**Unit V**

**Data privacy and security Issues and other risks in Cloud Computing**

Cloud computing is one of the most promising technology for the next generation of IT applications. The primary concern toward the accelerated growth of cloud services is data security and privacy issues. The main goal for any company is to reduce data storage and cost associated with it. As we all know data is playing a bigger role in taking business decisions, no company will deploy all their business data into the cloud unless they trust it completely. There are many techniques which have been introduced by IT researchers for data protection and to achieve the highest level of data security.

Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications

## Cloud Security Issues

There are many security issues in clouds as they provide hardware and services over the internet .

## Data Loss

Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. In a cloud computing environment, data loss occurs when our sensitive data is somebody else's hands, one or more data elements can not be utilized by the data owner, hard disk is not working properly, and software is not updated.

## Hacked Interfaces and Insecure APIs

As we all know, cloud computing is completely depends on Internet, so it is compulsory to protect interfaces and APIs that are used by external users. APIs are the easiest way to communicate with most of the cloud services. In cloud computing, few services are available in the public domain. These services can be accessed by third parties, so there may be a chance that these services easily harmed and hacked by hackers.

## Data Breach

Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.

## Increased complexity strains IT staff

Migrating, integrating, and operating the cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data to the cloud.

## Network security

Security data will be taken from enterprise in Saas and processes and stored by the Saas provides. To avoid the leakage of the confidential information Data all over the internet must be secured.

## Data locality

Data locality is much important in May of the countries laws and policies regarding the locality of data are strict.

## Data access

Data on clouds must be accessible from anywhere anytime and from any system. Cloud storages have some issues regarding the access of the data from any device . Information breaks and different sorts of assaults flourish in situations with poor client verification and weak passwords.

## Denial of Service (DoS) attacks

Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.

### Account hijacking

Account hijacking is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities.

### Malicious insiders

Most information loss or harm happening inside an association is human mistake. A malicious insider may be a present or previous worker, contractual worker, or accomplice who has the accreditations to get to organization information and intentionally uses, takes, or harms that information.

## How to Protect your Data – solution to security issuue

You can protect your business data in the cloud from unauthorised access. All you need is a sharp eye and an extra effort. Here are few practical tips to keep your cloud data safe and secure.

#### Always keep backup locally

When it comes to business data, you have to be extra conscious. Always have a backup for your data. It is always good to create hard copies of your business data and keep it with yourself so that you can have access them even if you lost the original one. You can use any cloud storage solutions to store your data. You can set up a cloud account & can keep the backup copies.

#### Don’t store sensitive data

Technology is changing. Businesses are also changing as per the technology. Data is playing an important role in businesses today. So, data privacy is one of the primary aspects of any business. But if something is there on the internet, it is hard to trust it is safe. So, one should avoid storing the most sensitive files or information in the cloud. Identity theft is on rising and you can't take any risk.

**Data encryption**

One of the best ways to protect your data while using cloud storage is to do data encryption. This is the best form of security because you need decryption before accessing the data. This will protect data against service providers and users also. To make it more protected, you can also ensure cloud encryption during uploading and downloading phases.

**Using password**

The first thing which can be done is to put strong password which can stand a hacking. You can take the help of internet to learn how to create a strong password. It is very important to change your password frequently and never use the same password for all the accounts or folders. You can opt for 2-step verification for login if your cloud service offers that option.

**Keep an eye on what you do online**

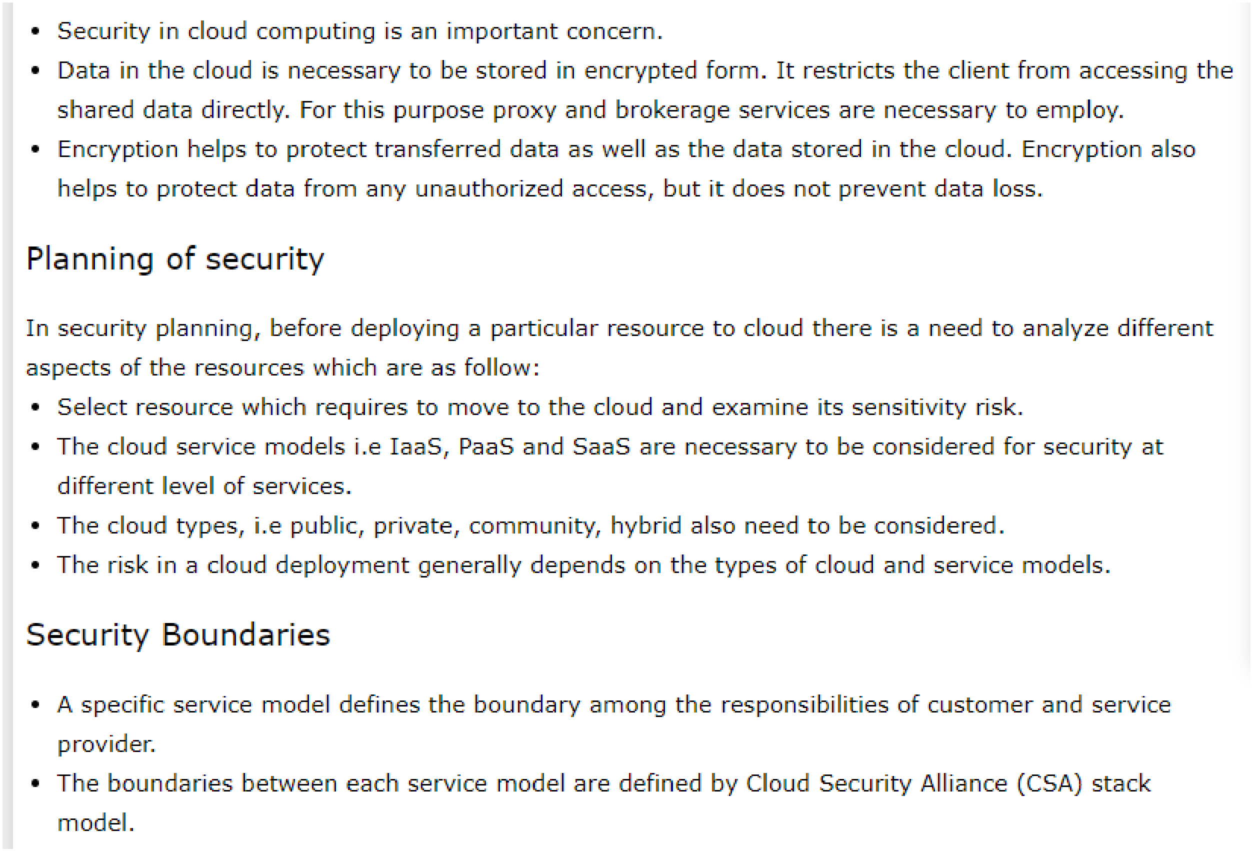
The security of your cloud data largely depends on your online behaviour. While using a public computer, never save your password, and always ensure that you logged out properly. Another biggest concern is accessing cloud data in unsecured or open Wi-Fi hotspots. Such connections are unencrypted, hackers can target your data easily. Never save your password in any of the public forum or social media. Change Wi-Fi passwords frequently.

**Anti-virus is a must**

Sometimes the weakest link happens to be the computer or device you use for cloud data access. You need to put proper protection in your system/device. It will help in securing your business data. If you expose yourself to bugs and viruses, hackers can access your system easily.

**Read your user agreement**

If you are new to the world of cloud computing and not sure what cloud storage to choose or how it really work, you have to read the user agreement of the service you are going to sign up for.



- Security in cloud computing is an important concern.
- Data in the cloud is necessary to be stored in encrypted form. It restricts the client from accessing the shared data directly. For this purpose proxy and brokerage services are necessary to employ.
- Encryption helps to protect transferred data as well as the data stored in the cloud. Encryption also helps to protect data from any unauthorized access, but it does not prevent data loss.

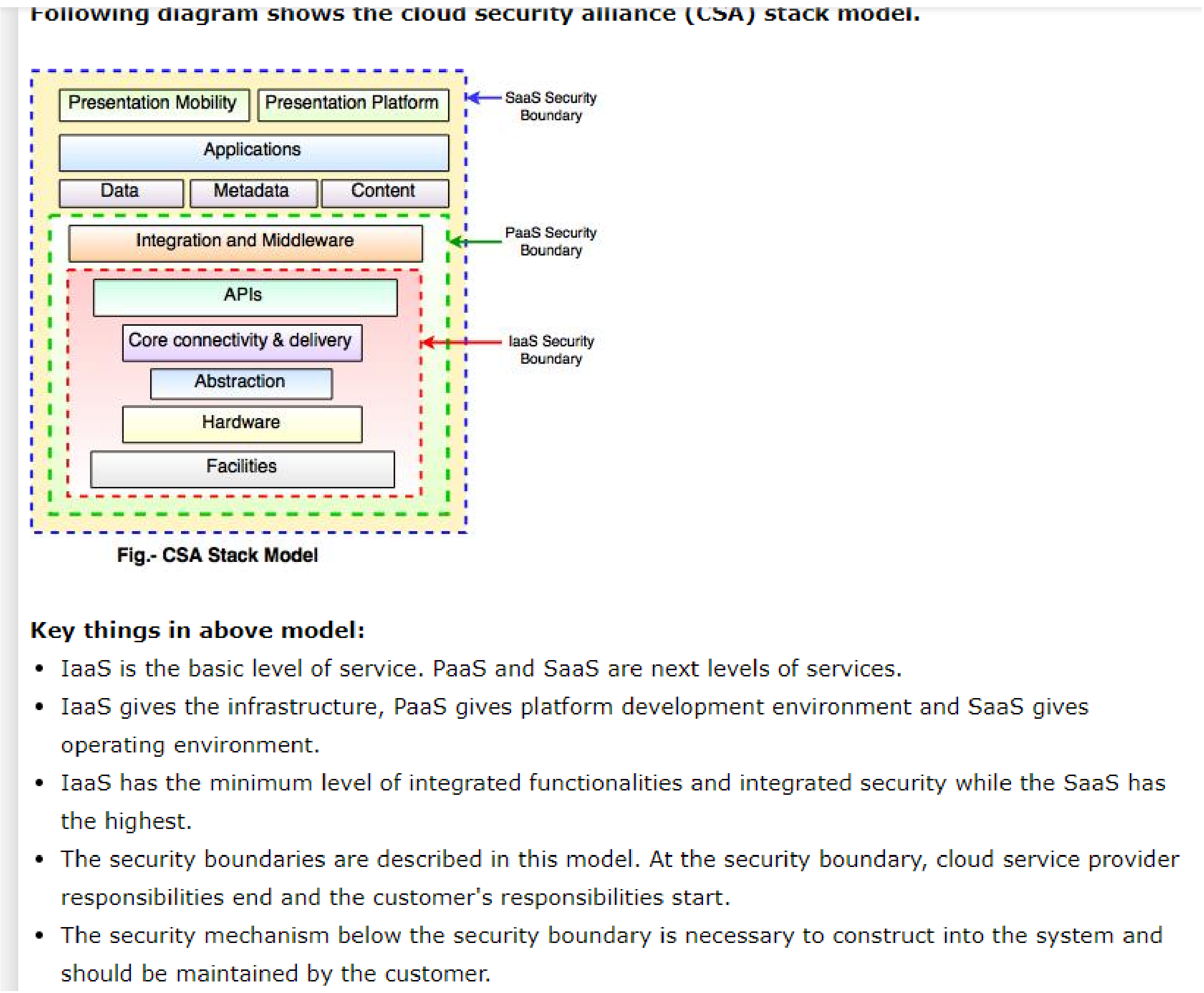
## Planning of security

In security planning, before deploying a particular resource to cloud there is a need to analyze different aspects of the resources which are as follow:

- Select resource which requires to move to the cloud and examine its sensitivity risk.
- The cloud service models i.e IaaS, PaaS and SaaS are necessary to be considered for security at different level of services.
- The cloud types, i.e public, private, community, hybrid also need to be considered.
- The risk in a cloud deployment generally depends on the types of cloud and service models.

## Security Boundaries

- A specific service model defines the boundary among the responsibilities of customer and service provider.
- The boundaries between each service model are defined by Cloud Security Alliance (CSA) stack model.



Following diagram shows the cloud security alliance (CSA) stack model.

Fig.- CSA Stack Model

**Key things in above model:**

- IaaS is the basic level of service. PaaS and SaaS are next levels of services.
- IaaS gives the infrastructure, PaaS gives platform development environment and SaaS gives operating environment.
- IaaS has the minimum level of integrated functionalities and integrated security while the SaaS has the highest.
- The security boundaries are described in this model. At the security boundary, cloud service provider responsibilities end and the customer's responsibilities start.
- The security mechanism below the security boundary is necessary to construct into the system and should be maintained by the customer.

## Data security in cloud

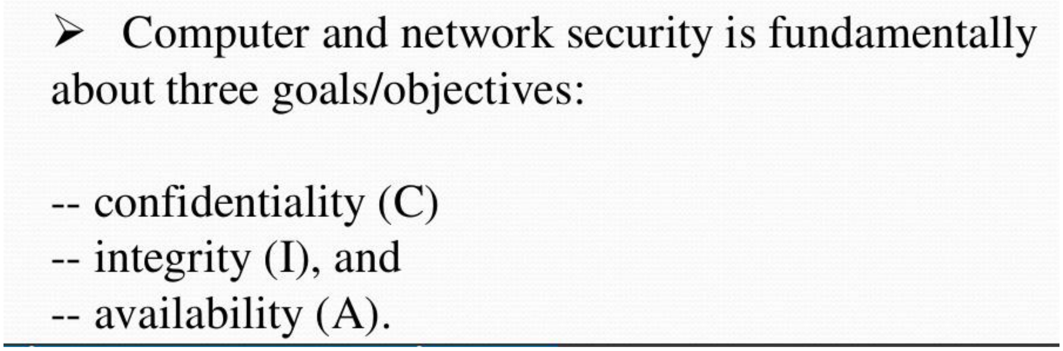
Data security in cloud is an important concern because all the data is transferred using Internet.

**Following are the mechanisms for data protection.**

I) Access Control
ii) Auditing
iii) Authentication
iv) Authorization

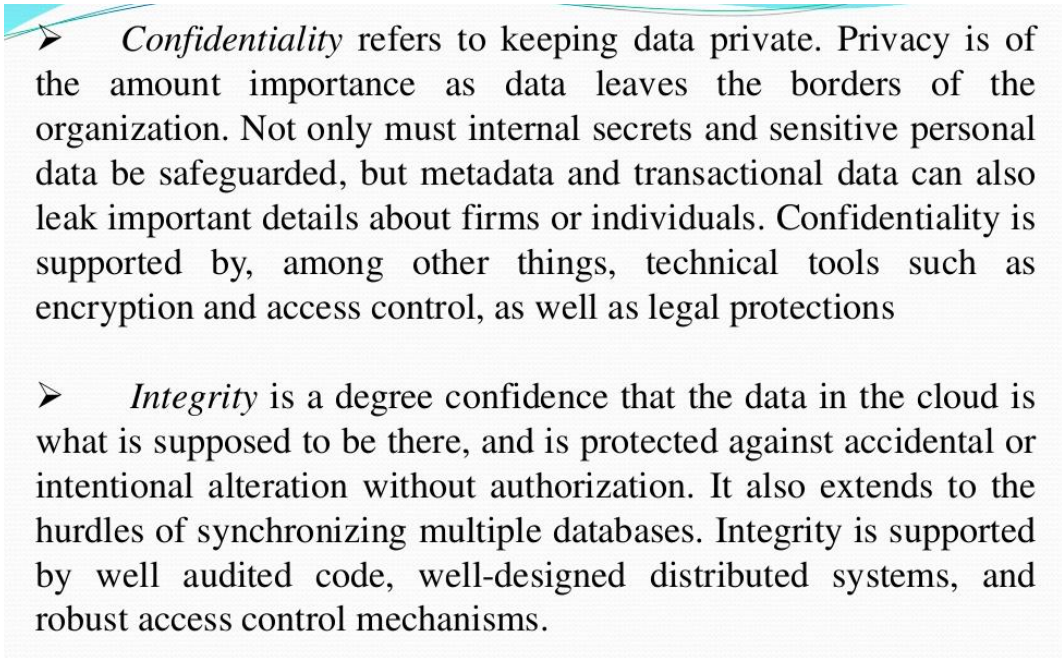
### Isolated Access to Data

- Data stored in cloud can be retrieved from anywhere, hence it should have a mechanism to isolate data and protect it from clients direct access.
- To isolate storage in the cloud, Brokered Cloud Storage Access is an approach.



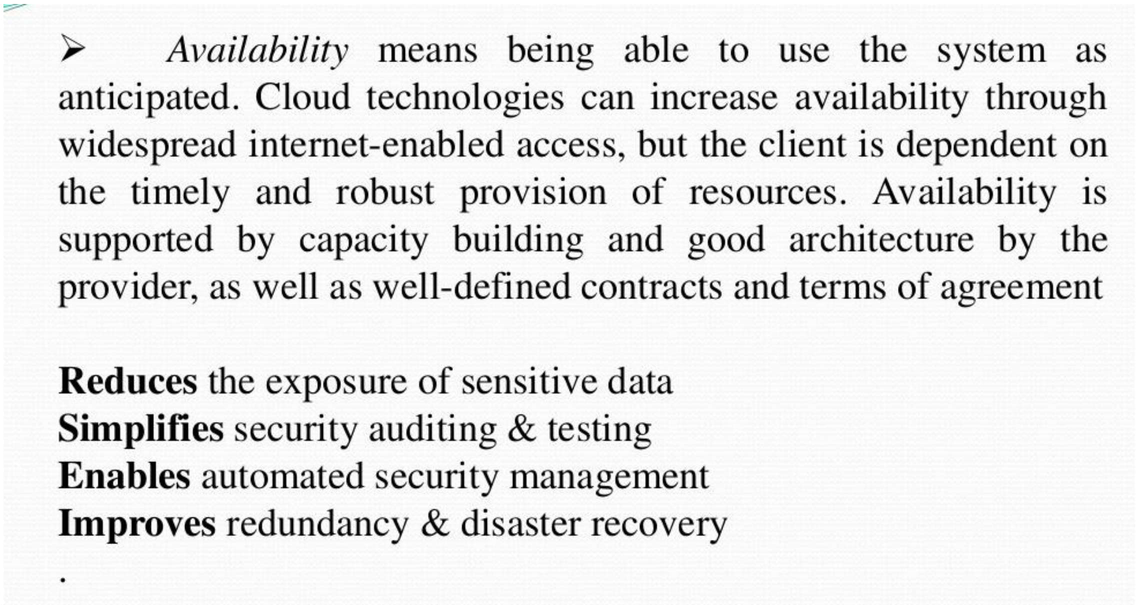
➢ Computer and network security is fundamentally about three goals/objectives:

-- confidentiality (C)
-- integrity (I), and
-- availability (A).



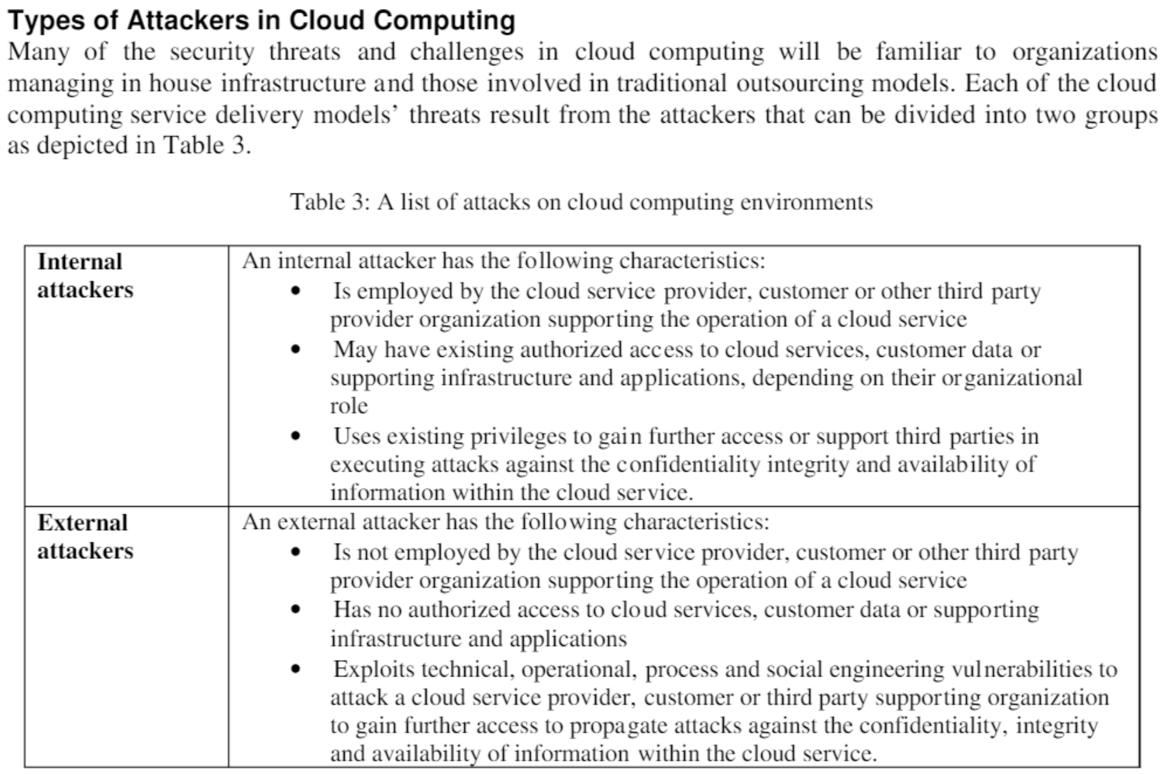
➢ *Confidentiality* refers to keeping data private. Privacy is of the amount importance as data leaves the borders of the organization. Not only must internal secrets and sensitive personal data be safeguarded, but metadata and transactional data can also leak important details about firms or individuals. Confidentiality is supported by, among other things, technical tools such as encryption and access control, as well as legal protections

➢ *Integrity* is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. It also extends to the hurdles of synchronizing multiple databases. Integrity is supported by well audited code, well-designed distributed systems, and robust access control mechanisms.



➢ *Availability* means being able to use the system as anticipated. Cloud technologies can increase availability through widespread internet-enabled access, but the client is dependent on the timely and robust provision of resources. Availability is supported by capacity building and good architecture by the provider, as well as well-defined contracts and terms of agreement

**Reduces** the exposure of sensitive data
**Simplifies** security auditing & testing
**Enables** automated security management
**Improves** redundancy & disaster recovery
.



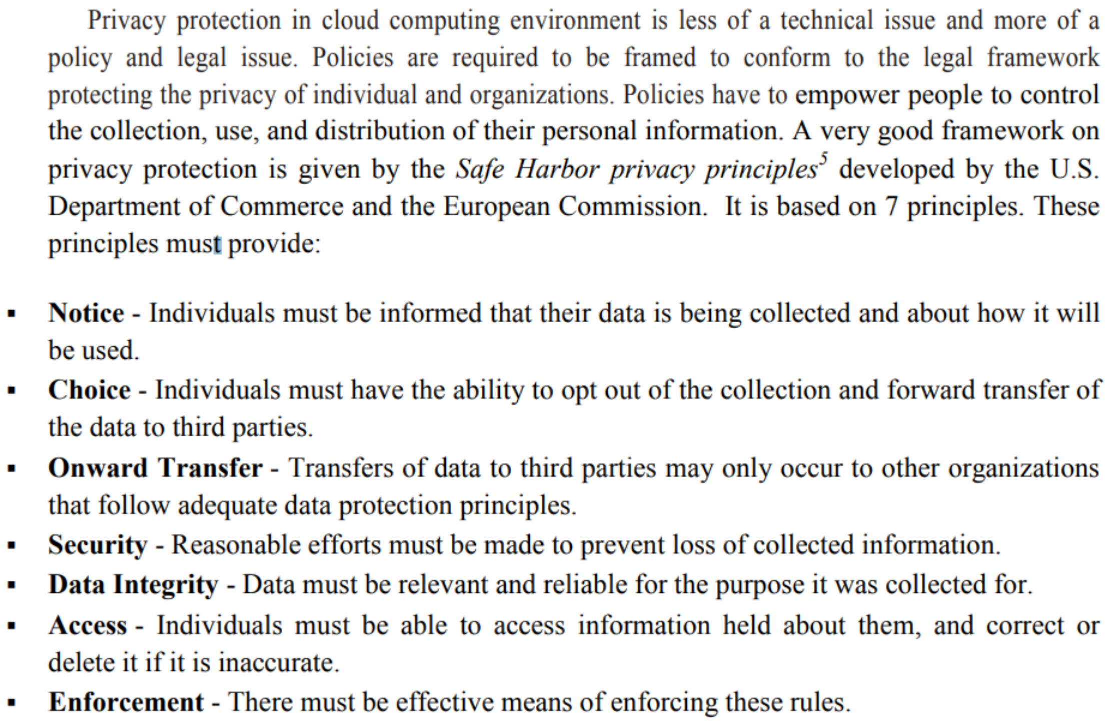
### Types of Attackers in Cloud Computing

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers that can be divided into two groups as depicted in Table 3.

Table 3: A list of attacks on cloud computing environments

| | |
|---|---|
| **Internal attackers** | An internal attacker has the following characteristics:<br>• Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service<br>• May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role<br>• Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service. |
| **External attackers** | An external attacker has the following characteristics:<br>• Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service<br>• Has no authorized access to cloud services, customer data or supporting infrastructure and applications<br>• Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service. |

# Privacy in cloud :

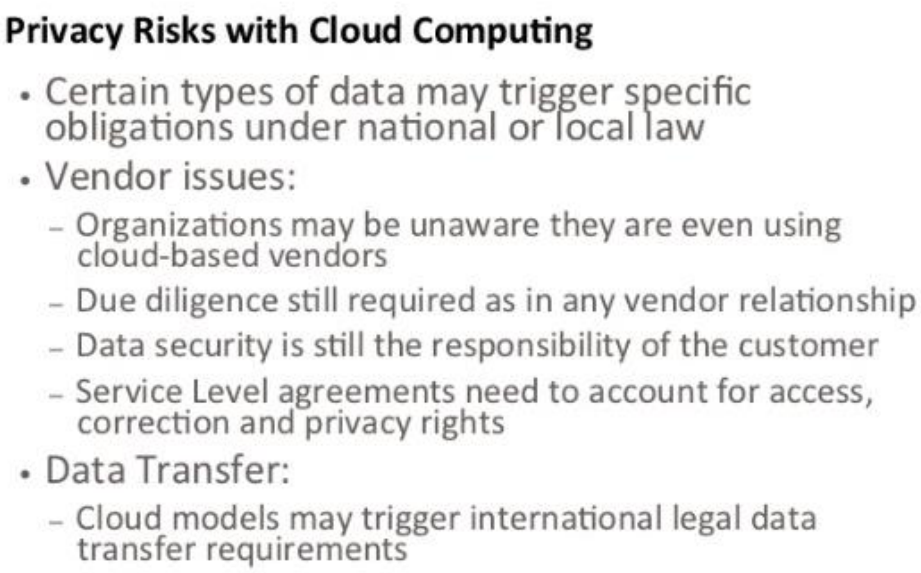


Privacy protection in cloud computing environment is less of a technical issue and more of a policy and legal issue. Policies are required to be framed to conform to the legal framework protecting the privacy of individual and organizations. Policies have to empower people to control the collection, use, and distribution of their personal information. A very good framework on privacy protection is given by the *Safe Harbor privacy principles*[5] developed by the U.S. Department of Commerce and the European Commission. It is based on 7 principles. These principles must provide:

- **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
- **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement** - There must be effective means of enforcing these rules.

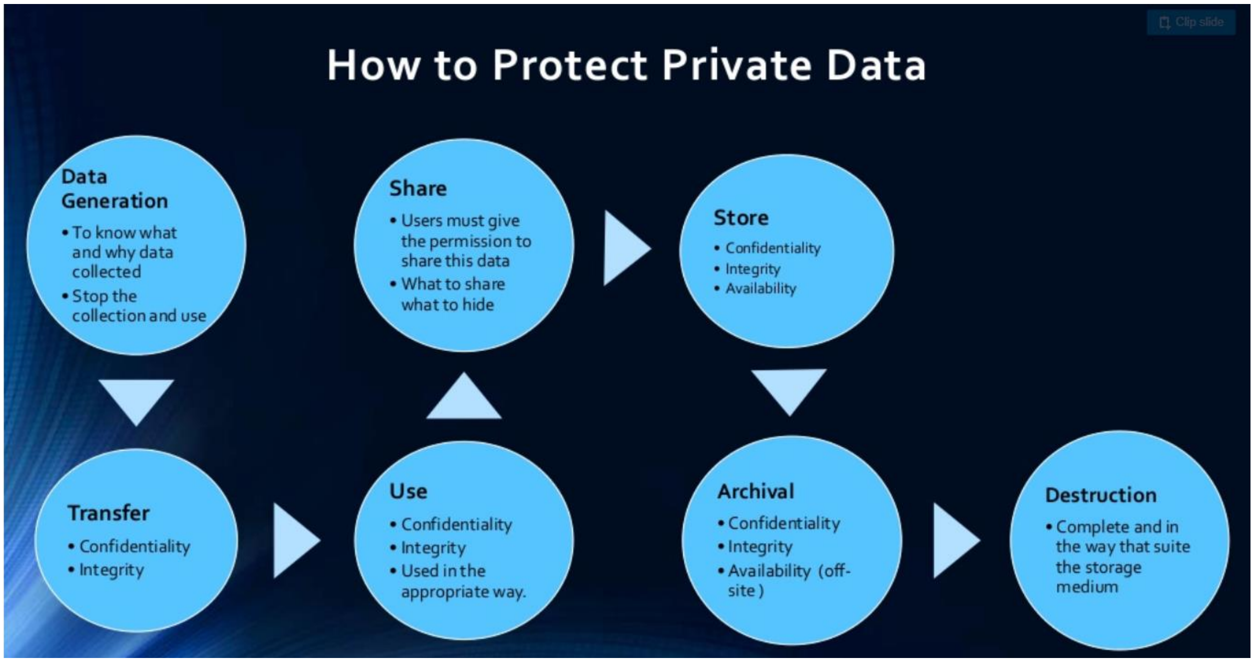
Privacy issues in cloud computing includes:

- **Data protection:** Data security plays an important role in cloud computing environment where encryption technology is the best option whether data at rest or transmitted over the internet. Hard drive producers are supplying self-encrypting drives that provide automated encryption, even if you can use encryption software to protect your data.
- **User control:** This can be both a legal issue and one raised by consumers themselves. SaaS environment offers the control of consumers' data to the service provider so; data visibility and control will be limited. In that case, there is a threat of data stolen, misused or theft, as consumers have no control over cloud.
- **Employee training and knowledge**: A full understanding of when cloud services should and be used needs to be a part of basic employee training in many jobs that involve managing information.
- **Unauthorized usage:** This can includes usage of data ranging from targeted advertising, to the re-sale of data on the cloud. The service provider may gain income from secondary usage of data.
- **Loss of legal protection:** Putting data on the cloud can involve a loss of legal protection of privacy. It can be impossible to follow all the legislation for a cloud computing for example, with Canada's privacy act or health laws.



**Privacy Risks with Cloud Computing**

- Certain types of data may trigger specific obligations under national or local law
- Vendor issues:
  - Organizations may be unaware they are even using cloud-based vendors
  - Due diligence still required as in any vendor relationship
  - Data security is still the responsibility of the customer
  - Service Level agreements need to account for access, correction and privacy rights
- Data Transfer:
  - Cloud models may trigger international legal data transfer requirements



## How to Protect Private Data

**Data Generation**
- To know what and why data collected
- Stop the collection and use

**Transfer**
- Confidentiality
- Integrity

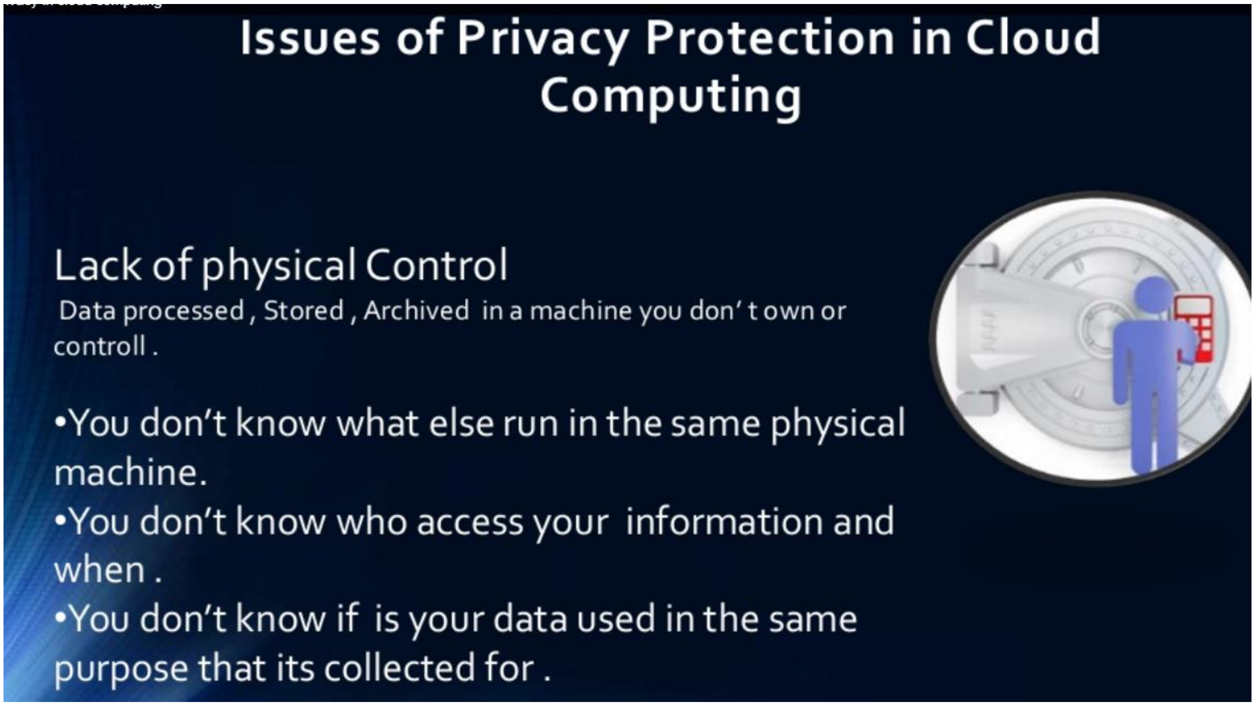
**Use**
- Confidentiality
- Integrity
- Used in the appropriate way.

**Share**
- Users must give the permission to share this data
- What to share what to hide

**Store**
- Confidentiality
- Integrity
- Availability

**Archival**
- Confidentiality
- Integrity
- Availability (off-site )

**Destruction**
- Complete and in the way that suite the storage medium



## Issues of Privacy Protection in Cloud Computing

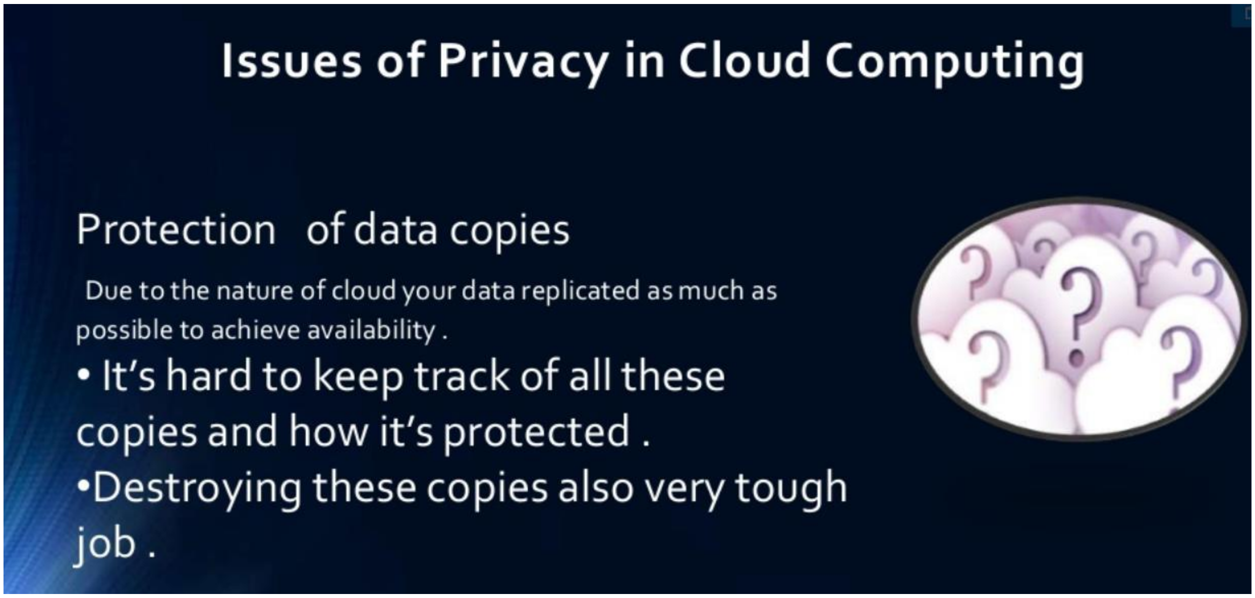
Lack of physical Control

Data processed , Stored , Archived in a machine you don' t own or controll .

•You don't know what else run in the same physical machine.

•You don't know who access your information and when .

•You don't know if is your data used in the same purpose that its collected for .



Issues of Privacy in Cloud Computing

Protection of data copies

Due to the nature of cloud your data replicated as much as possible to achieve availability .

• It's hard to keep track of all these copies and how it's protected .

•Destroying these copies also very tough job .

## Privacy Concern & Cloud Computing

Privacy present a strong barrier for users to adapt into Cloud Computing systems

There are certain measures which can improve privacy in cloud computing.

1. The administrative staff of the cloud computing service could theoretically monitor the data moving in memory before it is stored in disk.To keep the confidentiality of a data, administrative and legal controls should prevent this from happening.
2. The other way for increasing the privacy is to keep the data encrypted at the cloud storage site, preventing unauthorized access through the internet; even cloud vendor can't access the data either.