Cloud Computing
And it's Security

Guided by :

Ms. N. A. Peshwe

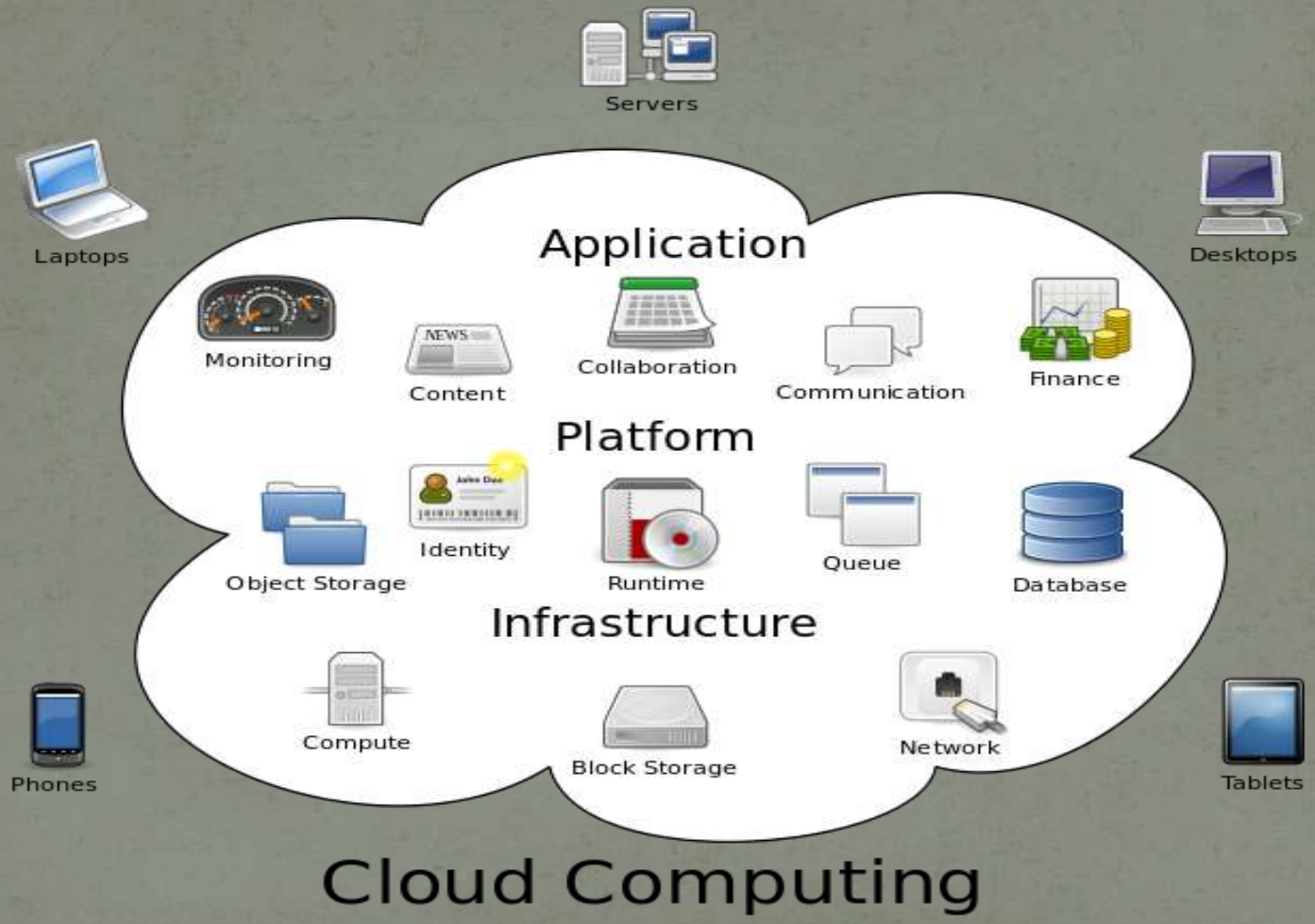
Presented by :

Ganesh S Pasnurwar

Topics :

- What is Cloud Computing?
- Various forms of Cloud Computing
- Benefits of Cloud computing
- Why we need cloud security?
- Cloud Security Concerns
- Cloud Security Threats
- Cloud Security Mechanisms

What is Cloud Computing ?

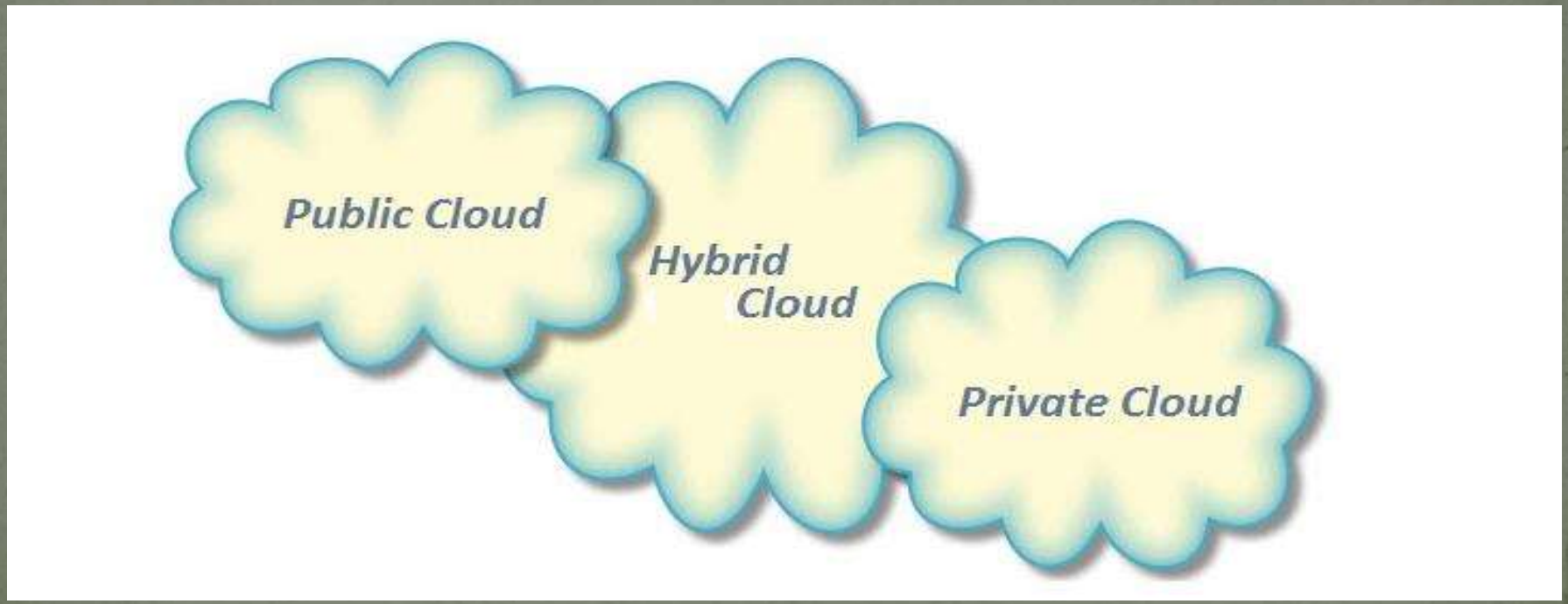


What is Cloud Computing ?

Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications .

Types of Cloud Computing

- Public Cloud
- Private Cloud
- Hybrid Cloud



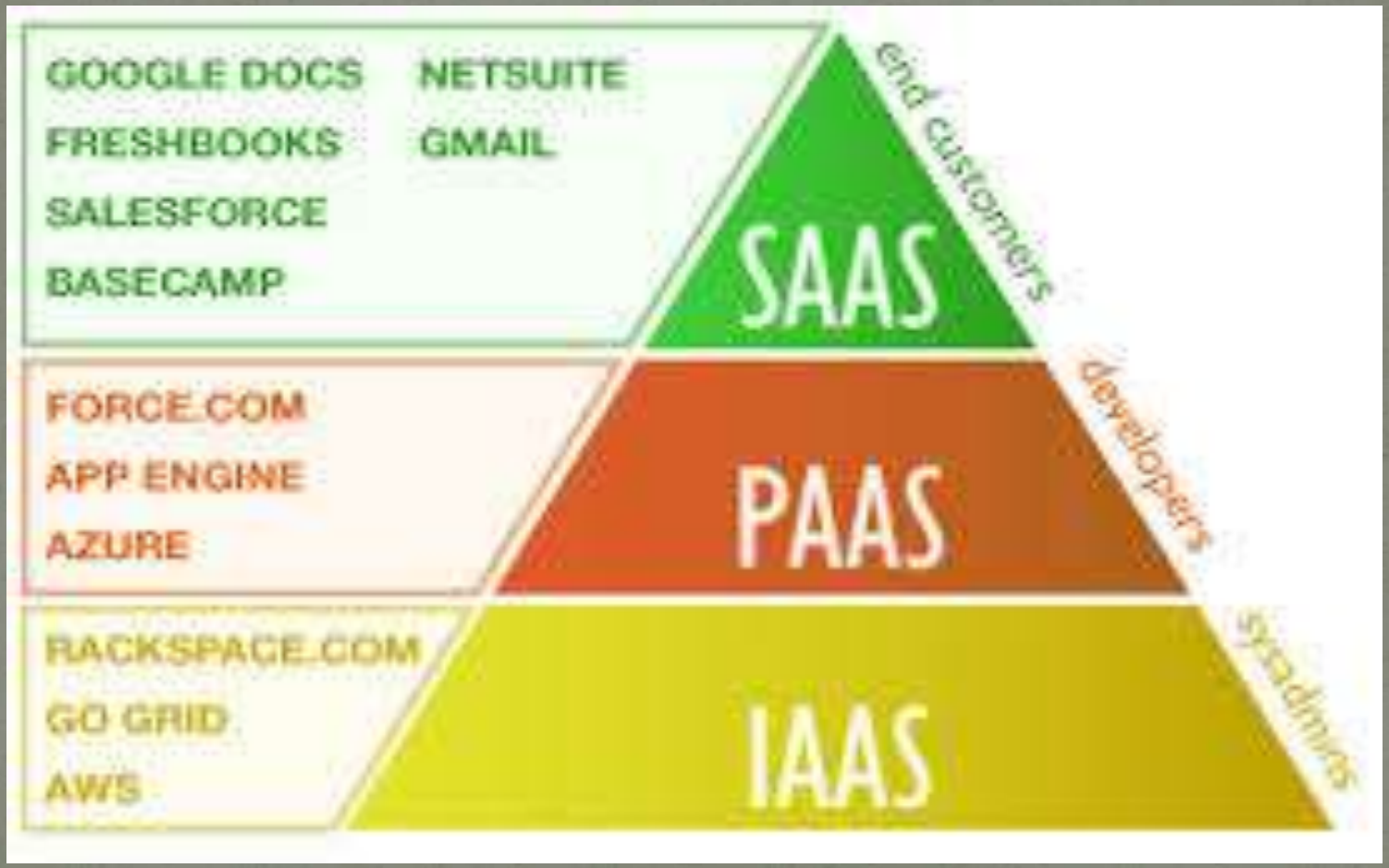
Various Forms of Cloud Computing

- Cloud Computing is some kind of hosted service

Cloud Computing models down into :

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

Various Forms of Cloud Computing



Benefits of Cloud Computing

- Cost (Pay as You Go)
- Multi-tenancy
- Accessibility
- Elasticity
- Easily upgraded

Why we need Cloud security?

Is my data secure on cloud?

Can others access my confidential data?

What if an hacker brings down my app hosted on cloud?

Cloud Security - Concerns

- Multitenancy
- Velocity of Attack
- Information Assurance
- Data privacy and Ownership

Security Concern - Multitenancy

- Multitenancy is a key security concern in cloud
  - For Cloud Clients
    - Co-location of multiple VMs in single server and sharing the same resources increases the attack surface
  - For CSPs
    - Enforcing uniform security controls and measures is difficult
- Mutual client isolation is key measure against multitenancy - related concerns

Security Concern – Velocity of Attack

- Security threats amplify and spread quickly in a Cloud – Known as "Velocity – of – Attack" (VOA) factor
  - Cloud infrastructure is comparatively larger
  - Similarity in the platforms/components employed by a CSP increases the speed at which an attack can spread
- Effects of high VOA
  - Potential loss due to an attack is comparatively higher
  - It is comparatively difficult to mitigate the spread of the attack

Security Concern – Information Assurance and Data Ownership

- Information assurance concern s for Cloud user involve
  - CIA
  - Authenticity
  - Authorized use

- Data ownership concerns for Cloud Clients
  - In Cloud, Data belonging to client is maintained by a CSP who has access to the data but is not the legitimate owner of it
  - Data should be protected using encryption and access control mechanism

Security Concern – Data Privacy

- Private data may include
  - Individual identity of client
  - Details of services requested by client
  - Proprietary data of client

- A CSP needs to ensure that private data of its client is protected from unauthorized user

  - A CSP needs to deploy data privacy mechanism, which are compliant with the regional legal regulations

Cloud Security - Threats

VM Theft

Hyper Jacking

Data Leakage

Denial of Service(DoS) Attack

Security Threat – VM Theft

- What is VM Theft ?
  - A Vulnerability that enables an attacker to copy or move VM in an unauthorized manner

- Result of inadequate controls on VM files allowing unauthorized copy or move operations

Security Threat – Hyper Jacking

- What is Hyper Jacking ?
  - ➢It enables an attacker to install a rogue hypervisor or Virtual Machine Monitor that can take control of the underlying server resources.

- An attacker can run unauthorized application on a guest OS without the OS realizing it
- An attacker could control the interaction between the VMs and underlying servers
- Regular security measures are ineffective against hyper jacking

Security Threat – Data Leakage

- Confidential data stored on third party Cloud is Potentially vulnerable to unauthorized access or manipulation
  - Attacks on service provider's control system(for example password lists) could make all the client s' data vulnerable
- Side Channel Attacks (SCA) can be used for data leakage in Cloud
  - An SCA extracts information by monitoring indirect actives; for example cache data

Security Threat – Denial of Service Attacks

- What is DoS attack?
  - It is an attempt to prevent legitimate user from accessing a resource or service

- Dos attack might affect software application and network component

- DoS involves
  - Exhausting resources
  - Exploiting weakness in communication protocols

Cloud Security - Mechanisms

Compute and Network Security

Secure Data at Rest

Identity and Access Management

Risk Analysis

Security at Compute Level

- Securing a compute system includes
  - Securing physical server
  - Securing hypervisor
  - Security at guest OS level
    - Guest OS Hardening
  - Security at application level

Securing Data-at -Rest

- Data-at-rest
  - Data which is not being transferred over a network

- Encryption of Data-at-rest
  - provides confidentiality
  - Provides integrity services

- Full disk encryption is a key method to encrypt data-at-rest residing on a disk

Identity Management (IM) in Cloud

- One-time password
  - Every new access request requires new password
  - A measure against “password compromises”

- Federated Identity Management is provided as a service on cloud
  - In it user identities across different organization can be managed together to enable collaboration on Cloud

Risk Analysis

- Risk refers to the effect of uncertainty on business objectives
- Risk management is a coordinated activity that direct and control an organization

Risk Assessment

- Aim to identify potential risks while operating in a Cloud environment
  - Should be performed before moving to cloud
  - Used to determine the actual scope for Cloud adoption


Thank you...