Lecture 8

- **Security in the Cloud**

What is security in cloud computing

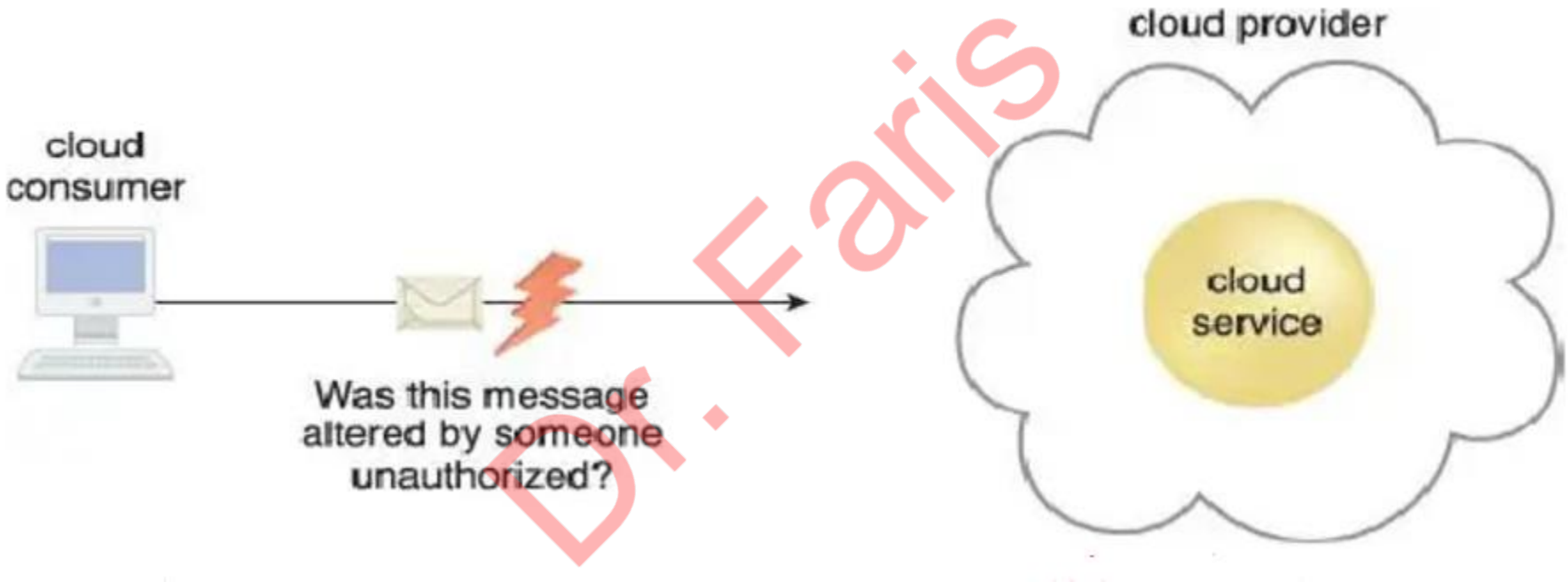
- Cloud computing security or cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDoS (distributed denial-of-service) attacks, malwares, hackers and other similar attack.

Basic Terms and Concepts

Confidentiality

- Confidentiality is the characteristic of something being made accessible only to authorized parties.

- Within cloud environments, confidentiality mainly be related to restricting access to data in transit and storage.


cloud provider
cloud consumer
cloud service
Was this message altered by someone unauthorized?

Integrity

- Integrity is the characteristic of not having been altered by an unauthorized party.

- An important issue that concerns data integrity in the cloud is whether a cloud consumer can be guaranteed that the data it transmits to a service matches the data received by that cloud service.

- Integrity can extend to how data is stored, processed, and retrieved by cloud services and cloud-based IT resources.

Authenticity

- Authenticity is the characteristic of something having been provided by the authorized source.

- For example, a user may not be able to access a non repudiable file after its receipt without also generating a record of this access.

Availability

- Availability is the characteristic of being accessible and usable during a specified time period.

- In typical cloud environments, the availability of cloud services can be a responsibility that is shared by the cloud provider and the cloud carrier.

- The availability of a cloud-based solution that extends to cloud service consumers is further shared by the cloud consumer.

Threat

- A threat is a potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm.

- Both manually and automatically instigated threats are designed to exploit known weaknesses, also referred to as vulnerabilities.

- A threat that is carried out results in an attack.

Vulnerability

- A vulnerability is a weakness that can be exploited either because it is protected by insufficient security controls, or because existing security controls are overcome by an attack.

- IT resource vulnerabilities can have a range of causes, including configuration deficiencies, security policy weaknesses, user errors, hardware or firmware flaws, software bugs, and poor security architecture.

Risk

- Risk is the possibility of loss or harm arising from performing an activity.
- Risk is typically measured according to its threat level and the number of possible or known vulnerabilities.
- Two metrics that Can be used to determine risk for an IT resource.
- The probability of a threat occurring to exploit vulnerabilities in the IT resource.
- The expectation of loss upon the IT resource being compromised.

Security Controls

- Security controls are countermeasures used to prevent or respond to security threats and to reduce or avoid risk.

Types of Cloud Computing Security Controls

- Deterrent Controls :

Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.

Types of Cloud Computing Security Controls

- Preventive Controls :

Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.

Types of Cloud Computing Security Controls

- Detective Controls :

It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.

Types of Cloud Computing Security Controls

- Corrective Controls :

In the event of a security attack these controls are activated. They limit the damage caused by the attack.