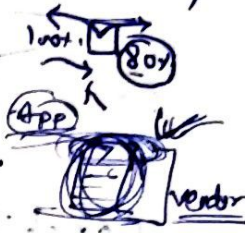



Cloud Security:- Cloud Security is the protection of data stored online via cloud computing platforms from theft, leakage & deleting.

Protection includes data from cloud infrastructure, applications & threats.

→ Security applications uses SaaS model.



Fundamentals of cloud Information Security:-

1. Risk Assessment:- To identify potential threats, vulnerabilities & risks specific to your organization's cloud env.
2. Data Classification & Encryption:-  Classify your data based on its sensitivity level to determine appropriate security controls.
3. Identity & Access Management:- Establish robust IAM practices to control user access to cloud resources. Use strong authentication mechanisms such as multi-factor authentication (MFA) and Principle of least privilege (PoLP) to ensure users have only the necessary permissions.

4. Network Security:- Implement appropriate network security controls, including firewalls, intrusion detection & prevention systems (IDS/IPS) & virtual private networks (VPNs).
5. Cloud Service Provider (CSP):- Carefully evaluate the security capabilities & reputation of CSPs before choosing one.
6. Data classification, Encryption, security monitoring, incident Response, Data backup & Recovery

Cloud Security Services:-

It refers to range of specialized solutions & offerings designed to enhance the security of cloud env.

These services are typically provided by third-party vendors.

1. Cloud Access Security Broker (CASB):-

They help organizations enforce security policies, monitor user ~~monitor~~ activities, detect & prevent data leakage & protect against threats.

2. Cloud Data Loss Prevention (DLP):-

DLP services for cloud help organizations identify & protect sensitive data stored in the cloud.

Er Sahil ka Gyan

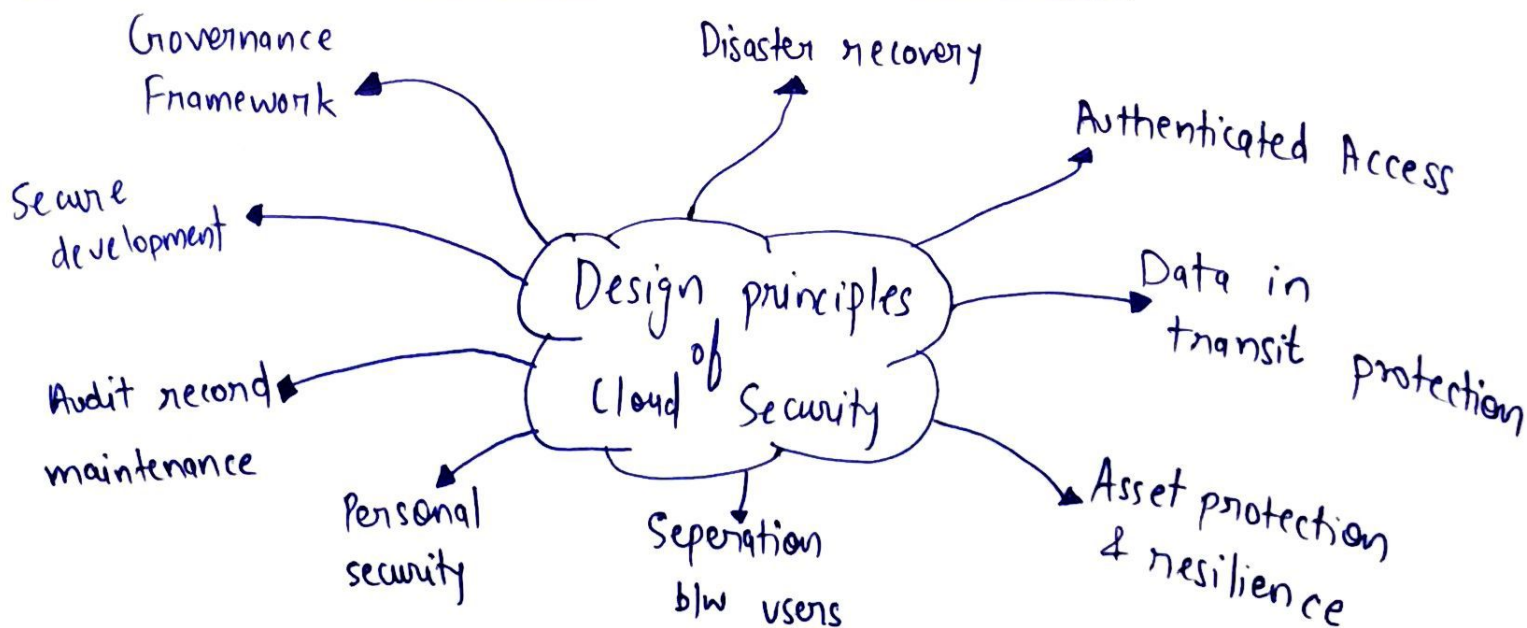
3. Cloud Encryption:- It Enables organizations to encrypt data before it is stored or transmitted to cloud.

4. Cloud Identity & Access Management:- It provides centralized control over user access to cloud resources. This includes role based access control (RBAC), single sign-on (SSO) & MFA.

5. Data protection & Firewall protection

— x —

Cloud Security Design Principles ⇒



Cloud Computing Security Challenges :-

1. DDoS and Denial of Service Attacks ⇒

Cloud providers are becoming a bigger target for malicious attacks. Distributed denial of service (DDoS) attacks are more common.

A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests.

Er Sahil ka Gyan

2. Data breaches ⇒ It is a growing challenge to secure

sensitive data. So choosing right vendor, with a strong record of implementing strong security measures, is vital to overcoming this challenge.

3. Data Loss : — Losing cloud data, either through accidental deletion & human error, malicious tampering including installation of malware (DDoS).

4. Insecure access control points:-

Cloud can be accessed from anywhere & from any device. But hackers can find & gain access to these types of vulnerabilities & exploit authentication via APIs if given enough time.

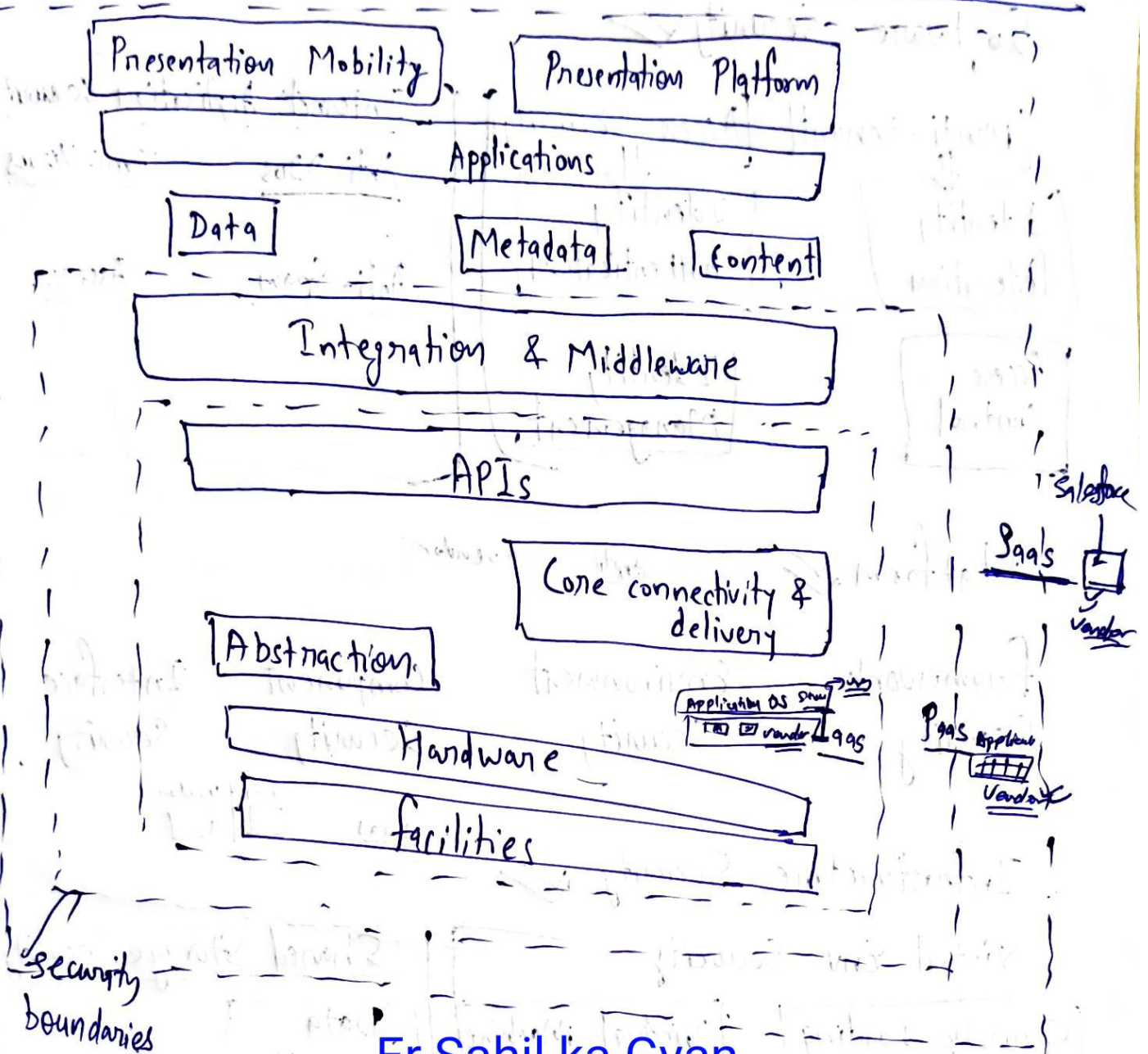
5. Legal & Regulatory Compliance :-

Cloud computing presents new security challenges that must be addressed to protect data & ensure compliance with legal & regulatory requirements.

Organizations must ensure data security & comply with legal & Regulatory requirements to ensure safety & integrity of their cloud-based systems.

Er Sahil ka Gyan

Cloud Computing Security Architecture

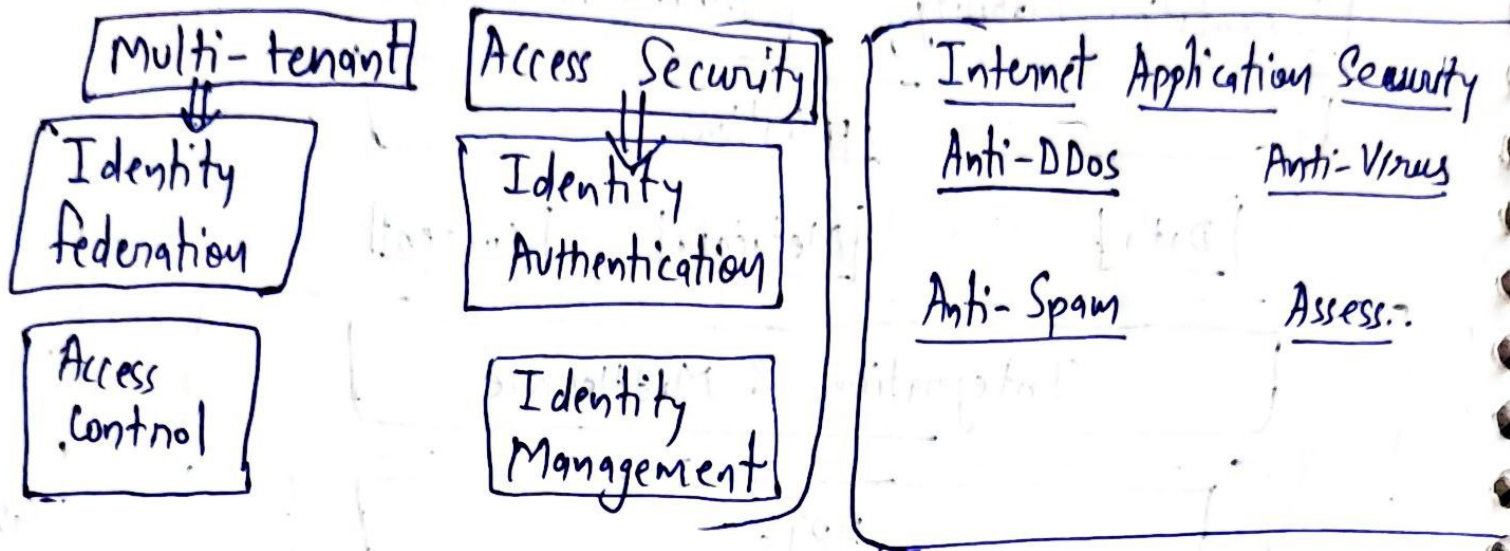


Er Sahil ka Gyan

The Cloud Security Alliance (CSA) stack model defines the boundaries b/w each service model & shows how different functional units relate.

→ A cloud security architecture can reduce or eliminate the holes in security that point-of-solution approaches are almost certainly about to leave.

Software Security ✓



Platform ✓

App/w → vendor

Er Sahil ka Gyan

Framework Security

Environment Security

Component Security

Interface Security

IaaS ☐ / ☐

Infrastructure Security ✓

Virtual Env. Security

Securely loading Virtual

Virtual Machine Isolation

Virtual Network border control

Shared Storage Security

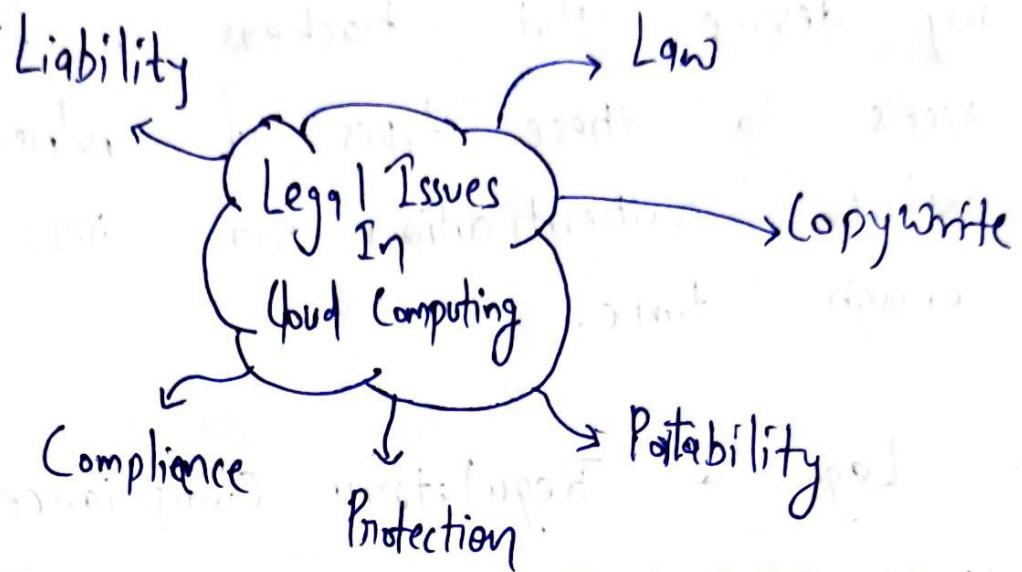
Data Segregation

Encryption

Data Destruction

Fig:- cloud Security Architecture

Legal Issues in Cloud Computing:-



Er Sahil ka Gyan

1.] Liability :- Cloud Computing involves the storage and processing of data on remote servers. In case of data breaches, service interruptions, questions may arise regarding liability. So it is essential to clearly define responsibilities and liabilities of both cloud service provider & customer.



2.] Copyright Compliance: Cloud Computing involves the transmission, storage & sharing of data, including copyrighted materials. They have appropriate licenses or permissions for any copyrighted content they store or share.

3.] Law :- → Organization must comply with applicable data protection laws, such as GDPR,

→ Clear contractual provisions should be established to address these issues & specify the rights.

→ Service Level Agreements (SLA) defines the terms of service, performance metrics, uptime guarantees & remedies for service failures in cloud computing.

ER Sahil ka Gyan

4.] Portability :- It arises when moving data, applications or services from one cloud provider to another.

Issues - → Data formats & Structures
→ Vendor Specific APIs & Tools
→ Data Transfer Costs & Bandwidth



5.] Compliance :- Organizations using cloud services must ensure that their operations meet relevant compliance requirements.

Eg - Data protection & Privacy ✓
Security Standards & Certifications ✓

Security Policies for

cloud computing

(attacks)

- Data Breaches ✓
- Data Loss ✓
- Account or Service Traffic Hijacking
- Insecure APIs
- Denial of Service ✓
- Malicious Insiders
- Abuse of cloud Services
- Insufficient due Diligence

Er Sahil ka Gyan

data breaches or natural disasters are all key security challenges that a company must address when considering cloud computing providers. Cloud computing security challenges as follows:

1. Data Breaches

The data breach at Target, resulting in the loss of personal and credit card information of up to 110 million individuals, was one of the series of startling thefts that took place during the normal processing and storage of data. "Cloud computing introduces significant new avenues of attack," said the CSA report authors. The absolute security of hypervisor operation and virtual machine operations is still to be proved. Indeed, critics question whether such absolute security can exist. The report's writers said there's lab evidence though none known in the wild that breaches via hypervisors and virtual machines may occur eventually.

2. Data Loss

A data breach is the result of a malicious and probably intrusive action. Data loss may occur when a disk drive dies without its owner having created a backup. It occurs when the owner of encrypted data loses the key that unlocks it. Small amounts of data were lost for some Amazon Web Service customers as its EC2 cloud suffered "a remirroring storm" due to human operator error on Easter weekend in 2011. And a data loss could occur intentionally in the event of a malicious attack.

3. Account or Service Traffic Hijacking

Account hijacking sounds too elementary to be a concern in the cloud, but CSA says it is a problem. Phishing, exploitation of software vulnerabilities such as buffer overflow attacks and loss of passwords and credentials can all lead to the loss of control over a user account. An intruder with control over a user account can eavesdrop on transactions, manipulate data, provide false and business-damaging responses to customers and redirect customers to a competitor's site or inappropriate sites.

4. Insecure APIs

The cloud era has brought about the contradiction of trying to make services available to millions while limiting any damage all these largely anonymous users might do to the service. The answer has been a public facing application programming interface or API, that defines how a third party connects an application to the service and providing verification that the third party producing the application is who he says he is.

Leading web developers, including ones from Twitter and Google, collaborated on specifying OAuth, an open authorization service for web services that controls third party access.

5. Denial of Service

Denial of service attacks are an old disrupter of online operations, but they remain a threat nevertheless. The assault by hundreds or thousands or millions of automated requests for service has to be detected and screened out before it ties up operations, but attackers have improvised increasingly sophisticated and distributed ways of conducting the assault, making it harder to detect which parts of the incoming traffic are the bad actors versus legitimate users.

6. Malicious Insiders

With the Edward Snowden case and NSA revelations in the headlines, malicious insiders might seem to be a common threat. If one exists inside a large cloud organization, the hazards are magnified. One tactic cloud customers should use to protect themselves is to keep their encryption keys on their own premises, not in the cloud.

"If the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack." Systems that depend "solely on the cloud service provider for security are at great risk" from a malicious insider, the report said.

7. Abuse of Cloud Services

Cloud computing brings large-scale, elastic services to enterprise users and hackers alike. "It might take an attacker years to crack an encryption key using his own limited hardware. But using an array of cloud servers, he might be able to crack it in minutes," the report noted. Or hackers might use cloud servers to serve malware, launch DDoS attacks or distribute pirated software.

8. Insufficient due Diligence

"Too many enterprises jump into the cloud without understanding the full scope of the undertaking," said the report. Without an understanding of the service providers' environment and protections, customers don't know what to expect in the way of incident response, encryption use and security monitoring. Not knowing these factors means "organizations are taking an unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks," wrote the authors.

Chances are, expectations will be mismatched between customer and service. Enterprises may push applications that have internal on-premises network security controls into the cloud, where those network security controls don't work. If enterprise architects don't understand the cloud environment, their application designs may not function with proper security when they're run in a cloud setting, the report warned.

Data Security in Cloud:

Business Continuity & Disaster Recovery Planning

BCP :- It is the act of proactively working out a way to prevent, if possible & manage the consequences of a disaster, limiting it to the extent that business can afford.

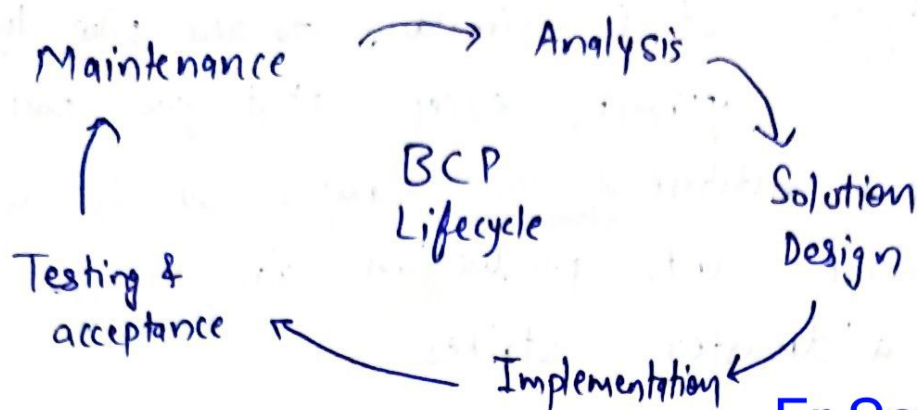
BCP Process :-

The first step is to identify the assets and processes that are critical to the business. The BCP should answer the following questions.

1. Which roles & individuals are vital for fulfilling business commitments?
2. What equipment, IT, transport will staff need to maintain operations?
3. How long can business function before full operations are restored?
4. What alternative resources are available?
5. Which suppliers & other 3-parties are integral to daily routines?

The initial response

Longer-term - planning



Er Sahil ka Gyan

Cloud Disaster Recovery Approaches:-

While all cloud disaster recovery plans involve the cloud in some way, the specific types of cloud resources that are used & the manner in which they are deployed, varies depending on DR approach you take.

There are ④ approaches to consider:-

1. Backup & Recovery :- It involves backing up data to the cloud & recovering it from the cloud when a disaster occurs. You need to ensure that it meets your RTO & RPO requirements.
2. Pilot light :- You keep a copy of your production virtual servers & databases stored in the cloud at all times. So when systems fail due to a disaster, the cloud backup env. functions like pilot light in your furnace.

3. Warm standby :- It is similar to the pilot light approach, except that your backup virtual servers & databases ^{at all times}. This enables you to put the backup resources into production almost instantaneously whenever a disaster strikes.

4. Multi-site :- This approach entails using the warm standby technique, but instead of having only one copy of your workloads running in the cloud at all times.

It ensures that you can restore your workloads very quickly even if part of your cloud provider's infrastructure has failed. OOOO

Risk Mitigation :- Mitigation cloud computing risks.

should be a priority for any organization that wants to move away from in-house h/w & applications.

When utilizing a cloud computing solution, following are the strategies to minimize the security risks:

1. Utilize a Single Sign-On (SSO) Solution to add Security :- Depending on size of organization, one could be creating many user accounts for several different cloud services.

By downsizing to a single-sign-on environment, one can reduce the number of potential security weaknesses.

Er Sahil ka Gyan

2. Work with a Third party to assure Cloud Security on Regular Basis :-

By having multiple parties, it increases the security risks. However, small & medium business without large IT departments, sometimes need assistance to audit & ensure cloud security.

3. Implement end-to-end Encryption :- It is particularly for cloud storage. It decreases likelihood of our data being breached. Most cloud storage solutions have encrypted data upload & downloads.

4.] Regularly Update - In-house Software :-

If we are running outdated OS & outdated internet browsers, we could be at risk despite encryption & third party audits.

— X —

4 points ✓

SLA (Service Level Agreement) :-

It is a contract between a service provider and its internal or external customers that documents what services the provider will furnish.

→ SLAs measure the service provider's performance and quality in a number of ways. Some metrics that SLAs may specify include:

1. Availability & uptime of percentage of time services will be available.
2. The number of concurrent users that can be served.
3. Specific performance benchmarks by which actual performance will be periodically compared.
4. Application response time.
5. The schedule for notification in advance of network changes that may affect users.
6. Usage statistics that will be provided.

SLA sets expectations for both parties & acts as the roadmap for change in the cloud services.

In order to consistently develop an effective SLA, a list of important criteria needs to be established.

Er Sahil ka Gyan

Availability, Performance, Security of Data, Access & Location of data, Change management Process, Dispute mediation process.



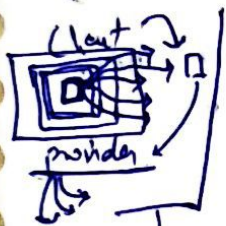
_____X_____

Threats in Cloud :-

The cloud has helped many companies scale their business, it has several security vulnerabilities.

Data Breach  security violation

Trojan Horse :- The main pillar for any company is its human resources, that is, its employees. Most of them work in a protocol that helps company with its normal functioning. But, at times they are people who take the wrong route & might leak their company's vital & confidential data through various means like social media or external pressure.



Vulnerable APIs :- CSPs manage a collection of APIs that customers use to operate & commⁿ with cloud services.

These APIs can be accessed through internet by their CSPs. They are equally vulnerable as an operating system & its libraries which can be accessed from anywhere online.

Support Issues :- Companies can face the issue of compatibility when launching their applications in cloud.

Er Sahil ka Gyan

Insufficient Data Backup :-

When a particular batch of data is being deleted, only 60-75% of it will be erased. Rest will be kept in cloud in various chunks which won't be ~~amended~~ ^{easily} accessible for further decision.

Lack of Trust :- This occurs when cloud vendor & company have signed an MOU but are in bitter terms about having a mutual trust with each other.