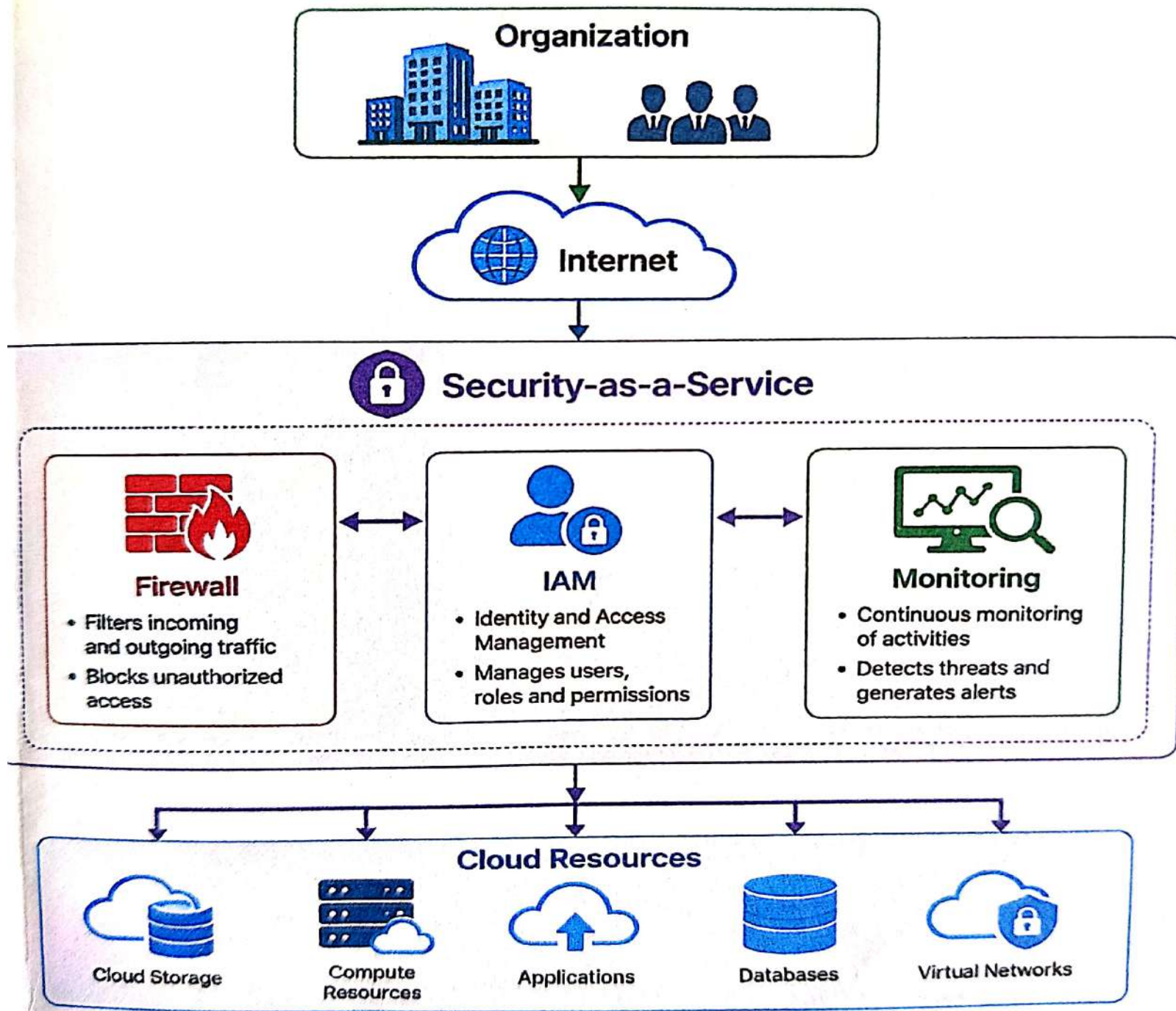
- security rules and policies can be managed, created, updated and applied from a centralized cloud platform.

2) Scalability :-

- Security services can increase or decrease according to requirement.

3) Remote Accessibility :-

- Users & administrators can securely access security services through the Internet.



4) Automatic Update :-

- Security Software & protection mechanisms can be updated automatic

5) Monitoring & Logging :-

- User activities & security events are continuously monitored.

6) Threat Detection:

- Detect malware, unauthorized access, & suspicious activities.

7) Integration:

- It can work with cloud application, storage, and other services.

8) Cost Effectiveness :-

- Reduce the need to purchase and maintain expensive security infrastructure.

* Add on topic concepts.

- Steps to implement cloud Data security :-

1. Identify & classify data.

2. Identify Risk. (find all threat)

3. Define Security policies. (create Rule)

4. Implement Strong Authentication.
(use username, password, MFA)

5. Apply access control.

6. Encrypt Data.

7. Take Regular backup.

8. monitor & Audit.

9. Update & Patch Systems.

10. Review and improve Security.

XOX.

Chauhan

Unit - IV Security in Cloud Computing (14 Marks)

Question Bank

R-Level (Remembering — 2 Marks)

- List the types of cloud risks. (QP1: Q.1f / QP2: Q.1d)
- List the three authentication factors used in Digital Identity Management with one example each.
- Define Metadata Security in cloud computing and state why it is important.

U-Level (Understanding — 4 / 6 Marks)

- Compare server side and client side encryption. (Write any four points) (QP1: Q.2d - 4M)
- Explain identity management and access facility in cloud computing. (QP1: Q.4c - 4M)
- Explain the importance of access control in cloud computing. (QP2: Q.4c - 4M)
- Explain the importance of trust management in cloud computing and its role in ensuring security between cloud providers and users. (QP2: Q.5c - 6M)
- Explain the Multi-tenancy, data outsourcing and metadata security in clouds. (QP1: Q.6a - 6M)
- Explain Policy & Organizational Risks and Legal Risks in cloud computing. (4 Marks)
- Describe any four Data Security Technologies used in cloud platforms. (4 Marks)
- What is Content-Level Security? Explain its key features along with any two advantages and two disadvantages. (6 Marks)
- Explain the key features and benefits of Security-as-a-Cloud Service (SECaaS). (4 Marks)

A-Level (Application / Scenario-Based — 4 / 6 Marks)

- Suggest any four best practices for cloud IAM. (QP1: Q.3b - 4M)
- A company uses multiple SaaS applications and wants to allow employees to log in with a single set of credentials. Which IAM feature would you recommend and why? (QP2: Q.6a - 6M)
- A banking enterprise wants to outsource sensitive customer transaction records to an untrusted public cloud storage. Write the step-by-step procedure and technical measures (such as data masking, encryption, and integrity verification) to implement cloud data security safely. (6 Marks)

