جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject: Privacy Concerns and Risk Management in Cloud Computing

Class: Third stage

Lecture: (7)

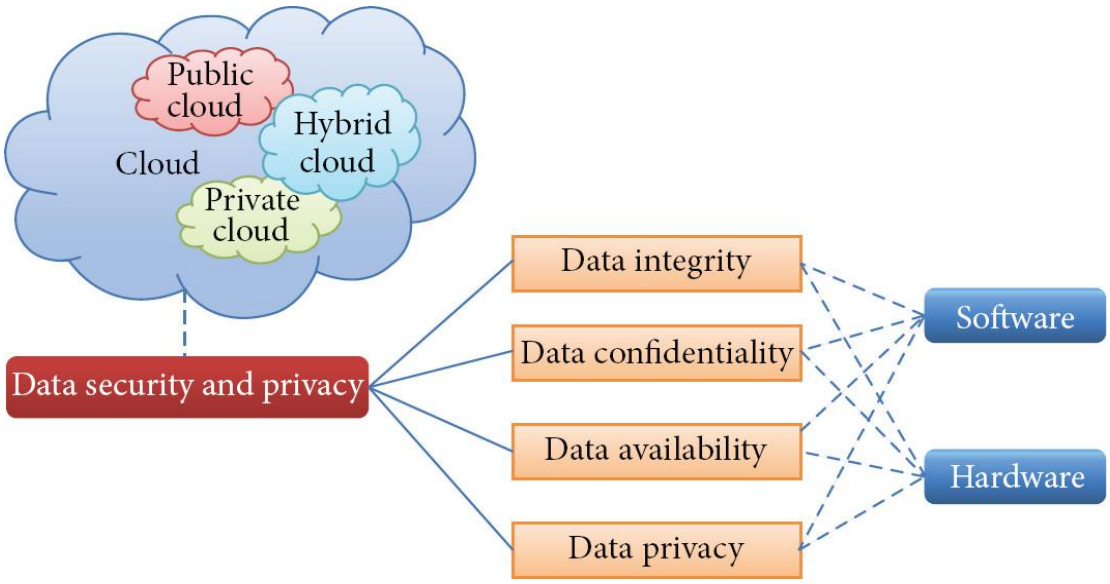
Lecturer: Msc :Najwan thaeer ali

1. Introduction to Cloud Privacy

Cloud computing allows organizations to store and process data on remote servers instead of local machines. While it provides scalability, flexibility, and cost savings, it also introduces **serious privacy concerns**.

Definition (Cloud Privacy):

Cloud privacy refers to the protection of **personal, sensitive, and organizational data** that is stored, processed, and managed in cloud computing environments, ensuring that such data is **not accessed, used, or disclosed without authorization**, and is handled in compliance with applicable privacy laws and regulations.



2. Key Privacy Concerns in the Cloud

1. Data Breaches

Unauthorized access to sensitive information due to weak security or attacks.

2. Data Loss

Loss of data due to accidental deletion, system failure, or cyberattacks.

3. Lack of Control

Users do not have full control over where and how their data is stored.

4. Insider Threats

Cloud provider employees may misuse access privileges.

5. Data Location Issues

Data may be stored in different countries with different laws.

6. Insecure APIs

Weak application interfaces can be exploited by attackers.

3. Who Is Responsible for Protecting Privacy?

Shared Responsibility Model

Privacy protection in cloud computing is a **shared responsibility** between:

1. **Cloud Service Provider (CSP)**

   A Cloud Service Provider (CSP) is a company that delivers cloud computing services such as storage, processing power, networking, and software over the internet to users and organizations.

   A CSP owns and manages the cloud infrastructure (data centers, servers, networks) and provides services that customers can access remotely without needing to build their own systems.

Examples of CSPs:

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

Key Responsibilities of a CSP:

1. Managing physical data centers
2. Ensuring infrastructure security
3. Providing availability and reliability
4. Maintaining network and hardware

2. Customer (User/Organization)

A **Customer (User/Organization)** in cloud computing is an individual, company, or institution that uses services provided by a Cloud Service Provider (CSP) to store data, run applications, or manage IT resources. The customer accesses cloud services over the internet and is responsible for **how the data is used, secured, and managed** within the cloud environment.

Examples of Customers:

- A university using cloud storage for student records
- A bank using cloud systems for financial data
- A company hosting its website on the cloud

Key Responsibilities of the Customer:

1. Protecting sensitive data
2. Managing user access and permissions
3. Applying security measures (e.g., encryption, passwords)
4. Ensuring compliance with laws and regulations
5. Configuring cloud services correctly

Key Idea (Shared Responsibility Model):

👉 The provider secures the cloud, while the customer secures what is in the cloud.

1.The **Cloud Service Provider (CSP)** (such as Amazon Web Services or Microsoft Azure) is responsible for protecting the **cloud infrastructure**, including:

A. Physical data centers
B. Servers and hardware
C. Networking systems

2.The **Customer (User/Organization)** is responsible for protecting what they put **inside the cloud**, including:

A. Data (files, records, databases)
B. User accounts and access control
C. Application security
D. Proper configuration settings

Example:

If a company stores student data in the cloud:

- The **provider** ensures the servers are secure and always running
- The **customer** must ensure:

1. Data is encrypted
2. Access is restricted
3. No misconfiguration exposes the data

4. Privacy Risk Management and Compliance in Cloud Computing

Privacy Risk Management and Compliance in Cloud Computing refers to the processes, policies, and practices used by organizations to **identify, assess, and reduce privacy risks** associated with storing and processing data in the cloud, while ensuring that all activities **comply with applicable laws, regulations, and privacy standards**.

Example of Privacy Risk Management and Compliance in Cloud Computing:

A university stores student data (names, grades, IDs) using Google Cloud Platform.

Privacy Risk:
Unauthorized access to student records.

How Risk is Managed:

1. The university uses **encryption** to protect data
2. Only authorized staff can access the system (access control)
3. Regular **security audits** are performed

5. Privacy Principles in Cloud Computing

Privacy Principles in Cloud Computing are a set of rules and guidelines that organizations follow to ensure that **personal and sensitive data** stored in the cloud is **collected, used, protected, and managed responsibly and legally**.

Main Privacy Principles:

1. Collection Limitation Principle

2. Use Limitation Principle

3. Security Principle

4. Retention and Destruction Principle

5. Transfer Principle

6. Accountability Principle

7. Multi-Tenancy

Discussion Questions (for students)

1. What is the biggest privacy risk in cloud computing?
2. Who is more responsible for data protection: the provider or the user?
3. How does multi-tenancy affect data security?
4. Why is data location important in cloud privacy?