Lecture	Asst. Prof. Dr. Thanachai T.	Assoc. Prof. Dr. Piyabute F.
Sections	541 (Tuesday, 9:00 – 12:00) 542 (Tuesday, 13:30 – 16:40)	543 (Thursday, 9:00 – 12:00) 544 (Thursday, 13:30 – 16:40)
Email	thanachaithm@au.edu	piyabutefng@msme.au.edu
Office	VMES0407	SCIT403

- Course Description
  - Cloud computing concepts and capabilities, cloud service models; IaaS, PaaS and SaaS, cloud containers, virtualization technologies, infrastructure migration approaches, cloud security and protection mechanisms, cloud resource management and monitoring capabilities, current trends and research in cloud computing
- Course materials:
  - Thomas Erl , Ricardo Puttini and Zaigham Mahmood , ***Cloud Computing: Concepts, Technology & Architecture***, The Prentice Hall Service Technology Series, ISBN-13: 978-0133387520
  - Christ Dotson, ***Practical Cloud Security A Guide for Secure Design and Deployment,*** O Reilly Media, ISBN-13 : 978-1492037514
  - AWS Academy

Course Outline

Week	Topics	Hours	Outcomes
1	Overview of computer networks: OSI, LAN, MAN, and WAN. Introduction to cloud computing and service models.	3.0	To understand an overview of computer networks. To understand basic cloud principles
2	Introduction to cloud computing and service models (cont.) Underlying cloud technologies.	3.0	To understand primary technology components that enable contemporary cloud computing.
3	Underlying cloud technologies (cont.) Overview of cloud security fundamentals.	3.0	Basic cloud security concepts: CIA, threats, attacks, vulnerabilities.
4	Cloud infrastructure mechanisms. Cloud computing mechanisms. AWS Lab 1	3.0	To understand the foundational building blocks of cloud environments.
5	Cloud computing mechanisms (cont.). AWS Lab 2	3.0	To understand the foundational building blocks of cloud environments.

Week	Topics	Hours	Outcomes
6	Cloud management mechanisms. AWS Lab 3	3.0	To understand remote administrator system, resource, and SLA management system, and billing management system.
7.	System reliability	3.0	To understand system reliability and availability
	Midterm Examination		
8.	Cloud delivery models, cost metrics, and pricing models. Cloud SLA.	3.0	To understand how to build IaaS, equip IaaS, and optimize IaaS. To understand business cost metrics and cost management.
9.	Fundamental cloud architecture AWS Lab 4	3.0	To understand workload distribution architecture, resource pooling architecture, dynamic scalability architecture, and other relevant architectures

Week	Topics	Hours	Outcomes
10.	Advance cloud architecture AWS Lab 5	3.0	To understand load-balanced virtual server instances architecture, non-disruptive service relocation architecture, zero downtime architecture, and other relevant architectures
11.	Specialized cloud architecture AWS Lab 6	3.0	To understand direct LUN access architecture, dynamic data normalization architecture, elastic network capacity architecture, and other relevant architectures
12.	Practical cloud security (1)	3.0	To understand concepts of least privilege, defense in depth, threats, cloud shared responsibility model, and risk management. To understand data asset management and to protect data in the cloud. To understand cloud assets and asset management.
13.	Practical cloud security (2)	3.0	To understand what to watch, how to watch, prepare for incidents, respond to incidents, and recover from incidents.
14.	**Review**		

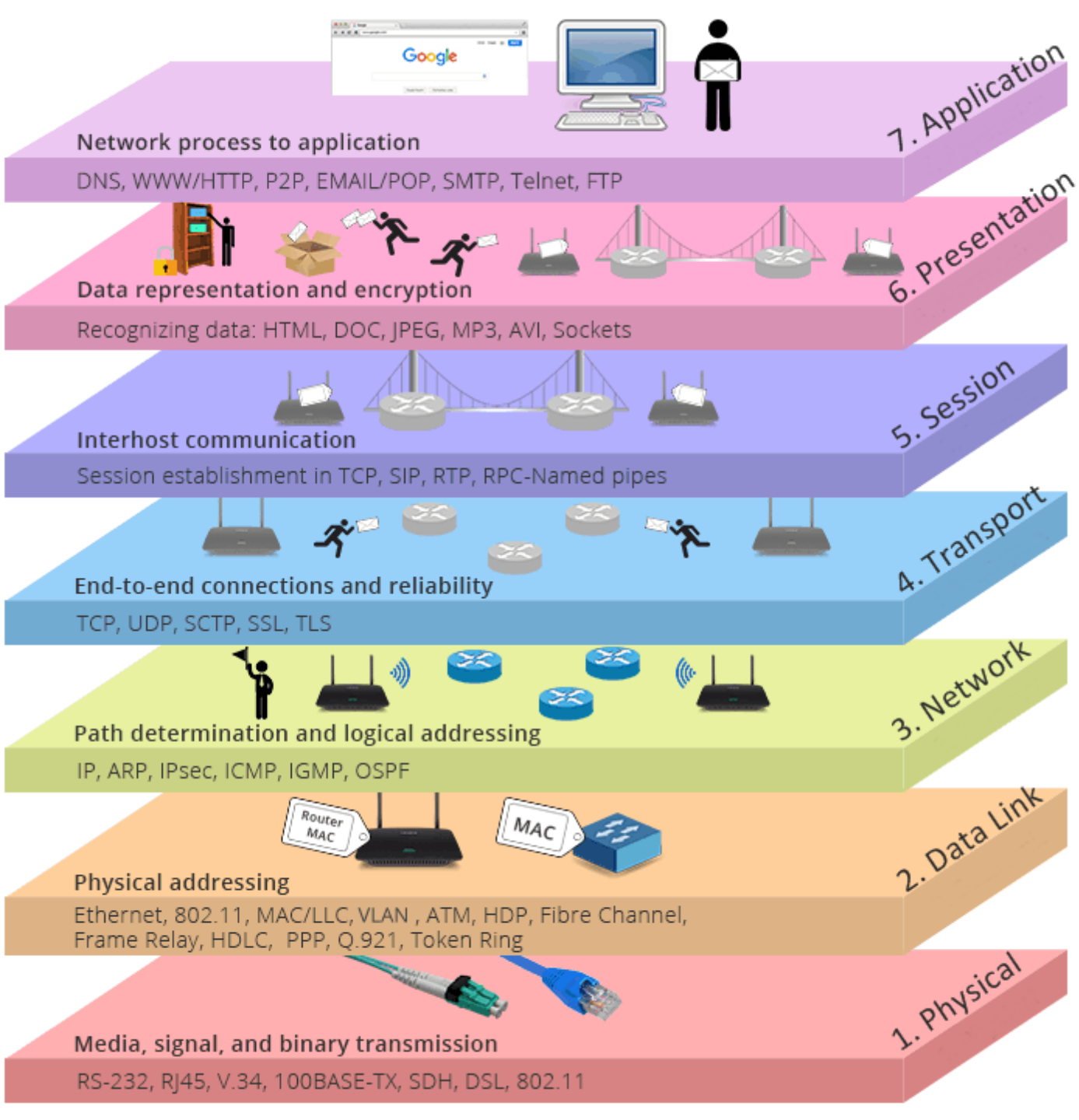
Course Evaluation

Assessment Topics	Score
Classwork, AWS Labs	20
Midterm	40
Final	40

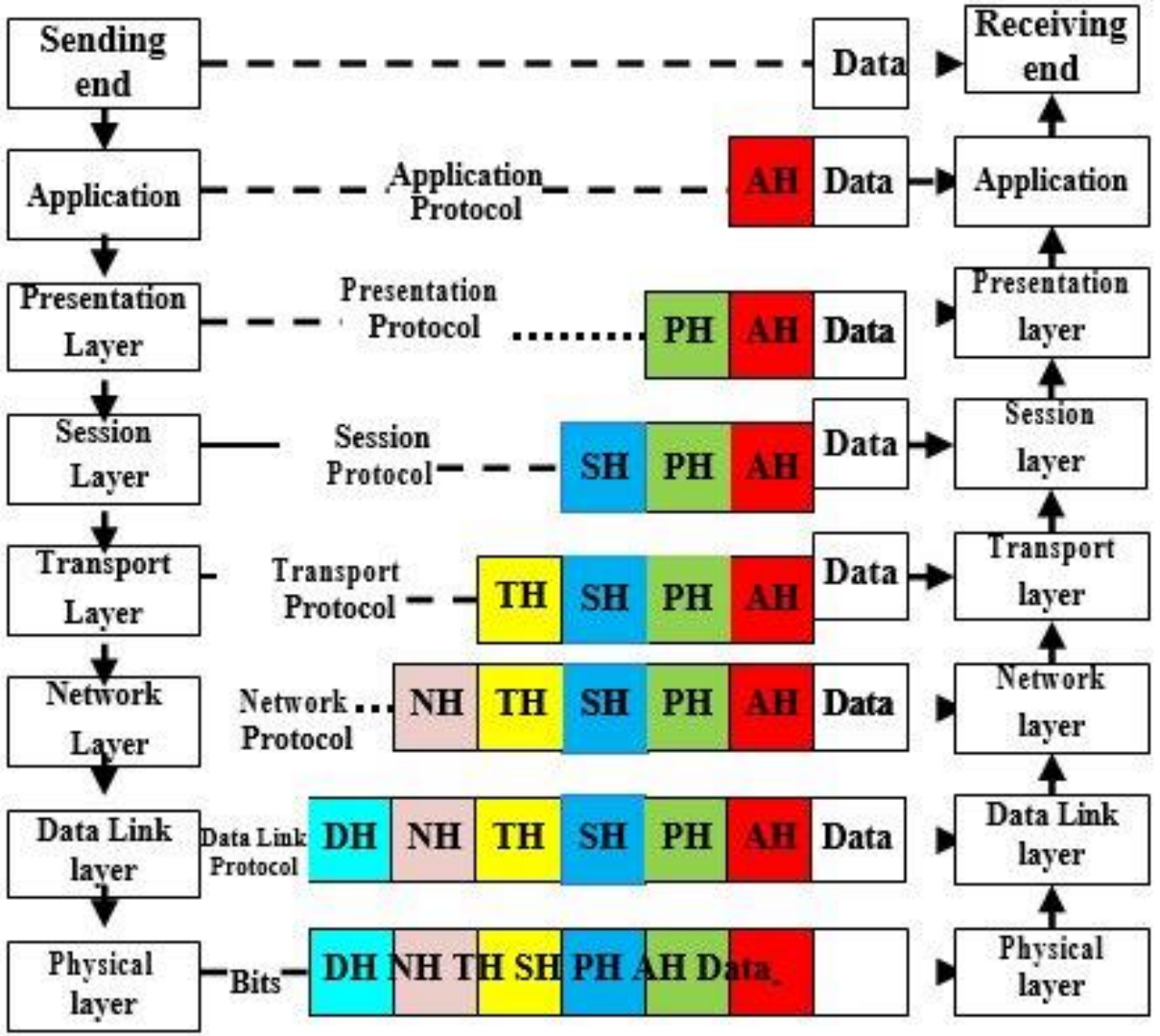
Overview of Computer Networks
OSI, LAN, MAN, WAN

OSI 7 Layers

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium


Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
Router MAC
MAC
2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VLAN , ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

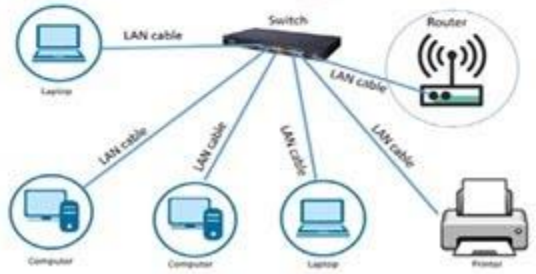
OSI 7-layer network architecture



Comparison Between LAN, MAN & WAN

LAN

- o Local Area Network
- o Small Area Covered
- o Ownership Private
- o Easy to Design & Maintain
- o Low setup cost
- o High data transfer rate
- o More Secure
- o Range up to 1km
- o Short Propagation Delay
- o More Fault Tolerance
- o Less Congestion

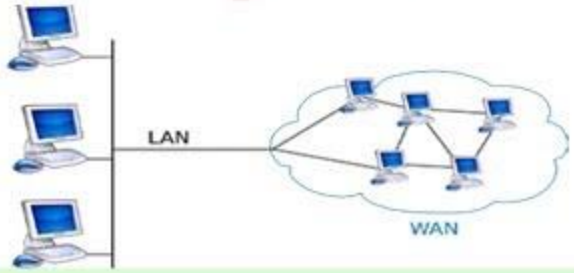


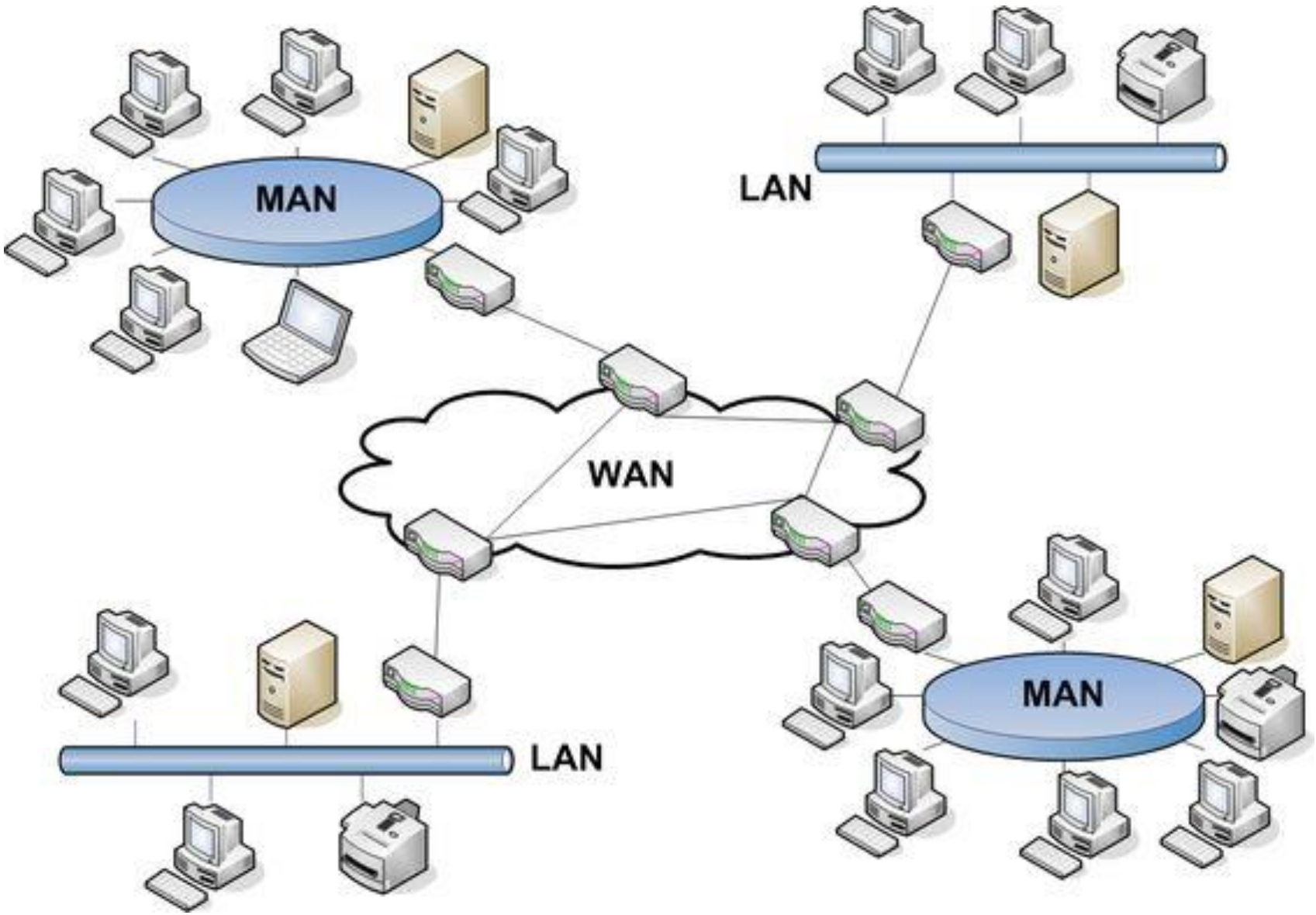
MAN

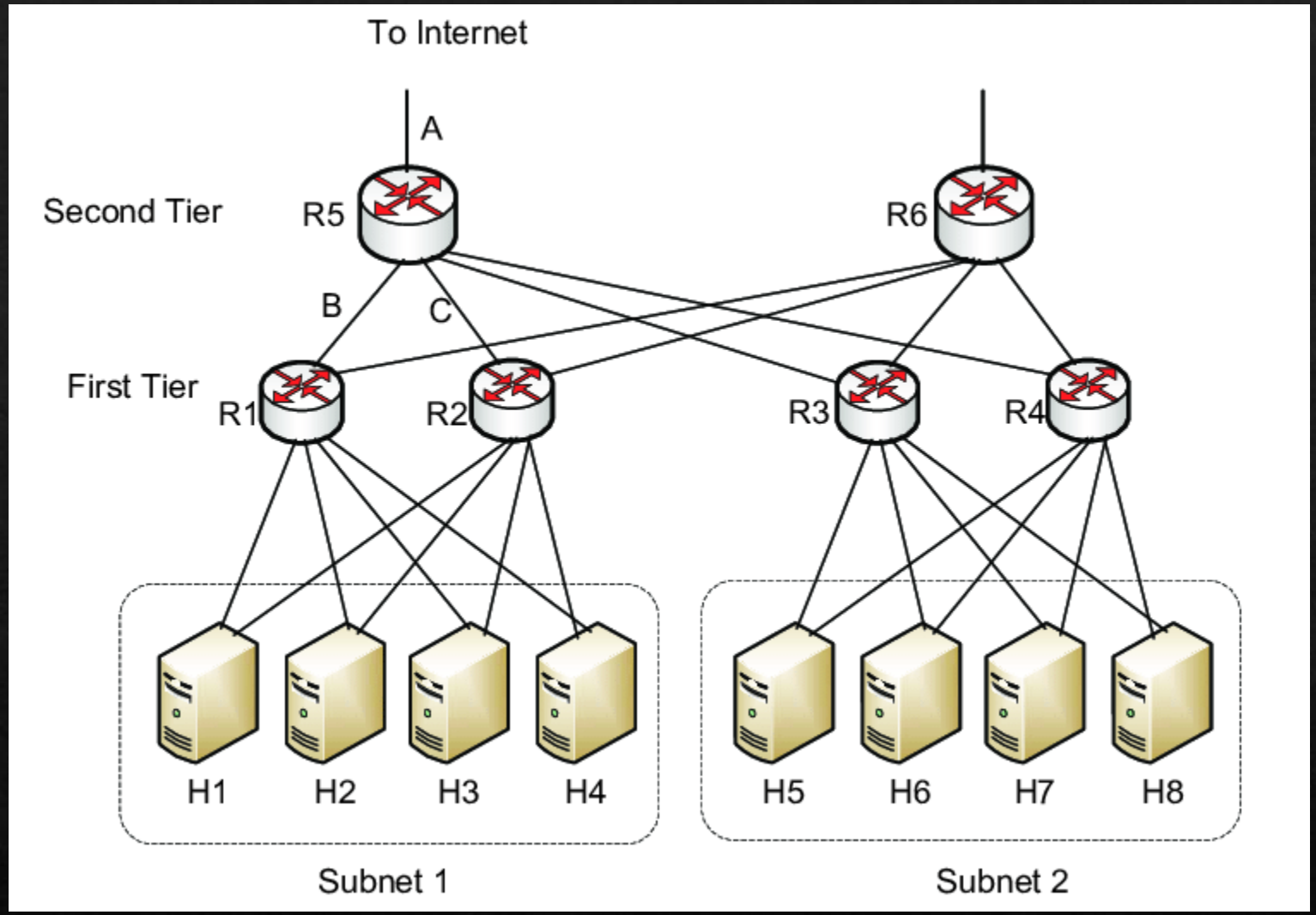
- o Metropolitan Area Network
- o Large Area Covered
- o Ownership Private & Public
- o Difficult to Design & Maintain
- o Moderate setup cost
- o Medium data transfer rate
- o Less Secure
- o Range up to 100 km
- o Moderate Propagation Delay
- o Less Fault Tolerance
- o More Congestion

WAN

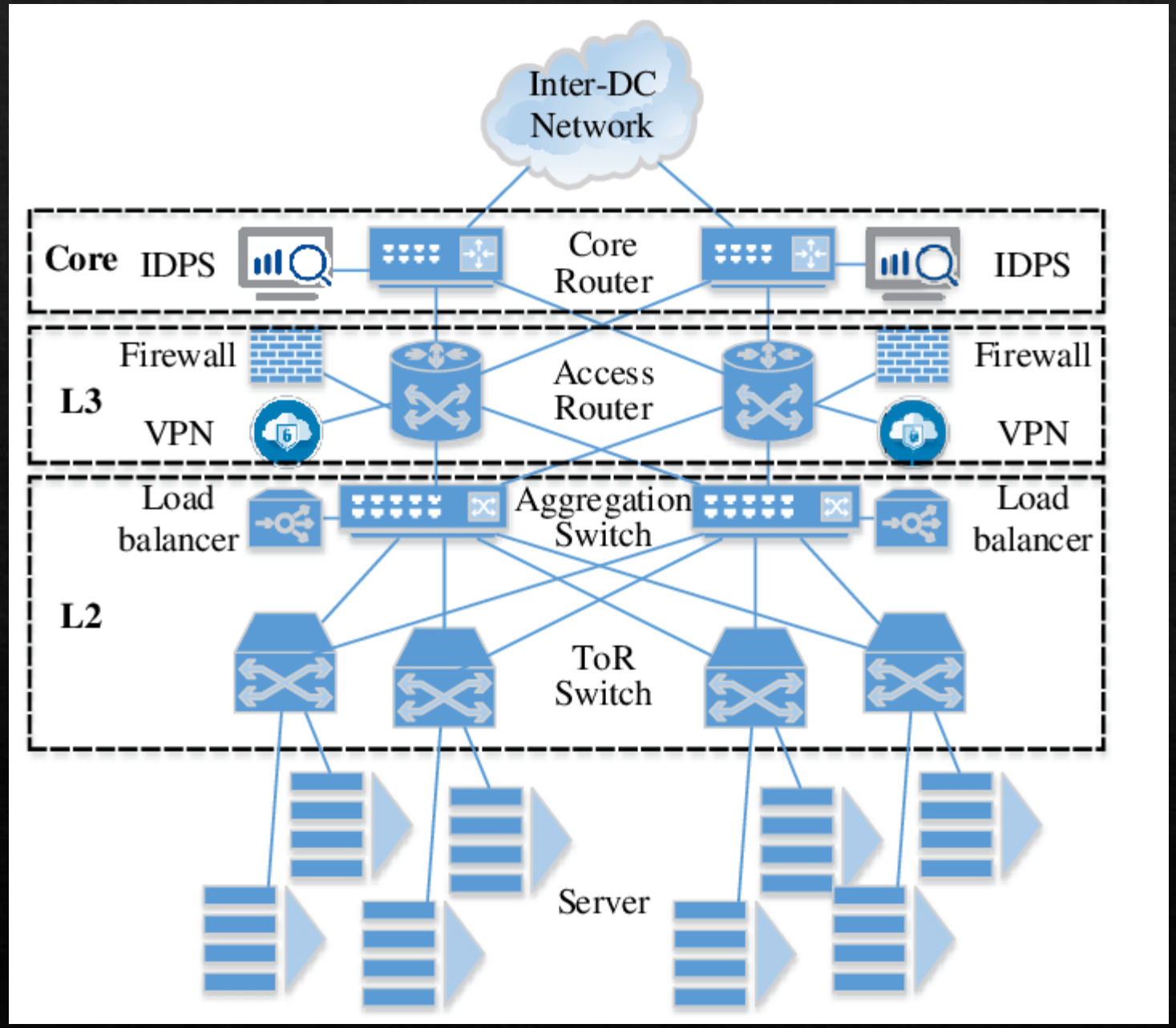
- o Wide Area Network
- o Large Area Covered
- o Ownership Private & Public
- o Difficult to Design & Maintain
- o High setup cost
- o Low data transfer rate
- o Less Secure
- o Range up to 100000km
- o Long Propagation Delay
- o Less Fault Tolerance
- o More Congestion




MAN
LAN
WAN
LAN
MAN



- Loads of servers
- Underutilization
- Not scalable


Inter-DC
Network
Core
IDPS
Core
Router
IDPS
Firewall
L3
Access
Router
Firewall
VPN
VPN
Load
balancer
Aggregation
Switch
Load
balancer
L2
ToR
Switch
Server

Introduction to Cloud Computing

What is cloud computing?

- A model for enable ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., network servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing defined

Cloud computing is the **on-demand** delivery of compute power, database, storage, applications, and other IT resources **via the internet** with **pay-as-you-go** pricing.

Infrastructure as software

Cloud computing enables you to **stop thinking of your infrastructure as hardware**, and instead **think of (and use) it as software.**

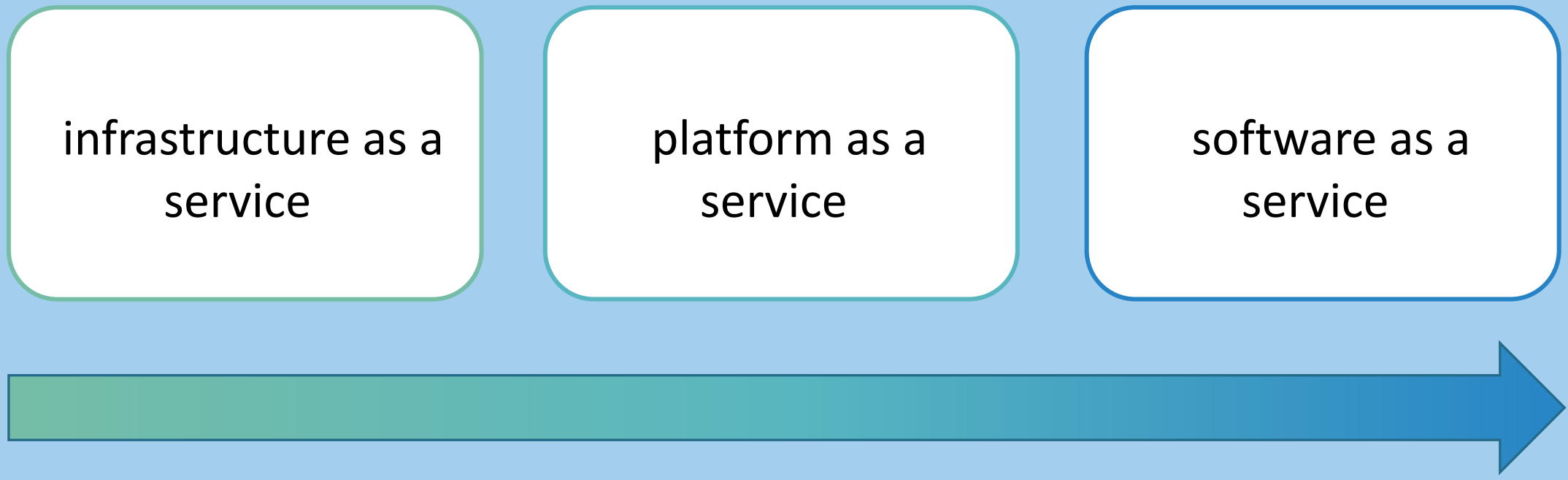
Traditional computing model

- Infrastructure as hardware
- Hardware solutions:
  - Require space, staff, physical security, planning, capital expenditure
  - Have a long hardware procurement cycle
  - Require you to provision capacity by guessing theoretical maximum peaks

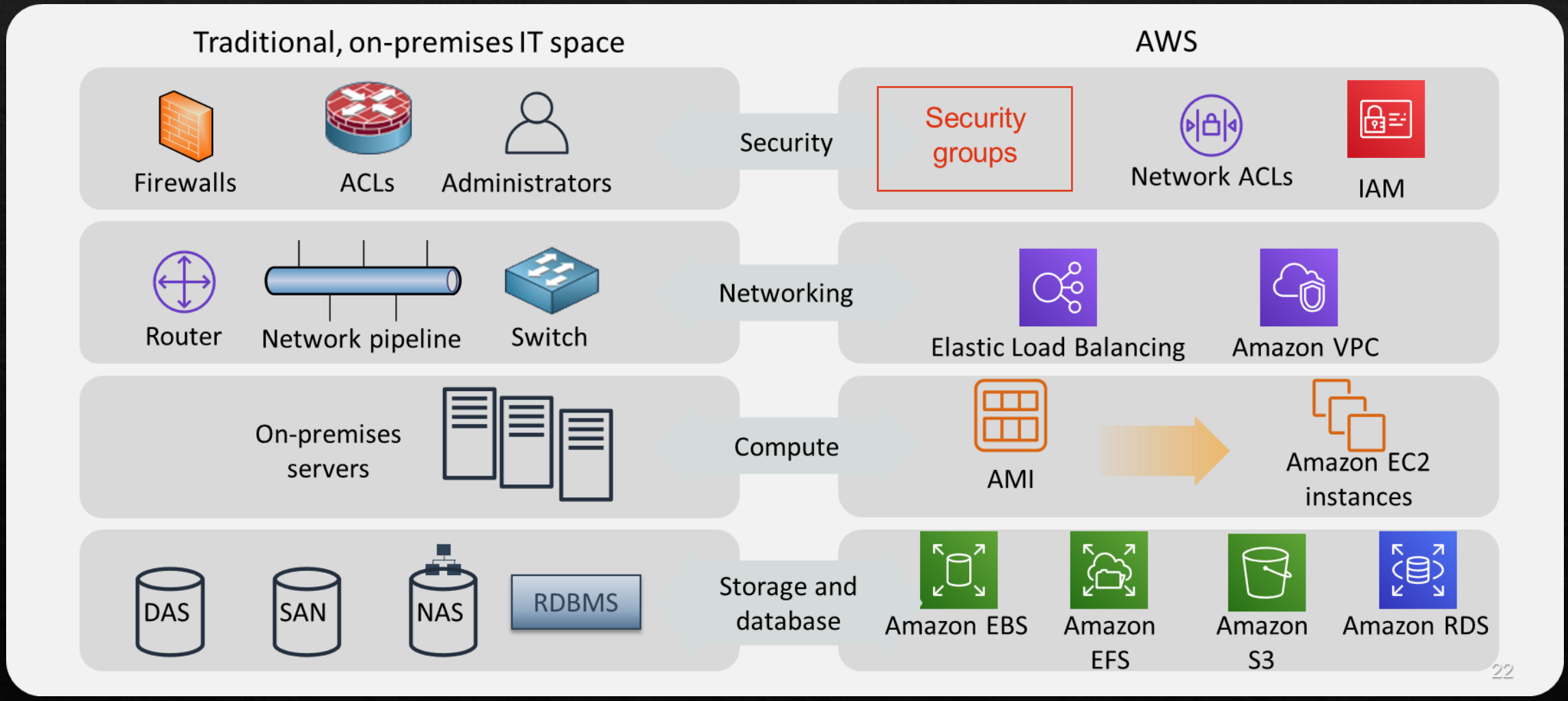
Cloud computing model

- Infrastructure as software
- Software solutions:
  - Are flexible
  - Can change more quickly, easily, and cost-effectively than hardware solutions
  - Eliminate the undifferentiated heavy-lifting tasks

Cloud service models



Similarities between AWS and traditional IT



Key Benefits

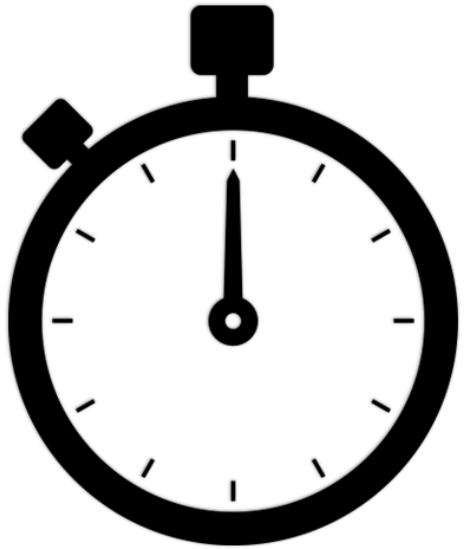
- Cloud computing is the on-demand delivery of IT resources via the internet with pay-as-you-go pricing.
- Cloud computing enables you to think of (and use) your infrastructure as software.
- There are three cloud service models: IaaS, PaaS, and SaaS.
- There are three cloud deployment models: cloud, hybrid, and on-premises or private cloud.
- Almost anything you can implement with traditional IT can also be implemented as an AWS cloud computing service.

Origin and Influences

- Envisioned as computing utilities for all (like water or electricity utilities)
- Business drivers:
  - Capacity planning - the process of determining and fulfilling future demands of an organization’s IT resources, products, and services.
    - Lead strategy
    - Lag strategy
    - Match strategy
  - Cost reduction – infrastructure-related operating overhead includes
    - Technical personnel, upgrades/patches cost, security and access control measures, administrative/account staffs → on-going ownership of technology.
  - Organizational agility - ability to adapt and evolve to successfully fast change caused by both internal and external factors.

Trade capital expense for variable expense

Data center investment based on forecast



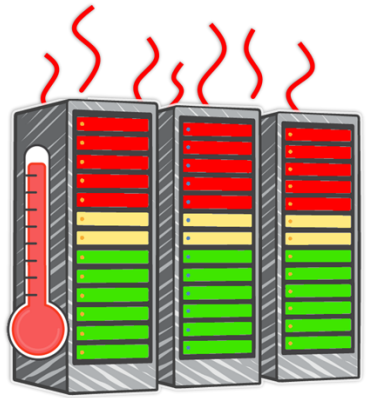
Pay only for the amount you consume

Massive economies of scale

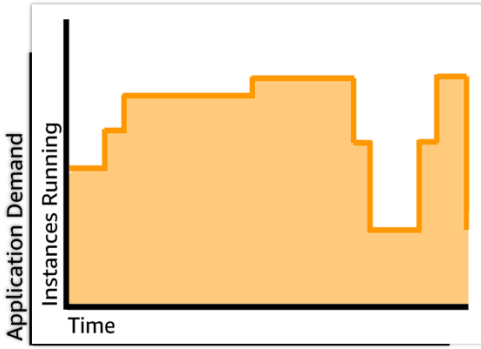
Because of aggregate usage from all customers, AWS can achieve higher economies of scale and pass savings on to customers.

Stop guessing capacity

Overestimated server capacity



Underestimated server capacity



Scaling on demand

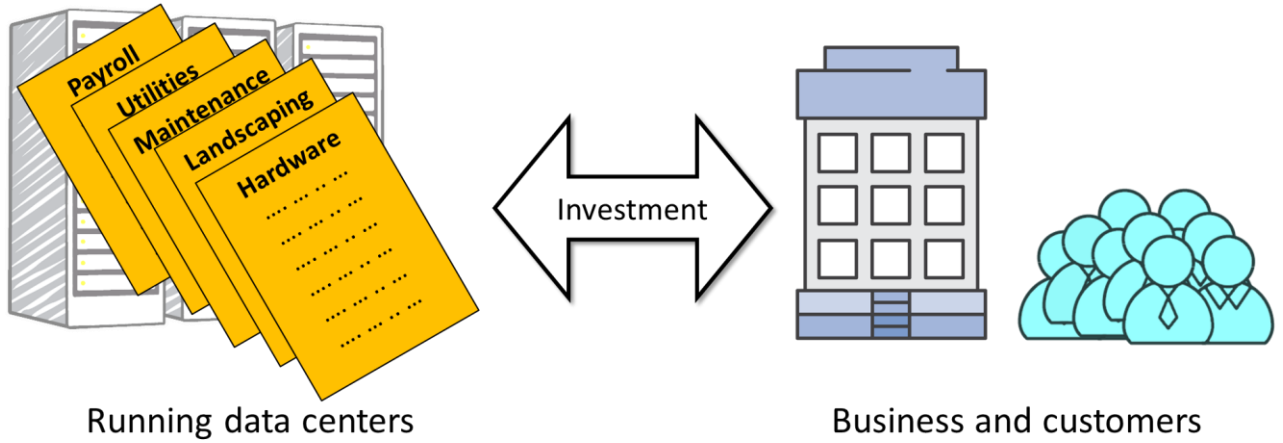
Increase speed and agility

Weeks between wanting resources and having resources

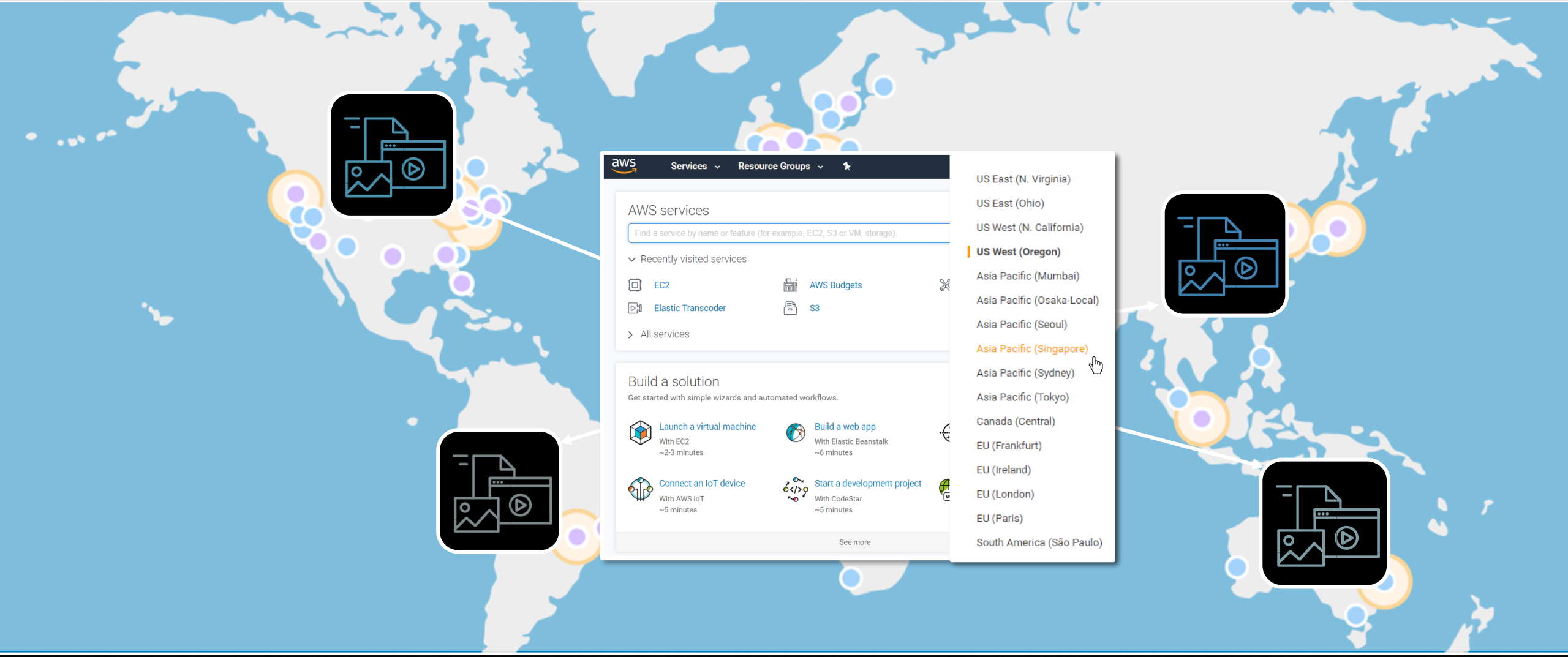
Weeks between wanting resources and having resources

Minutes between wanting resources and having resources

Stop spending money on running and maintaining data centers

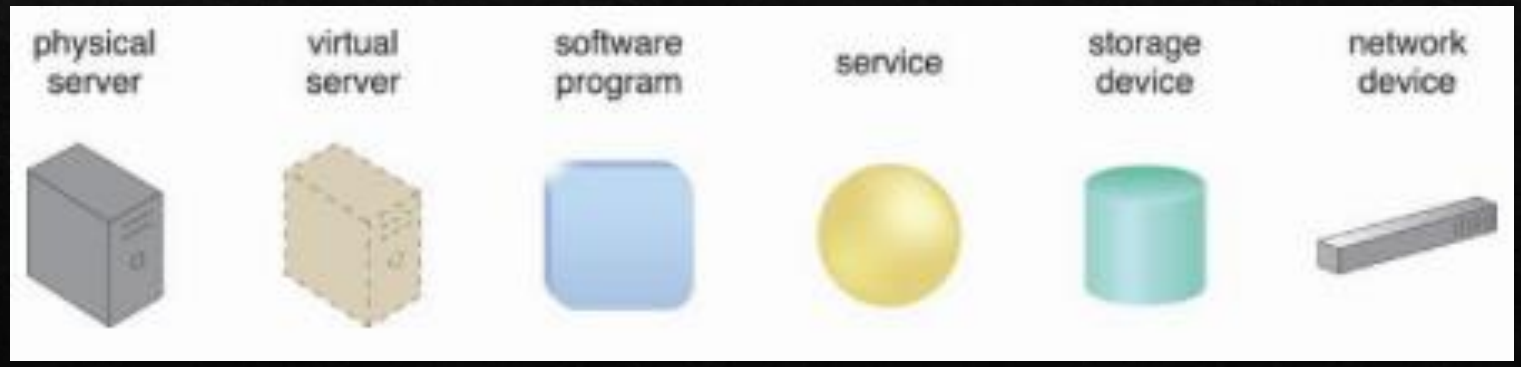


Go global in minutes



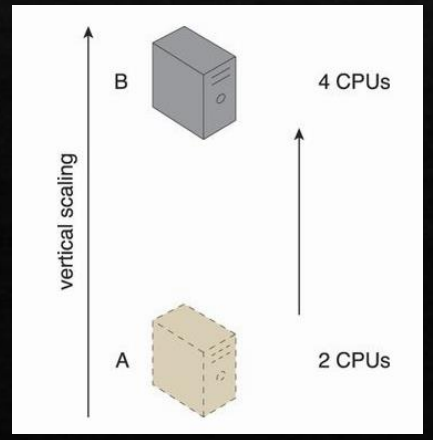
Basic Terminology

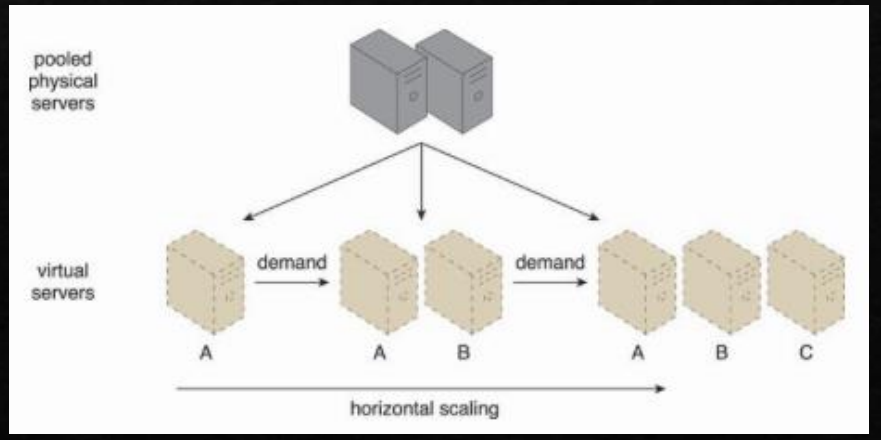
- Cloud - a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measured IT resources.
- IT resources - a physical or virtual IT-related artifact that can be either software-based, such as a virtual server or a custom software program, or hardware-based, such as a physical server or a network device.

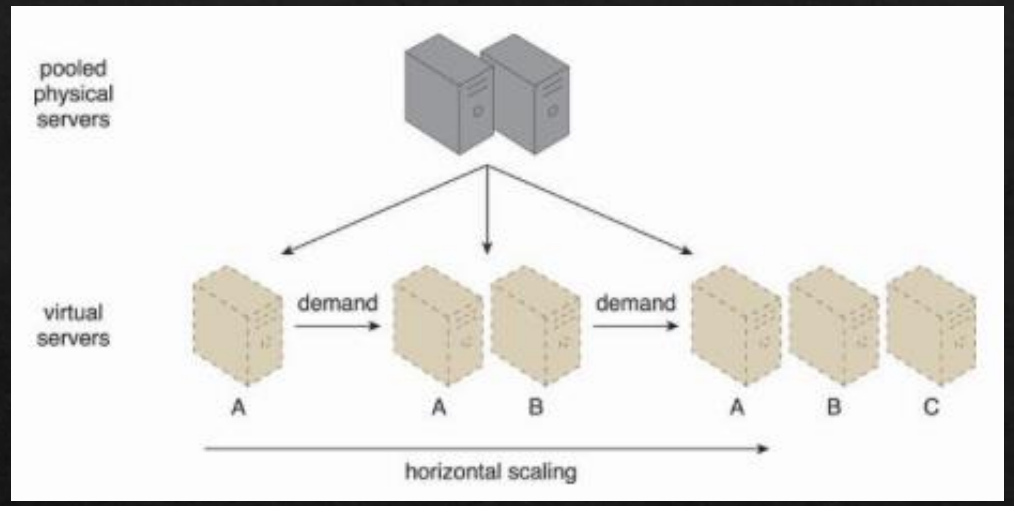


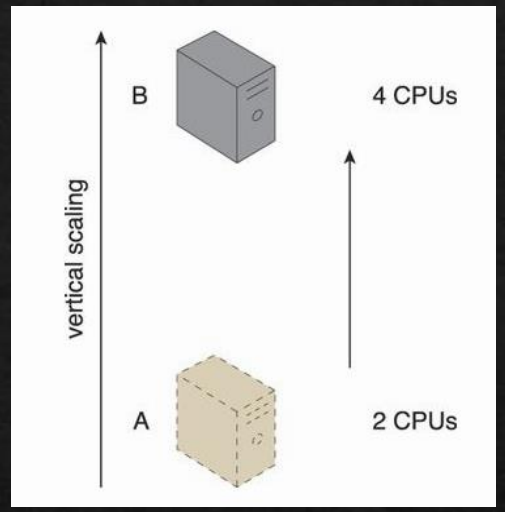
Basic Terminology (2)

- On-premise - an IT resource that is hosted in a conventional IT enterprise within an organizational boundary.
- Cloud consumers/providers
- Scaling - the ability of the IT resource to handle increased or decreased usage demands.
  - Horizontal – scaling out and in
  - Vertical – scaling up and down





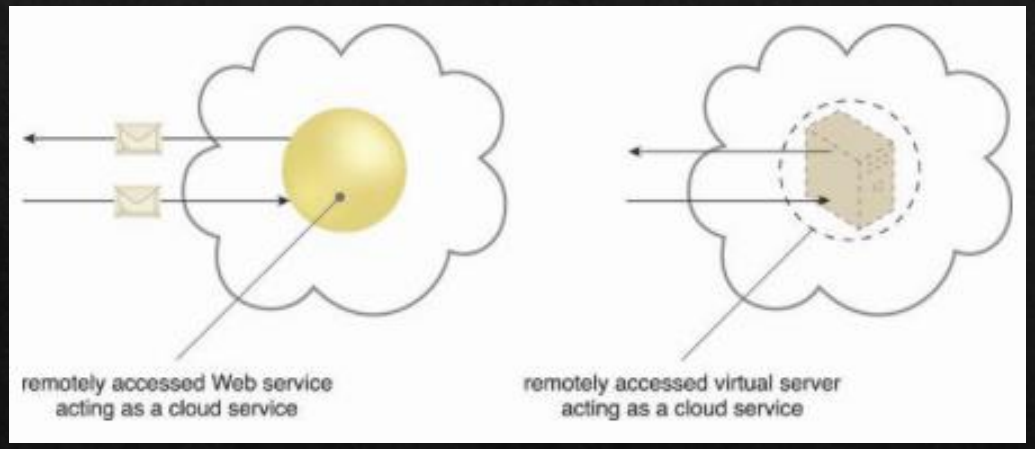




Horizontal Scaling	Vertical Scaling
less expensive (through commodity hardware components)	more expensive (specialized servers)
IT resources instantly available	IT resources normally instantly available
resource replication and automated scaling	additional setup is normally needed
additional IT resources needed	no additional IT resources needed
not limited by hardware capacity	limited by maximum hardware capacity

Basic Terminology (3)

- Cloud service - any IT resource that is made remotely accessible via a cloud.



- Cloud service consumer - a temporary runtime role assumed by a software program when it accesses a cloud service.

Benefits

Reduced investments and proportional costs

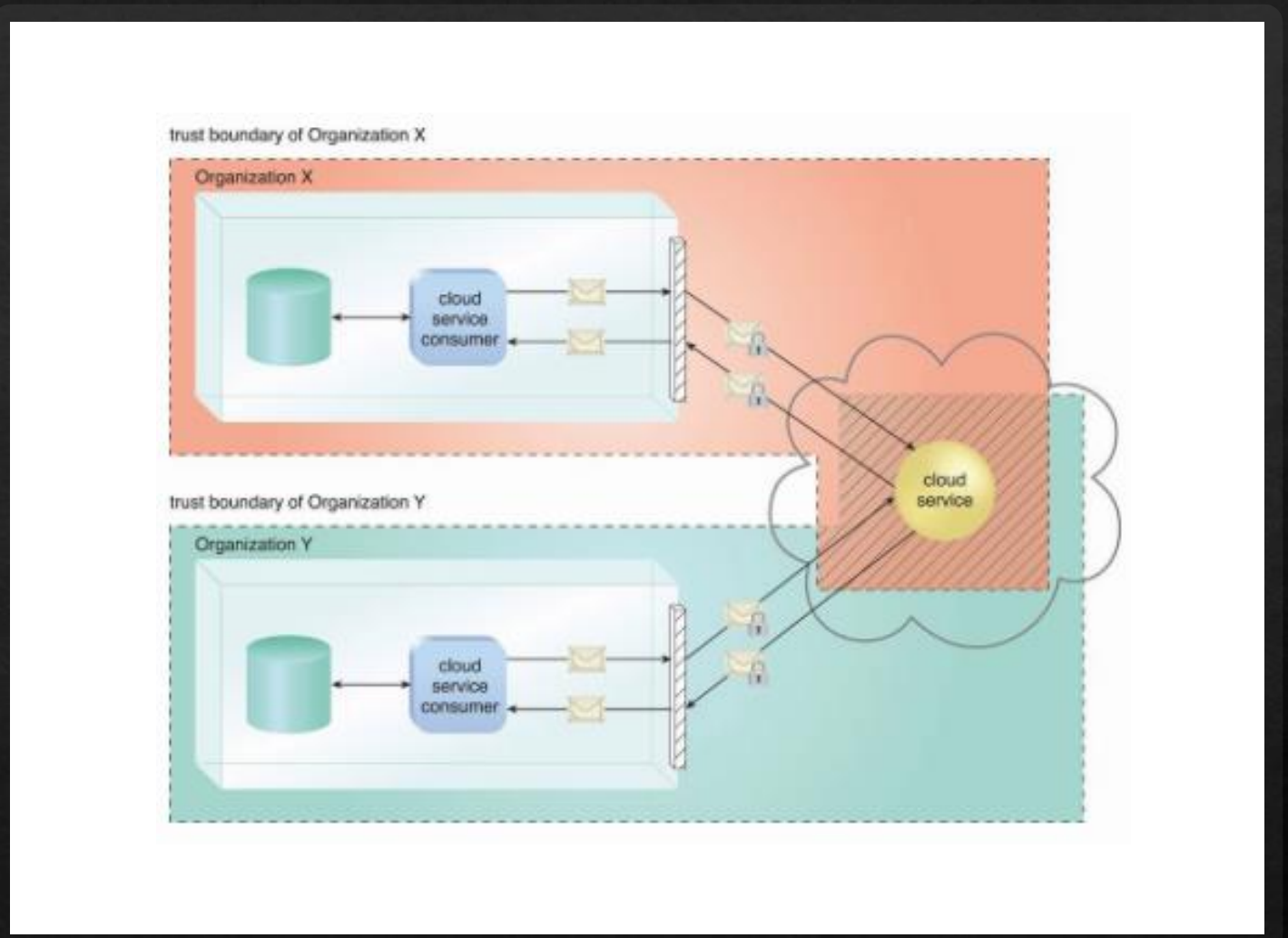
On demand access to pay-as-you-go
The perception of having unlimited computing resources
Ability to add/remove IT resources
Abstract of IT infrastructure

Increased scalability

Increased availability and reliability

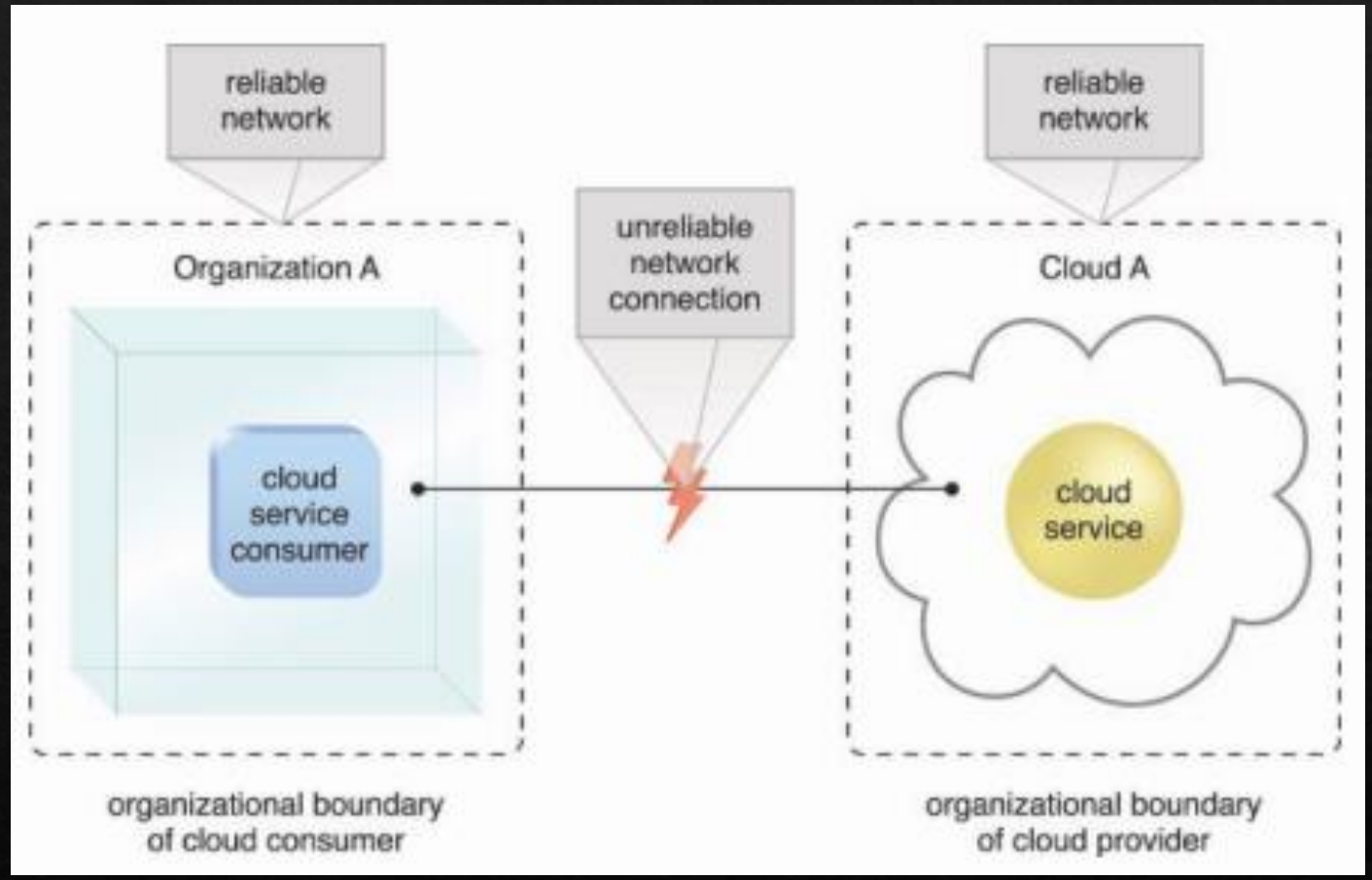
Risks and Challenges

- Increased security vulnerabilities



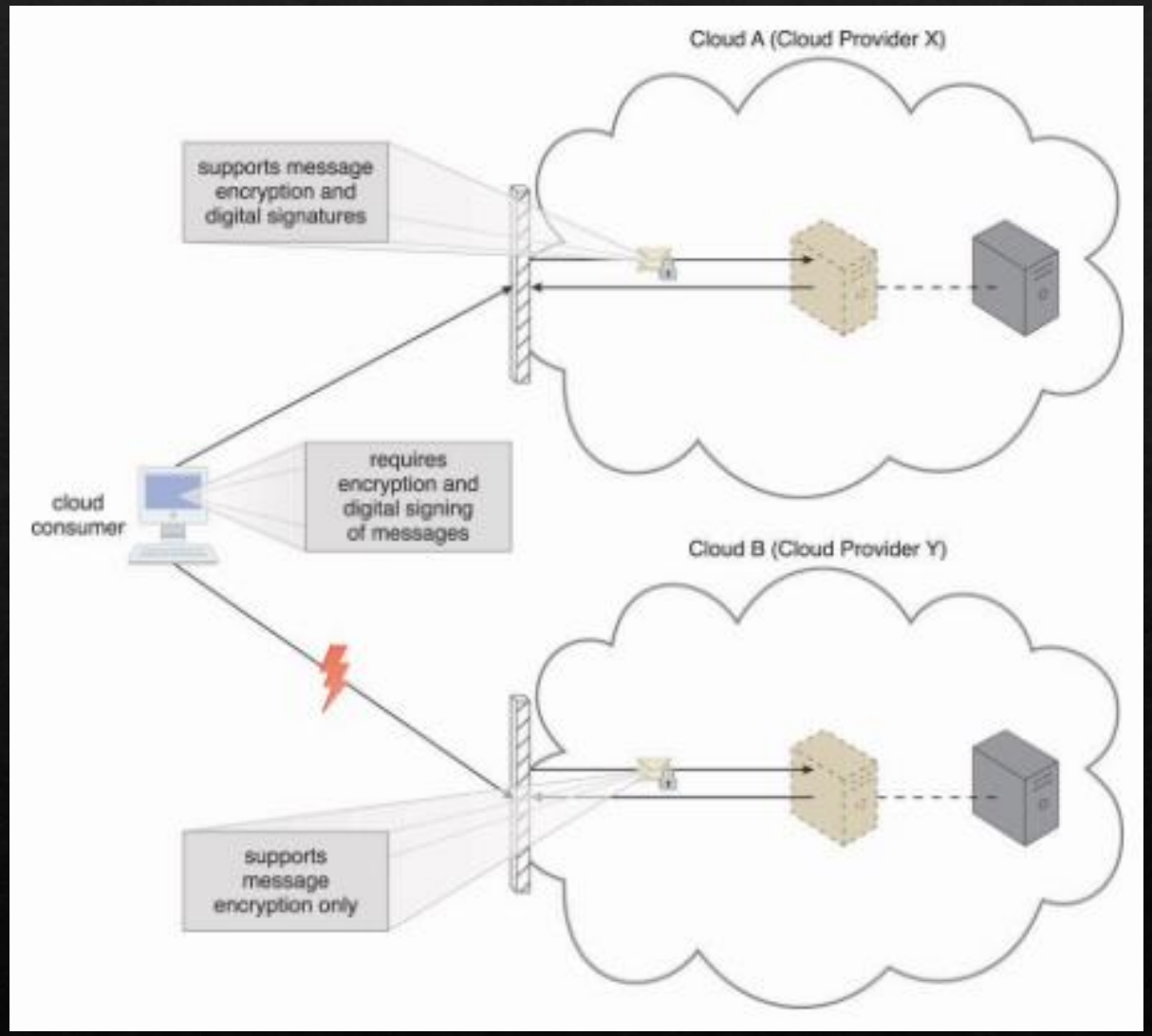
Risks and Challenges (2)

- Reduced Operational Governance Control
  - An unreliable cloud provider may not maintain the guarantees it makes in the SLAs.
  - Longer geographic distances between the cloud consumer and cloud provider can require additional network hops that introduce fluctuating latency and potential bandwidth constraints.



Risks and Challenges (3)

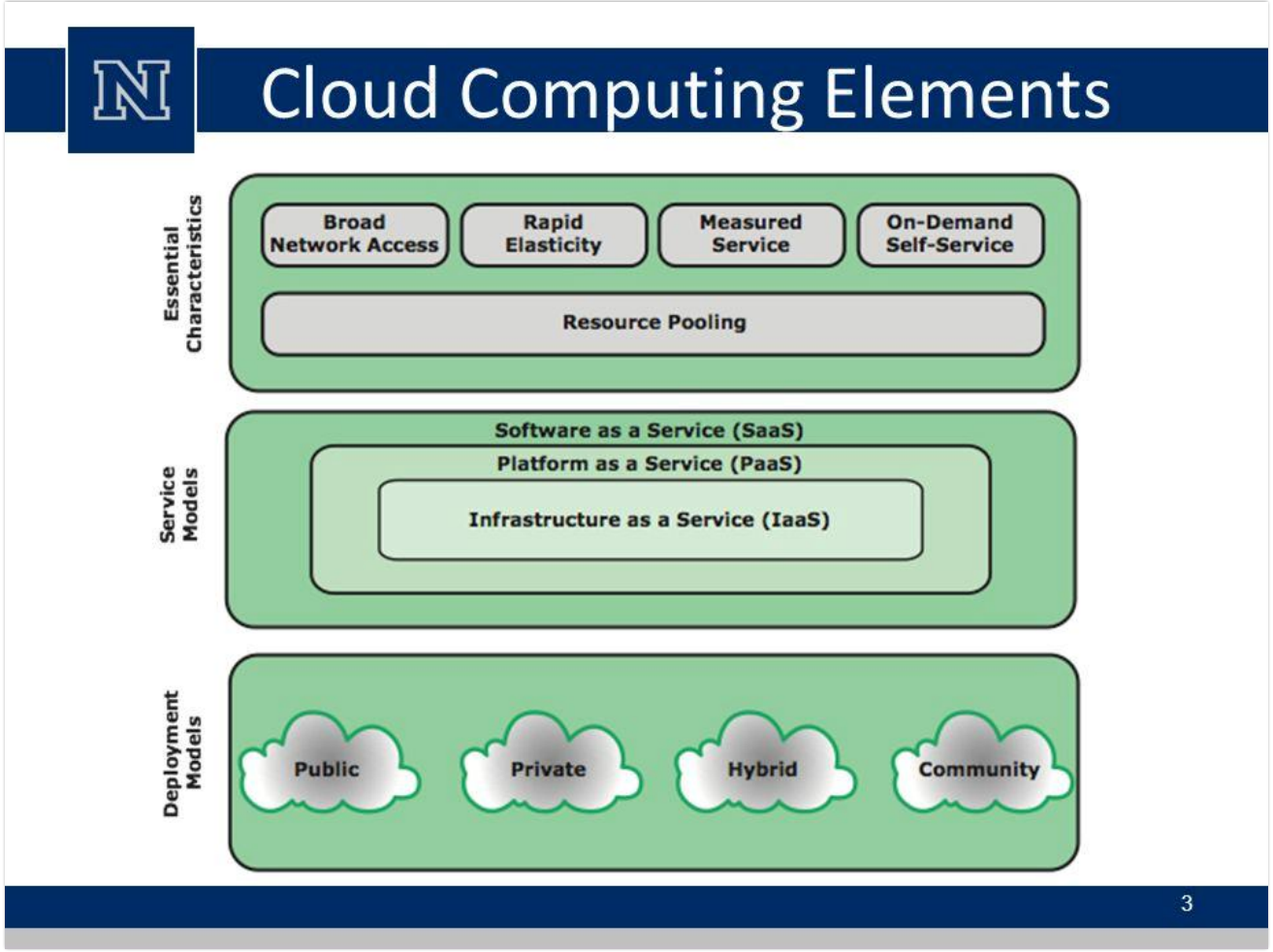
- Limited portability between cloud providers



Cloud Computing Elements

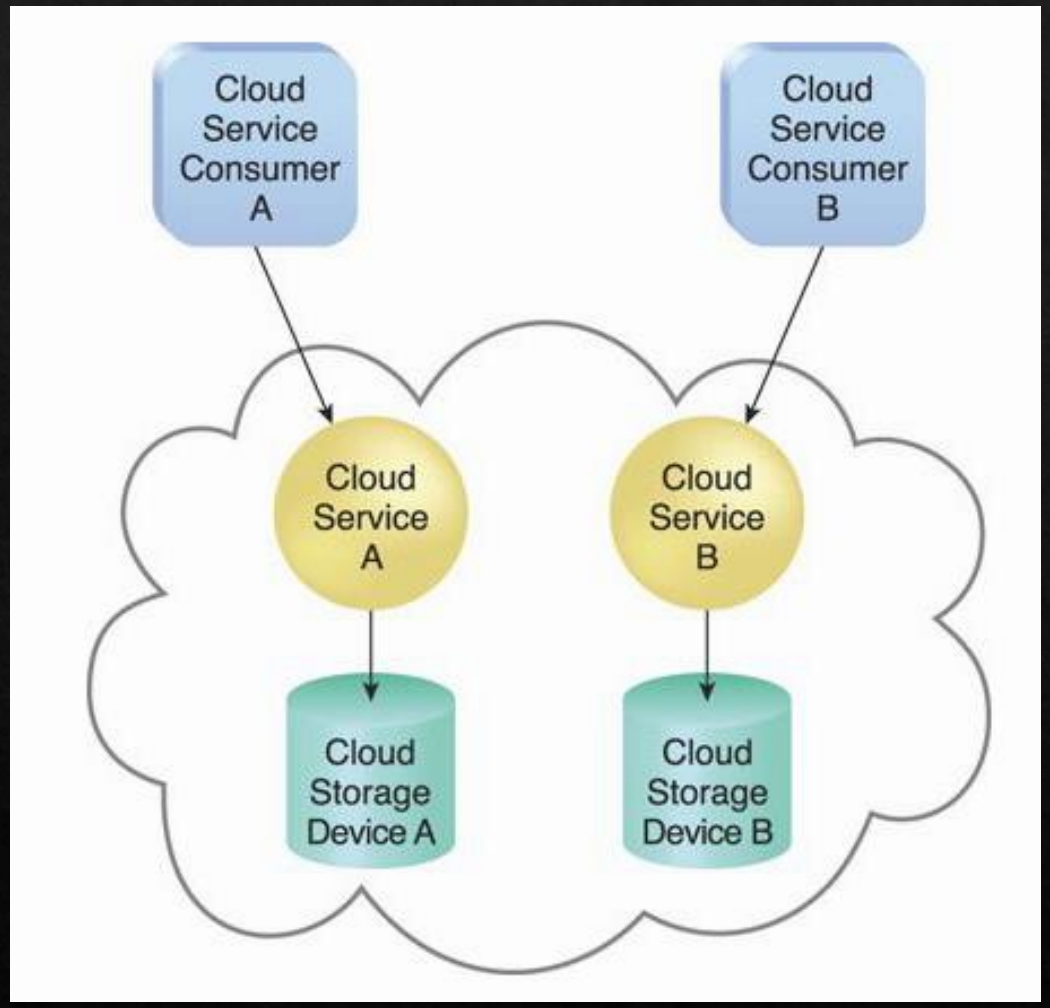
- Five essential characteristics
  - Broad network access, rapid elasticity, measured service, on-demand and resource pooling.
- Three service models
  - Software as a service (SaaS), Platform as a service (Paas), Infrastructure as a service (Iaas).
- Four deployment models
  - Public, private, community and hybrid

Cloud Computing Elements

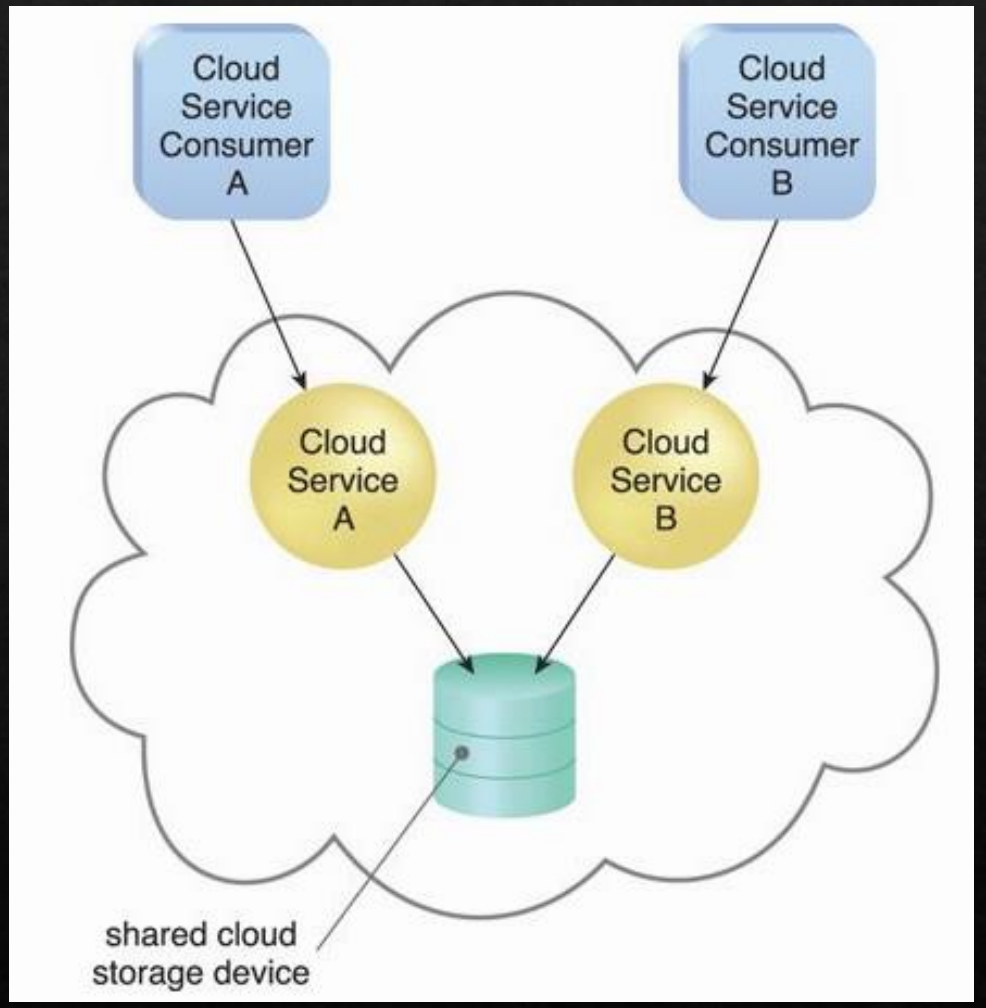


Cloud Characteristics

- On-demand (self-service) usage
- Ubiquitous access (broad network access)
- Multitenancy (and resource pooling)
- Elasticity
- Measured usage



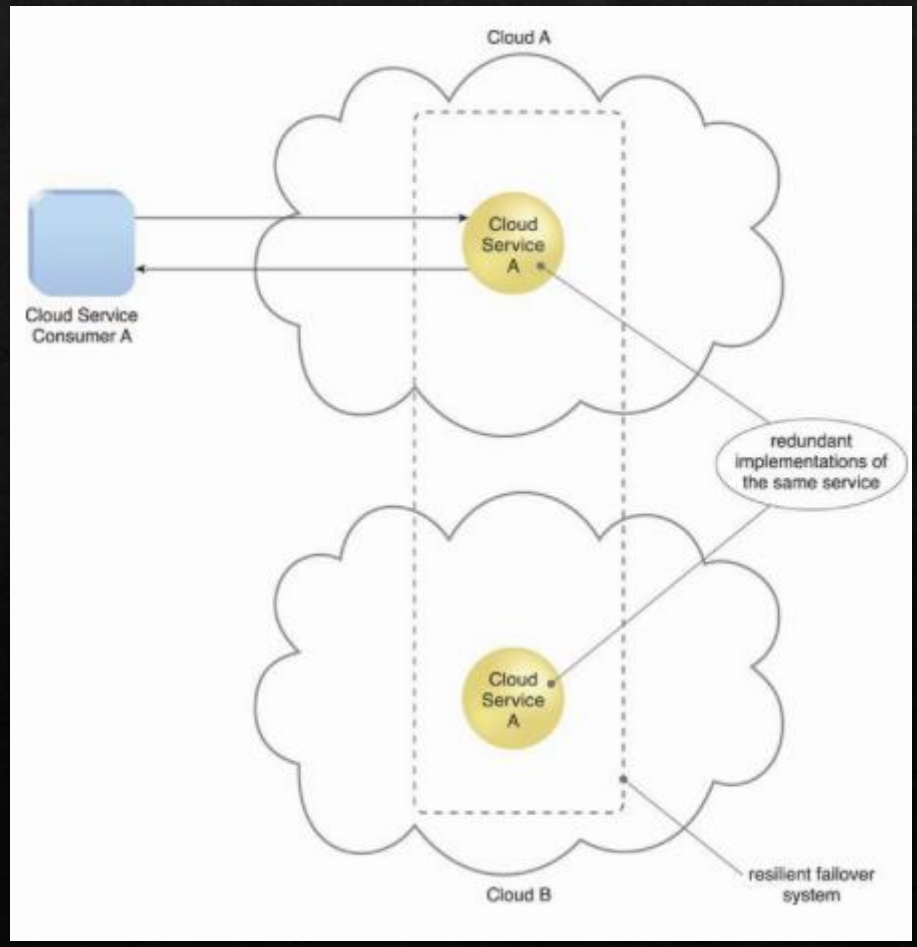
Single tenant



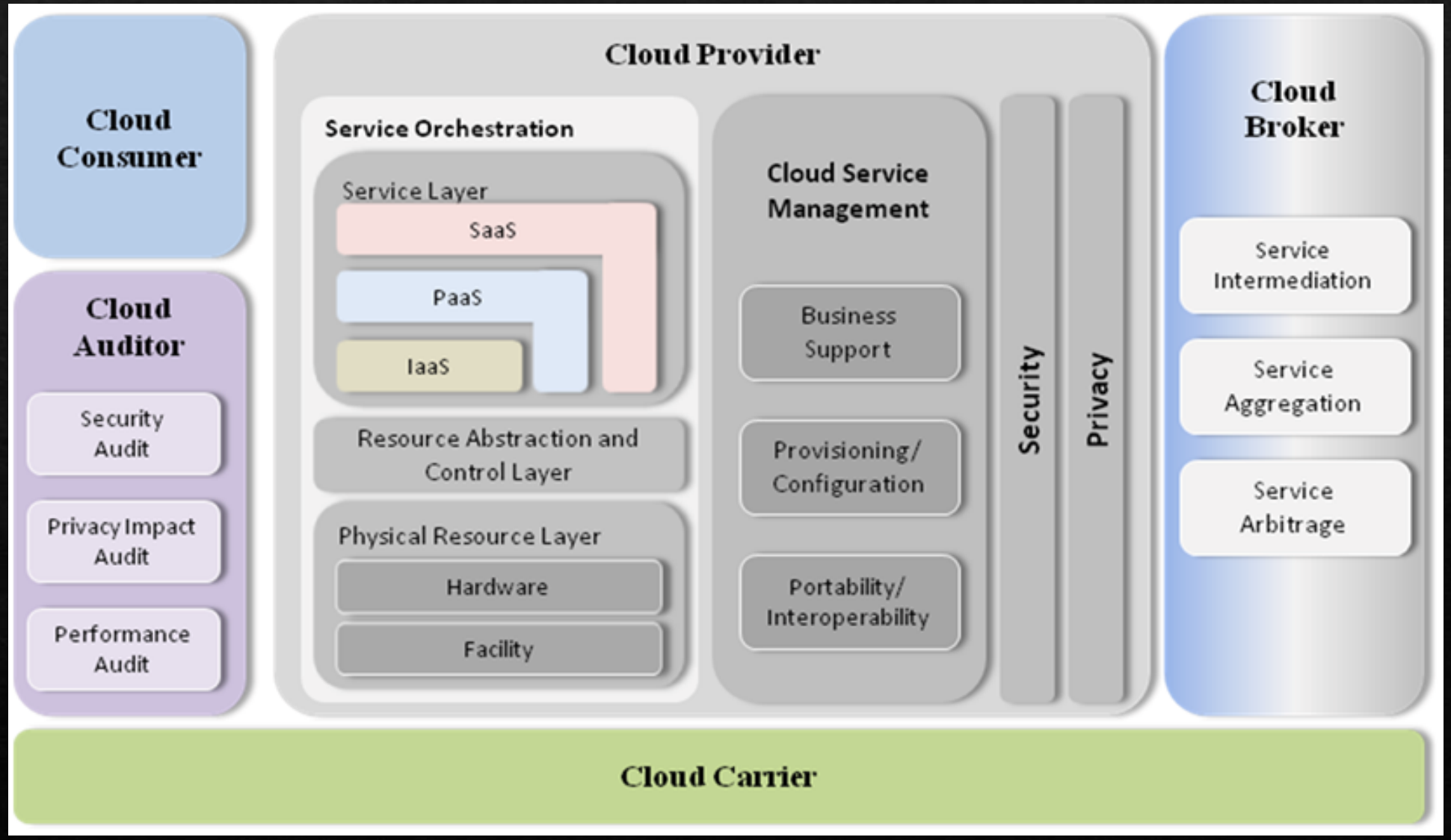
Multitenant

Resiliency

“A form of failover that distributes redundant implementations of IT resources across physical locations.”

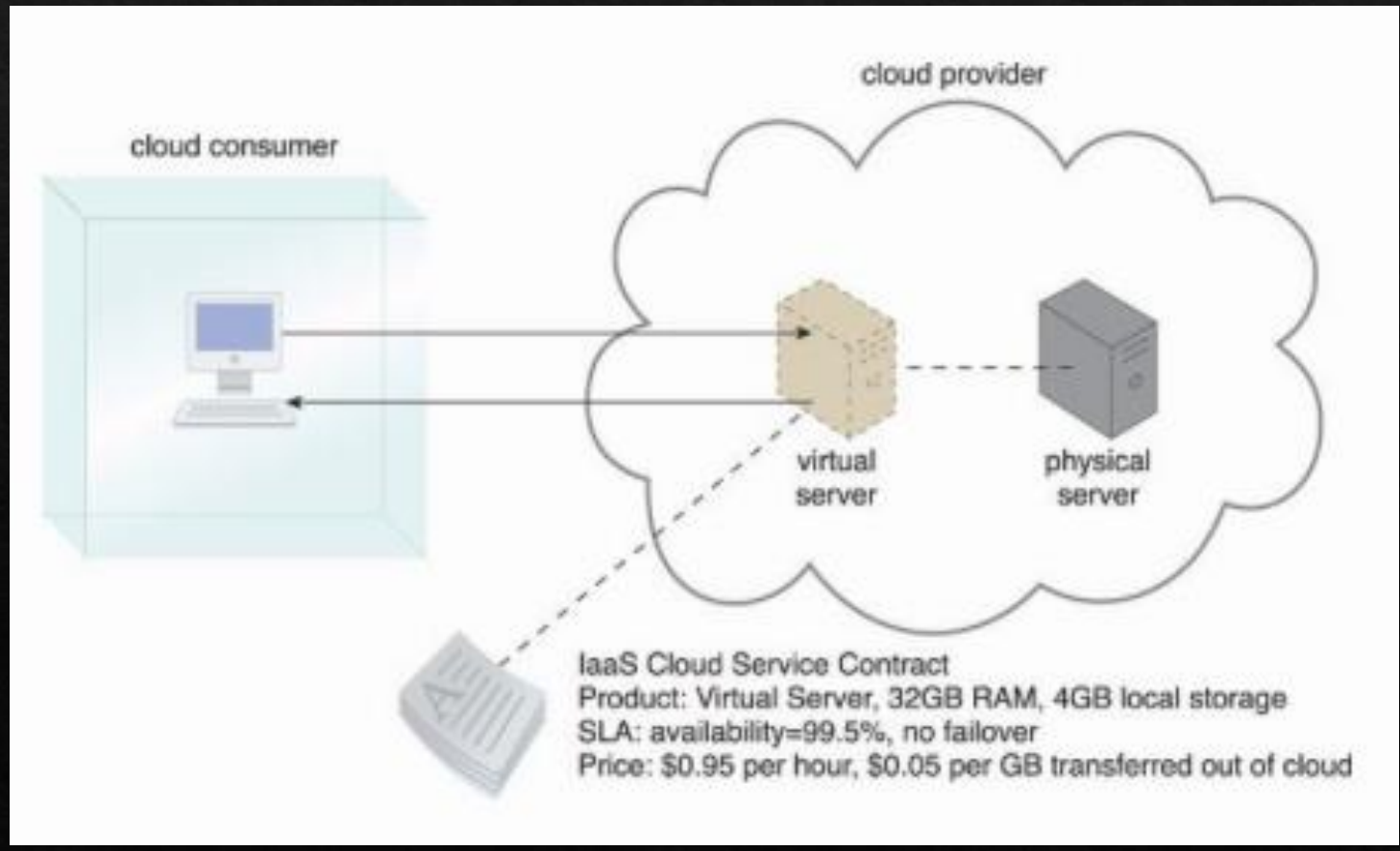


Cloud Computing Reference Architecture



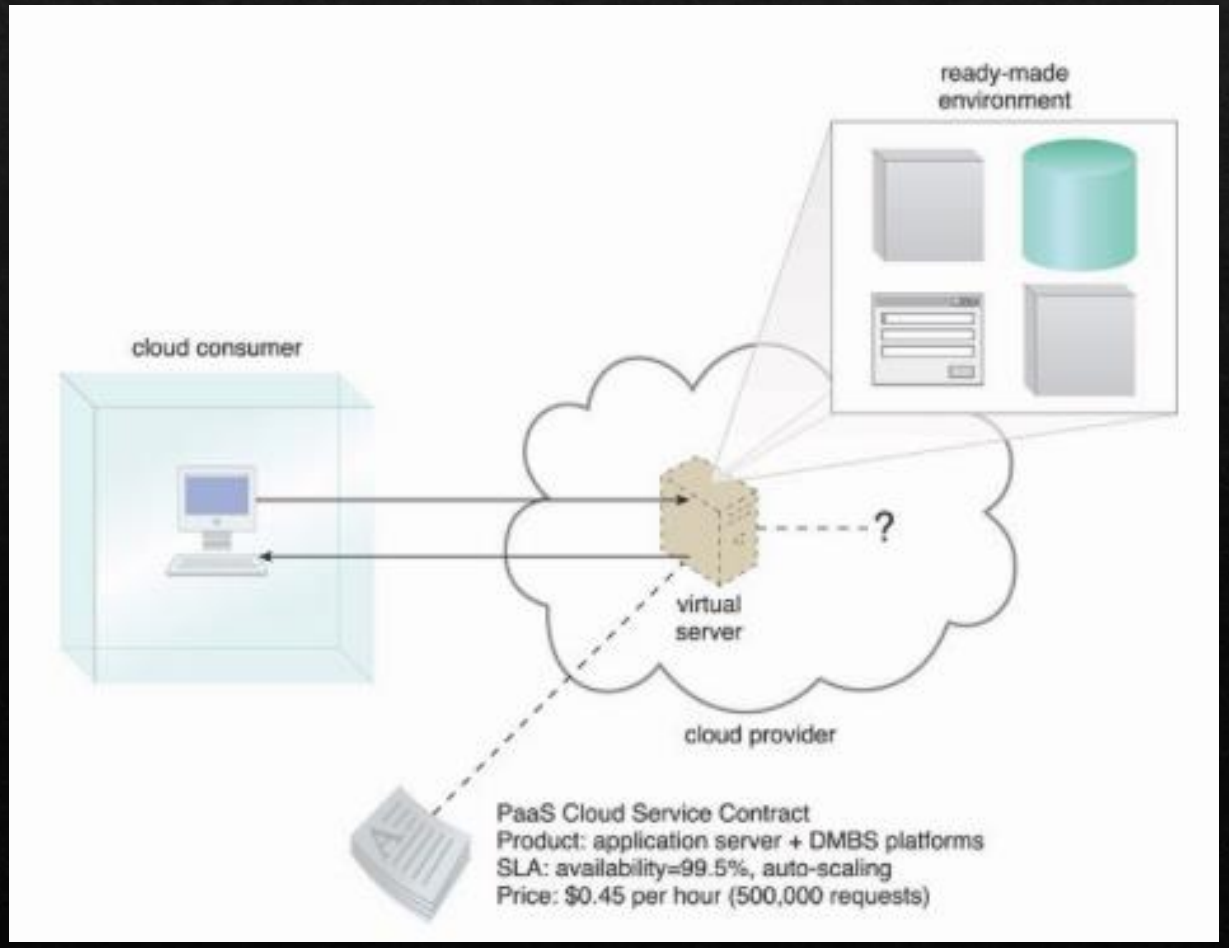
IaaS

- A self-contained IT environment comprised of infrastructure-centric IT resources that can be accessed and managed via cloud service-based interfaces and tools.



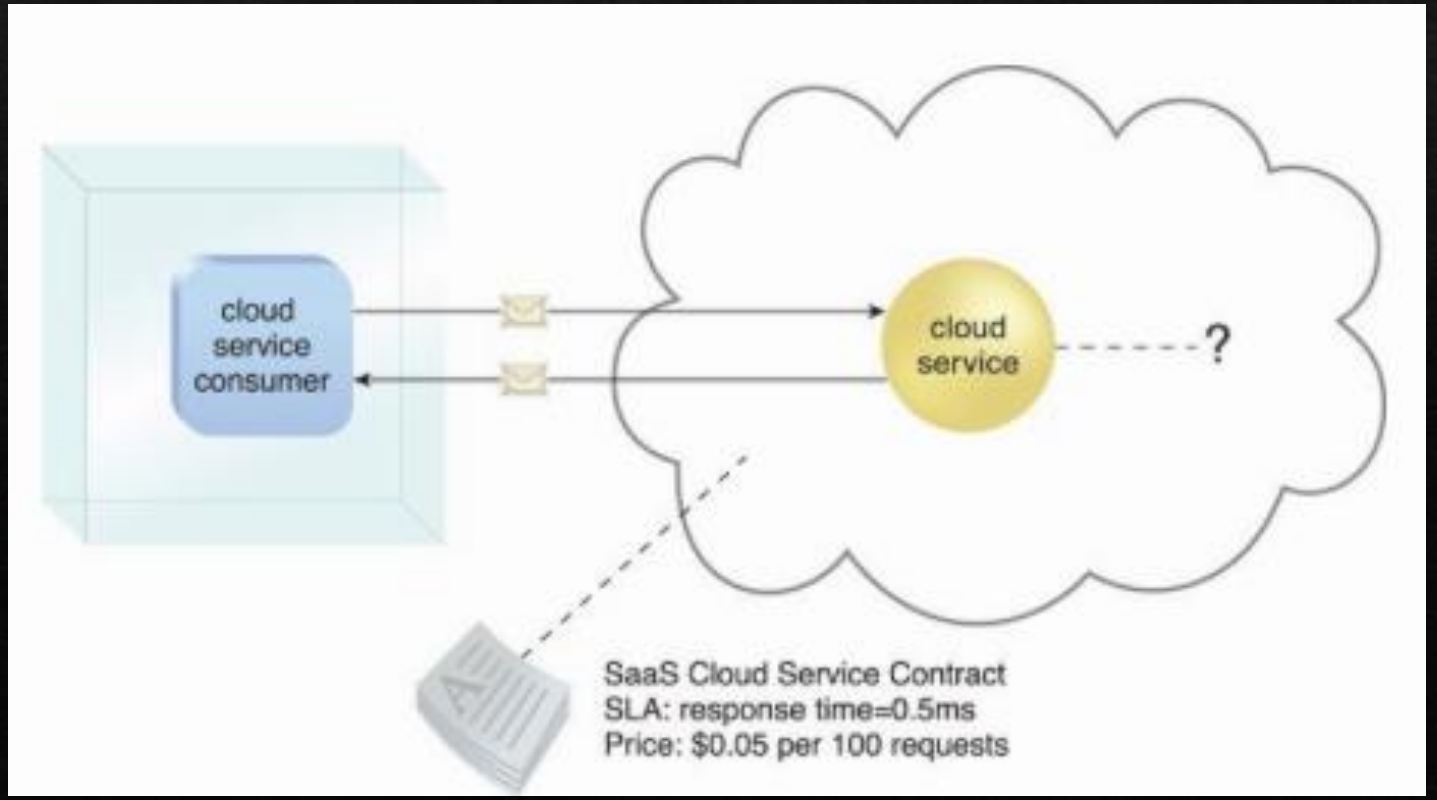
PaaS

- A pre-defined “ready-to-use” environment typically comprised of already deployed and configured IT resources.
  - The cloud consumer wants to extend on-premise environments into the cloud for scalability and economic purposes.
  - The cloud consumer uses the ready-made environment to entirely substitute an on-premise environment.
  - The cloud consumer wants to become a cloud provider and deploys its own cloud services to be made available to other cloud consumers.
  - E.g., Google App Engine offers a Java and Python-based environment.

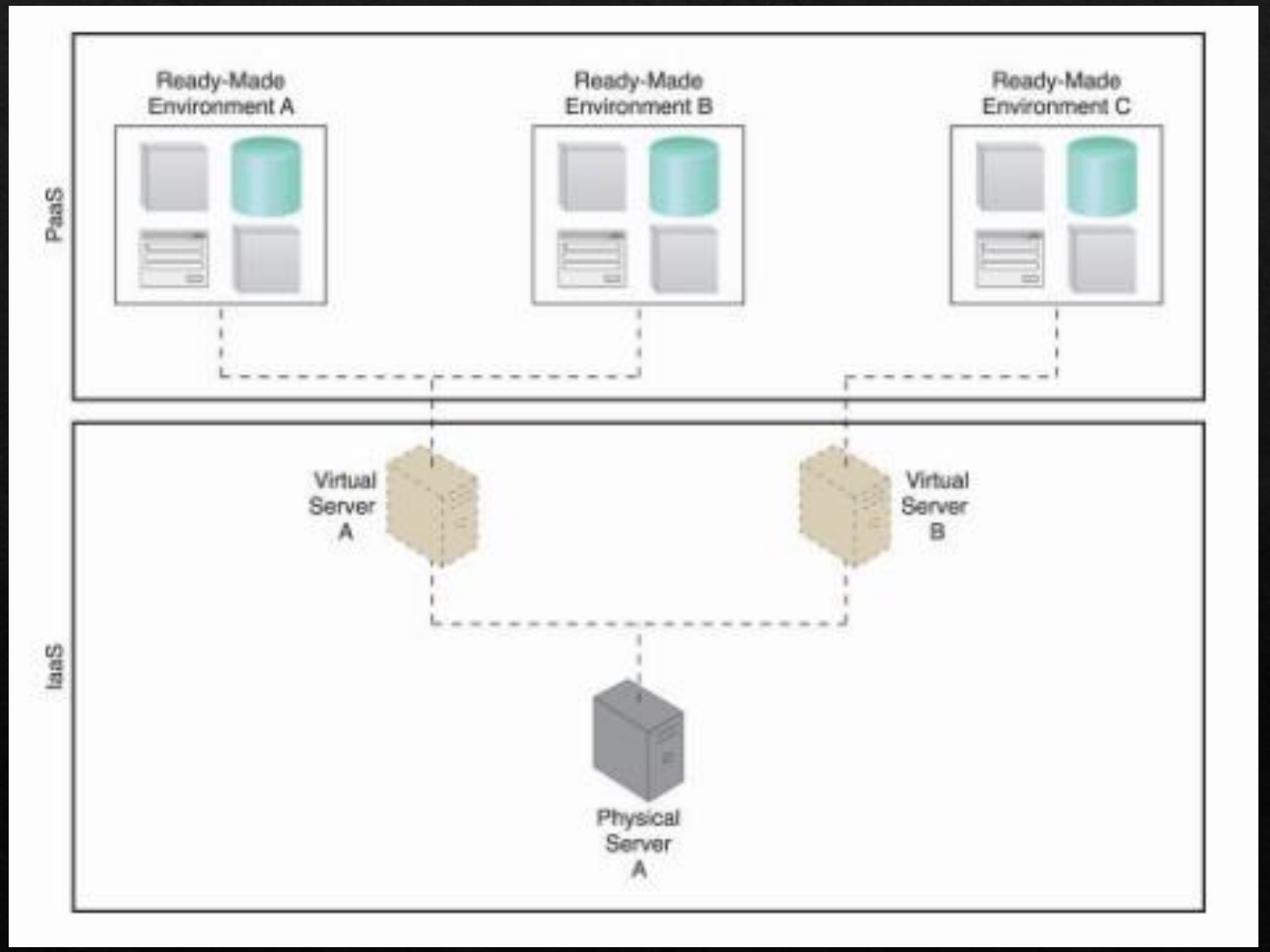


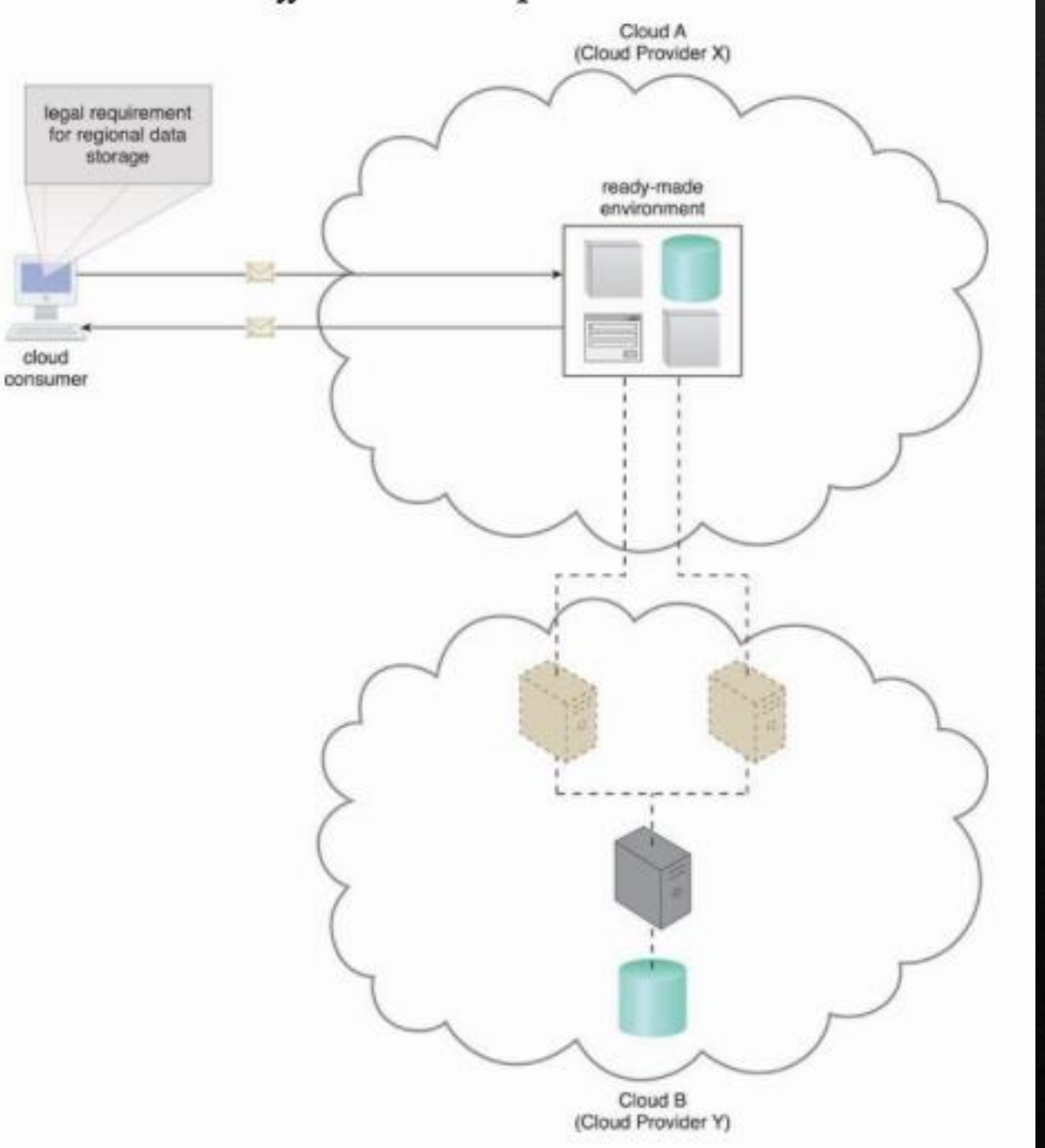
SaaS

- A software program positioned as a shared cloud service and made available as a “product” or generic utility represents the typical profile of a SaaS offering.

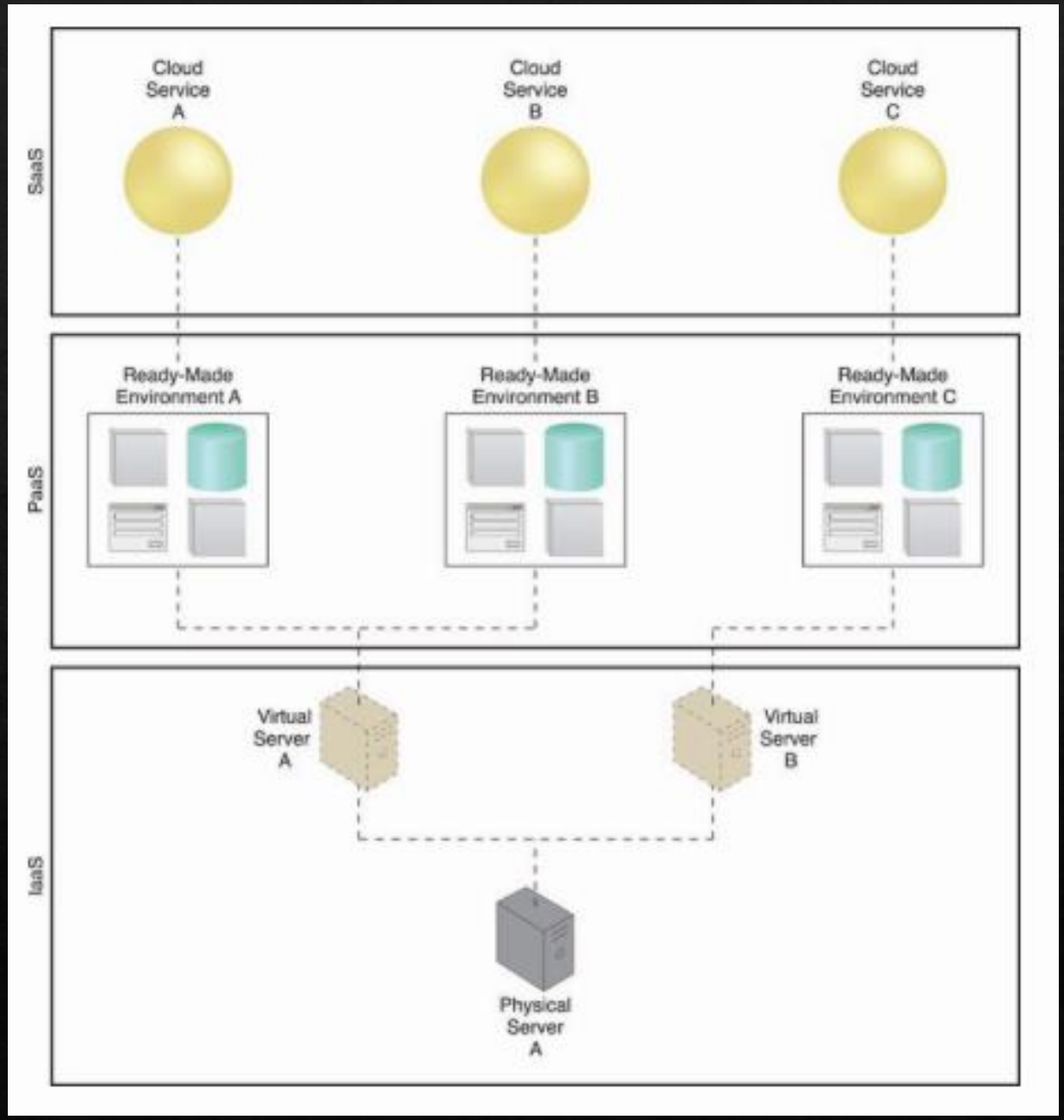


Combining Delivery Model: IaaS + PaaS




Cloud A
(Cloud Provider X)
legal requirement
for regional data
storage
ready-made
environment
cloud
consumer
Cloud B
(Cloud Provider Y)

IaaS + PaaS + SaaS



Cloud Security Risk and Countermeasures

- Abuse or nefarious use of cloud computing
  - Free trail period -> attackers may use this period to get into the cloud to conduct various attacks.
- Countermeasures – stricter initial registration and validation processes, enhanced credit card fraud monitoring and coordination, comprehensive observation of customer network traffic, check public's black lists

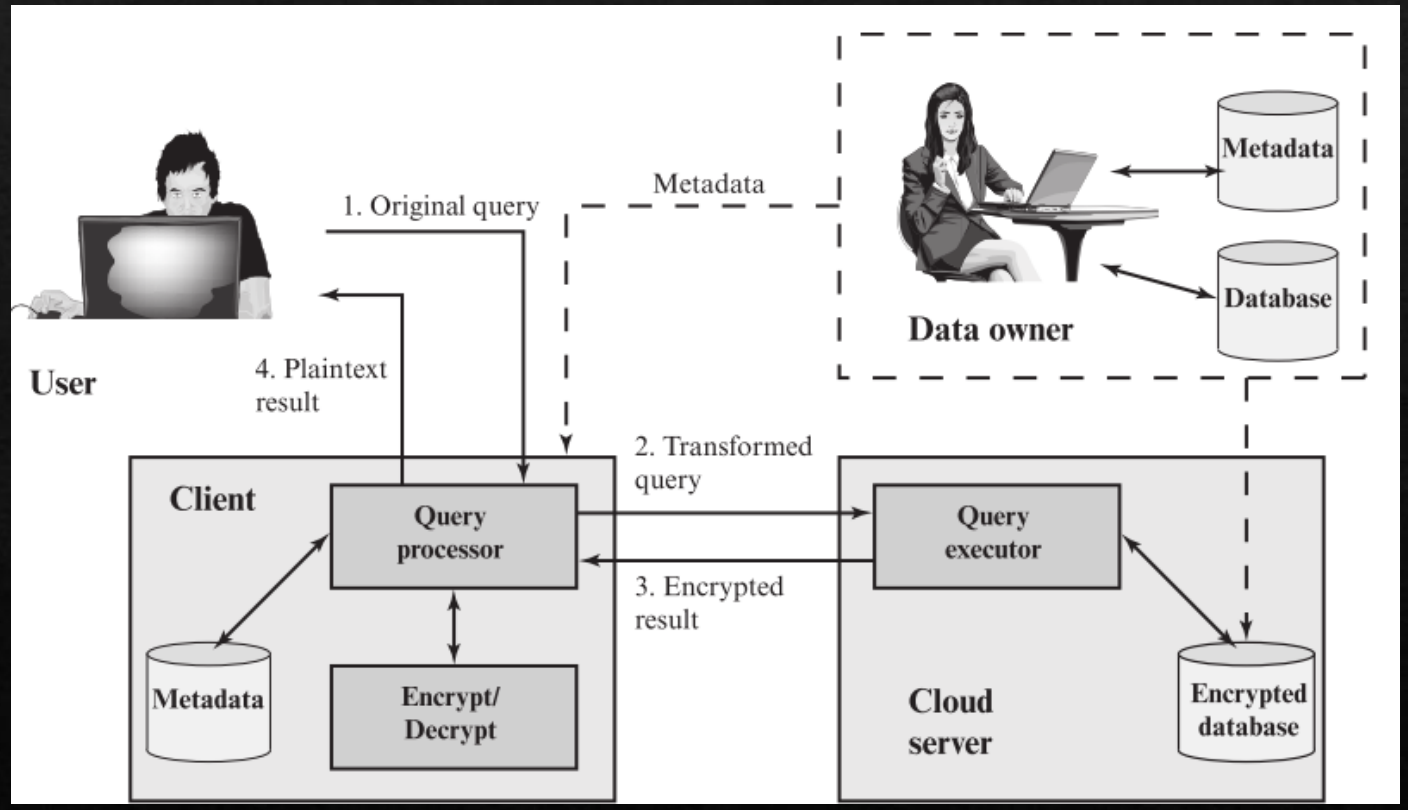
Cloud Security Risk and Countermeasures (2)

- Insecure interfaces and APIs
  - A set of software interfaces or APIs available to customers enabling them to manage and interact with cloud services (from authentication, access control to encryption and monitoring).
  - The design of interfaces and APIs must be secure. Why?
- Countermeasures – CP interfaces model analyzing, strong authentication/access controls/encryptions implemented, understand APIs dependency chains

Cloud Security Risk (3)

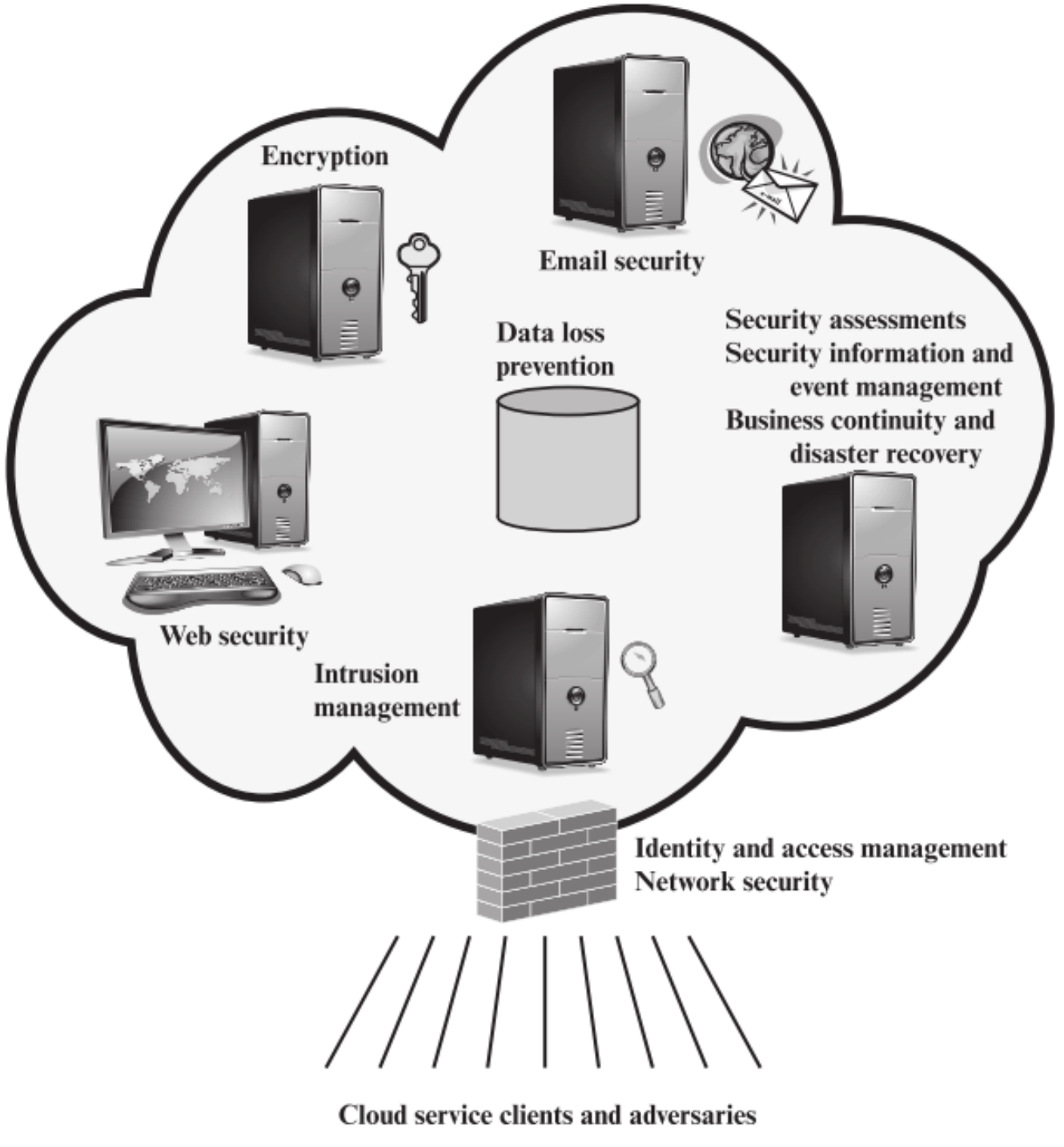
- Malicious insider (unprecedented level of trust onto CP, e.g., CP system administrators)
  - HR requirements as part of legal contract
- Shared technology issues (how to isolate multi-tenant sharing the same resources)
  - Security best practice implementation
- Data loss or leakage
  - Strong API access control, encryption, etc.
- Account or service hijacking (due to stolen credentials)
  - Strong two-factor authentication (OTP, etc.)
- Unknown risk profile

Example: Encrypted Database to Prevent Data Loss or Leakage



Cloud Security as a Service

- The Cloud Security Alliance defines security as a service (SecaaS) the provision security applications and services via the cloud either cloud-based infra and software or from cloud to the customer’s premise system.
- SecaaS categories of service
  - Identity and access management, data loss prevention, web security, email security, security assessments, intrusion management, security information and event management, encryption, business continuity and disaster recovery and network security.


Encryption
Email security
Data loss prevention
Security assessments
Security information and event management
Business continuity and disaster recovery
Web security
Intrusion management
Identity and access management
Network security
Cloud service clients and adversaries