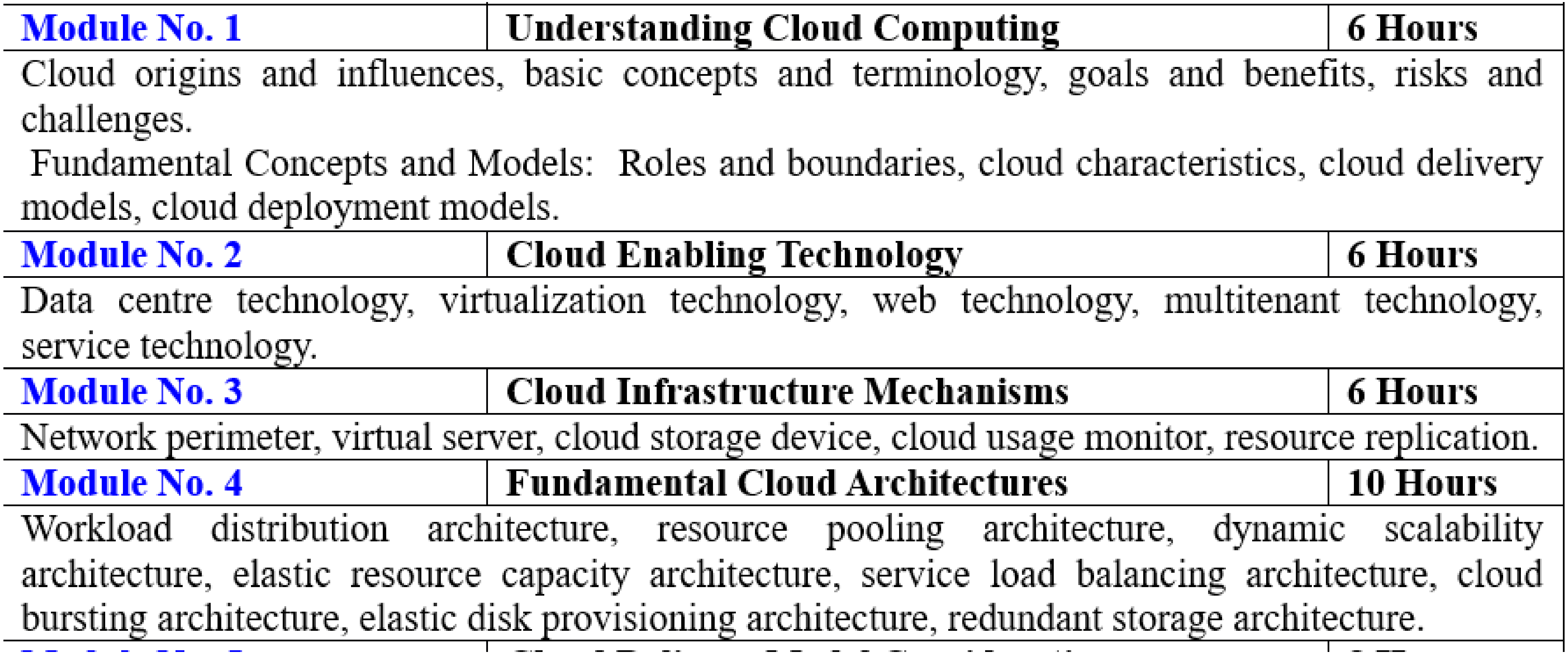
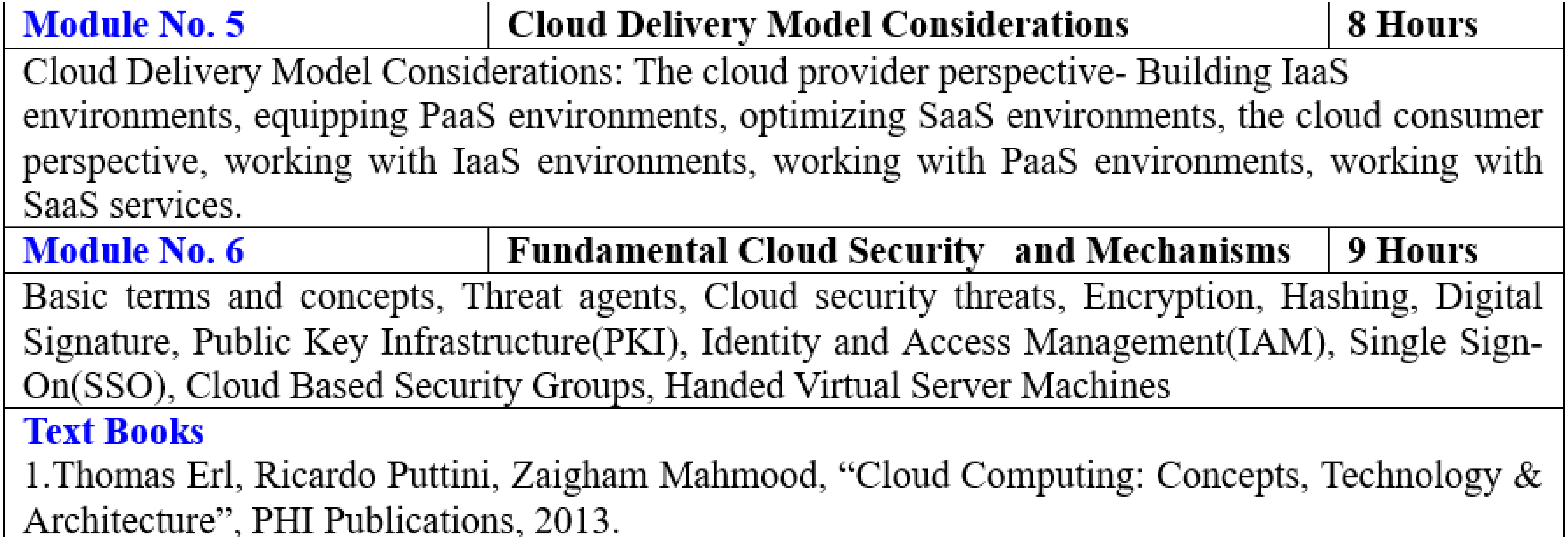
Course code	: **CSE4001**
Course title	: **Cloud Computing**
Module	: **5**
Topic	: **1**

Cloud Delivery Models



Module No. 1	Understanding Cloud Computing	6 Hours
Cloud origins and influences, basic concepts and terminology, goals and benefits, risks and challenges. Fundamental Concepts and Models: Roles and boundaries, cloud characteristics, cloud delivery models, cloud deployment models.		
Module No. 2	Cloud Enabling Technology	6 Hours
Data centre technology, virtualization technology, web technology, multitenant technology, service technology.		
Module No. 3	Cloud Infrastructure Mechanisms	6 Hours
Network perimeter, virtual server, cloud storage device, cloud usage monitor, resource replication.		
Module No. 4	Fundamental Cloud Architectures	10 Hours
Workload distribution architecture, resource pooling architecture, dynamic scalability architecture, elastic resource capacity architecture, service load balancing architecture, cloud bursting architecture, elastic disk provisioning architecture, redundant storage architecture.		



Module No. 5	**Cloud Delivery Model Considerations**	**8 Hours**
Cloud Delivery Model Considerations: The cloud provider perspective- Building IaaS environments, equipping PaaS environments, optimizing SaaS environments, the cloud consumer perspective, working with IaaS environments, working with PaaS environments, working with SaaS services.		
Module No. 6	**Fundamental Cloud Security and Mechanisms**	**9 Hours**
Basic terms and concepts, Threat agents, Cloud security threats, Encryption, Hashing, Digital Signature, Public Key Infrastructure(PKI), Identity and Access Management(IAM), Single Sign-On(SSO), Cloud Based Security Groups, Handed Virtual Server Machines		
Text Books 1.Thomas Erl, Ricardo Puttini, Zaigham Mahmood, "Cloud Computing: Concepts, Technology & Architecture", PHI Publications, 2013.		

Objectives

This session will give the knowledge about

- *14.1 Cloud Delivery Models: The Cloud Provider Perspective*
- 14.2 Cloud Delivery Models: The Cloud Consumer Perspective
- 14.3 Case Study Example

The Cloud Provider Perspective

- Building IaaS Environments
- Equipping PaaS Environments
- Optimizing SaaS Environments

The Cloud Consumer Perspective

- Working with IaaS Environments
- Working with IaaS Environments
- Working with SaaS Services

Cloud Providers ?

- A cloud provider is a person, or an organization; it is the entity responsible for making a service available to interested parties.

- A Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

Cloud Consumer ?

- The cloud consumer is the principal stakeholder for the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider.

- The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.
- Cloud consumers need SLAs to specify the technical performance requirements fulfilled by a cloud provider. SLAs can cover terms regarding the quality of service, security, remedies for performance failures.

List of Cloud Service Providers

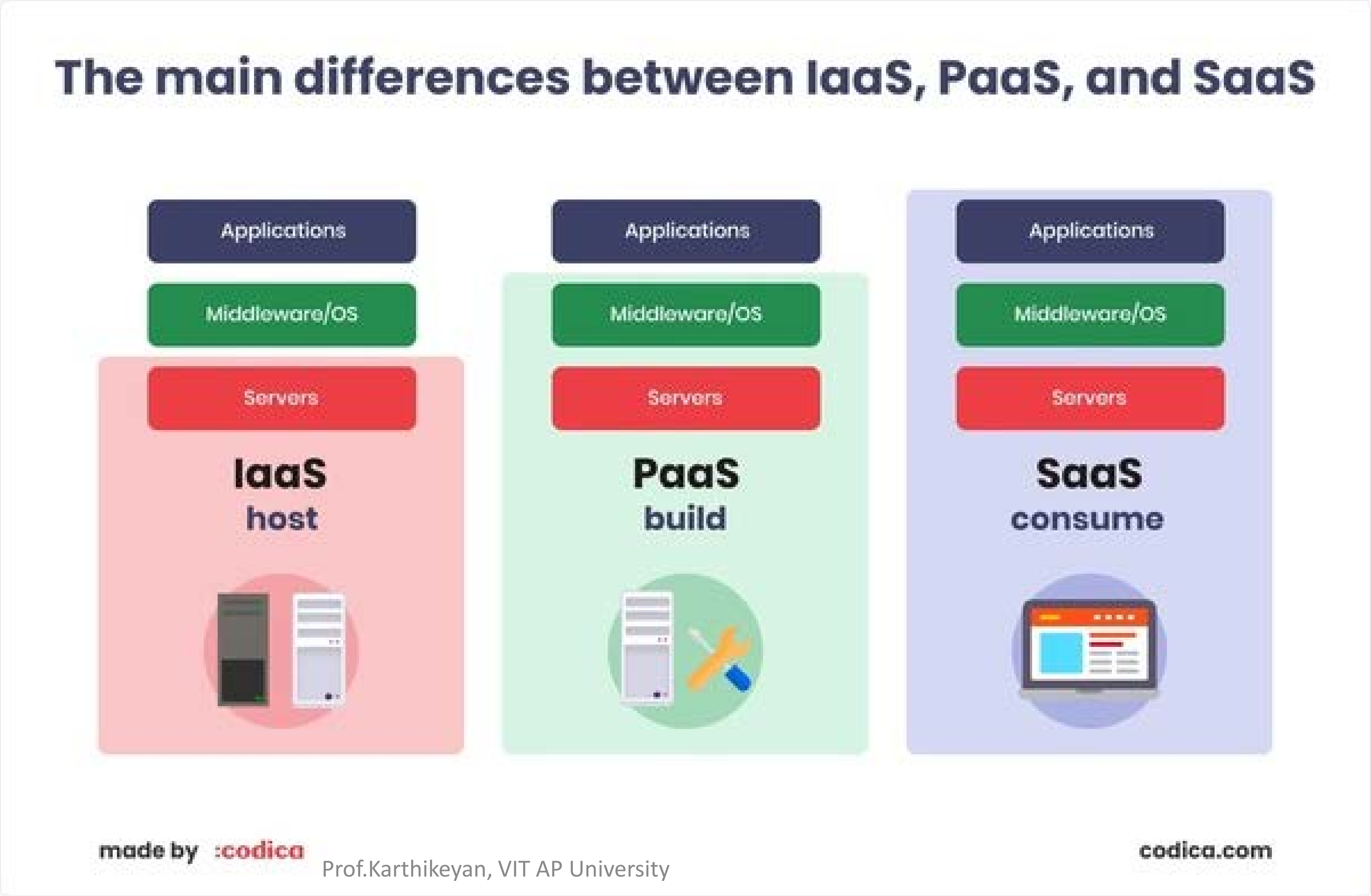
- **Amazon Web Service (AWS)**
- Microsoft Azure
- Google Cloud Platform
- IBM Cloud Services
- Adobe Creative Cloud
- Kamatera
- VMware
- Rackspace
- Red Hat

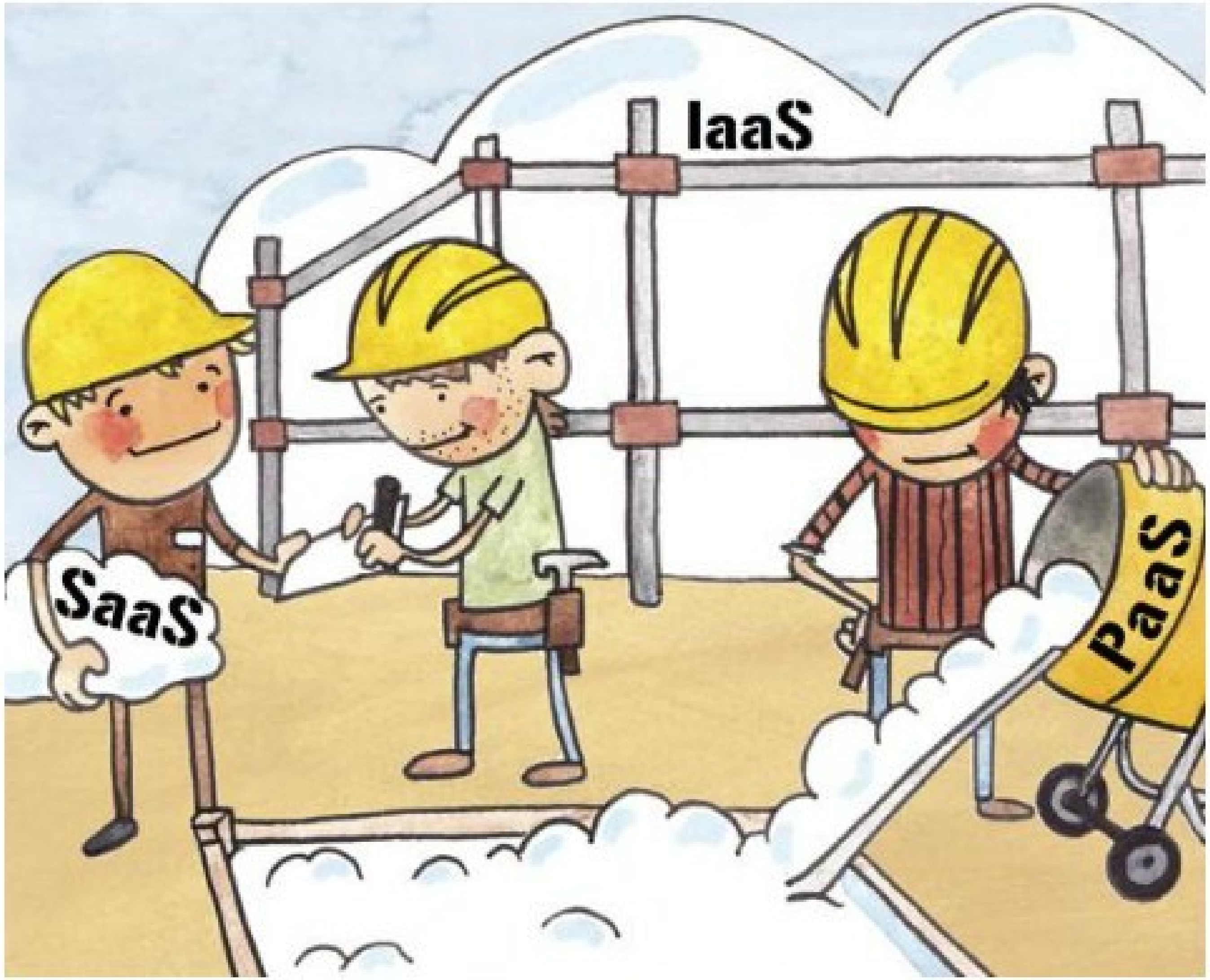
- **Salesforce**
- Oracle Cloud
- SAP
- Verizon Cloud
- Navisite
- Dropbox

The Cloud Provider Perspective

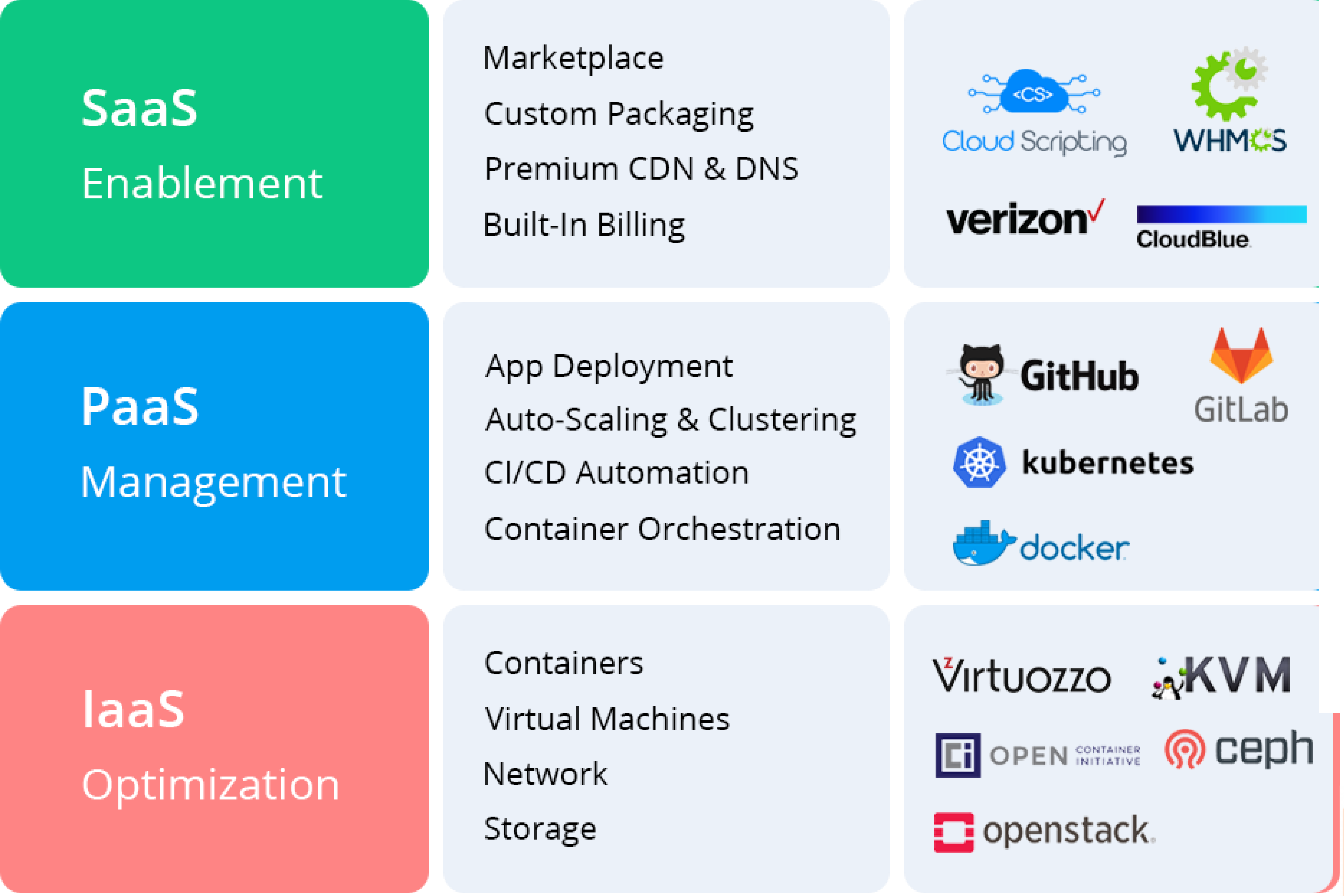
- Explores the architecture and administration of IaaS, PaaS, and SaaS
- The integration and management of these cloud-based environments as part of greater environments.
- How they can relate to different technologies and cloud mechanism combinations are examined.

Iaas,Paas, Saas ?

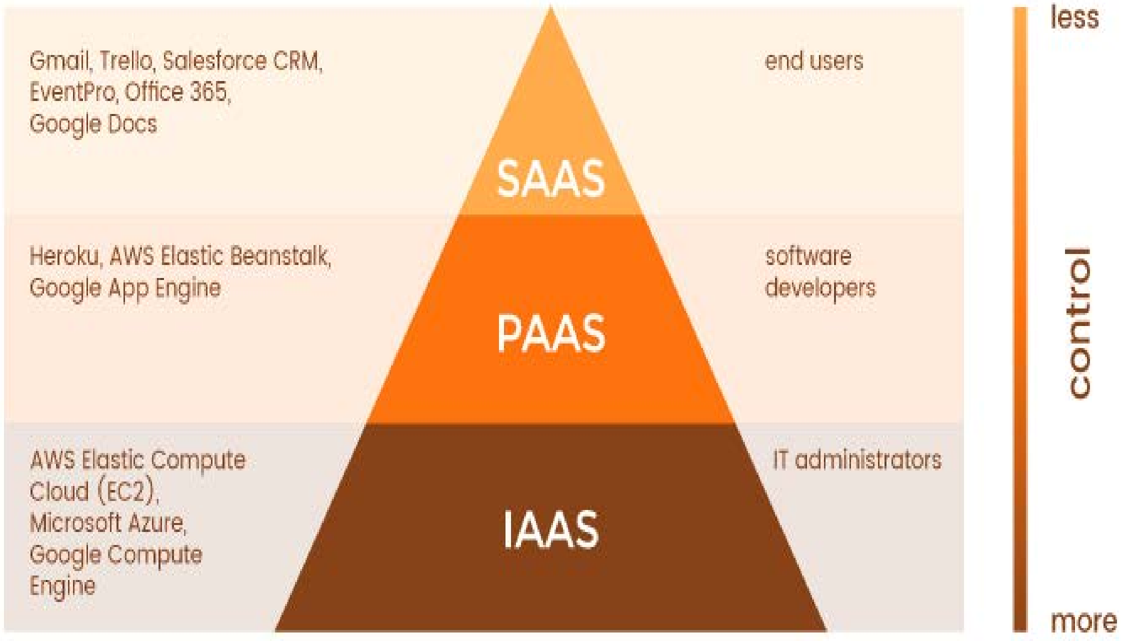




SaaS, PaaS and IaaS - The cloud Computing Services



SaaS Enablement	Marketplace Custom Packaging Premium CDN & DNS Built-In Billing	Cloud Scripting WHMCS verizon CloudBlue
PaaS Management	App Deployment Auto-Scaling & Clustering CI/CD Automation Container Orchestration	GitHub GitLab kubernetes docker
IaaS Optimization	Containers Virtual Machines Network Storage	Virtuozzo KVM OPEN CONTAINER INITIATIVE ceph openstack


Gmail, Trello, Salesforce CRM, EventPro, Office 365, Google Docs
SAAS
end users
Heroku, AWS Elastic Beanstalk, Google App Engine
PAAS
software developers
AWS Elastic Compute Cloud (EC2), Microsoft Azure, Google Compute Engine
IAAS
IT administrators
less
control
more

IaaS

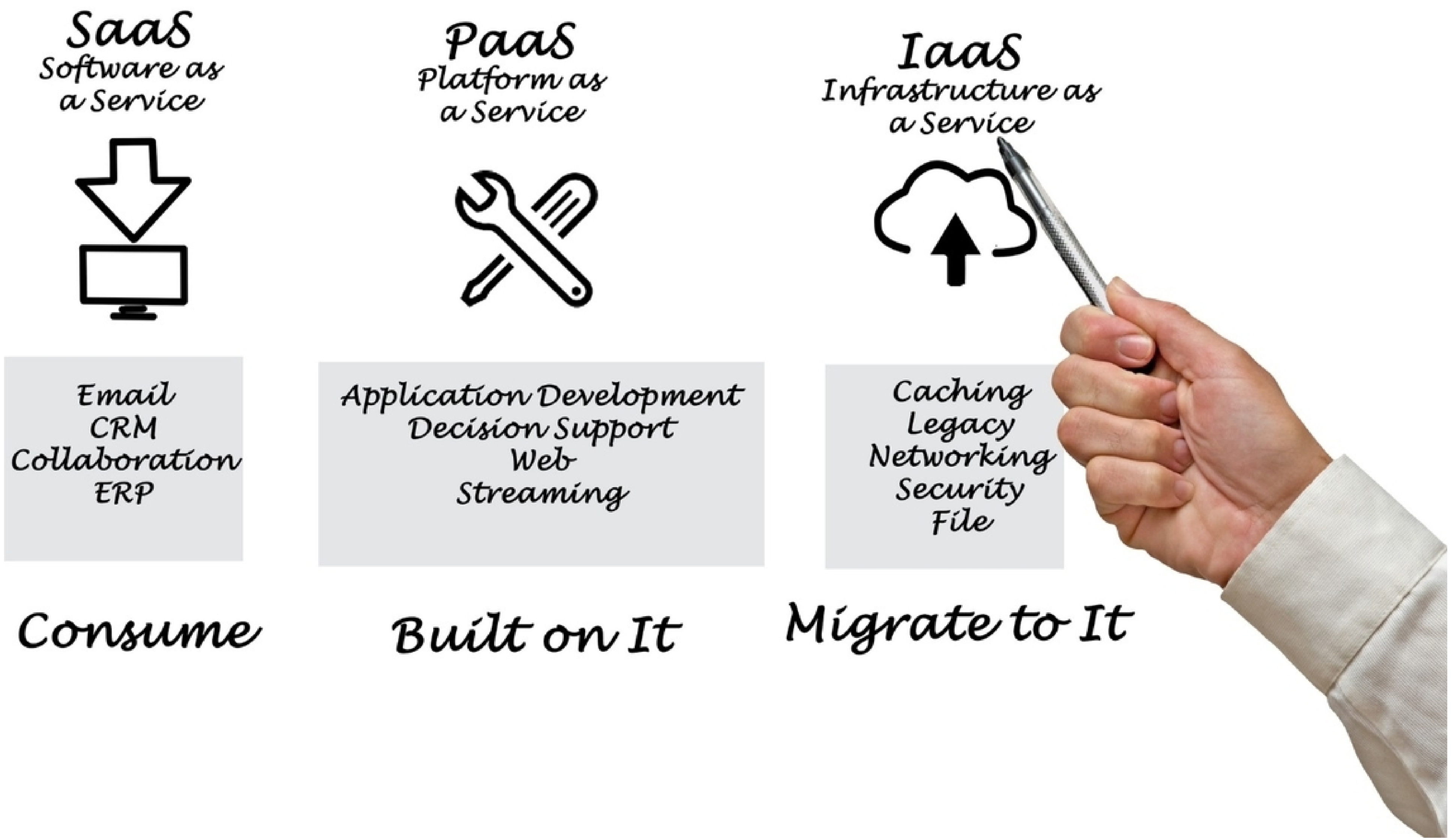
DigitalOcean
Linode
Rackspace
AWS
Cisco Metapod
Microsoft Azure
Google Compute Engine (GCE)

PaaS

AWS Elastic Beanstalk
Windows Azure
Heroku
Force.com
Google App Engine Apache
Stratos OpenShift

SaaS

Google Apps
Dropbox
Salesforce
Cisco WebEx
Concur
GoToMeeting



SaaS
Software as
a Service

Email
CRM
Collaboration
ERP

Consume

PaaS
Platform as
a Service

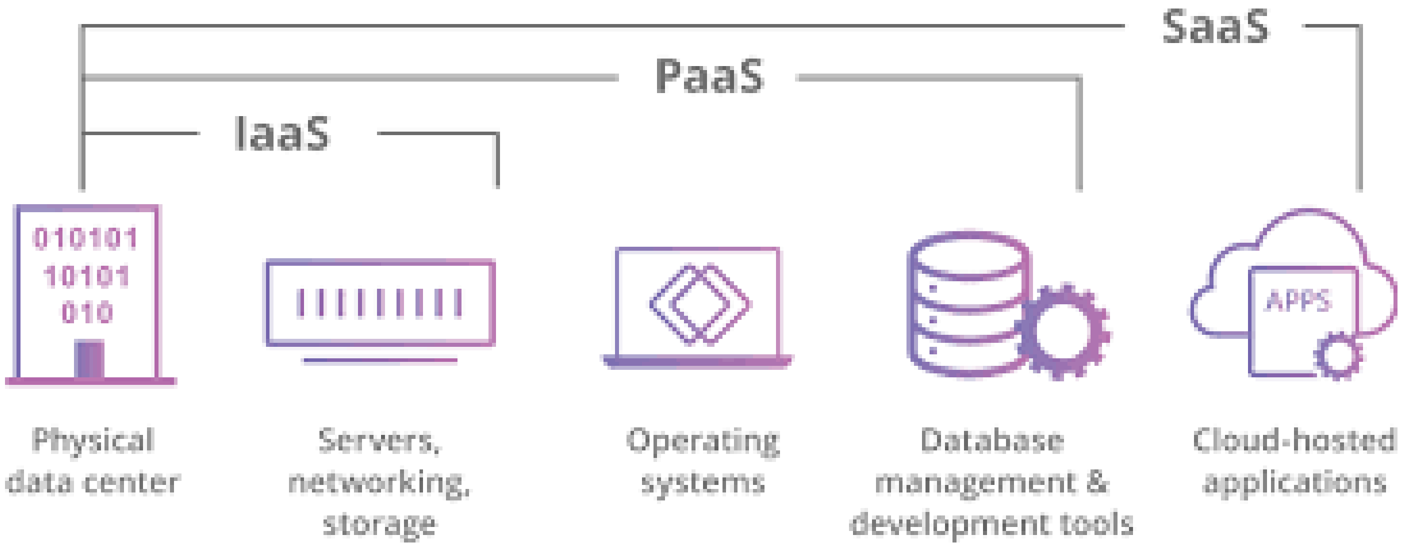
Application Development
Decision Support
Web
Streaming

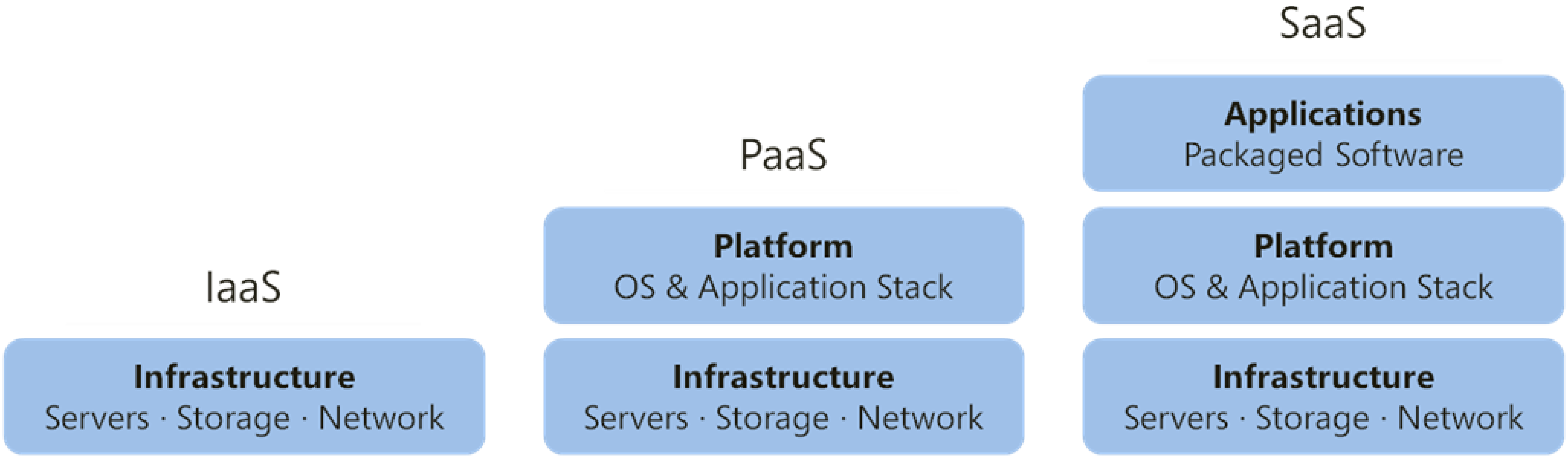
Built on It

IaaS
Infrastructure as
a Service

Caching
Legacy
Networking
Security
File

Migrate to It


SaaS
PaaS
IaaS
010101
10101
010
APPS
Physical data center
Servers, networking, storage
Operating systems
Database management & development tools
Cloud-hosted applications



SaaS

Applications
Packaged Software

Platform
OS & Application Stack

Infrastructure
Servers · Storage · Network

PaaS

Platform
OS & Application Stack

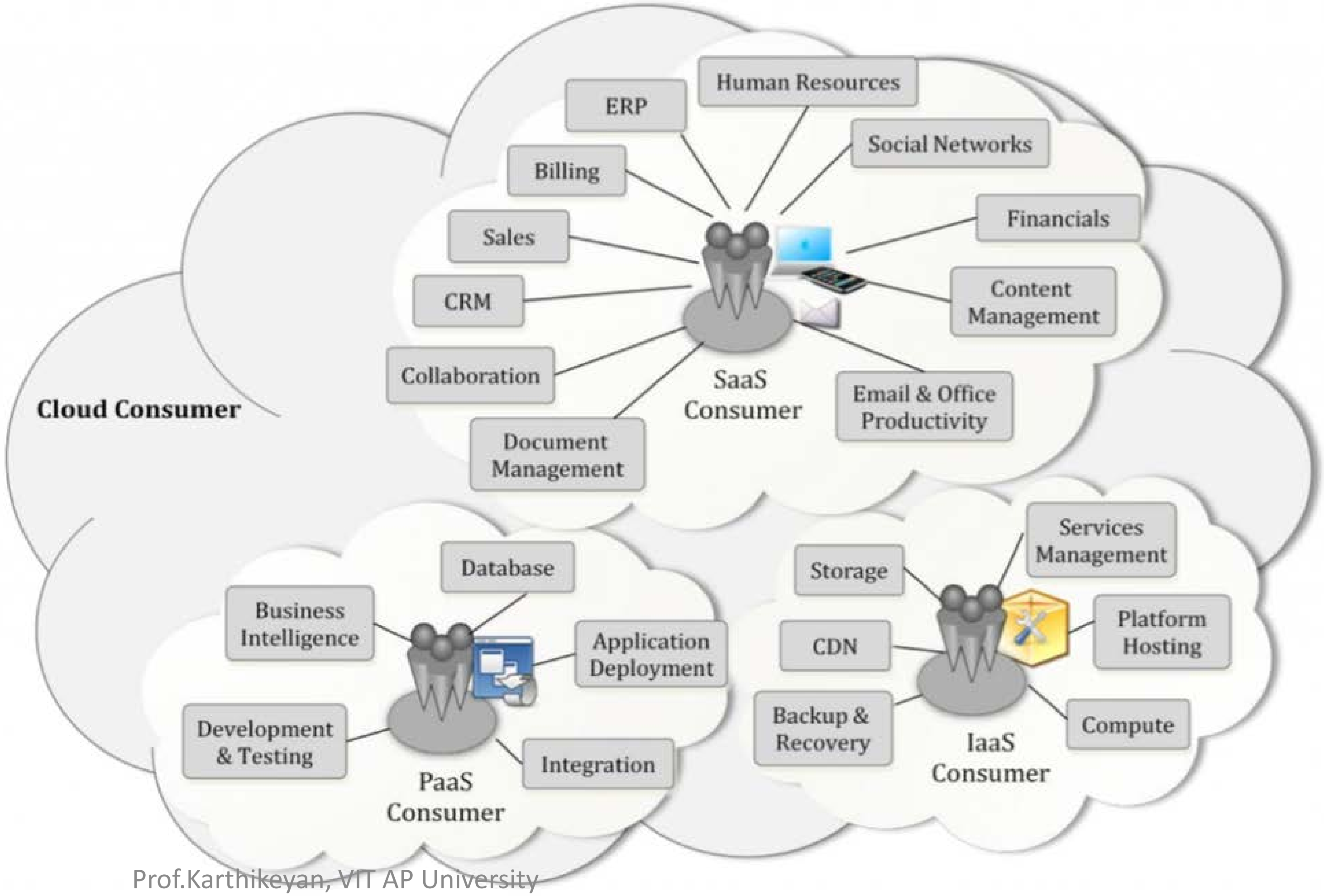
Infrastructure
Servers · Storage · Network

IaaS

Infrastructure
Servers · Storage · Network

Examples of Cloud Services

- Some example cloud services available to a cloud consumer are listed below:



1. Building IaaS Environments

- The virtual server and cloud storage device mechanisms represent the <u>two most fundamental IT resources</u> that are delivered as part of a standard rapid provisioning architecture within IaaS environments.

- They are offered in various standardized configurations that are defined by the following properties:
  - operating system
  - primary memory capacity
  - processing capacity
  - virtualized storage capacity

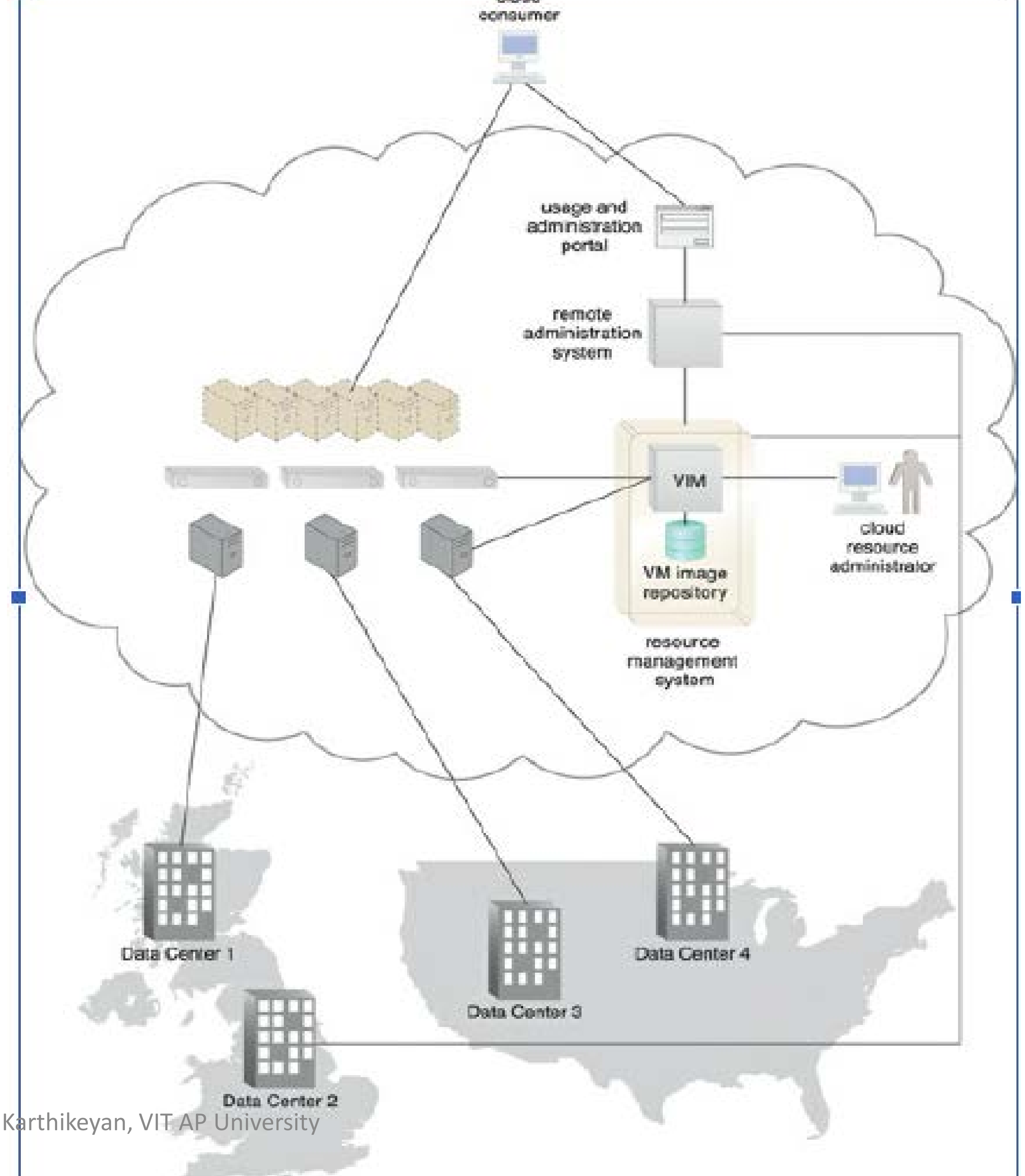
- Memory and virtualized storage capacity is usually allocated with increments of 1 GB to simplify the provisioning of underlying physical IT resources.
- When limiting cloud consumer access to virtualized environments, IaaS offerings are preemptively assembled by cloud providers via virtual server images that capture the pre-defined configurations.
- Some cloud providers may offer cloud consumers direct administrative access to physical IT resources, in which case the bare-metal provisioning architecture may come into play.
- Snapshots can be taken of a virtual server to record its current state, memory, and configuration of a virtualized IaaS environment for backup and replication purposes, in support of horizontal and vertical scaling requirements.
- For example, a virtual server can use its snapshot to become reinitialized in another hosting environment after its capacity has been increased to allow for vertical scaling. The snapshot can alternatively be used to duplicate a virtual server. The management of custom virtual server images is a vital feature that is provided via the remote administration system mechanism. Most cloud providers also support importing and exporting options for custom-built virtual server images in both proprietary and standard formats.

1. Data Centres

Cloud providers can offer IaaS-based IT resources from multiple geographically diverse data centers, which provides the following primary benefits:

- Multiple data centers can be linked together for increased resiliency(free from failure). Each data center is placed in a different location to lower the chances of a single failure forcing all of the data centers to go offline simultaneously.
- Connected through high-speed communications networks with, low latency(less delay) data centers can perform load balancing, IT resource backup and replication, and increase storage capacity, while improving availability and reliability. Having multiple data centers spread over a greater area further reduces network latency.
- Data centers that are deployed in different countries make access to IT resources more convenient for cloud consumers that are constricted by legal and regulatory requirements.

Example of a cloud provider that is managing four data centers that are split between two different geographic regions.


cloud consumer
usage and administration portal
remote administration system
VIM
VM image repository
resource management system
cloud resource administrator
Data Center 1
Data Center 2
Data Center 3
Data Center 4

- When an IaaS environment is used to provide cloud consumers with virtualized network environments, each cloud consumer is segregated into a tenant environment that isolates IT resources from the rest of the cloud through the Internet.
- VLANs and network access control software collaboratively realize the corresponding logical network perimeters.

2. Scalability and Reliability

- Within IaaS environments, cloud providers can automatically provision virtual servers via the dynamic vertical scaling type of the dynamic scalability architecture. This can be performed through the VIM, as long as the host physical servers have sufficient capacity.
- The VIM can scale virtual servers out using resource replication as part of a resource pool architecture, if a given physical server has insufficient capacity to support vertical scaling. The load balancer mechanism, as part of a workload distribution architecture, can be used to distribute the workload among IT resources in a pool to complete the horizontal scaling process.

- Manual scalability requires the cloud consumer to interact with a usage and administration program to explicitly request IT resource scaling.
- In contrast, automatic scalability requires the automated scaling listener to monitor the workload and reactively scale the resource capacity.
- This mechanism typically acts as a monitoring agent that tracks IT resource usage in order to notify the resource management system when capacity has been exceeded.

- Replicated IT resources can be arranged in high-availability configuration that forms a failover system for implementation via standard VIM features.
- Alternatively, a high-availability/high-performance resource cluster can be created at the physical or virtual server level, or both simultaneously. The multipath resource access architecture is commonly employed to enhance reliability via the use of redundant access paths, and some cloud providers further offer the provisioning of dedicated IT resources via the resource reservation architecture.

3. Monitoring

- Cloud usage monitors in an IaaS environment can be implemented using the VIM or specialized monitoring tools that directly comprise and/or interface with the virtualization platform. Several common capabilities of the IaaS platform involve monitoring:
    - Virtual Server Lifecycles – Recording and tracking uptime periods and the allocation of IT resources, for pay-per-use monitors and time-based billing purposes.
    - Data Storage – Tracking and assigning the allocation of storage capacity to cloud storage devices on virtual servers, for pay-per-use monitors that record storage usage for billing purposes.
    - Network Traffic – For pay-per-use monitors that measure inbound and outbound network usage and SLA monitors that track QoS metrics, such as response times and network losses.
    - Failure Conditions – For SLA monitors that track IT resource and QoS metrics to provide warning in times of failure.
    - Event Triggers – For audit monitors that appraise and evaluate the regulatory compliance of select IT resources.
    - Monitoring architectures within IaaS environments typically involve service agents that communicate directly with backend management systems.

4.Security

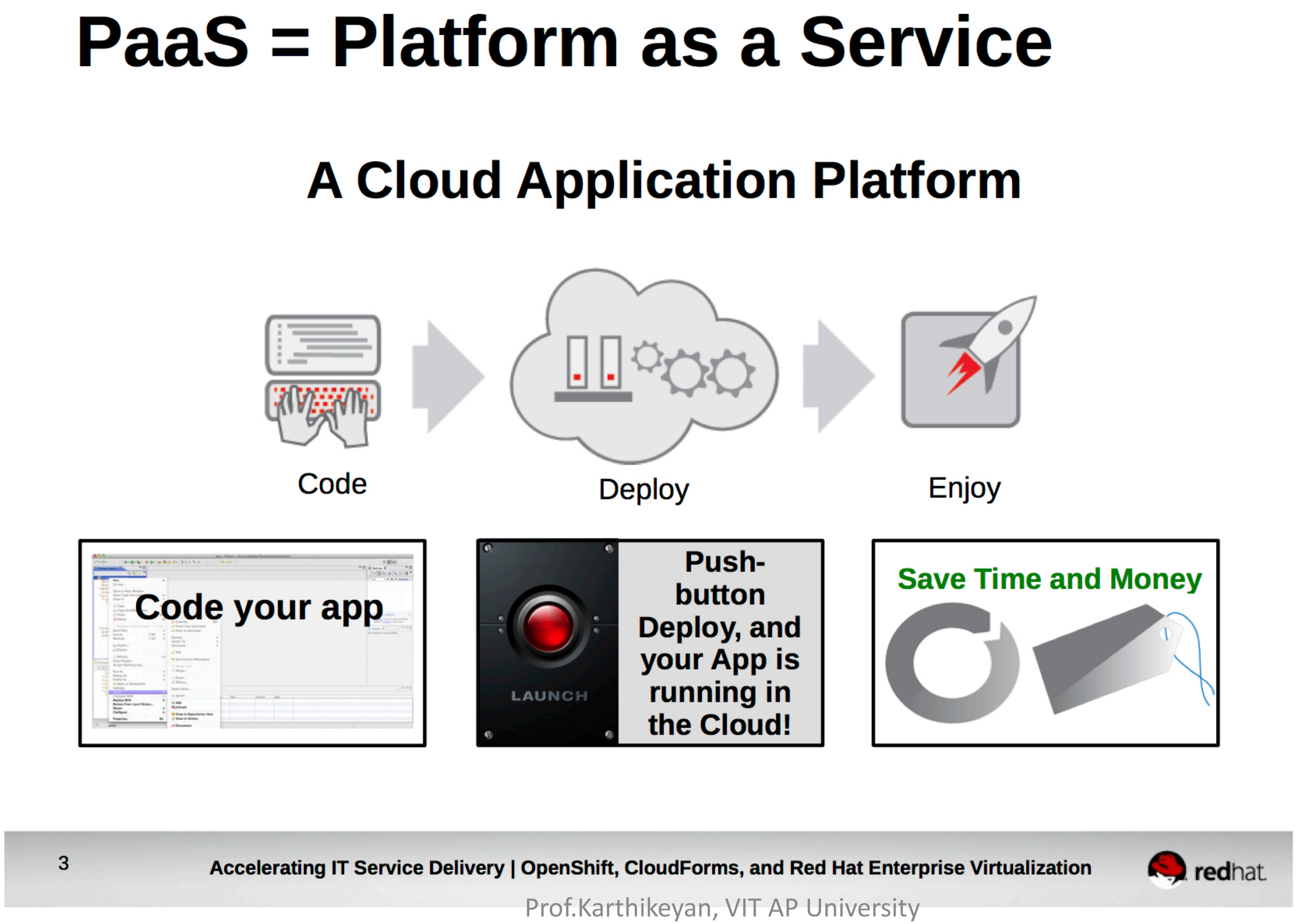
- Cloud security mechanisms that are relevant for securing IaaS environments include:
  - encryption, hashing, digital signature, and PKI mechanisms for overall protection of data transmission.
  - IAM and SSO mechanisms for accessing services and interfaces in security systems that rely on user identification, authentication, and authorization capabilities
  - cloud-based security groups for isolating virtual environments through hypervisors and network segments via network management software
  - hardened virtual server images for internal and externally available virtual server environments
  - various cloud usage monitors to track provisioned virtual IT resources to detect abnormal usage patterns

*IAM-Identify and Access Management , SSO-Single Sign-on

Session 2

Equipping PaaS Environments

2. Equipping PaaS Environments(deploy)



PaaS = Platform as a Service

A Cloud Application Platform

Code → Deploy → Enjoy

Code your app

Push-button Deploy, and your App is running in the Cloud!

Save Time and Money

3 Accelerating IT Service Delivery | OpenShift, CloudForms, and Red Hat Enterprise Virtualization redhat

- PaaS environments typically need to be outfitted with a selection of application development and deployment platforms in order to accommodate different programming models, languages, and frameworks.
- A separate ready-made environment is usually created for each programming stack that contains the necessary software to run applications specifically developed for the platform.
- Each platform is accompanied by a matching SDK and IDE, which can be custom-built or enabled by IDE plugins supplied by the cloud provider. IDE toolkits can simulate the cloud runtime locally within the PaaS environment and usually include executable application servers.
- The security restrictions that are inherent to the runtime are also simulated in the development environment, including checks for unauthorized attempts to access system IT resources.

- Cloud providers often offer a resource management system mechanism that is customized for the PaaS platform so that cloud consumers can create and control customized virtual server images with ready-made environments.
- This mechanism also provides features specific to the PaaS platform, such as managing deployed applications and configuring multitenancy. Cloud providers further rely on a variation of the rapid provisioning architecture known as platform provisioning, which is designed specifically to provision ready-made environments.

1. Scalability and Reliability

- The scalability requirements of cloud services and applications that are deployed within PaaS environments are generally addressed via dynamic scalability and workload distribution architectures that rely on the use of native automated scaling listeners and load balancers.
- The resource pooling architecture is further utilized to provision IT resources from resource pools made available to multiple cloud consumers.
- Cloud providers can evaluate network traffic and server-side connection usage against the instance's workload, when determining how to scale an overloaded application as per parameters and cost limitations provided by the cloud consumer.
- Alternatively, cloud consumers can configure the application designs to customize the incorporation of available mechanisms themselves.

- The reliability of ready-made environments and hosted cloud services and applications can be supported with standard failover system mechanisms (Figure 14.2), as well as the non-disruptive service relocation architecture, so as to shield cloud consumers from failover conditions.
- The resource reservation architecture may also be in place to offer exclusive access to PaaS-based IT resources. As with other IT resources, ready-made environments can also span multiple data centers and geographical regions to further increase availability and resiliency.

reliability of ready-made environments

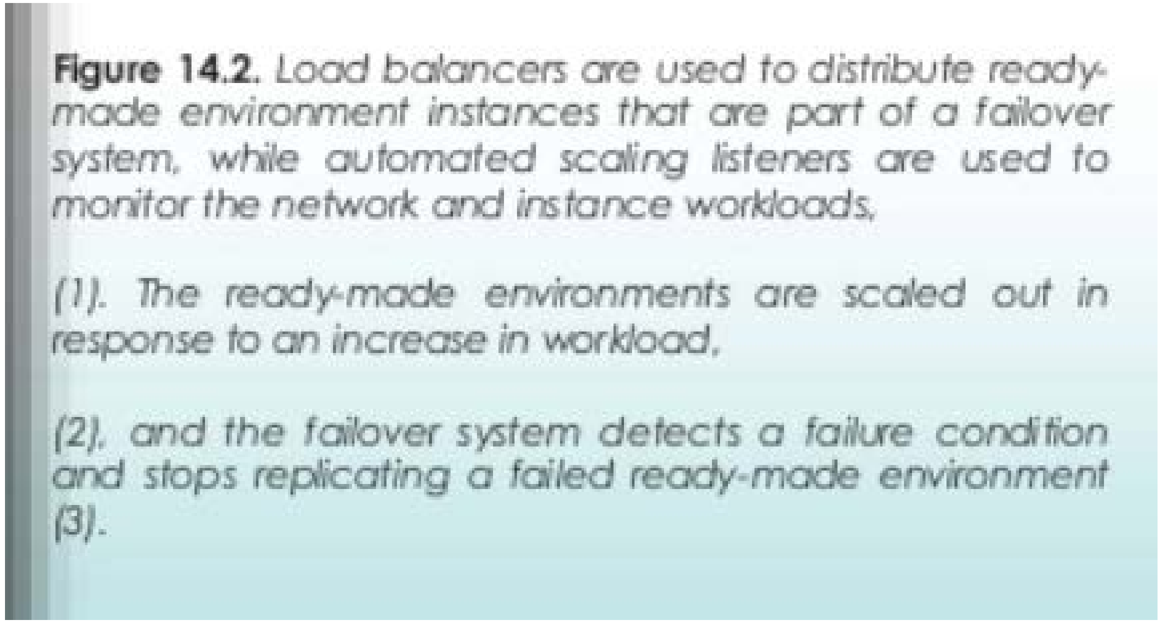
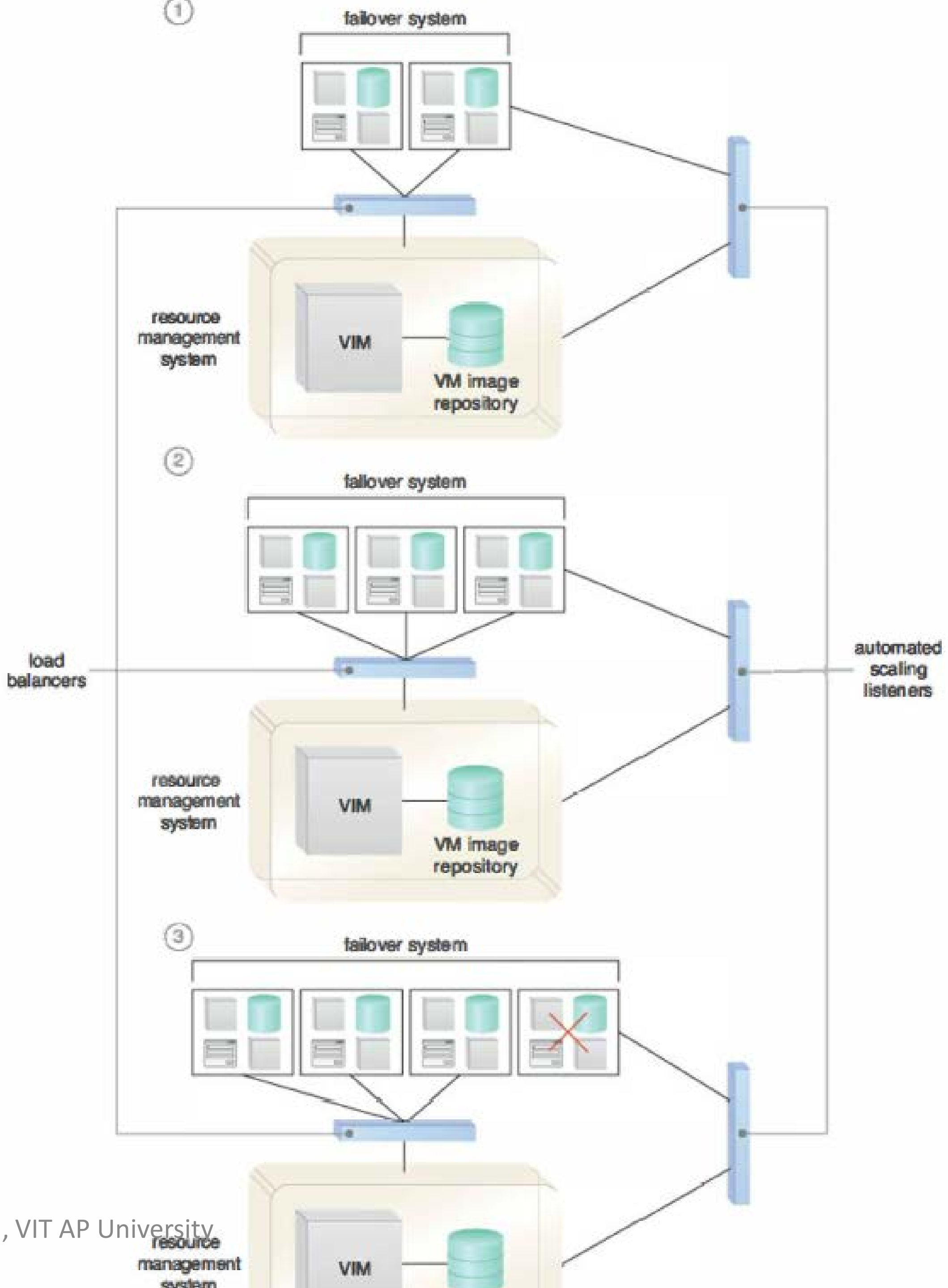


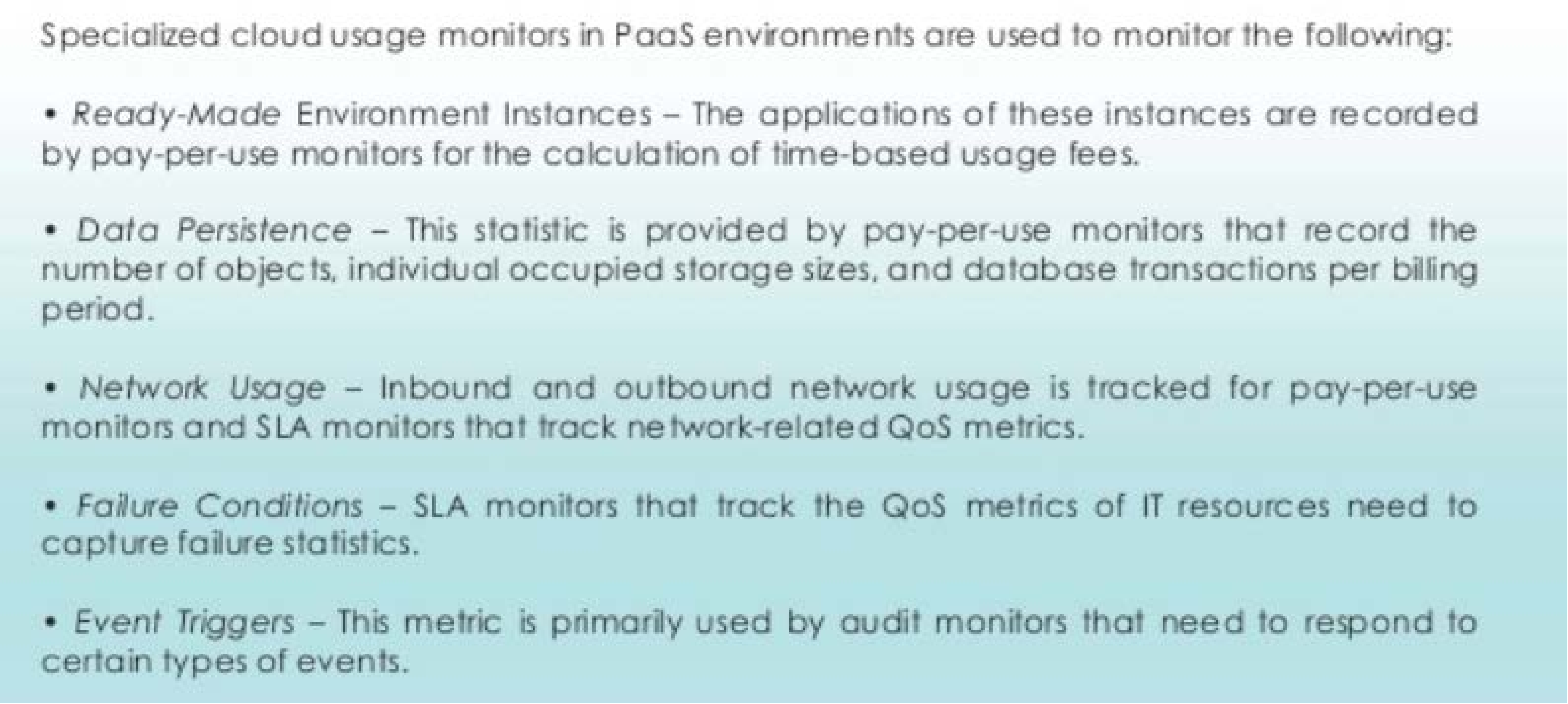
Figure 14.2. *Load balancers are used to distribute ready-made environment instances that are part of a failover system, while automated scaling listeners are used to monitor the network and instance workloads.*

(1). The ready-made environments are scaled out in response to an increase in workload,

(2). and the failover system detects a failure condition and stops replicating a failed ready-made environment (3).



2.Monitoring



Specialized cloud usage monitors in PaaS environments are used to monitor the following:

- *Ready-Made* Environment Instances – The applications of these instances are recorded by pay-per-use monitors for the calculation of time-based usage fees.

- *Data Persistence* – This statistic is provided by pay-per-use monitors that record the number of objects, individual occupied storage sizes, and database transactions per billing period.

- *Network Usage* – Inbound and outbound network usage is tracked for pay-per-use monitors and SLA monitors that track network-related QoS metrics.

- *Failure Conditions* – SLA monitors that track the QoS metrics of IT resources need to capture failure statistics.

- *Event Triggers* – This metric is primarily used by audit monitors that need to respond to certain types of events.

3.Security

- The PaaS environment, by default, does not usually introduce the need for new cloud security mechanisms beyond those that are already provisioned for IaaS environments.

Session 3

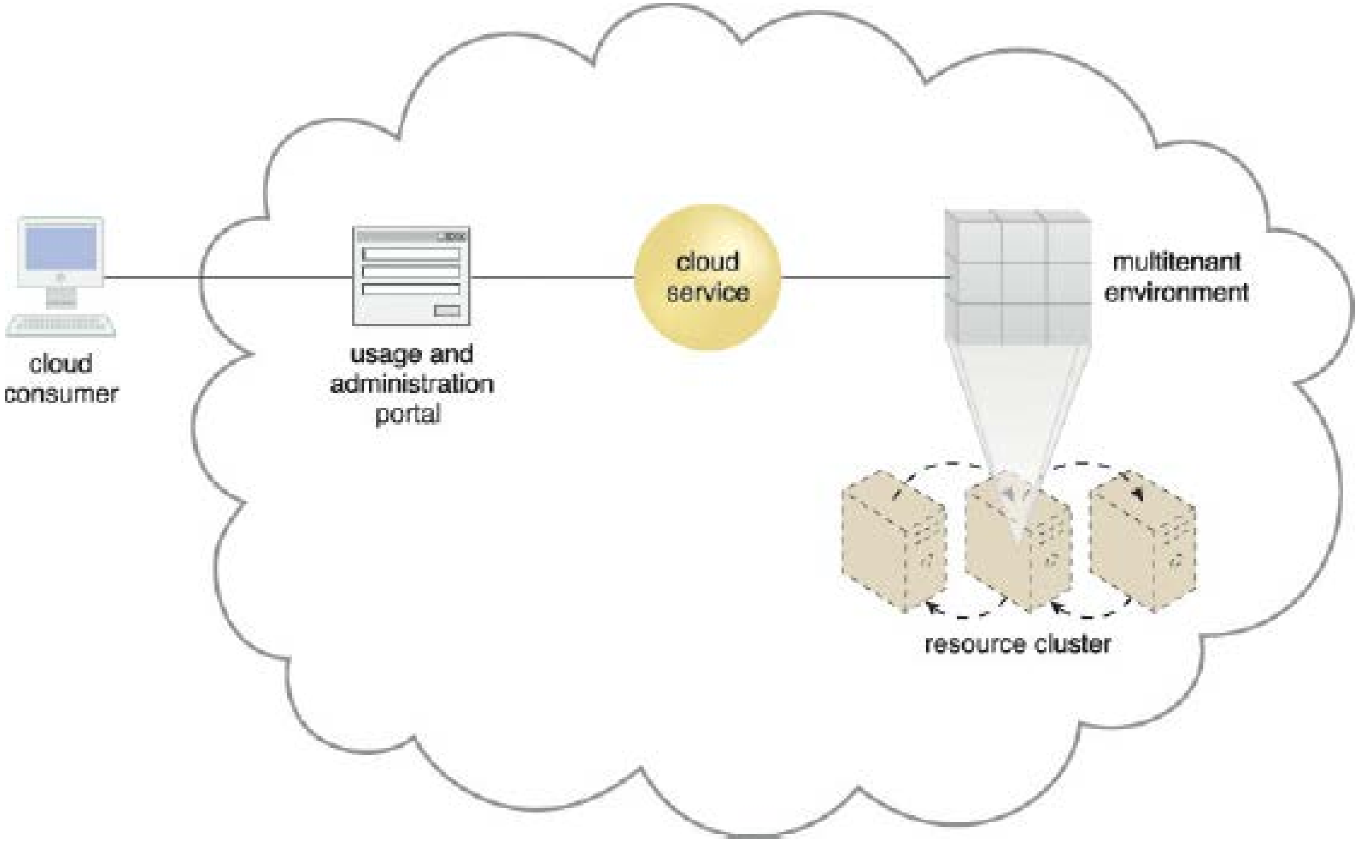
Optimizing SaaS Environments

- In SaaS implementations, cloud service architectures are generally based on multitenant environments that enable and regulate concurrent cloud consumer access (Figure 14.3).

- SaaS IT resource segregation does not typically occur at the infrastructure level in SaaS environments, as it does in IaaS and PaaS environments.

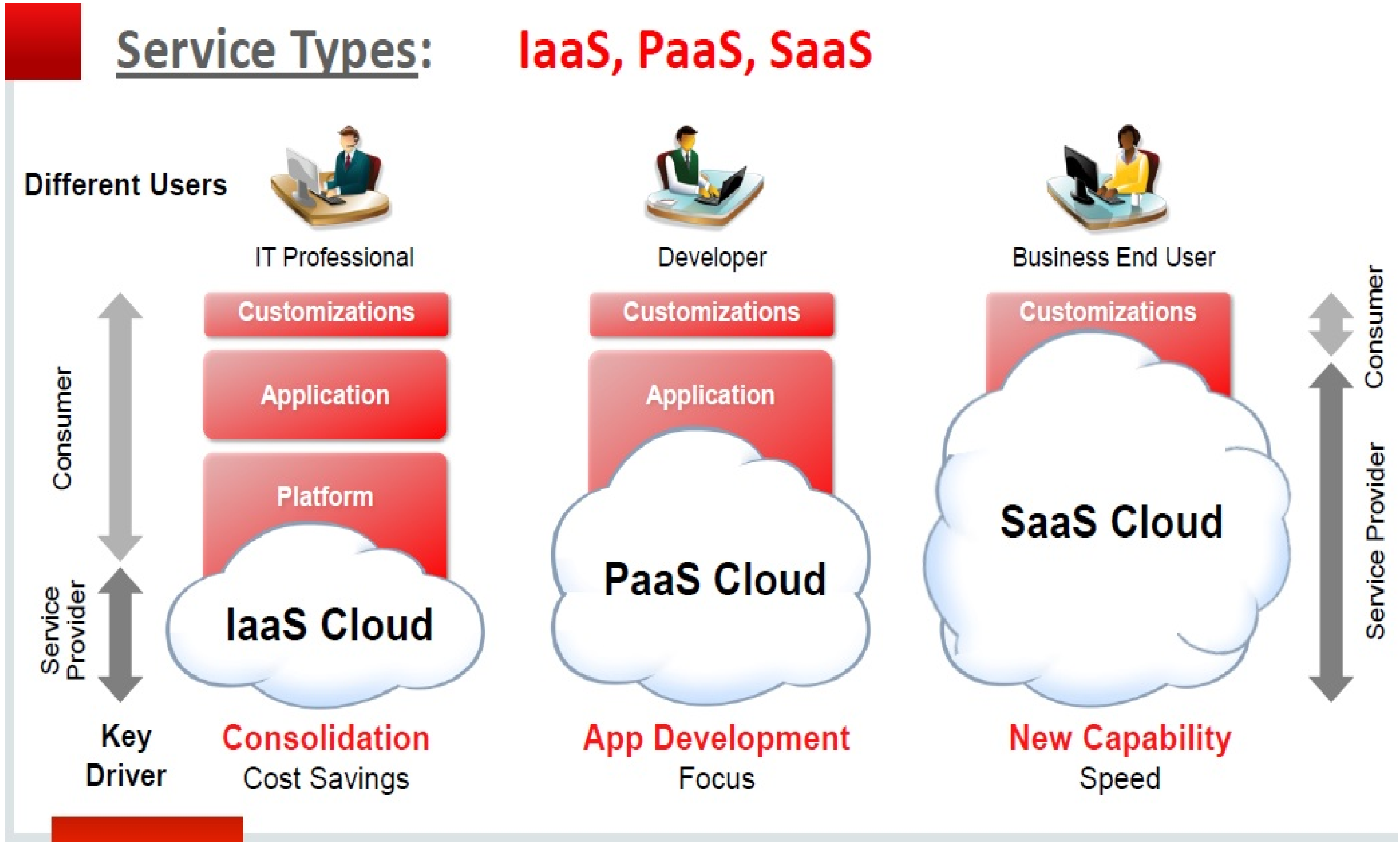
Figure 14.3 The SaaS-based cloud service is hosted by a multitenant environment deployed in a high-performance virtual server cluster.

A usage and administration portal is used by the cloud consumer to access and configure the cloud service.



- SaaS implementations rely heavily on the features provided by the native dynamic scalability and workload distribution architectures, as well as non-disruptive service relocation to ensure that failover conditions do not impact the availability of SaaS-based cloud services.

- However, it is vital to acknowledge that, unlike the relatively vanilla designs of IaaS and PaaS products, each SaaS deployment will bring with it unique architectural, functional, and runtime requirements. These requirements are specific to the nature of the business logic the SaaS-based cloud service is programmed with, as well as the distinct usage patterns it is subjected to by its cloud service consumers.



For example, consider the diversity in functionality and usage of the following recognized online SaaS offerings:

- collaborative authoring and information-sharing (Wikipedia, Blogger)
- collaborative management (Zimbra, Google Apps)
- conferencing services for instant messaging, audio/video communications (Skype, Google Talk)
- enterprise management systems (ERP, CRM, CM)
- file-sharing and content distribution (YouTube, Dropbox)
- industry-specific software (engineering, bioinformatics)
- messaging systems (e-mail, voicemail)
- mobile application marketplaces (Android Play Store, Apple App Store)
- office productivity software suites (Microsoft Office, Adobe Creative Cloud)
- search engines (Google, Yahoo)
- social networking media (Twitter, LinkedIn)

- Now consider that many of the previously listed cloud services are offered in one or more of the following implementation mediums:

    - Mobile application
    - REST service
    - Web service

- Each of these SaaS implementation mediums provide Web-based APIs for interfacing by cloud consumers.
- Examples of online SaaS-based cloud services with Web-based APIs include:
  - Electronic payment services (PayPal)
  - Mapping and routing services (Google Maps)
  - Publishing tools (WordPress)

- The potentially diverse nature of SaaS functionality, the variation in implementation technology, and the tendency to offer a SaaS-based cloud service redundantly with multiple different implementation mediums makes the design of SaaS environments highly specialized. Though not essential to a SaaS implementation, specialized processing requirements can prompt the need to incorporate architectural models, such as:

  - Service Load Balancing – for workload distribution across redundant SaaS-based cloud service implementations
  - Dynamic Failure Detection and Recovery – to establish a system that can automatically resolve some failure conditions without disruption in service to the SaaS implementation
  - Storage Maintenance Window – to allow for planned maintenance outages that do not impact SaaS implementation availability
  - Elastic Resource Capacity/Elastic Network Capacity – to establish inherent elasticity within the SaaS-based cloud service architecture that enables it to automatically accommodate a range of runtime scalability requirements
  - Cloud Balancing – to instill broad resiliency within the SaaS implementation, which can be especially important for cloud services subjected to extreme concurrent usage volumes

Specialized cloud usage monitors can be used in SaaS environments to track the following types of metrics:

- Tenant Subscription Period – This metric is used by pay-per-use monitors to record and track application usage for time-based billing. This type of monitoring usually incorporates application licensing and regular assessments of leasing periods that extend beyond the hourly periods of IaaS and PaaS environments.
- Application Usage – This metric, based on user or security groups, is used with pay-per-use monitors to record and track application usage for billing purposes.
- Tenant Application Functional Module – This metric is used by pay-per-use monitors for function-based billing. Cloud services can have different functionality tiers according to whether the cloud consumer is free-tier or a paid subscriber.

3. Security

- SaaS implementations generally rely on a foundation of security controls inherent to their deployment environment. Distinct business processing logic will then add layers of additional cloud security mechanisms or specialized security technologies.

Thank You!

Next Class

Cloud Delivery Models: The Cloud Consumer Perspective