Module 20

Cloud Computing

Ansh Bhawnani

Cloud Computing Concepts

Module 20

Cloud Computing Concepts

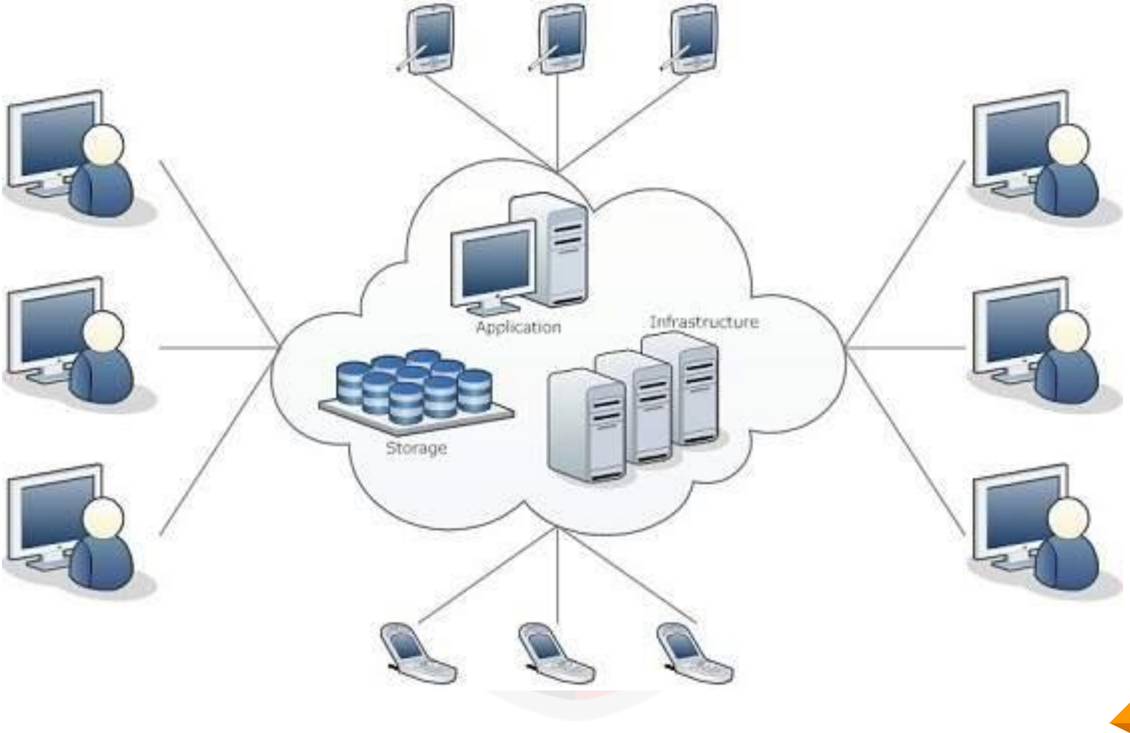
- Cloud Computing provides us means of accessing the applications as utilities over the Internet. It allows us to create, configure, and customize the applications online.
- **What is Cloud?**
  - The term **Cloud** refers to a **Network** or **Internet.** In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN.
  - Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

Cloud Computing Concepts

What is Cloud Computing?

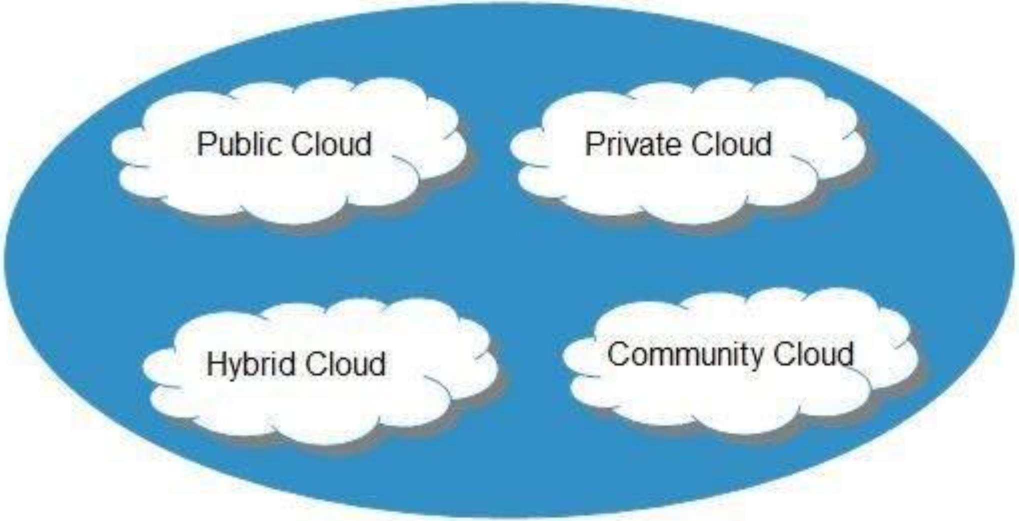
- Cloud Computing refers to **manipulating, configuring,** and **accessing** the hardware and software resources remotely. It offers online data storage, infrastructure, and application.
- Cloud computing offers **platform independency,** as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications **mobile** and **collaborative.**

Cloud Computing Concepts



Cloud Computing Concepts

Deployment Models



Cloud Computing Concepts

- **Public Cloud:** It allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.
- **Private Cloud:** It allows systems and services to be accessible within an organization. It is more secured because of its private nature.
- **Community Cloud:** It allows systems and services to be accessible by a group of organizations.
- **Hybrid Cloud:** It is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

Cloud Computing Concepts

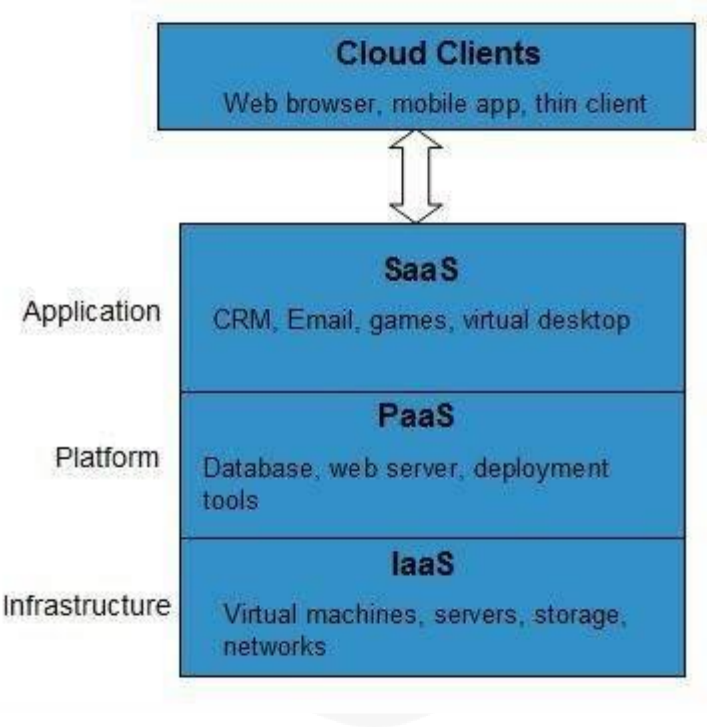
Service Models

- Cloud computing is based on service models. These are categorized into three basic service models which are -
  - *Infrastructure-as–a-Service* (IaaS)
  - *Platform-as-a-Service* (PaaS)
  - *Software-as-a-Service* (SaaS)

Cloud Computing Concepts

- **Anything-as-a-Service (XaaS)** is yet another service model, which includes ***Network-as-a-Service***, ***Business-as-a-Service***, ***Identity-as-a-Service***, ***Database-as-a-Service*** or ***Strategy-as-a-Service***.
- The **Infrastructure-as-a-Service (IaaS)** is the most basic level of service. Each of the service models inherit the security and management mechanism from the underlying model. It provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.
- **Platform-as-a-Service (PaaS):** It provides the runtime environment for applications, development and deployment tools, etc.
- **Software-as-a-Service (SaaS):** It allows to use software applications as a service to end-users.

Cloud Computing Concepts



Cloud Clients

Web browser, mobile app, thin client

Application

SaaS

CRM, Email, games, virtual desktop

Platform

PaaS

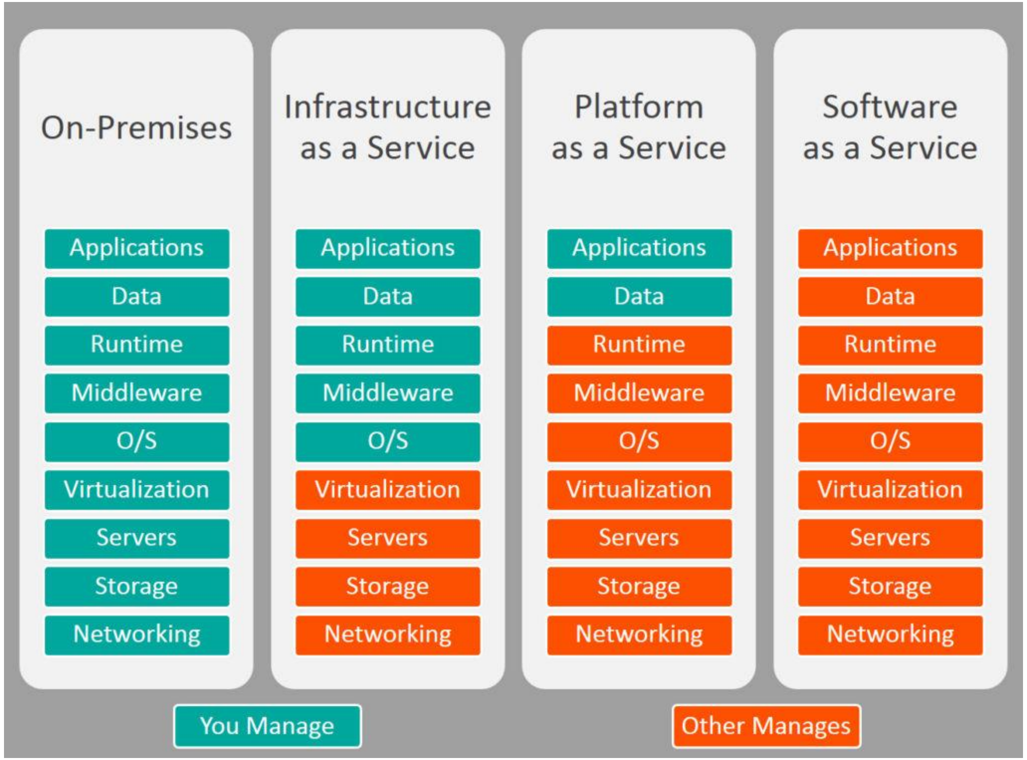
Database, web server, deployment tools

Infrastructure

IaaS

Virtual machines, servers, storage, networks

Cloud Computing Concepts



On-Premises	Infrastructure as a Service	Platform as a Service	Software as a Service
🟩 Applications	🟩 Applications	🟩 Applications	🟧 Applications
🟩 Data	🟩 Data	🟩 Data	🟧 Data
🟩 Runtime	🟩 Runtime	🟧 Runtime	🟧 Runtime
🟩 Middleware	🟩 Middleware	🟧 Middleware	🟧 Middleware
🟩 O/S	🟩 O/S	🟧 O/S	🟧 O/S
🟩 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟩 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟩 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟩 Networking	🟧 Networking	🟧 Networking	🟧 Networking

🟩 You Manage

🟧 Other Manages

Cloud Computing Concepts

Benefits

- One can access, manipulate and configure the applications online at any time.
- It does not require to install a software to access or manipulate cloud application.
- It is highly scalable in terms of bandwidth and performance and upto 100% uptime.
- Cloud Computing offers **on-demand self-service.** The resources can be used without interaction with cloud service provider.
- Cloud Computing is highly cost effective (pay per use) and operates at high efficiency with optimum utilization.
- Offers virtualization
- Cloud Computing offers load balancing that makes it more reliable.

Cloud Computing Concepts

Risks related to Cloud Computing

Security and Privacy

- It is always a risk to handover the sensitive information to cloud service providers.
- Any sign of security breach may result in loss of customers and businesses.

Lock In

- It is very difficult for the customers to switch from one **Cloud Service Provider (CSP)** to another. It results in dependency on a particular CSP for service.

Cloud Computing Concepts

Isolation Failure (Multi-tenancy)

- This risk involves the failure of isolation mechanism that separates storage, memory, and routing between the different tenants.

Management Interface Compromise

- In case of public cloud provider, the customer management interfaces are accessible through the Internet.

Insecure or Incomplete Data Deletion

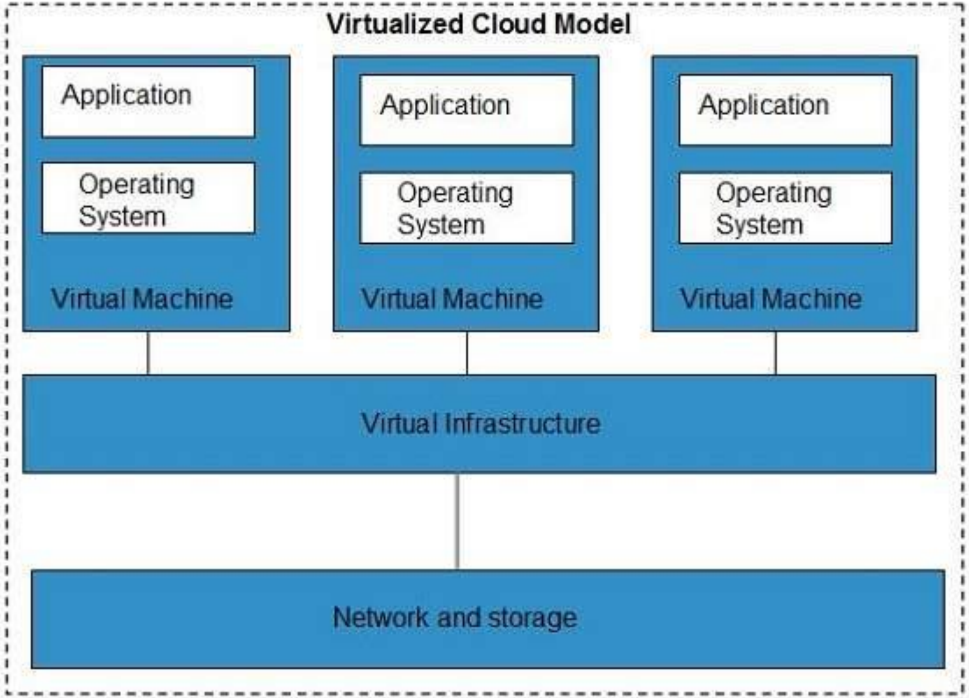
- It is possible that the data requested for deletion may not get deleted. It happens because extra copies of data are stored but are not available at the time of deletion.

Cloud Computing Concepts

Virtualization

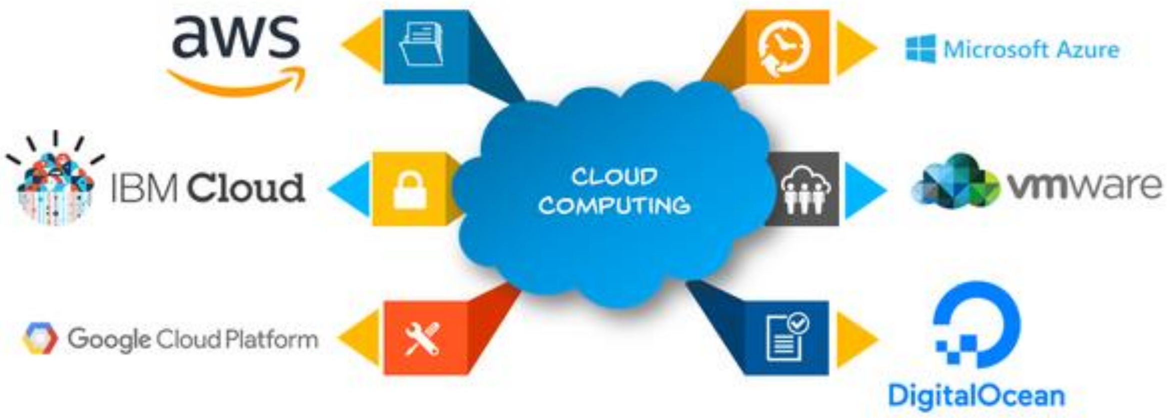
- **Virtualization** is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants (customers). It does this by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.
- The **Multitenant** architecture offers **virtual isolation** among the multiple tenants. Hence, the organizations can use and customize their application as though they each have their instances running.

Cloud Computing Concepts



Cloud Computing Concepts

Top Cloud Computing Providers



Cloud Computing Threats

Module 20

“ *Is Cloud Security really a concern?*

Cloud Computing Threats

- Lack of visibility
- Insecure Interfaces/APIs
- Data breaches
- Denial of service
- Insider threats
- Hijacking accounts
- Insecure applications
- Inadequate training
- Cryptojacking

Cloud Computing Threats

Lack of visibility

- An organization’s cloud-based resources are located outside of the corporate network and run on infrastructure that the company does not own.
- Some organizations lack cloud-focused security tools. This can limit an organization’s ability to monitor their cloud-based resources and protect them against attack.

Cloud Computing Threats

Insecure Interfaces/APIs

- CSPs often provide a number of well documented application programming interfaces (APIs) and interfaces for their customers.
- The documentation designed for the customer can also be used by a *cybercriminal* to identify and exploit potential methods for accessing and exfiltrating sensitive data

Cloud Computing Threats

Data breaches

- A data breach typically occurs when a business is attacked by cybercriminals who are able to gain unauthorized access to the cloud network or utilize programs to view, copy, and transmit data.
- Losing data can violate the *General Data Protection Regulation* (GDPR), which could cause your business to face heavy fines.

Cloud Computing Threats

Denial of service

- Cybercriminals can flood your system with a very large amount of web traffic that your servers are not able to cope with. This means that the servers will not buffer, and nothing can be accessed.
- If the whole of your system runs on the cloud, this can then make it impossible for you to manage your business.

Cloud Computing Threats

Insider threats

- Sometimes the problem originates from the inside of the company. In fact, recent statistics suggest that insider attacks could account for more than 43 percent of all data breaches.
- Insider threats can be malicious – such as members of staff going rogue – but they can also be due to negligence or simple human error. It is important, then, to provide your staff with training, and also ensure that you are tracking the behavior of employees to ensure that they cannot commit crimes against the business.

Cloud Computing Threats

Hijacking accounts

- If a criminal can gain access to your system through a staff account, they could potentially have full access to all of the information on your servers without you even realizing any crime has taken place.
- Cybercriminals use techniques such as password cracking and phishing emails in order to gain access to accounts

Cloud Computing Threats

Insecure applications/Misconfigurations

- Sometimes it can be the case that your own system is highly secure, but you are let down by external applications. Third-party services, such as applications, can present serious cloud security risk.
- For example, using older versions of *PHP*, *database* applications, *Wordpress*, etc.

Cloud Computing Threats

Inadequate training

- Most cybersecurity threats come in the form of outsider attacks, but this issue is one caused by a problem inside the company. And this problem is in failing to take the threat of cybercrime seriously.
- Your team is your first line of defense against any kind of data breach.

Cloud Computing Threats

Cryptojacking

- You need computing power, and cybercriminals have found methods of accessing cloud computing systems and then using their computing power to mine for cryptocurrency, such as Bitcoins.
- Many IT teams mistake the symptoms of cryptojacking as a flaw with an update or a slower internet connection, meaning it takes them much longer to establish the real problem.

Cloud security

Module 20

Cloud security

- **Cloud computing security** or, more simply, **cloud security** 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. It is a sub-domain of computer security, network security, and, more broadly, information security.
- According to a recent *Cloud Security Alliance* report, insider attacks are the sixth biggest threat in cloud computing.
- *Virtualization* alters the relationship between the OS and underlying hardware.

Cloud security

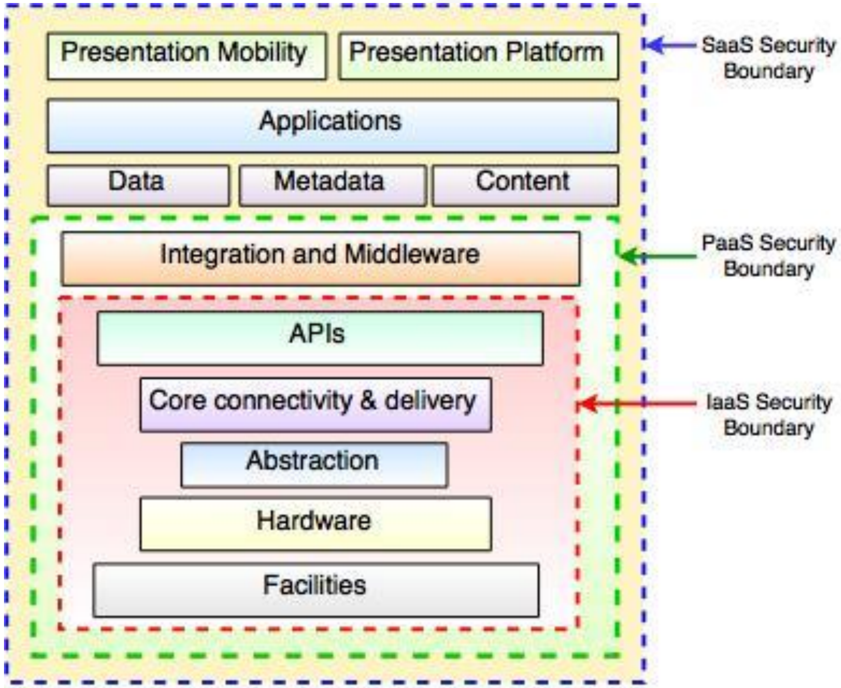
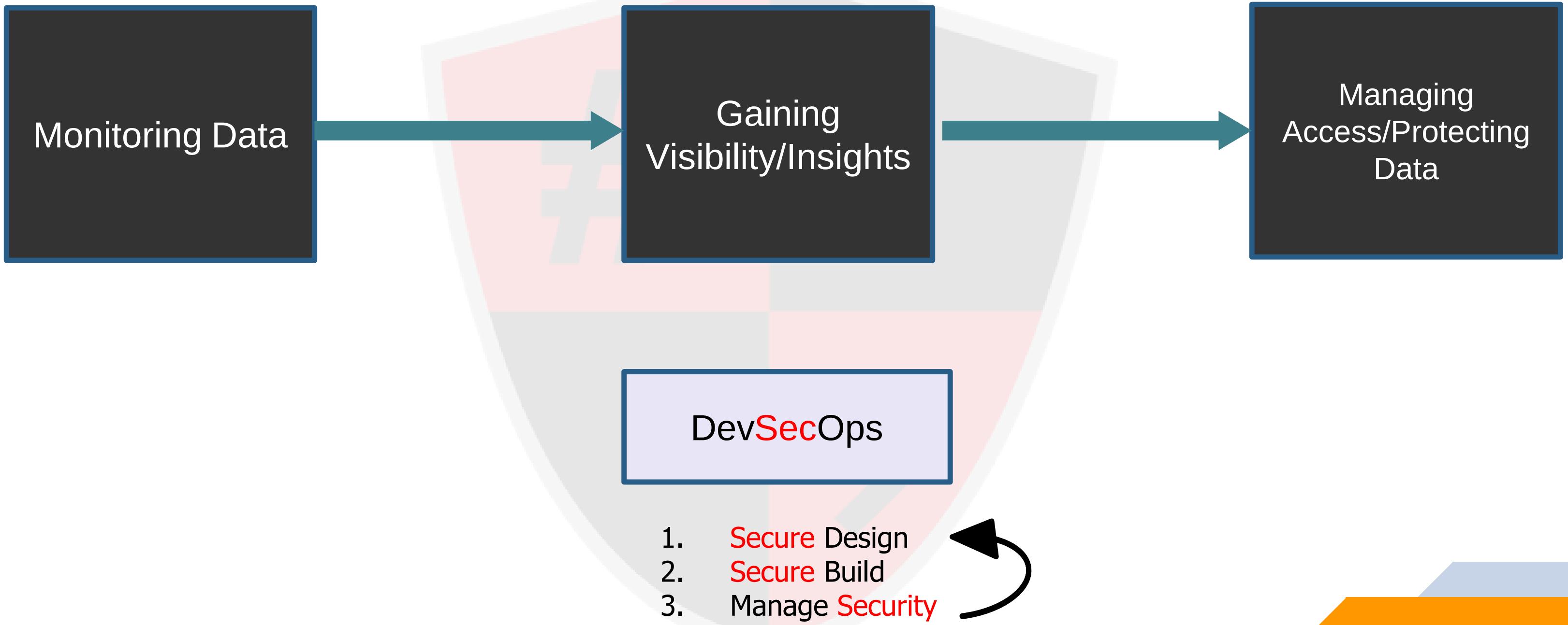


Fig.- CSA Stack Model

1. Cloud security controls

Module 20

Cloud security



Monitoring Data

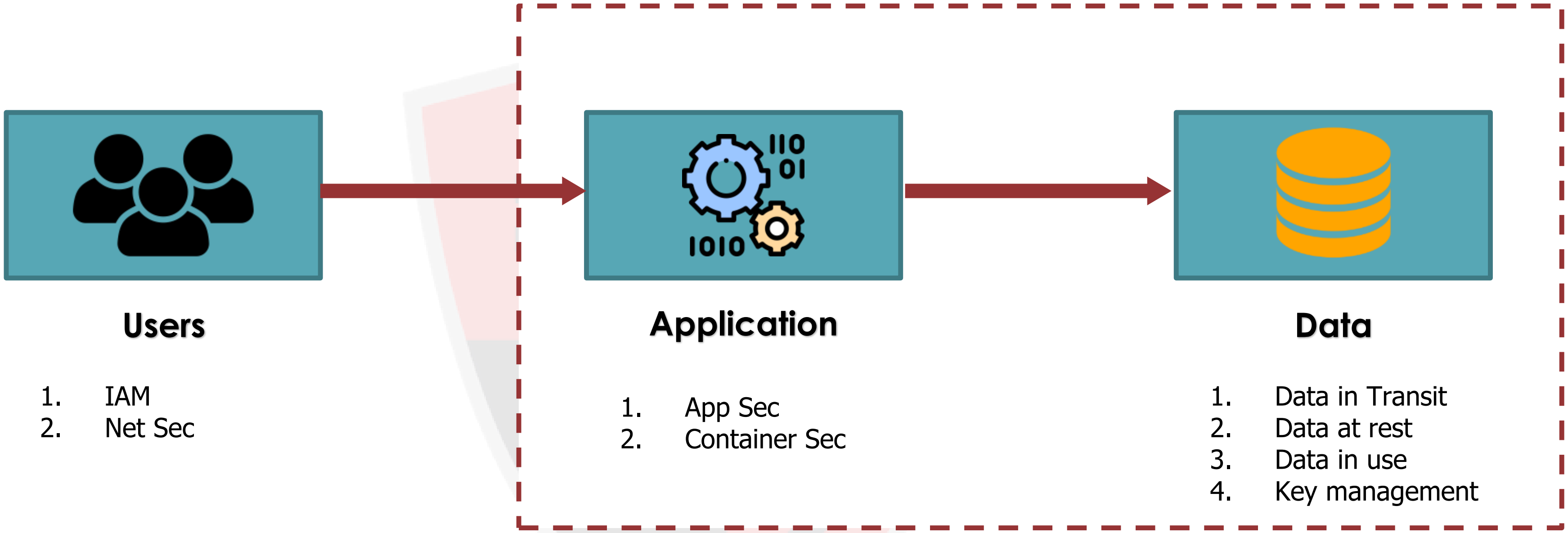
Gaining Visibility/Insights

Managing Access/Protecting Data

DevSecOps

1. Secure Design
2. Secure Build
3. Manage Security

Cloud security



Users

1. IAM
2. Net Sec

Application

1. App Sec
2. Container Sec

Data

1. Data in Transit
2. Data at rest
3. Data in use
4. Key management

Cloud security

- **Deterrent controls:** These controls are intended to reduce attacks on a cloud system
- **Preventive controls:** Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities.
- **Detective controls**: Detective controls are intended to detect and react appropriately to any incidents that occur
- **Corrective controls**: Corrective controls reduce the consequences of an incident, normally by limiting the damage.

2. Security and privacy

Module 6

Cloud security

- **Identity management:** Cloud providers either integrate the customer's *identity management system* into their own infrastructure, using federation or SSO technology, or a biometric-based identification system
- **Physical security:** Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access
- **Personnel security:** IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive.
- **Privacy:** Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and authorized.

3. Data security

Module 6

Cloud security

- **Confidentiality:** Data confidentiality is the property that data contents are not made available or disclosed to illegal users.
- **Access controllability:** Access controllability means that a data owner can perform the selective restriction of access to their data outsourced to the cloud.
- **Integrity:** Data integrity demands maintaining and assuring the accuracy and completeness of data.

4. Encryption

Module 6

Cloud security

- **Attribute-based encryption (ABE):** type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has).
- **Ciphertext-policy ABE (CP-ABE):** The encryptor controls access strategy.
- **Key-policy ABE (KP-ABE):** Attribute sets are used to describe the encrypted texts and the private keys are associated to specified policy that users will have.
- **Fully homomorphic encryption (FHE):** Allows computations on encrypted data.
- **Searchable encryption (SE):** Searchable encryption is a cryptographic system which offer secure search functions over encrypted data.

Cloud security

- It is important, then, to provide your staff with training, and also ensure that you are tracking the behavior of employees to ensure that they cannot commit crimes against the business.
- The point at which someone leaves the company – you need to ensure that their access to any crucial data is removed and that their credentials no longer work in the system. (*off-boarding*)
- Ensure proper permissions management. This means that every account across the business should only be given access to the information that they need to do their job.
- Make it necessary for the IT team to approve any application before it is installed on the system.

Cloud security

- They need to be prepared with the latest information or relevant threats to businesses like yours. Allocate time and budget for staff training, and also make sure that this training is regularly updated so that your staff is being taught about issues that are genuinely affecting organizations.

HACKING

Is an art, practised through a creative mind.