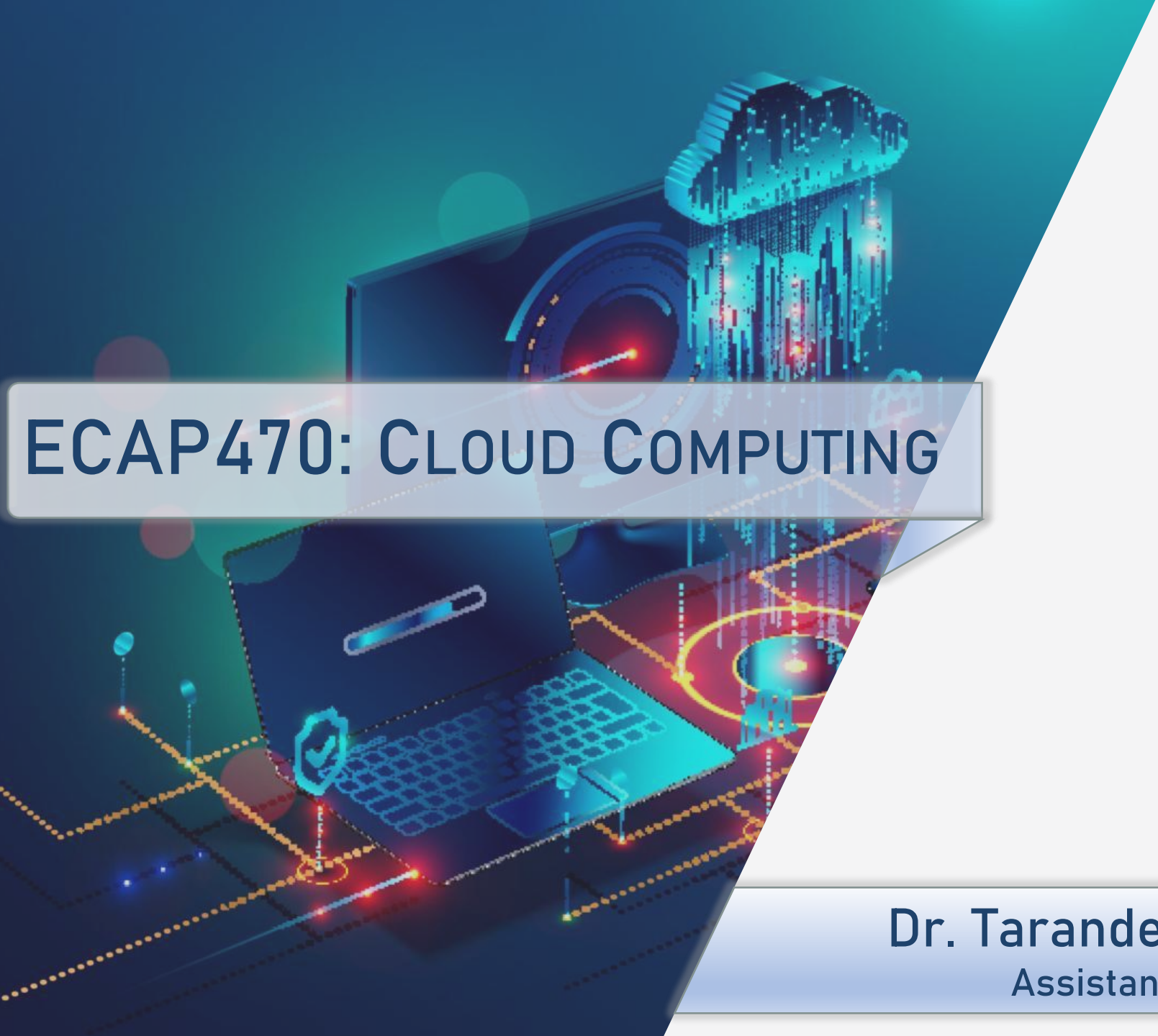


ECAP470: Cloud Computing

Dr. Tarandeep Kaur
Assistant Professor

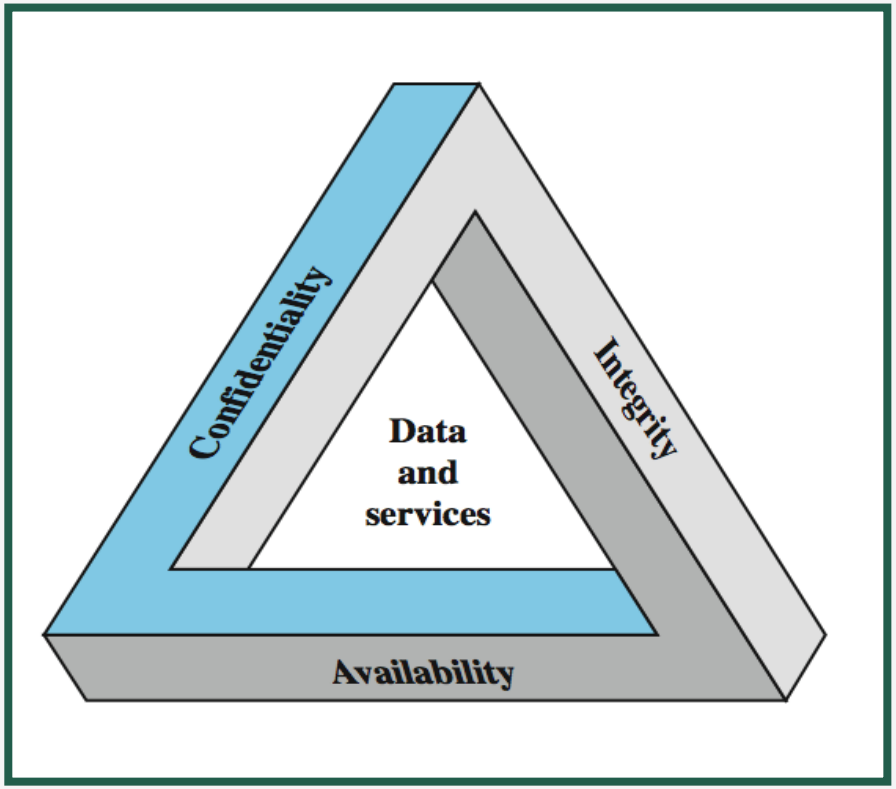
Learning Outcomes

After this lecture, you will be able to,

- ✓ know about security in clouds and Software as a Service Security
- ✓ explore different security challenges in clouds

What is Security?

- Security is the protection of assets.
- Three main aspects are:
  - prevention
  - detection
  - re-action
- CIA Triad



Confidentiality

- Prevention of unauthorized disclosure of information.
  - Data confidentiality
  - Privacy

Integrity

- Integrity is the unauthorized writing or modification of information.
  - Data integrity
  - System Integrity

Availability

Availability

- Assure that systems works promptly, and service is not denied to authorized users.
- Denial of service attacks are a common form of attack.

Other Concepts Related to Security

Authenticity

- Property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator.

Accountability

- Generates requirement for actions of an entity to be traced uniquely to that individual to support non-repudiation, deference, fault isolation etc.

Other Concepts Related to Security

Authenticity

- Property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator.

Accountability

- Generates requirement for actions of an entity to be traced uniquely to that individual to support non-repudiation, deference, fault isolation etc.

Security in Clouds

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

Security in Clouds

- Refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing.
- Sub-domain of computer security, network security, and, more broadly, information security.

Security in Clouds

- Security concerns associated with cloud computing are typically categorized in two ways: as security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).

Security in Clouds

- Shared security responsibility model" or “Shared responsibility model.“
- Extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service.

Security in Clouds

Cloud Security Controls

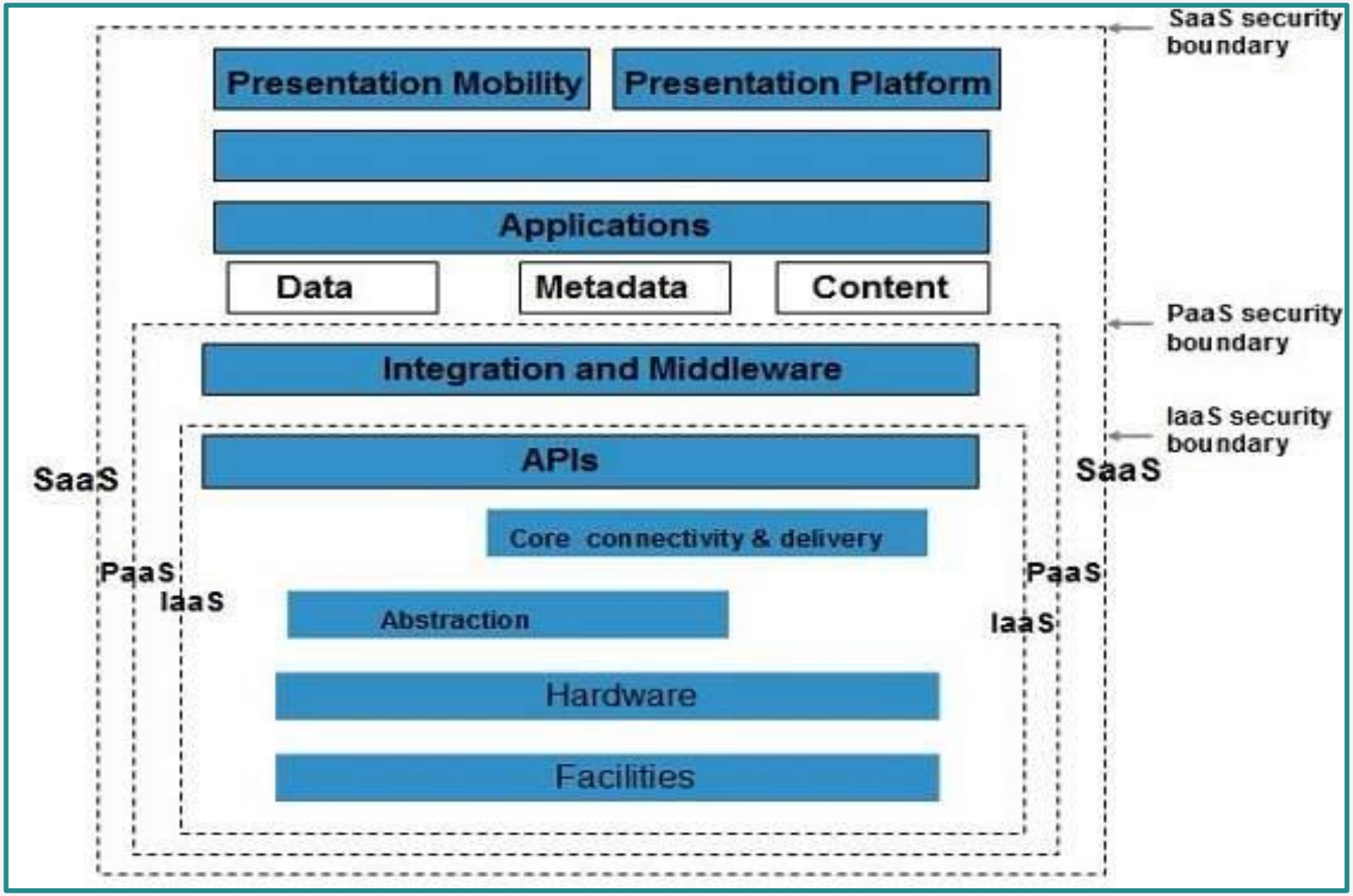
Security in Clouds

Security Boundaries

- A particular service model defines the boundary between the responsibilities of service provider and customer.
- Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate to each other.

Security in Clouds

CSA Stack Model



Security in Clouds

Key Points- CSA Model

- IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
- Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.

Security in Clouds

- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.

Security in Clouds

- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.

Security Challenges

Number of security challenges associated with cloud computing that must be adequately addressed.

1. Managing Complex Environments.
2. Compliance With Rules and Regulations.
3. Lack of Visibility.
4. Data Center or Physical Security Issues.

Other Security Challenges

1. Organizations are afraid of losing their data stored in the cloud.
2. Threats to data privacy put cloud computing at risk.
3. Breaches of confidentiality challenge the integrity of cloud computing.
4. Changing Service Provider.
5. Lack of skills.
6. Data Leakage or Loss.
7. Lack of Control.

Software-as-a-Service Security

- Cloud computing models of the future likely to combine the use of SaaS (and other XaaS's as appropriate), utility computing, and Web 2.0 collaboration technologies to leverage the Internet to satisfy their customers' needs.

Security Issues

Technology analyst & consulting firm “Gartner” lists 7 security issues that need to be discussed with cloud vendor:

- Privileged User Access.
- Regulatory Compliance.
- Data Location.
- Data Segregation.
- Recovery.
- Investigative Support.
- Long-term Viability.

Some Security Practices

- Security Management and Governance
- Risk Management and Risk Assessment
- Security Portfolio Management

Some Security Practices

Secure Software Development Life Cycle (SecSDLC)

1. Investigation
2. Analysis
3. Logical design
4. Physical design
5. Implementation
6. Maintenance

Some Security Practices

- Physical Security of Data Centres
  - Physical access control and monitoring.
  - Environmental controls and backup power.
  - Policies, processes, and procedures.

That's all for now...