UNIT-V

Security in Cloud Computing

* Types of Risk in Cloud Computing -

→ I) Loss of data:

Data stored on cloud servers can be lost through natural disaster, malicious attacks, etc.

II) Increased customer agitation:

Growing no. of cloud service critics are keen to see which service providers are weak & encourage customers to avoid them.

III) Malware Attacks:

Cloud services can be a vector for data exfiltration.

- Threats identified by Cloud Security Alliance (CSA):

i) Insecure interfaces & API:

ii) Malicious Insiders:

- Threat of malicious insiders is well-known to most organizations

- Remediation - Determine security breach notification processes.

iii) Shared Technology issues :

- IaaS vendors delivers their services in scalabe way by sharing infiastructure

- Remediation - Implement security best practices for installation / configuration.

iv) Data loss or Leakage :

- There are many ways to compromise data
- Deletion / alteration of records without backup of original content is obvious example.

- Remediation - Implement strong API access contol

v) Account or service hijacking :

- Attack methods such as phishing, fraud, etc still achieve results

- Remediation - Prohibit sharing of account credentials between users & services.

* Content Level Security (CLS) -

→ • Content-based security features include restricting who can open Email, print or edit content & place time limit on how long user can access given piece of content.

• Content can expire from a given repository and no longer be viewable by anyone.

• It refers to protection of data at granular level, ensuring that sensitive information remains secure whether it's in transit, at rest or being processed

• Uses of content level security are manifold.

• In industries like healthcare & finance, protecting individual pieces of data, such as patient records or financial transactions is crucial.

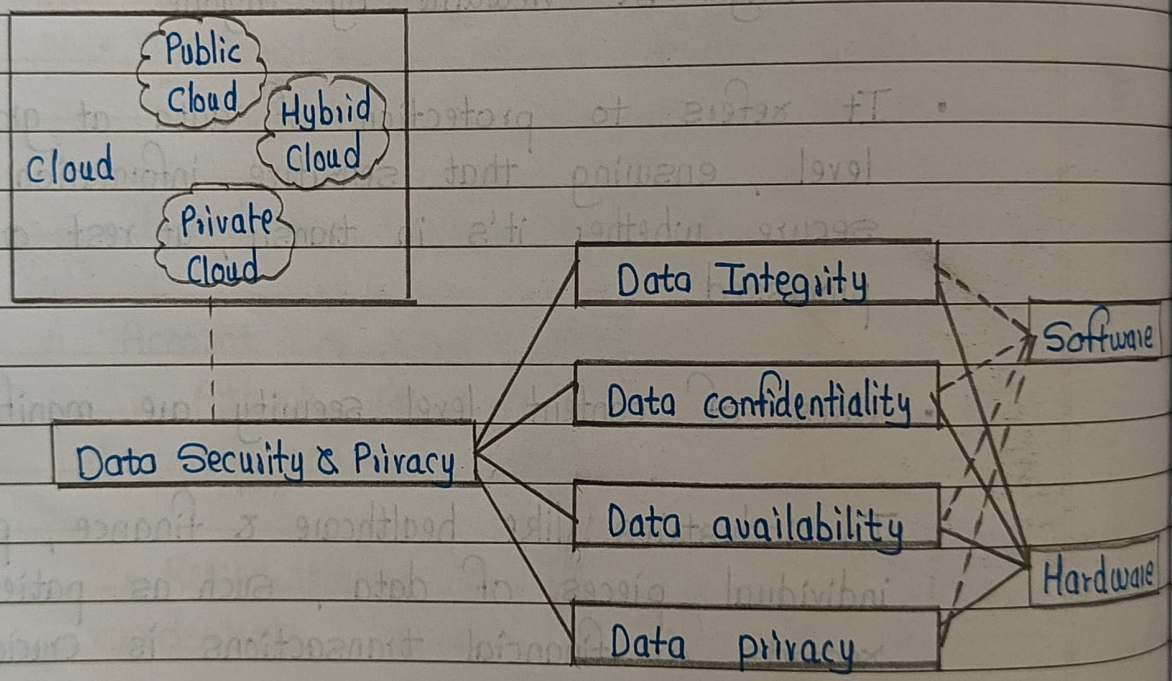
• Content Level Security also supports secure data sharing & collaboration, enabling businesses to safely exchange sensitive information.

• By embedding security directly into data, organizations can enhance their overall security posture & maintain trust with stakeholders.

- Content-based security can be useful for organizations that extensively use CC & enterprise mobility technologies.

★ Cloud Security Services -

→ • Diagram -



I) Integrity :

- This service protects data from malicious modification.

- Integrity can extend to how data is stored, processed & retrieved by cloud services.

- Data Integrity in cloud system means preserving information integrity.

- Data integrity is the basis to provide cloud computing services like SaaS, PaaS & IaaS.

II) Confidentiality -

- Confidentiality refers to limiting information access.

- Sensitive information should be kept secret from individuals who are not authorized to see information

- Data confidentiality is important for users to store their private or confidential data in cloud.

III) Availability -

- This service assures that data stored in cloud are available on each user retrieval request.

- This service is particularly important for data at rest in cloud servers & related to fullfilment of service level agreement.

- The cloud service provider should ensure the data security, particularly data confidentiality and integrity.

- Cloud service provider should share all the concerns with client & build trust relationship in this connection.

* Cloud Testing & Types -

→ • Cloud Testing is one type of software testing in which the software applications are tested by using cloud computing services.

- Cloud Testing offers users, pay-per-use pricing, flexibility & reduced time-to-market.

- Cloud Testing ensures faster availability, scalability & flexibility that saves time & cost for software testing.

- Types of Testing: These are real types

i) Functional Testing -

- Functional software testing checks all the features & functions of software and its interaction with hardware.

- For conducting functional testing, testers can use tools like Rapise, Sauce Labs, etc.

ii) Non - Functional Testing -

- It is also known as performance testing, as it allows you to check non-functional aspects of software like its performance, usability, reliability, etc

- For conducting this type of testing, you can use tools like CloudTest, CloudTestGo, AppLoader, etc

iii) Ability Testing -

- Ability testing is necessary to verify whether users really receive application services on demand.

- The whole cloud testing is segmented into 4 main categories:

a) Testing on whole cloud -
The cloud is viewed as whole entity and based on its features, testing is carried out

b) Testing within a cloud -
By checking each of its internal features, testing is carried out

c) Testing across cloud -
Testing is carried out on different types of cloud like private, public, hybrid cloud

d) SaaS Testing in cloud -
Functional & Non-functional testing is carried out on basis of application requirements.