ENCE606035 KOMPUTASI AWAN

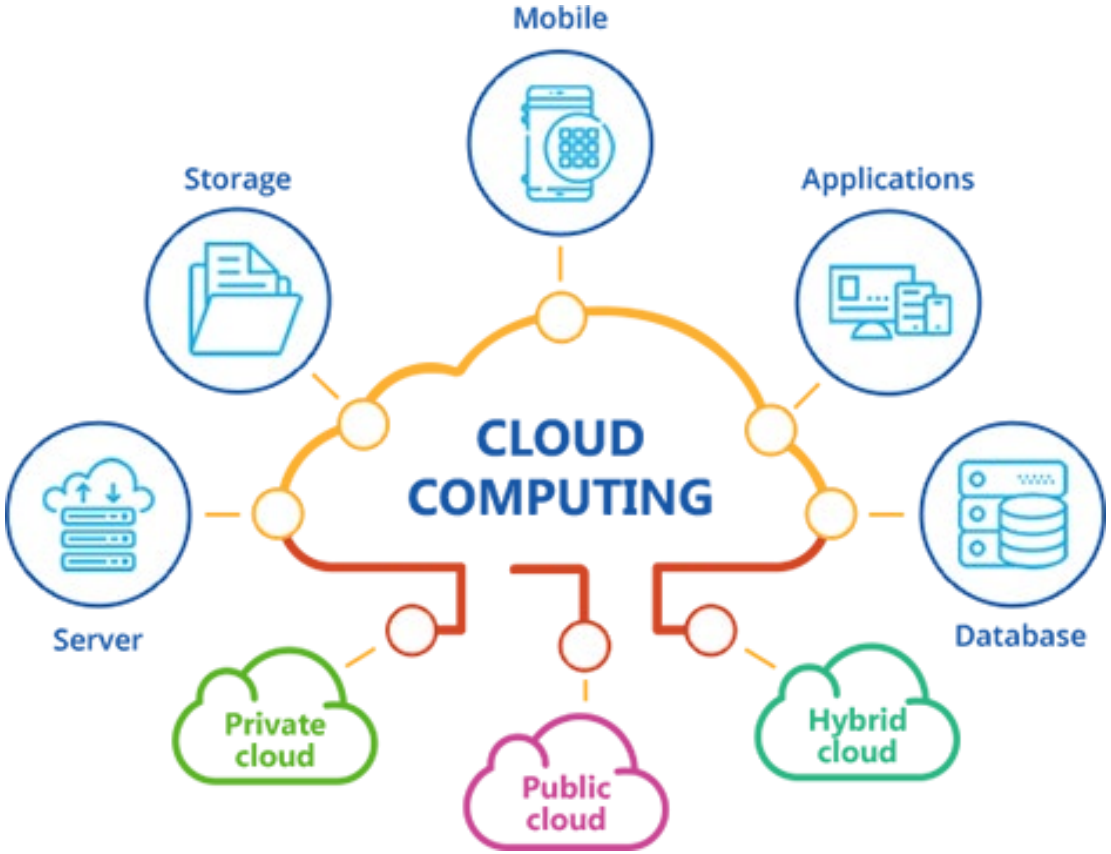
I Gde Dharma Nugraha, Ph.D

Topik

- Pengantar Kelas
- Silabus
- Referensi
- Sistem Penilaian
- Aturan Kelas
- Perkenalan Komputasi Awan

Pengantar Kelas

- Merupakan Mata Kuliah Pilihan bagi Mahasiswa Teknik Komputer.
- MK ini akan memperkenalkan model layanan dan pemanfaatan komputasi awan serta mengenalkan teknologi-teknologi yang mendukung komputasi awan.



Pengantar Kelas

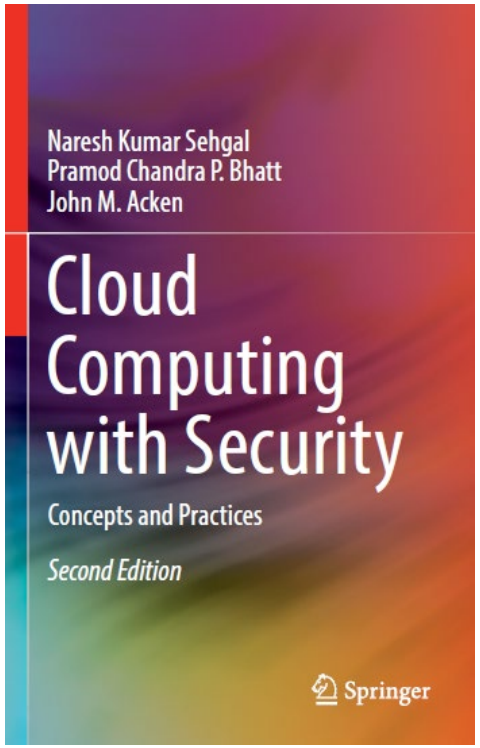
- CPMK
  - Mampu membuat rancangan teknologi komputasi awan untuk memenuhi kebutuhan komputasi.
  - Mampu memanfaatkan komputasi dalam pengembangan suatu aplikasi.

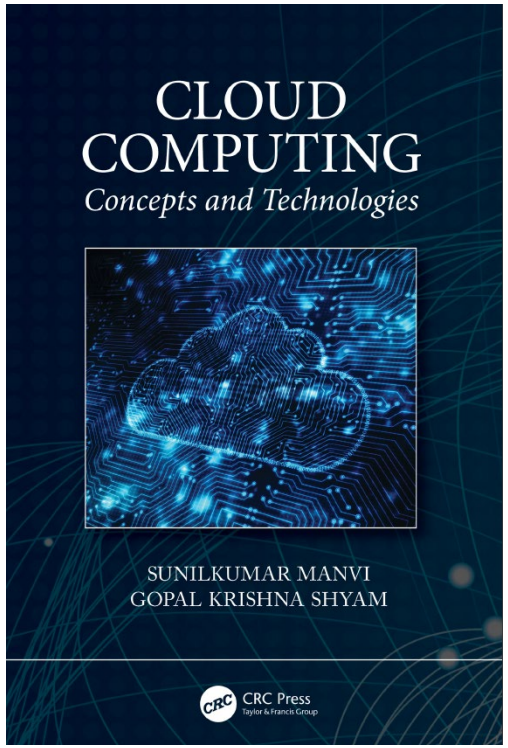
Silabus

- Pengenalan Komputasi Awan
- Teknologi Pondasi Komputasi Awan
- Piramida
- Komputasi Awan
- Private dan Public Komputasi Awan
- Karakteristik Kerja Cloud
- Manajemen dan Pengawasan Komputasi Awan
- Pengenalan Aplikasi Komputasi Awan

Referensi

- Naresh Kumar S., Pramod Chandra P. B., John M. A., “Cloud Computing with Security – Concept and Practice”, 2nd Edition, Springer, 2020
- Sunilkumar M., Gopal K. S., “Cloud Computing – Concept and Technologies”, CRC Press, 2021





Sistem Penilaian

- Scoring
  - Tugas (Individu+Kelompok) : 10%
  - Tugas Praktek : 25%
  - UTS : 25%
  - Project/UAS : 35%
  - Quiz : 5%
- No late project are accepted
- Link Emas:
  - https://emas2.ui.ac.id/course/view.php?id=87769
  - Enroll Key: QWRTIH

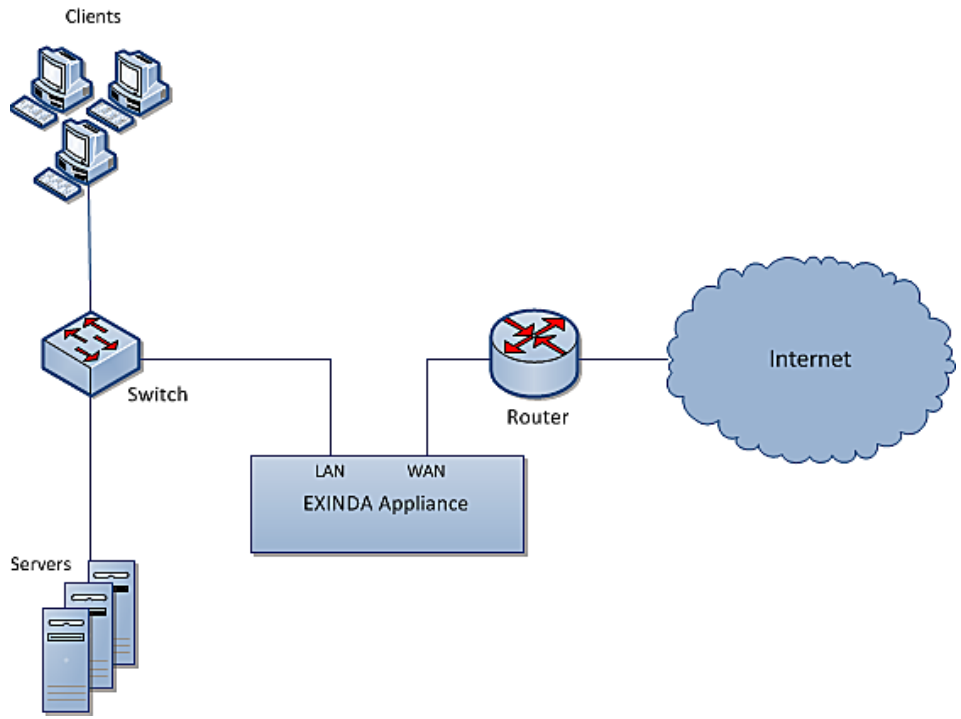
Aturan Kelas

- Active Communication
- Attention & Respect
- Attitude, no chit chat, no eating/drinking at the class
- Participation in Individual/Group activities
- Self Motivation
- Code of Ethics (Cheating, Plagiarism, Collusion etc)
- Hand in the assignment on time

PERKENALAN KOMPUTASI AWAN

Komputasi Awan

- Awal mula nama Komputasi Awan (Cloud) adalah merujuk pada icon internet yang banyak dipakai pada rancangan jaringan computer.



Komputasi Awan

- Komputasi Awan merujuk kepada proses manipulasi, konfigurasi dan mengakses aplikasi online.
- Aplikasi online ini diantara penyimpanan, infrastruktur dan aplikasi online
- Komputasi Awan adalah kombinasi dari perangkat lunak dan perangkat keras berbasis pada sumber daya komputasi yang diakses melalui layanan jaringan.

Arsitektur Komputasi Awan

Model Komputasi Awan

- Ada banyak layanan dan model pada komputasi awan.
- Pengelompokan komputasi awan didasarkan pada
  - Model Penyebaran
  - Model Layanan

Model Penyebaran

- Model Penyebaran mendefinisikan kelompok komputasi awan berdasarkan cara akses.
- Ada empat cara akses komputasi awan:
  - Public Cloud
  - Private Cloud
  - Hybrid Cloud
  - Community Cloud

Model Penyebaran

- Public Cloud: Memungkinkan layanan komputasi awan di akses oleh semua orang.
- Private Cloud: Akses layanan komputasi awan hanya diijinkan di dalam lingkungan suatu organisasi.
- Hybrid Cloud: Merupakan gabungan dari public dan private cloud.
- Community Cloud: Mengijinkan akses layanan komputasi awan oleh sekelompok organisasi.

Model Layanan

- Model Layanan mendefinisikan kelompok komputasi awan berdasarkan jenis layanan yang dapat diterima pengguna.
- Ada tiga kelompok:
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)

Keuntungan Komputasi Awan

- Biaya yang rendah
- Meningkatkan Kinerja
- Mengurangi biaya perangkat lunak
- Selalu diperbaharui
- Meningkatkan reliabilitas data
- Memudahkan kolaborasi kelompok

Kerugian Komputasi Awan

- Membutuhkan akses internet yang stabil
- Tidak dapat bekerja dengan baik pada koneksi yang lambat
- Data yang disimpan bisa hilang
- Data yang disimpan belum tentu aman

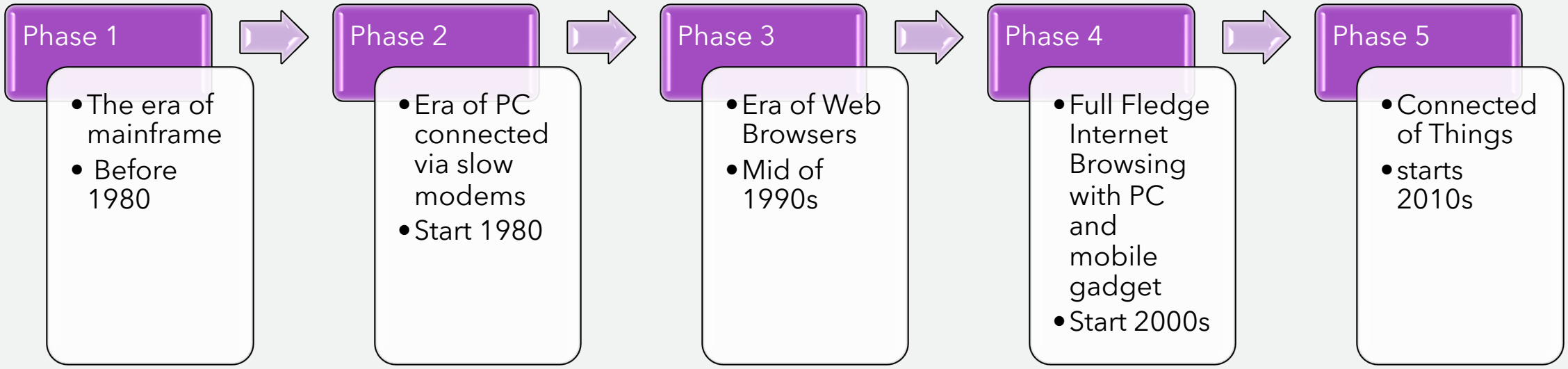
Foundations of Cloud Computing and Information Security

I Gde Dharma Nugraha, Ph.D

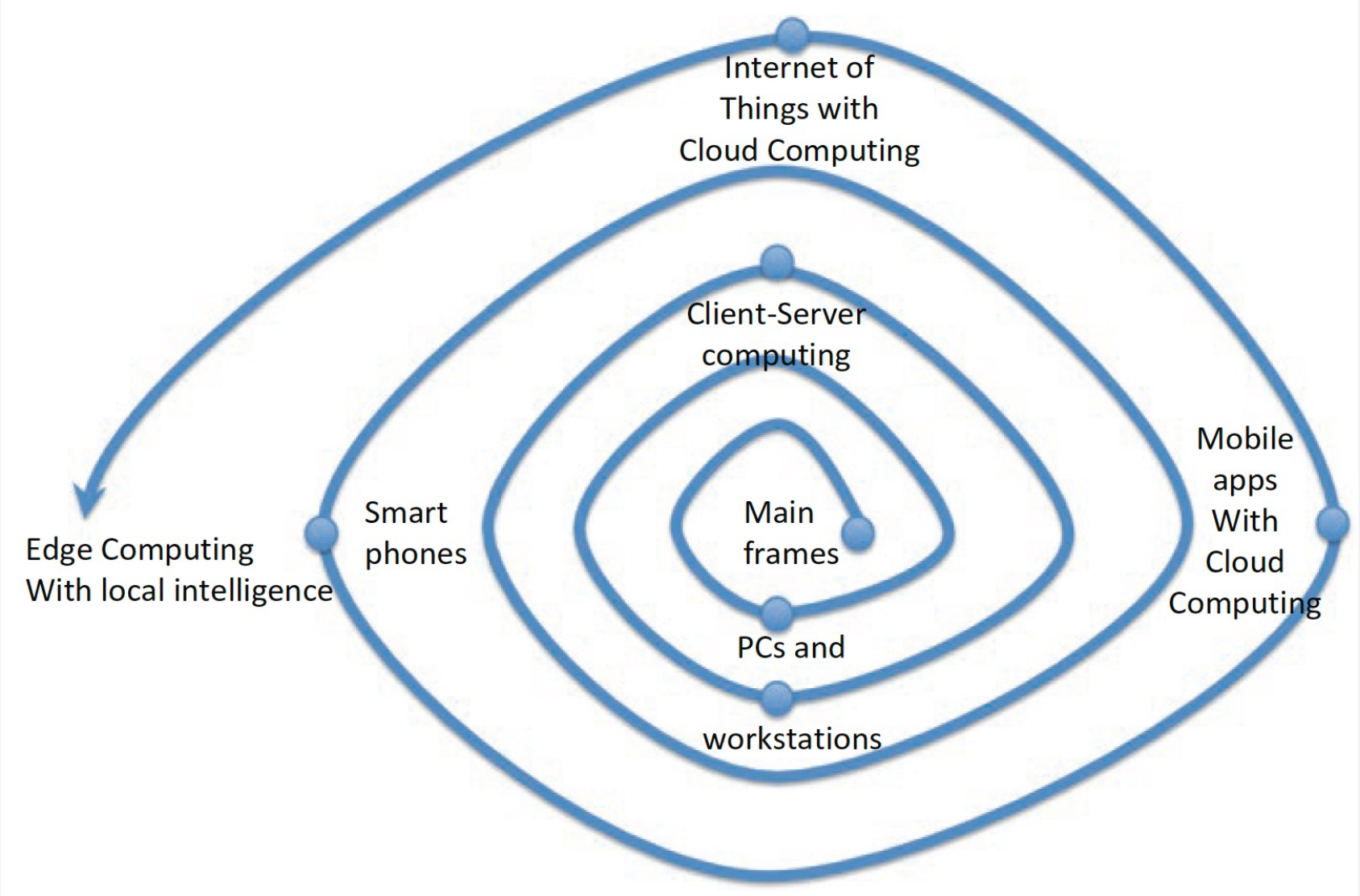
Outlined

- Historical Evolution
- Network Protocol for Cloud Computing
- Data Center Architecture and Connectivity
- IT Evolution
- Server Operation in Data Center
- Evolution of Service Orientation Architecture
- Basic Concept of Cloud Computing Security

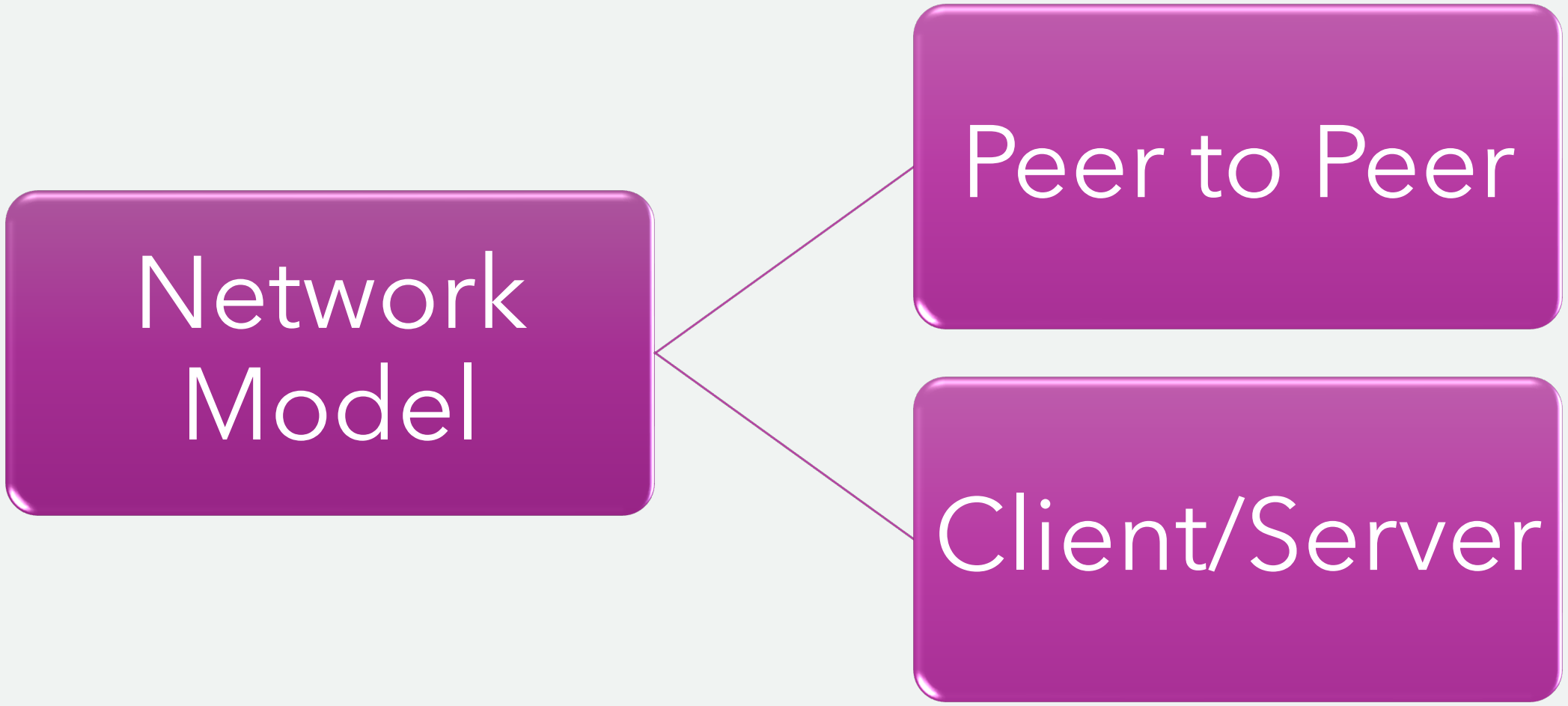
Historical Evolution



Historical Evolution

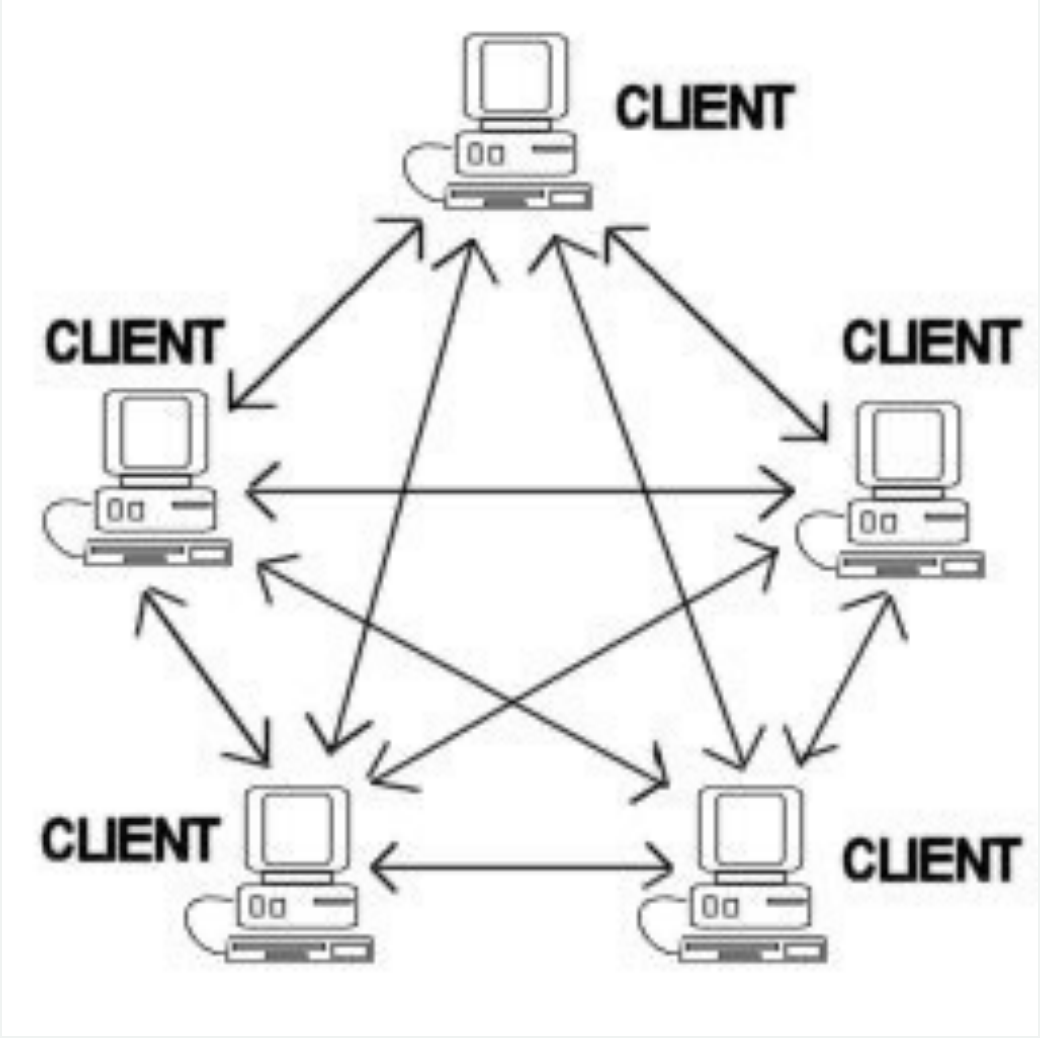


Network Protocols for Cloud Computing



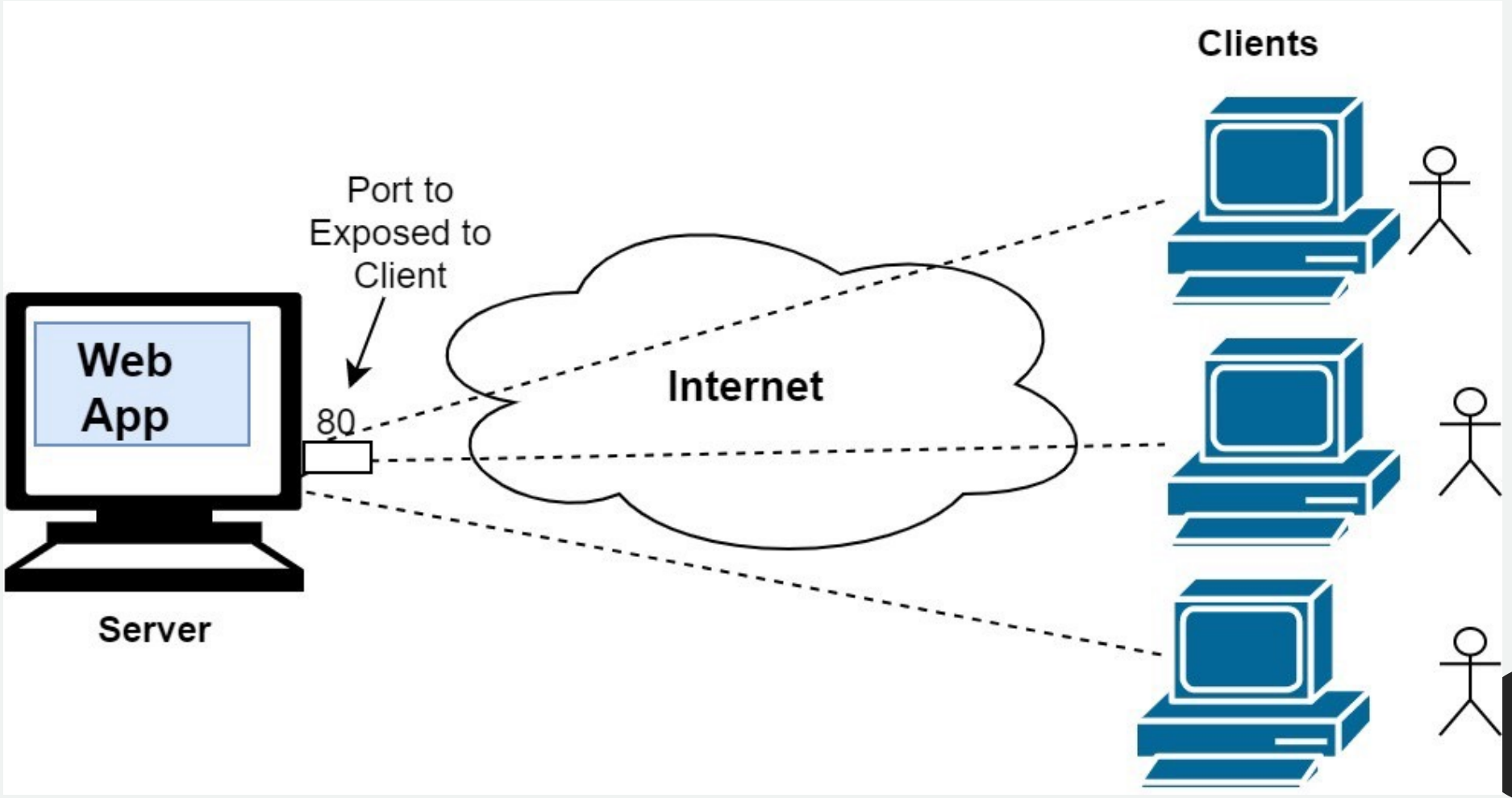
Network Protocols for Cloud Computing

- Peer to Peer Model

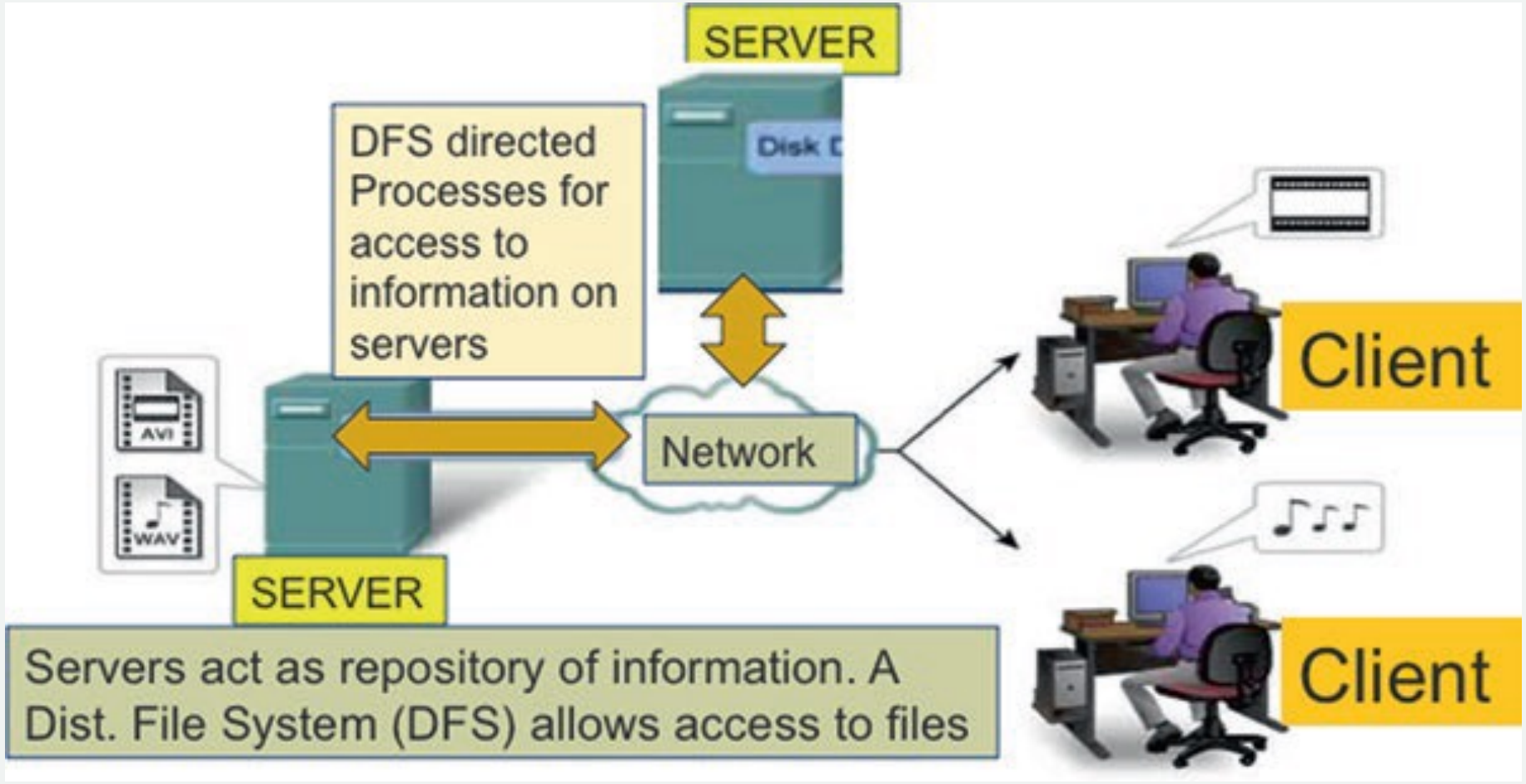


Network Protocols for Cloud Computing

- Client/Server Architecture

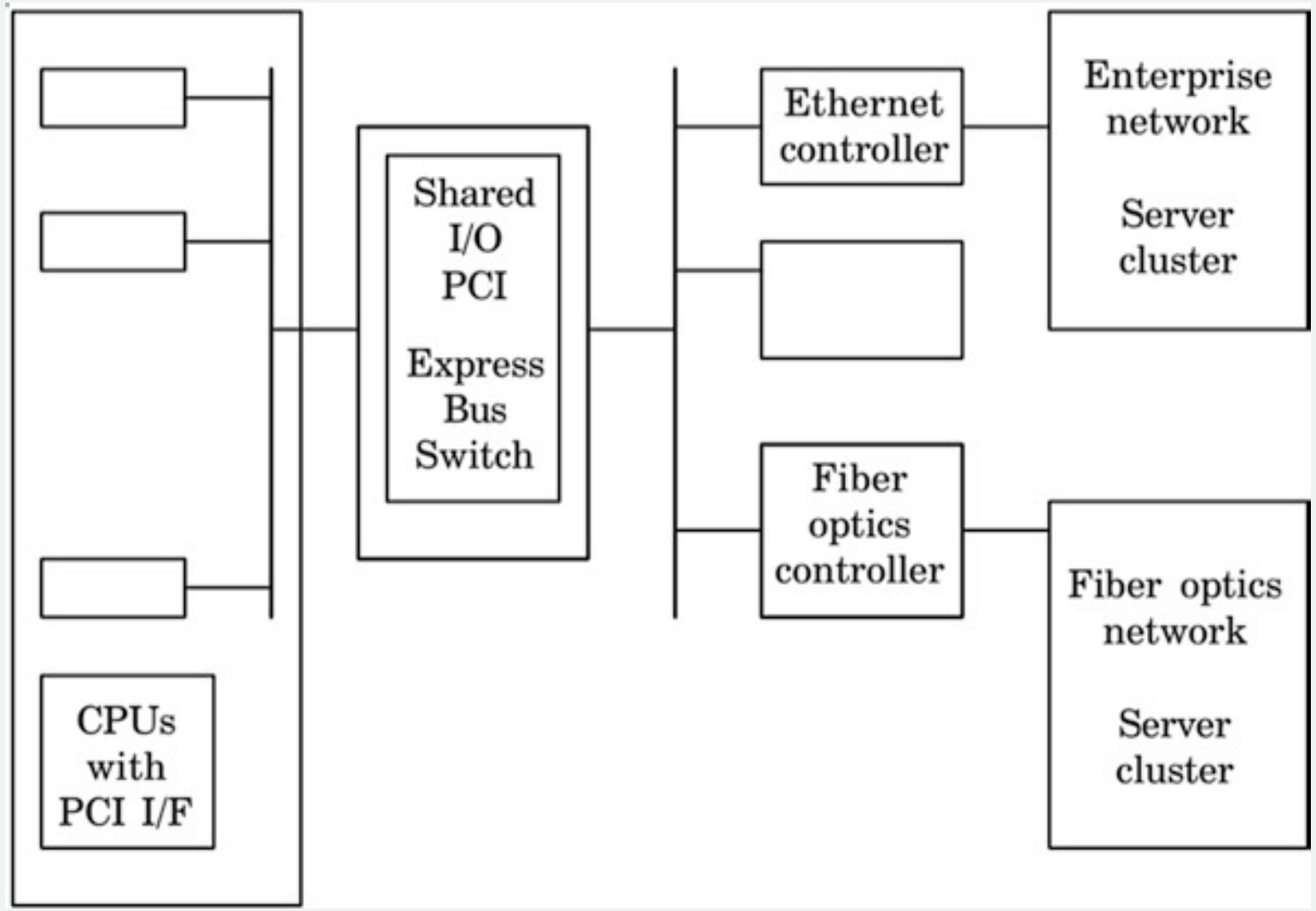


Typical Network Model in Data Center



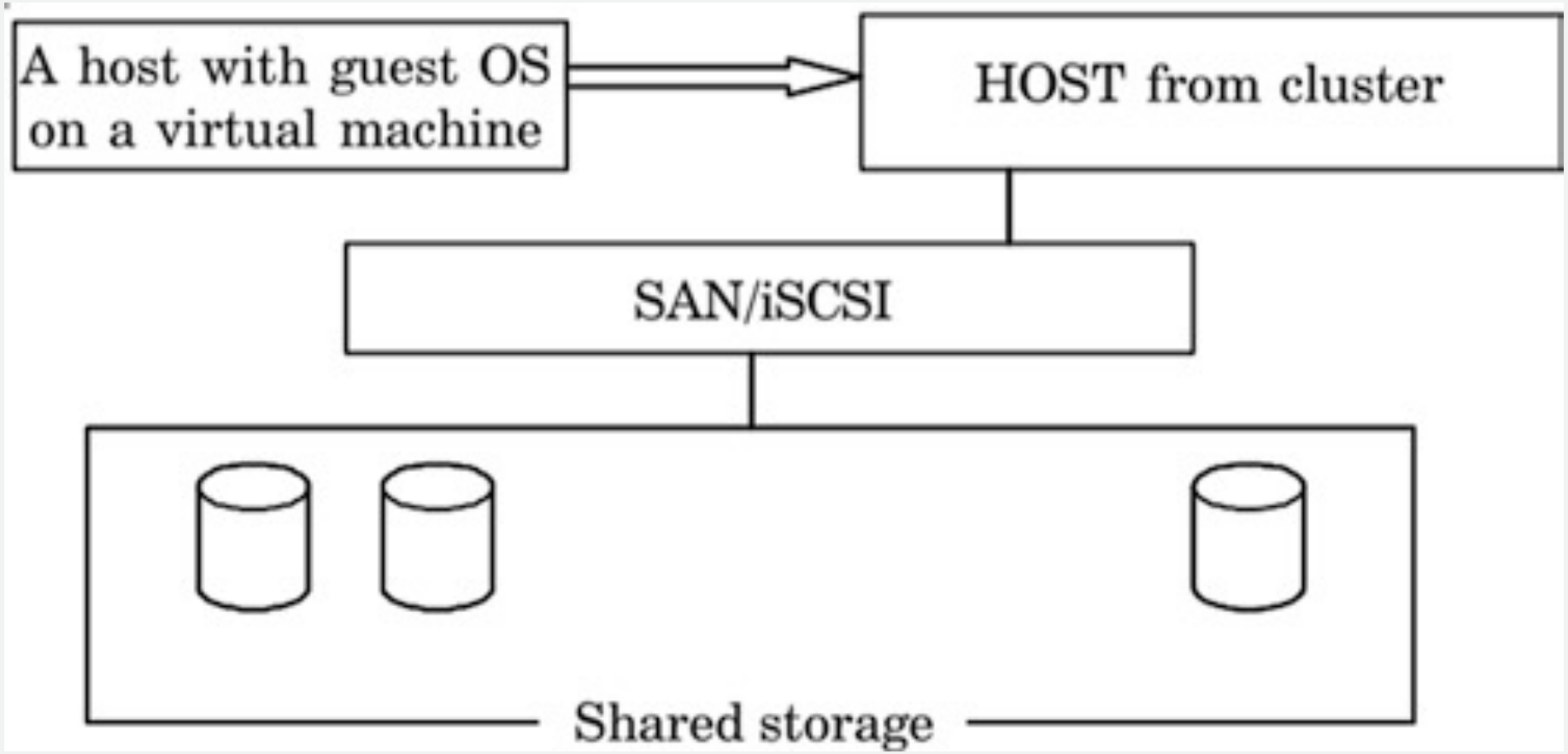
Typical Network Model in Data Center

- Server Cluster



Typical Network Model in Data Center

- Shared Storage

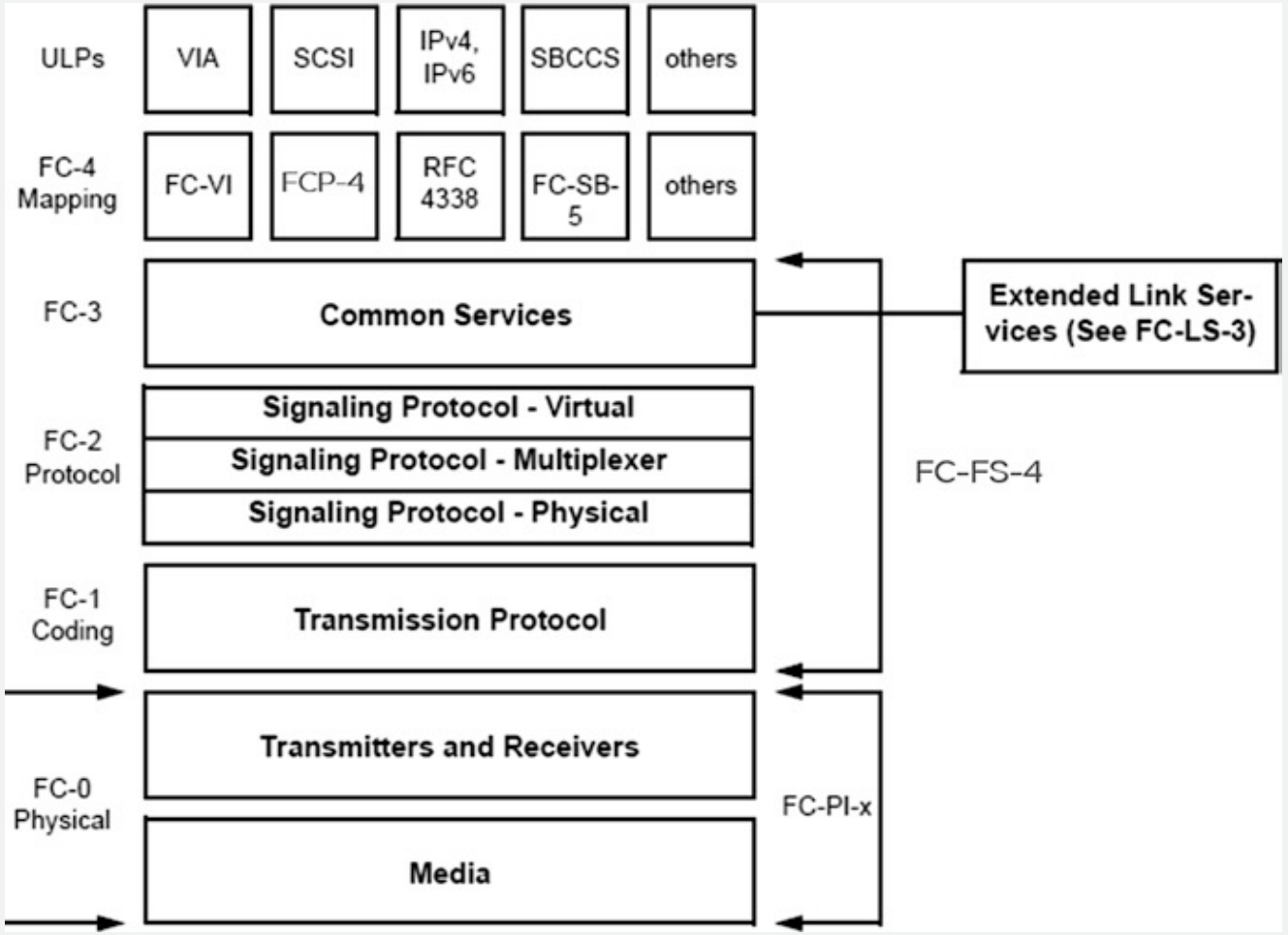


Role of Internet Protocols in a Data Center

- Many public data centers need to share their hardware among different customers, to optimize their infrastructure investments.
- One way to enable this sharing, while preserving isolation and privacy between their customers, data center operators use virtualization.
- The purposes are Isolation and Security, so VLAN is used.
- However, it also can lead to heavy network traffic in a Data Center, so Fibre Channels (FC) are used.

Role of Internet Protocols in a Data Center

- Layers of Fibre Channel Technology Implementation



Role of Internet Protocols in a Data Center

- Layers of Fibre Channel Technology Implementation
- Fibre Channel does not follow the OSI model layers and, is split into five layers:
  - *FC-4 – Protocol-mapping layer, in which upper-level protocols are grouped into Information Units (IUs) for delivery to FC-2.*
  - *FC-3 – Common services layer, a thin layer that implements functions like encryption or RAID redundancy algorithms; multiport connections.*
  - *FC-2 – Signaling Protocol consists of the low-level Fibre Channel protocols; port-to-port connections.*
  - *FC-1 – Transmission Protocol, which implements line coding of signals.*
  - *FC-0 – PHY includes cabling, connectors, etc.*

Data Center Architecture and Connectivity

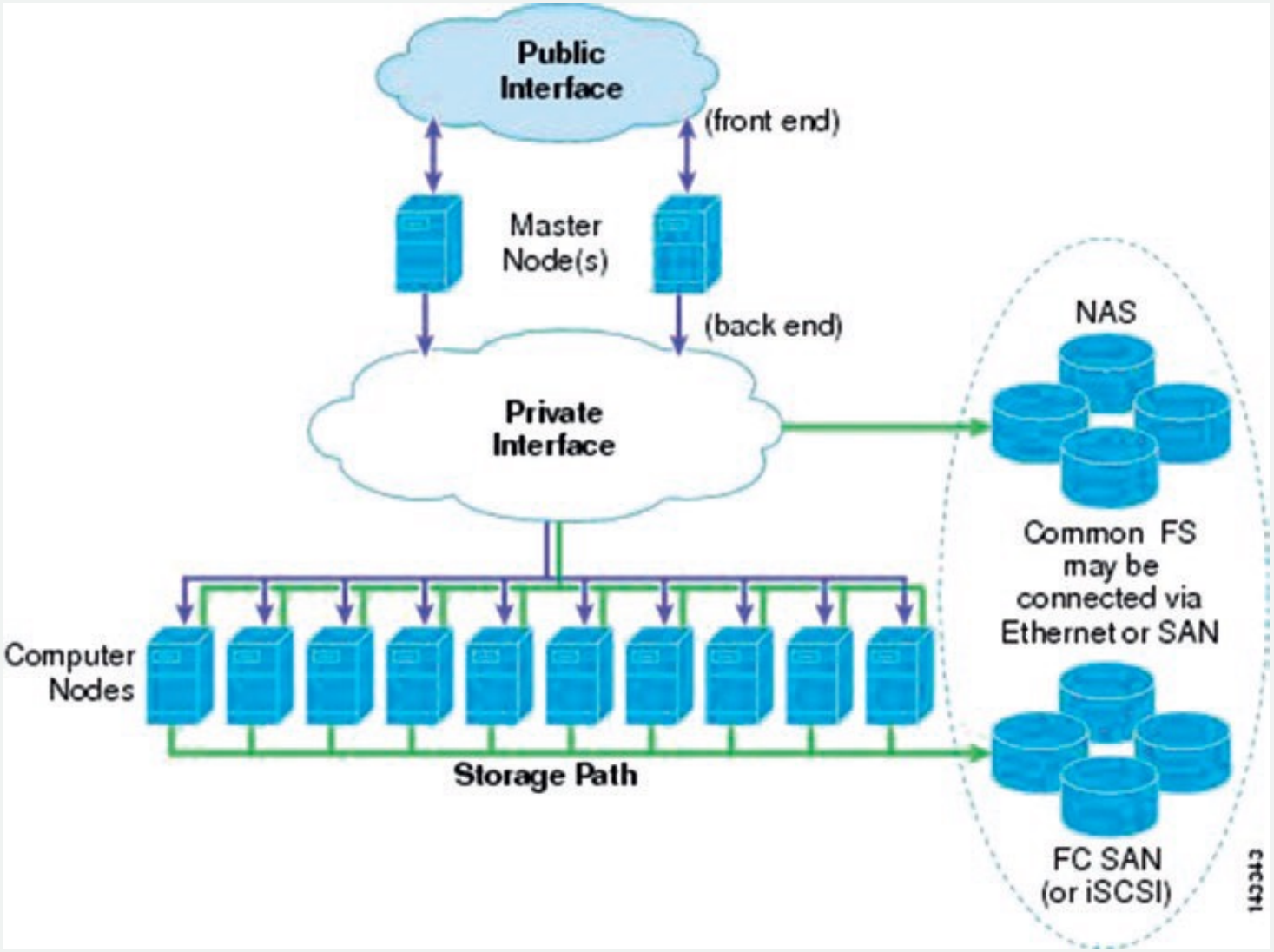
- Data center architecture is the physical and logical layout of the resources and equipment within a data center facility.
- A comprehensive design takes into account:
    1. Power and cooling requirements
    2. Racks of servers
    3. Storage arrays
    4. Network switches
    5. Security aspects
    6. IT management practices

Data Center Architecture and Connectivity

- Typically, the goal of a data center is to support one or more business services while considering the following factors:

  1. *Scalability: ability to increase compute or storage capacity as demand grows*
  2. *Performance*
  3. *Flexibility*
  4. *Resiliency*
  5. *Maintenance aspects*

Data Center Architecture and Connectivity



IT Evolution

- In regards Cloud Computing, evolution happen for:

Enterprise IT

Web Services

Enterprise IT

- Enterprise computing refers to business-oriented information technology that is critical to a company's day-to-day operations.
- One key aspect of enterprise computing is its high availability, as crash of a hardware or software component can lead to loss of revenue and customer base.
- Thus, multiple redundant computers exist for mission critical applications, as well as regular data backups are taken to ensure that there is no single point of failure within an enterprise.
- Nowadays, IT is the lifeblood of successful enterprise.

Web Services

- A Web service is an interface described by some form of service from a remote provider.
- These evolved from client-server and distributed computing concepts, to offer a "Web of Services," such that distributed applications can be assembled from a Web of software services in the same way that Websites are assembled from a Web of HTML pages.
- The advent of the Internet is based on a set of open standards, some of which are:

1. **TCP/IP**: Transmission Control Protocol/Internet Protocol, for network applications to exchange data packets in real time. Data is packed in byte packages, ranging up to 64 K (65,535 bytes). These are sent and acknowledged and, if not acknowledged, then sent again with multiple retries, until each packet arrives at the destination. These packets are then reassembled to create a complete copy of the information content in whole.
2. **RPC**: Remote Procedure Call allows functions written in C, Java, or any other procedural languages to involve each other across a network, allowing software services to reach other servers across the network.

Web Services

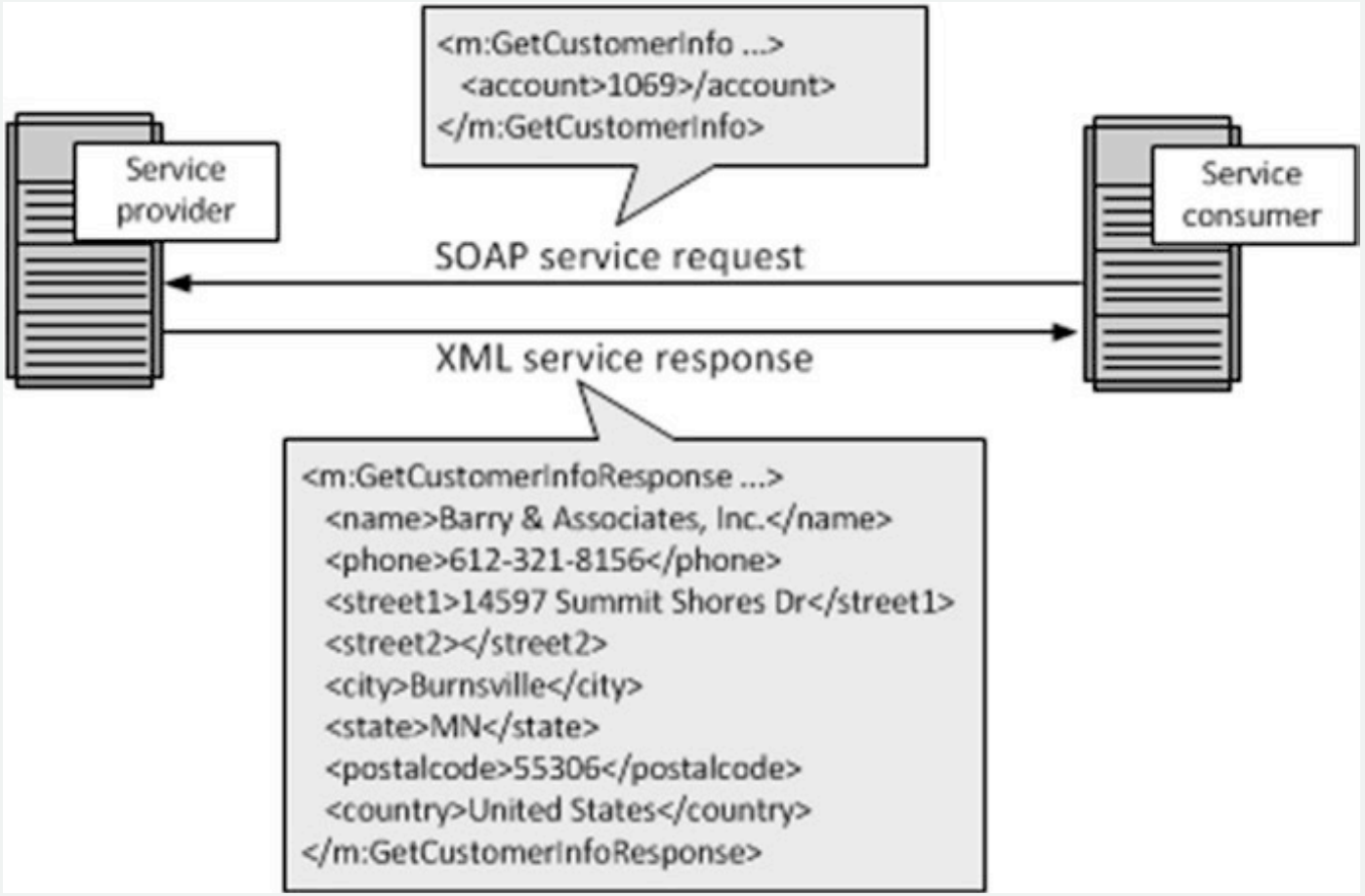
- The advent of the Internet is based on a set of open standards, some of which are:

3. **HTTP**: Hypertext Transport Protocol, for sharing data between machines based on top of TCP/IP protocol.
4. **HTML**: Hypertext Markup Language, the format for representing data in a browser-friendly manner.
5. **XML**: It stands for Extensible Markup Language. It enables any data to be represented in a simple and portable way. Users can define their own customized markup language, to display documents on the Internet.

Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

6. **SOAP**: Service-Oriented Architecture Protocol, for connecting computers. It allows message passing between endpoints and may be used for RPC or document transfer. These messages are represented using XML and can be sent over a transport layer, e.g., HTTP or SMTP. An example of communication using SOAP and XML is shown in Figure.



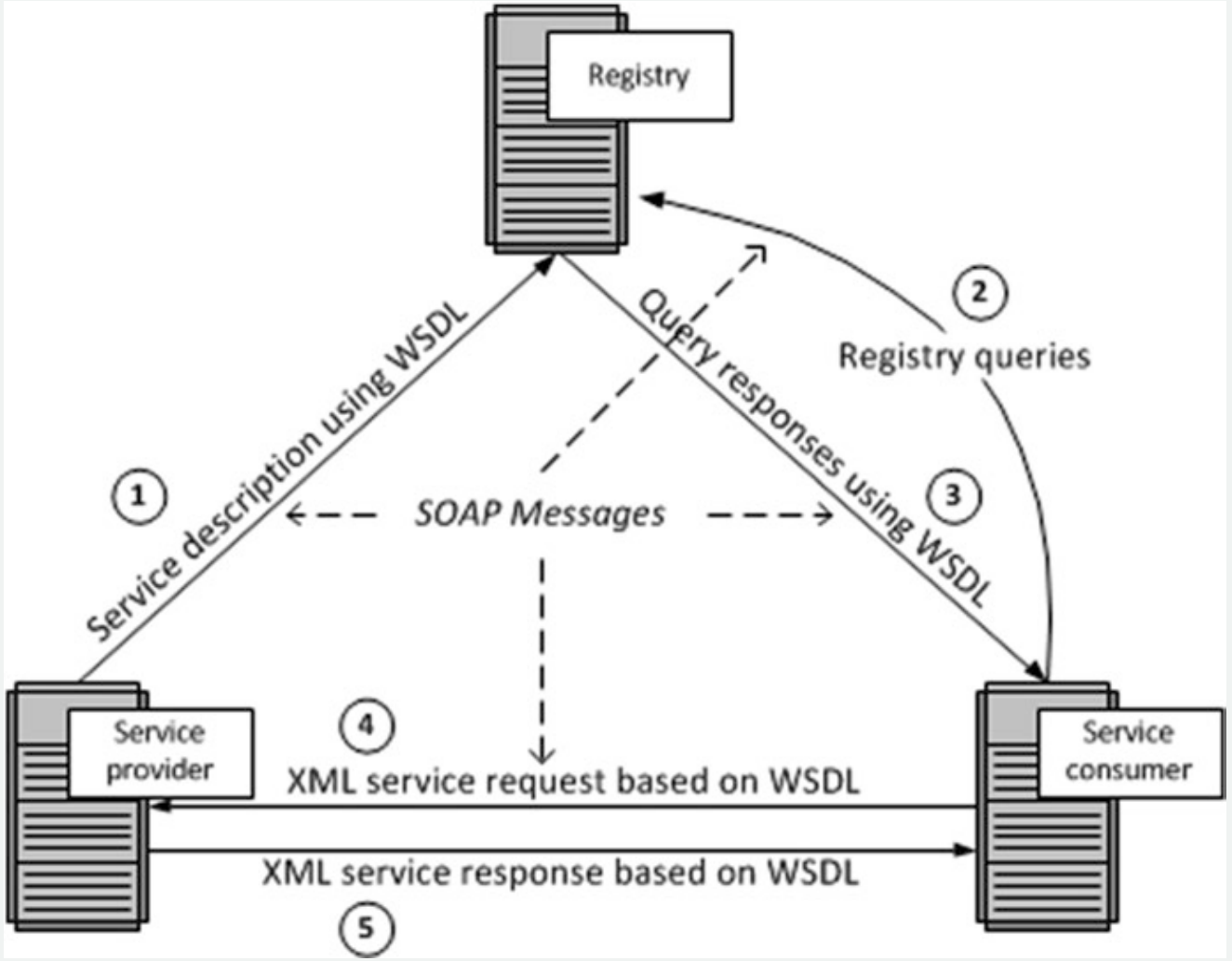
Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

7. **UDDI**: Universal Description, Discovery, and Integration is an XML-based registry for businesses to list themselves on the Internet. It can streamline online transactions by enabling companies to find one another on the Web and make their systems interoperable for e-commerce.
8. **WSDL**: Web Services Description Language is used to describe a Web service in a document. It uses an XML format for describing network services as a set of end points operating on messages. These can contain either document-oriented or procedure-oriented information. The operations and messages are described abstractly and then bound to a concrete network protocol and message format to define an end point. The Web Services Description Language (WSDL) forms the basis for the original Web Services specification.

Web Services

- Message Protocol using WSDL



Web Services

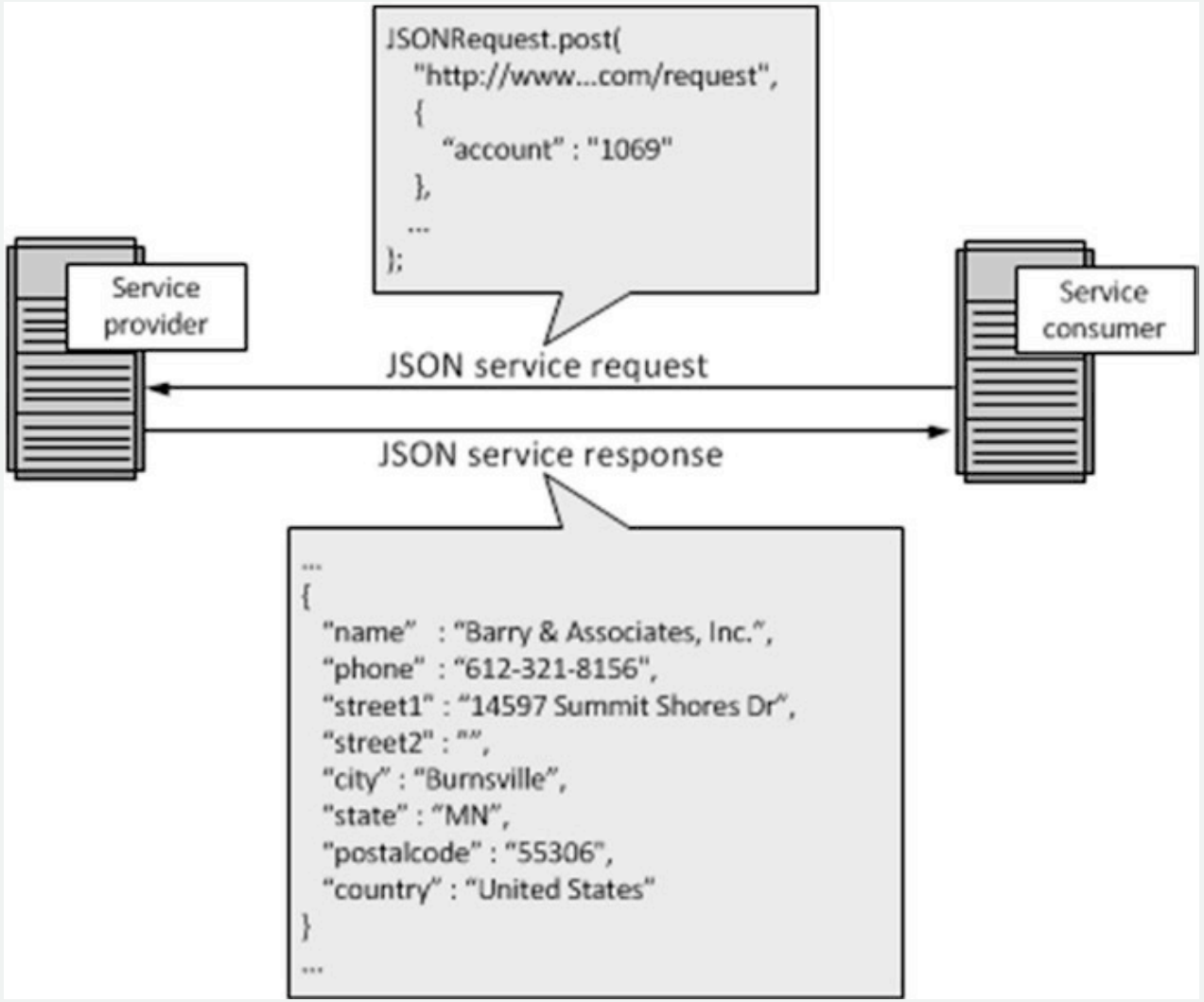
- The advent of the Internet is based on a set of open standards, some of which are:

9. **REST**: Representational State Transfer is a protocol used to create and communicate with the Web services. REST is language independent. Developers prefer REST due to a simpler style that makes it easier to use than SOAP. It is less verbose so less data wrappers are sent when communicating. An interaction is illustrated in Figure.

Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

10. **JSON**: JavaScript Object Notation uses a subset of JavaScript. An example is shown in Figure. It uses name/value pairs and is similar to tags used by XML. Also, like XML, JSON provides resilience to changes and avoids the brittleness of fixed record formats. These pairs do not need to be any specific order.



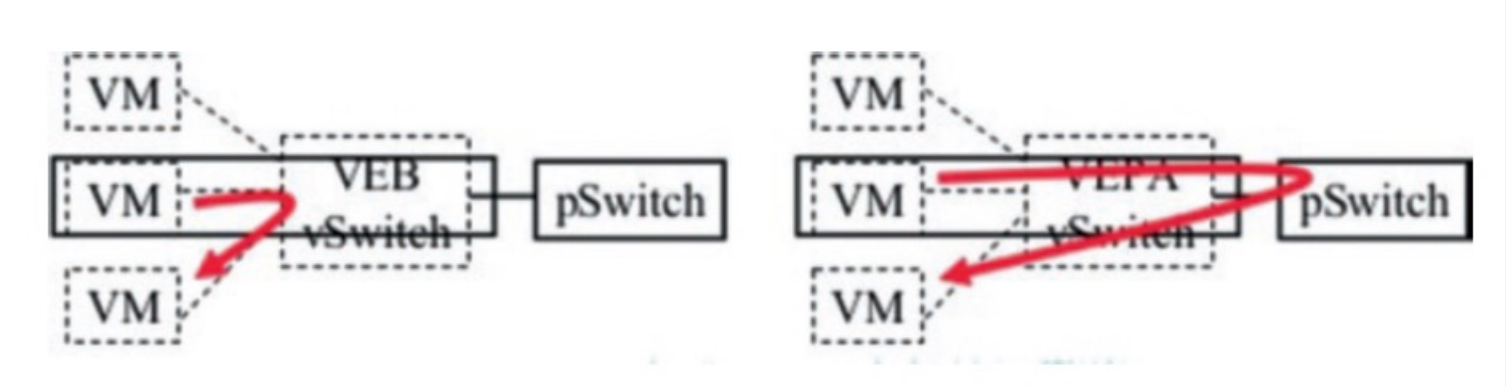
Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

11. **DCB**: Datacenter Bridging (DCB) is a set of enhancements to the Ethernet protocol for use with clustering and storage area networks. Ethernet was originally designed to be a best-effort-based network, which can experience packet loss when the network or devices are preoccupied. TCP/IP adds end-to-end reliability to Ethernet but lacks the finer granularity to control the bandwidth allocation. This is especially required with a move to 10 Gbit/sec and even faster transmission rates, as such a network pipe can't be utilized fully by TCP/IP. DCB eliminates loss due to queue overflows (hence, called lossless Ethernet). It also includes a Priority-based Flow Control (PFC), an IEEE 802.1 standard that provides a link-level control mechanism.

Web Services

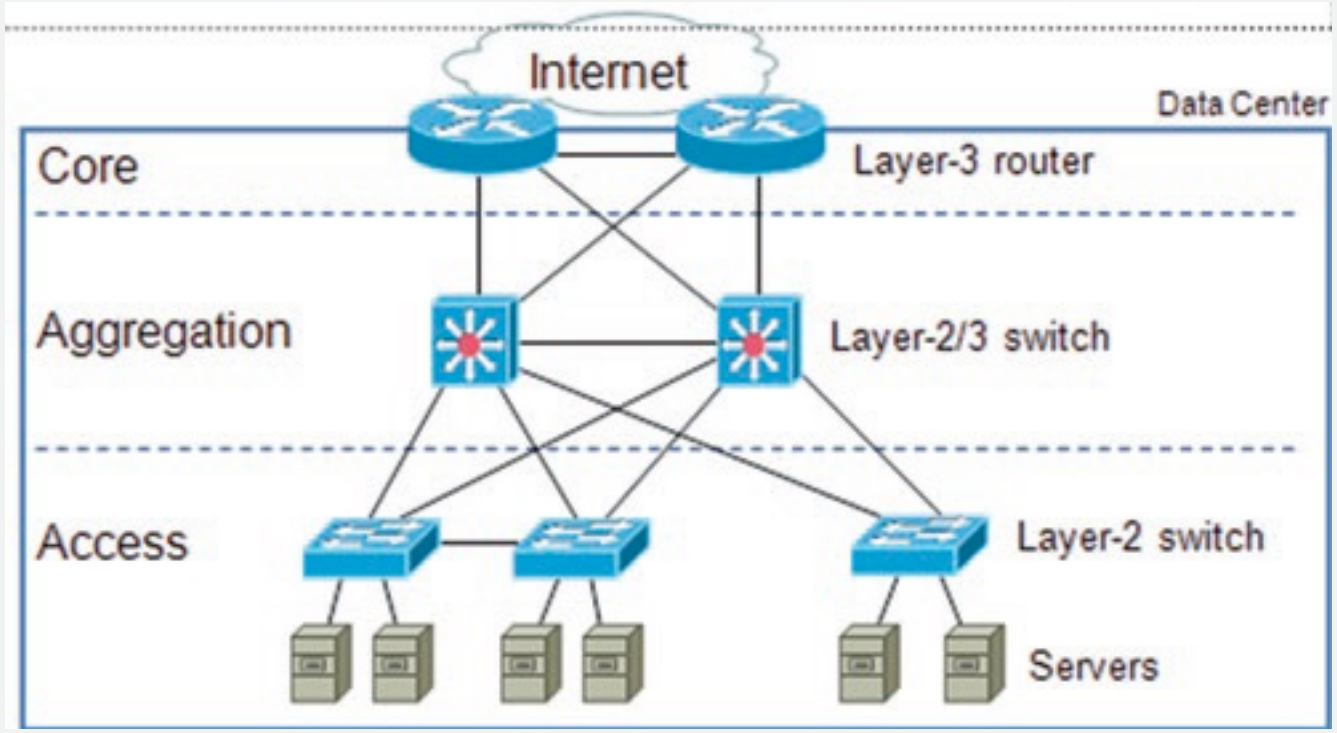
- Two methods for inter-VM communications



1. *Virtual Edge Bridge (VEB):* Switch internally in a VMM using CPU instructions.
2. *Virtual Ethernet Port Aggregator (VEPA):* An external switch that could be in a network interface card.

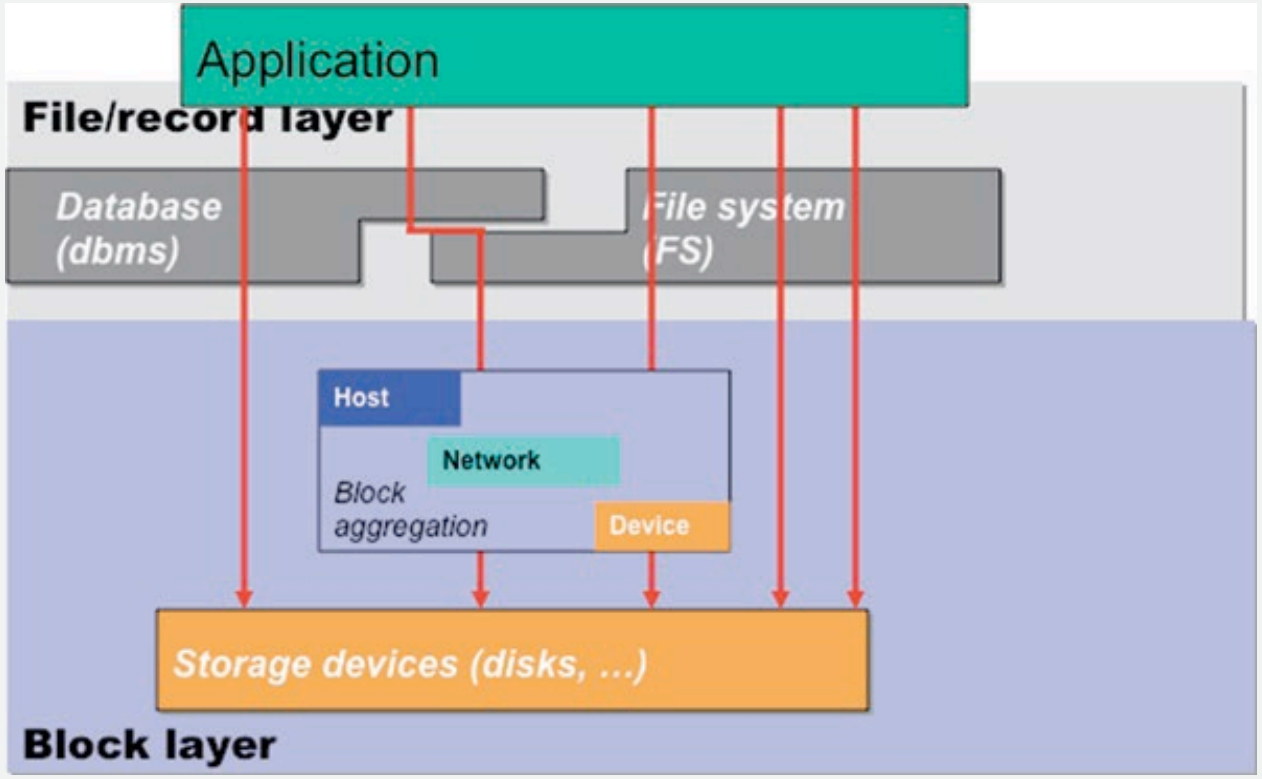
Server Operations in a Data Center

- The server stores or has access to a database, for which clients initiate queries from terminals.
- To support many servers in one place, in turn serving many users spread across a large area, one needs a lot of servers, routers, and switches. These server clusters are also called data centers (DCs).



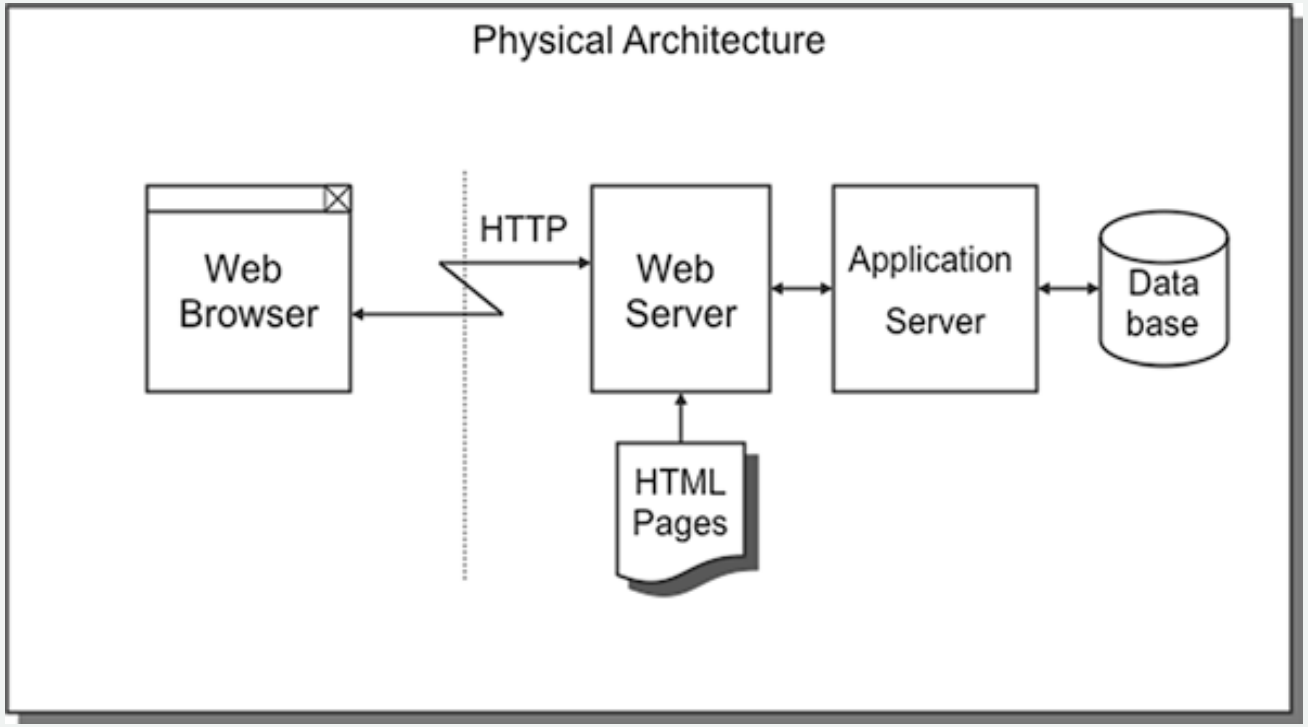
Server Operations in a Data Center

- These servers need to have massive storage, connectivity, and traffic management capability using switches. Of these, storage is a key capability required to provide large amounts of data needed by remote users, for which SNIA (Storage Networking Industry Association) has recommended storage architecture, as depicted in Figure.



Server Operations in a Data Center

- Web services are provisioned from a client's browser to access applications and data resident on remote servers in a remote data center. Figure represent this linkage.



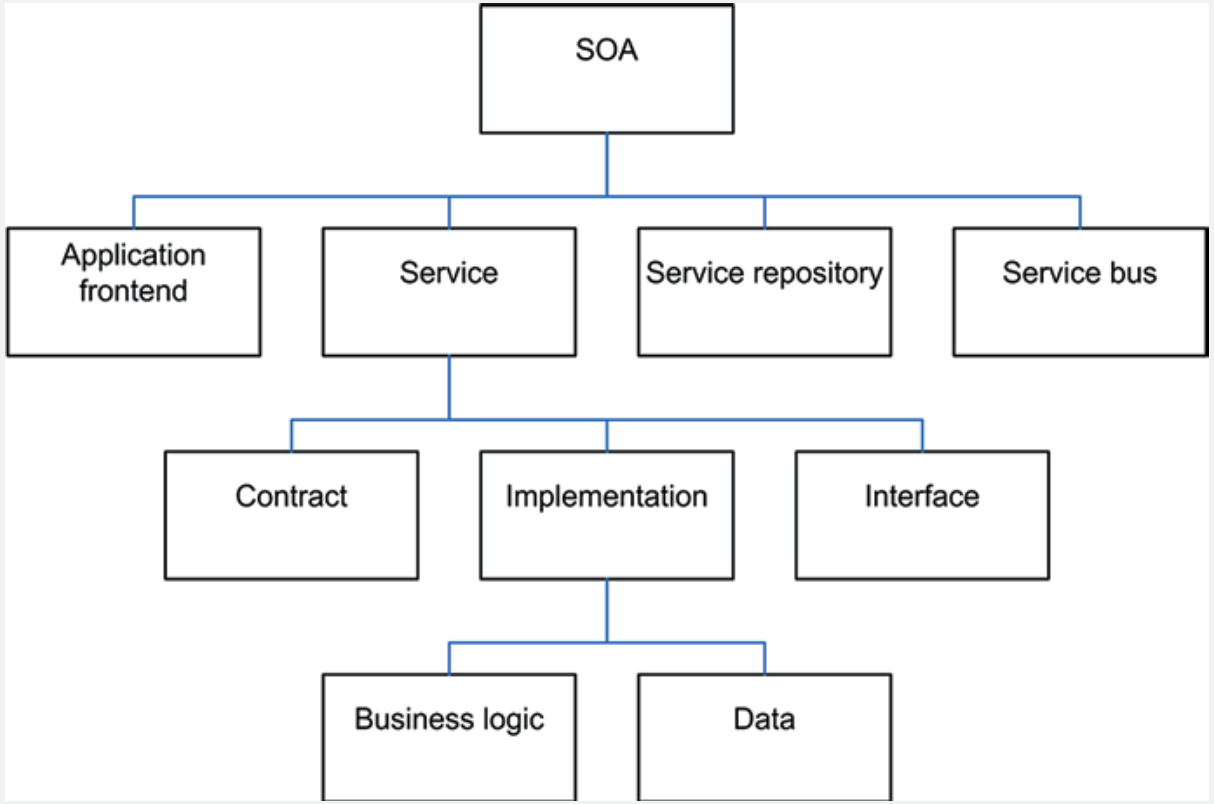
Evolution of Service-Oriented Architecture

- **A service-oriented architecture (SOA)** is a style of software design where services are provided to the other components by **application components**, through a **communication protocol** over a network.
- SOA is composed of loosely coupled set of services with well-defined interfaces. These services communicate with each other and are used for building higher-level applications.
- A service has four properties according to one of the many definitions of SOA:

1. It logically represents a business activity with a specified outcome.
2. It is self-contained.
3. It is a black box for its consumers.
4. It may consist of other underlying services.

Evolution of Service-Oriented Architecture

- Different services can be used in conjunction to provide the functionality of a large software application. So far, the definition could be a definition of modular programming in the 1970s. Service-oriented architecture is about how to compose an application by integration of distributed, separately maintained, and deployed software components, as shown in Figure.

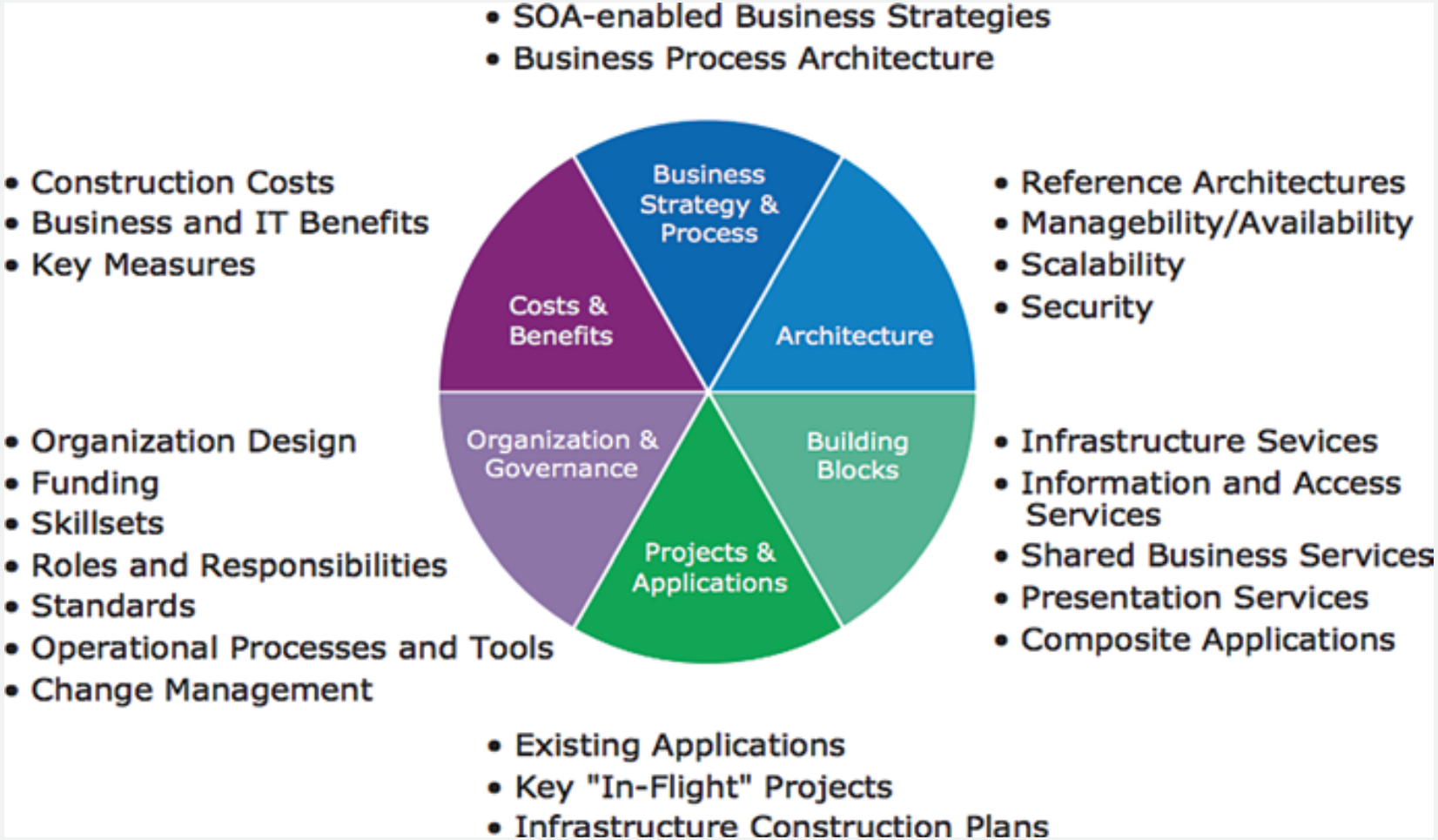


Evolution of Service-Oriented Architecture

- By organizing enterprise IT around services instead of around applications, SOA provides the following key benefits:
- Improves productivity, agility, and speed for both business and IT
- Enables IT to deliver services faster and align closer with business
- Allows the business to respond quicker and deliver optimal user experience

Evolution of Service-Oriented Architecture

- Six SOA Domains as Follow:



Transition from SOA to Cloud Computing

- SOA accelerates and supports Cloud Computing through the following vectors:

1. Faster application development
2. Reuse of services
3. Reduction of application maintenance
4. Reduced integration costs
5. Support of application portfolio consolidation

Basic Concept of Cloud Computing Security

- The previously defined Cloud Computing business models and implementation architectures have extended access to a wide variety of capabilities. Consequently, its security needs have also extended beyond the basic information security issues.
- However, basic security concepts still apply. Information security or INFOSEC begins with access control.
- Access control is based upon identity authentication.

  The entity to be identified can be a person, a device, or a computational process.
- These factors involve answering the four key questions of identity authentication:

1. What you have?
2. What you know?
3. What you are?
4. Where you are?

Basic Concept of Cloud Computing Security

- The next category of security for Cloud Computing is protecting information both during transmission and during storage.
- Protection of information includes keeping secrets and private data away from unauthorized entities, preventing changes by unauthorized entities, and detection of attempts at tampering with the data.
- Separate from security is the detection of errors due to transmission noise or equipment problems.
- While access control and information protection are required for preventing security breaches, some security attacks will occur.
- The detection of positional attacks and an appropriate response mechanism is required.

CLOUD COMPUTING PYRAMID

I Gde Dharma Nugraha

Outlined

- Roots of Cloud Computing
- Essential Characteristics of Cloud Computing
- Role of Virtualization
- Cloud Players and Their Concern
- Considerations for Cloud Data Centers

Roots of Cloud Computing

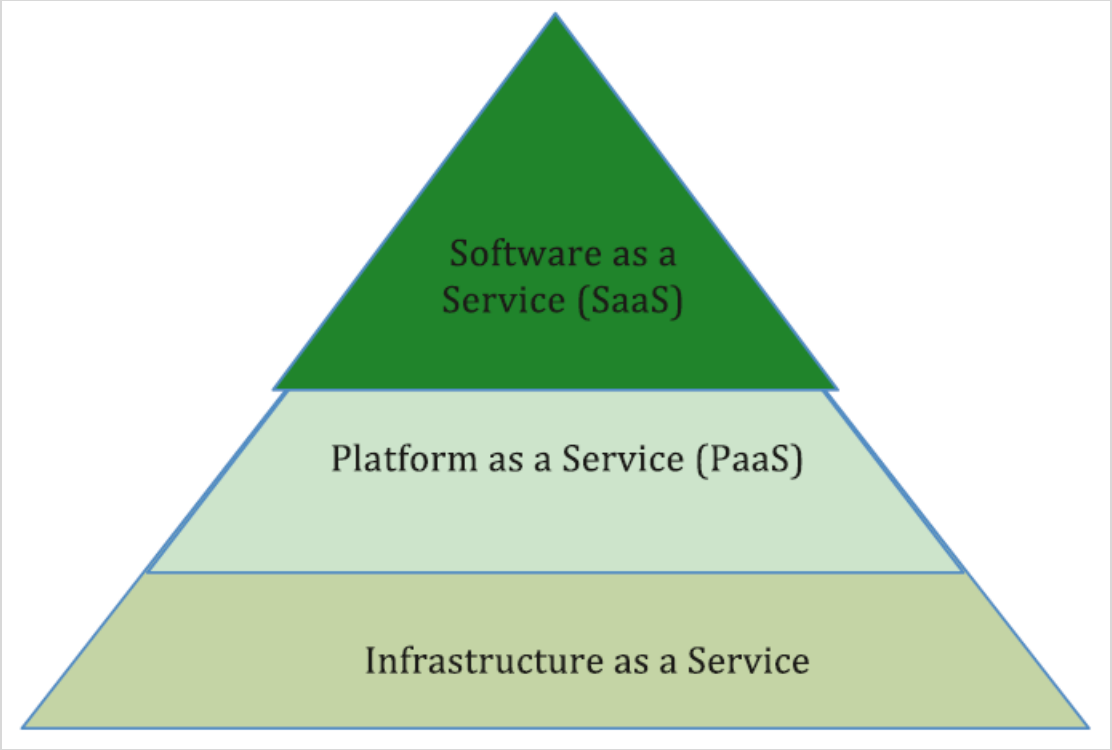
- "Cloud Computing" term became popular about two decades ago. However, its roots extend at least half a century back when users sat in front of blinking terminals far away from mainframe computers connected via cables.
  - Telecommunication engineers about a century ago used Cloud concepts.
- The following list briefly explains the evolution of Cloud Computing:
  - Grid computing: Solving large problems using parallelized solutions, e.g., in a server farm
  - Utility computing: Computing resources offered as a metered service
  - SaaS: Network-based subscriptions to applications
  - Cloud Computing: "Anytime, anywhere" access to IT resources delivered dynamically as a service

Roots of Cloud Computing

- The NIST (National Institute of Standards and Technology) in the USA has defined Cloud Computing as "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."
- This Cloud model is composed of five essential characteristics, three service models, and five deployment models.

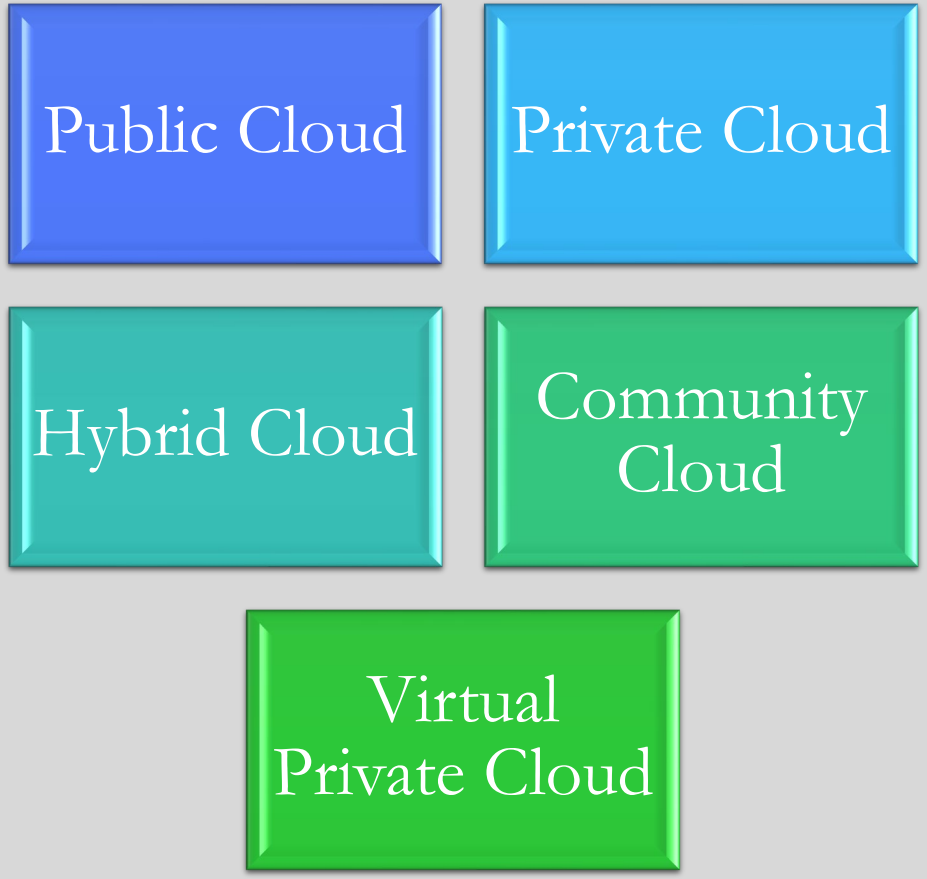
Roots of Cloud Computing

- The three service models of NIST:



Roots of Cloud Computing

- Five deployment model of NIST:



Essential Characteristics of Cloud Computing

- According to NIST, five characteristics of Cloud are

Essential Characteristics of Cloud Computing

1. ***Rapid Elasticity***: Elasticity is defined as the ability to scale resources both up and down as needed. To the consumers, the Cloud appears to be infinite, and they can purchase as much or as little computing power as they need. This is one of the essential characteristics of Cloud Computing in the NIST definition.
2. ***Measured Service***: In a measured service, aspects of the Cloud service are controlled and monitored by the Cloud provider. This is crucial for billing, access control, resource optimization, capacity planning, and other tasks.

Essential Characteristics of Cloud Computing

3. *On-Demand Self-Service*: The on-demand and self-service aspects of Cloud Computing mean that a consumer can use Cloud services as needed without any human interaction with the Cloud provider.
4. *Ubiquitous Network Access*: Ubiquitous network access means that the Cloud provider's capabilities are available over the network and can be accessed through standard mechanisms by both thick and thin clients.

Essential Characteristics of Cloud Computing

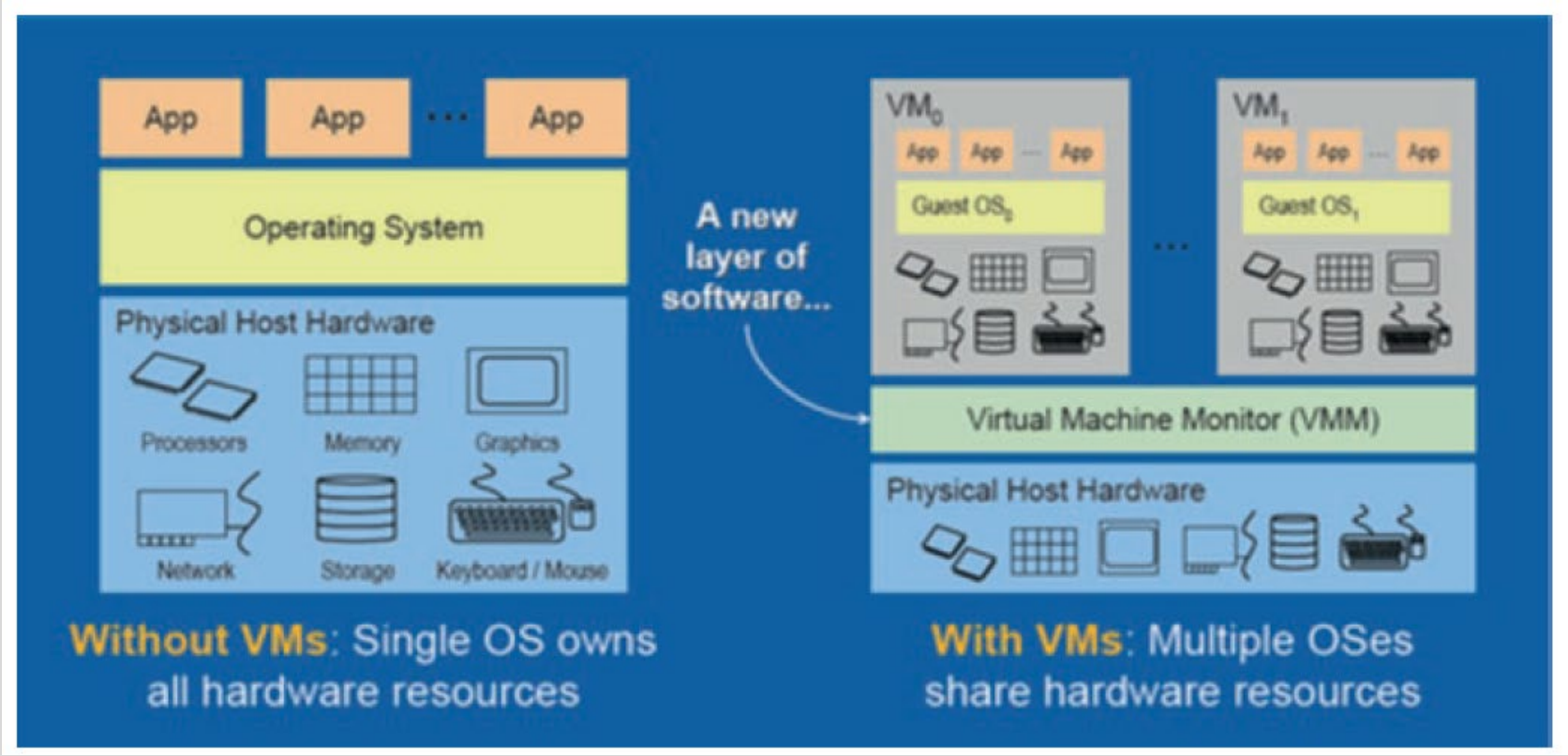
5. ***Resource Pooling:*** Resource pooling allows a Cloud provider to serve its consumers via a multi-tenant model. Physical and virtual resources are assigned and reassigned according to consumers' demand. There is a sense of location independence in that the customers generally have no control or knowledge over the exact location of the provided resources but may be able to specify a geographical location (e.g., country, state, or data center).

Role of Virtualization

- Virtualization is the technology enabler of sharing data center's resource among many different users.
- Virtualization refers to the act of creating a virtual image of the computer hardware, including CPU, memory, storage, and network elements.
  - It is done to isolate the software stack from the underlying hardware.
- Virtualization makes each user feel that he or she has full access and control of the machine.

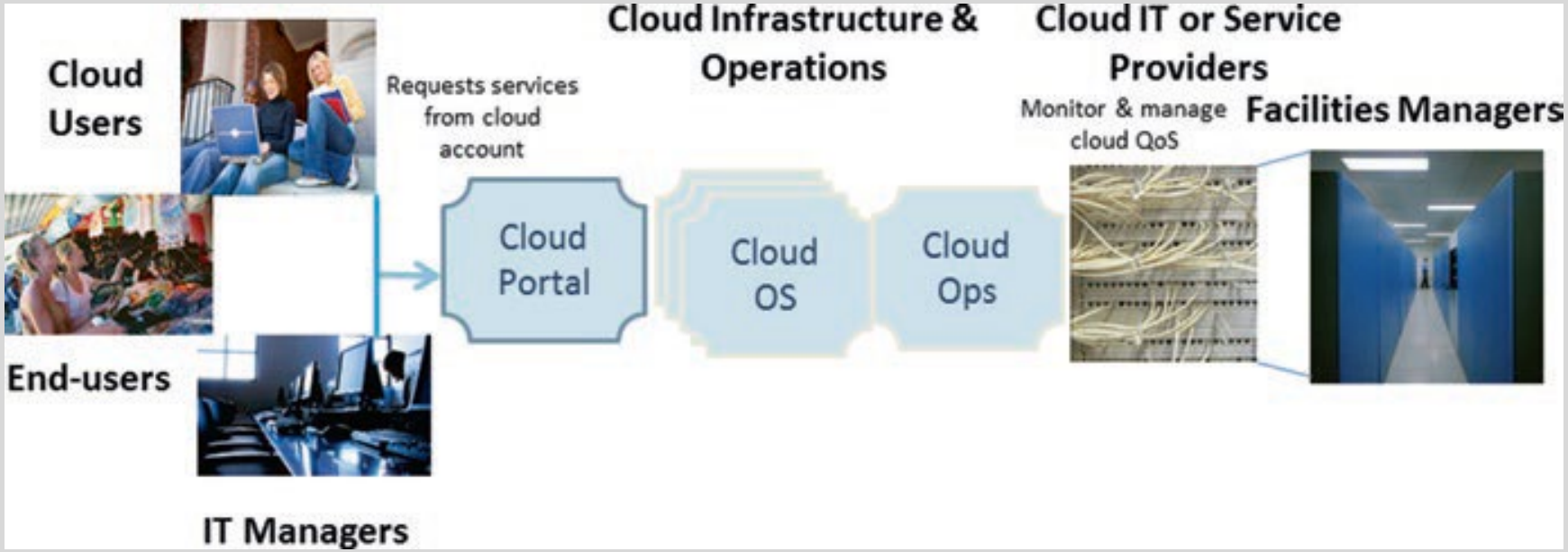
Role of Virtualization

- An OS vs a Virtualization Stack



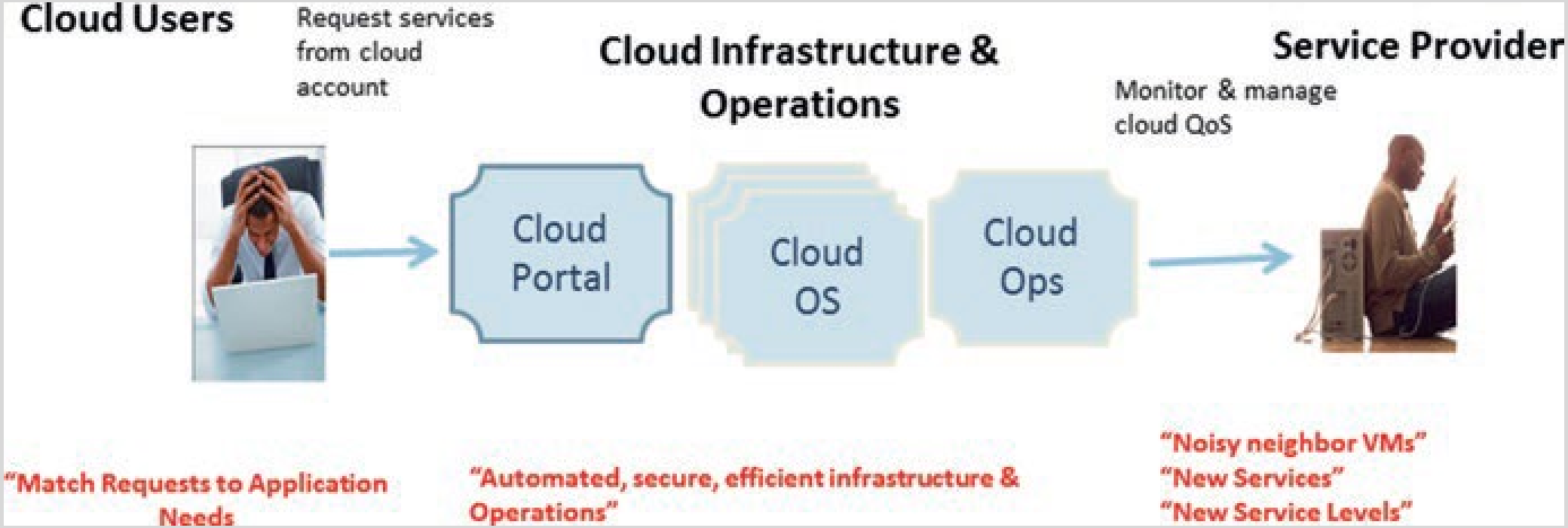
Cloud Players and Their Concern

- In a typical Public Cloud, the following actors are involved



Cloud Players and Their Concern

- Pain points in the Cloud



Considerations for Cloud Data Centers

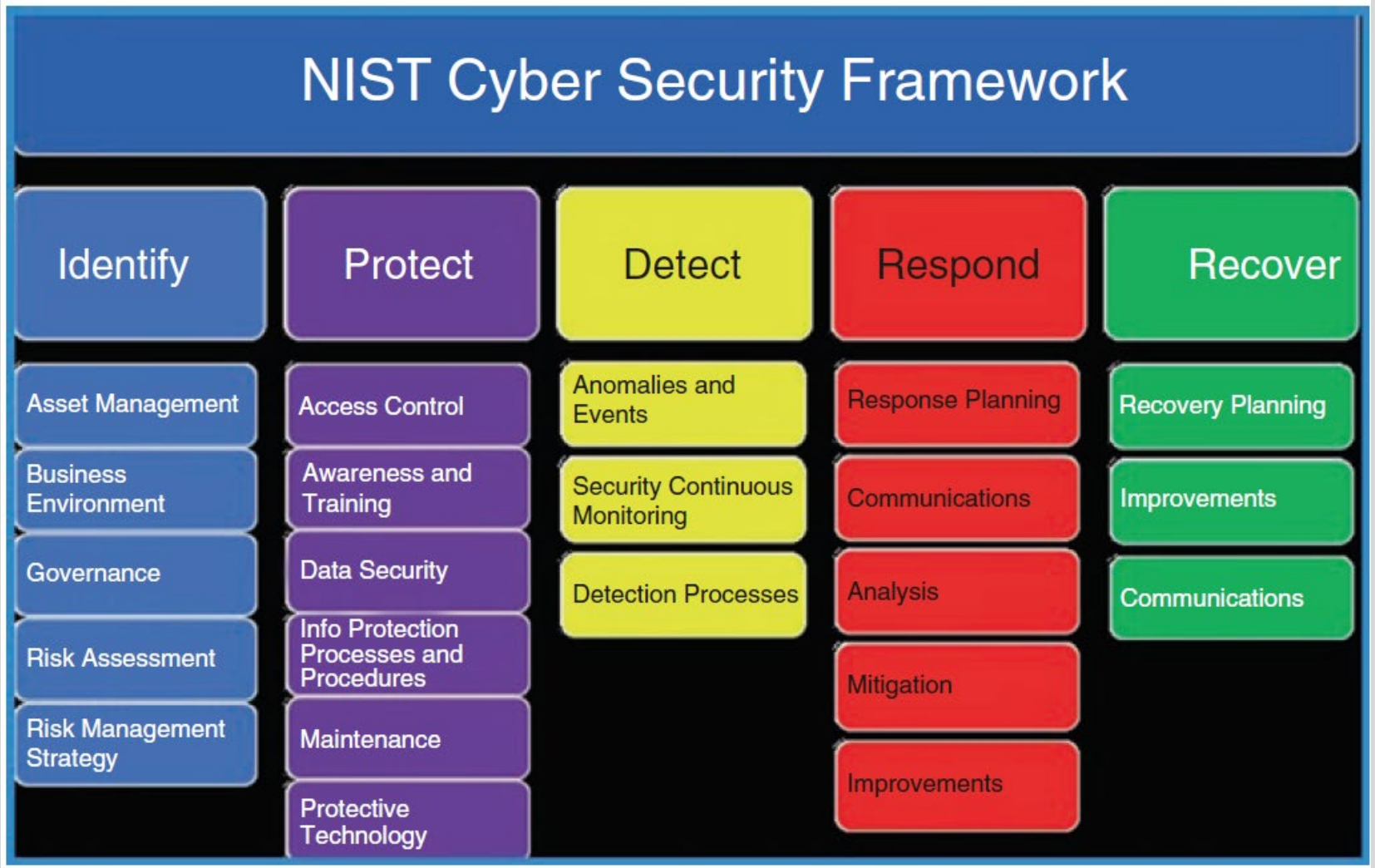
- A major consideration in selecting a Cloud service provider is the service-level agreements (SLA).
- SLAs define measurable considerations, such as listed below:
  1. Response time
  2. Output bandwidth
  3. Number of active servers to monitor for SLA violations
  4. Changes in the environment and
  5. Responding appropriately to guarantee quality of service

Considerations for Cloud Data Centers

- Migration
  - Another challenge is migrating traditional workloads that require computer clusters such as HPC (high-performance computing) workloads from captive data centers to a Cloud.
- Performance
- Security

Considerations for Cloud Data Centers

- NIST Cyber Security Framework



Considerations for Cloud Computing Data Centers

- Five functions of NIST cyber security framework include:
  1. ***Identify***: Develop an organizational understanding to manage cyber security risk to systems, people, assets, data, and capabilities.
  2. ***Protect***: Develop and implement appropriate safeguards to ensure delivery of critical services.
  3. ***Detect***: Develop and implement appropriate activities to identify the occurrence of a cyber security event.
  4. ***Respond***: Develop and implement appropriate activities to take action regarding a detected cyber security incident.
  5. ***Recover***: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident.

Questions?

Cloud Workload Characterization and Monitoring

I Gde Dharma Nugraha

Agenda

Motivation

Background on Workload Characterization

Top-Level Cloud Workload Categorization

Cloud Workload Categories

Low-Level or Hardware Metrics of Computer Utilization

Cloud Management Requirements

Motivation

- Evolution of Cloud services which has different workload challenges.
- Each player in the Cloud has different business and technical needs.
- Therefore, each player has a different viewpoint regarding their Cloud Services' workload.

Background on Workload Characterization

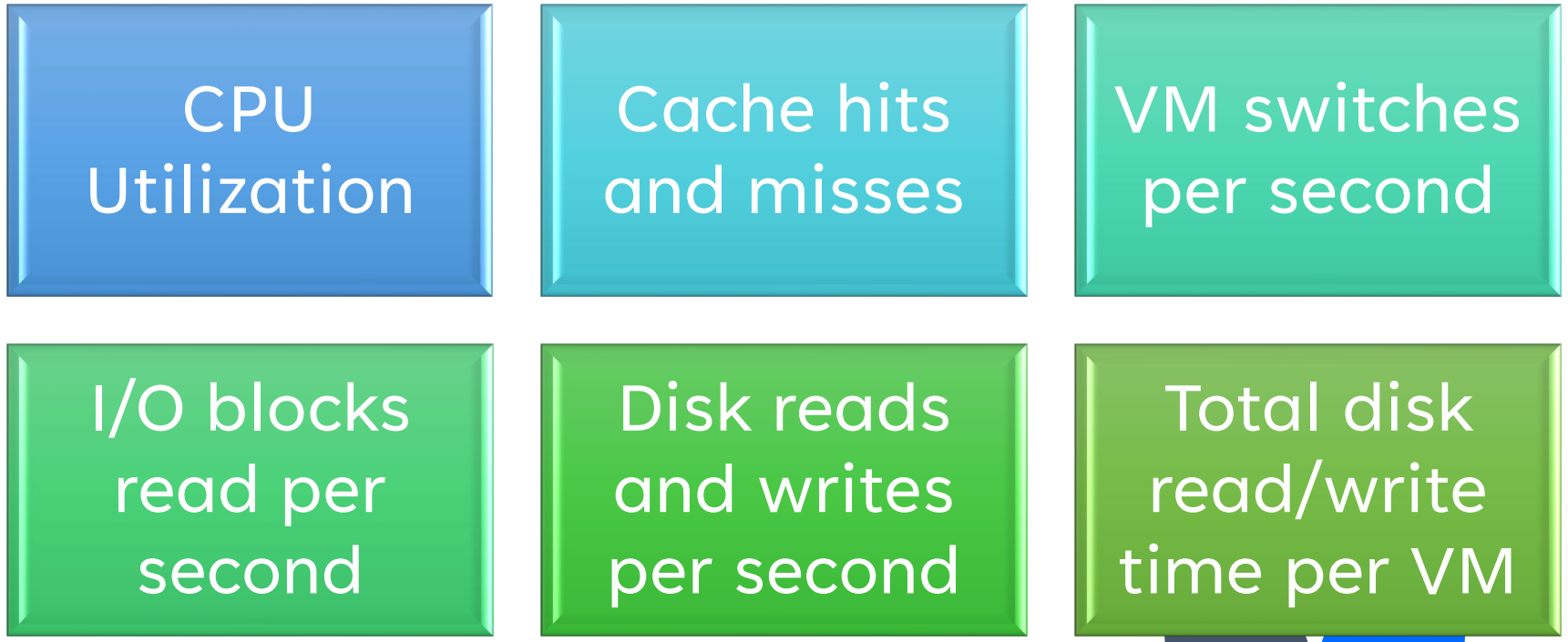
- Characterization of computer workloads has been extensively studied with many practical applications.
- Several existing studies for workload characterization have used targeted benchmarks for resource utilization.
- Jackson et al. evaluate the performance of HPC applications on Amazon's EC2 to understand the trade-offs in migrating HPC workloads to Public Cloud.
- Xie and Loh studied the dynamic memory behavior of workloads in a shared cache environment.

Background on Workload Characterization

- Xie and Loh grouped workloads into four classes:
  1. Applications that do not make much use of the cache (turtle)
  2. Applications that are not perturbed by other applications (sheep)
  3. Applications that are sensitive and will perform better when they do not have to share the cache (rabbit)
  4. Applications that do not benefit from occupying the cache and negatively impact other applications (devil)

Background on Workload Characterization

- Koh et al. [20] studied hidden contention for resources in a virtualized environment.

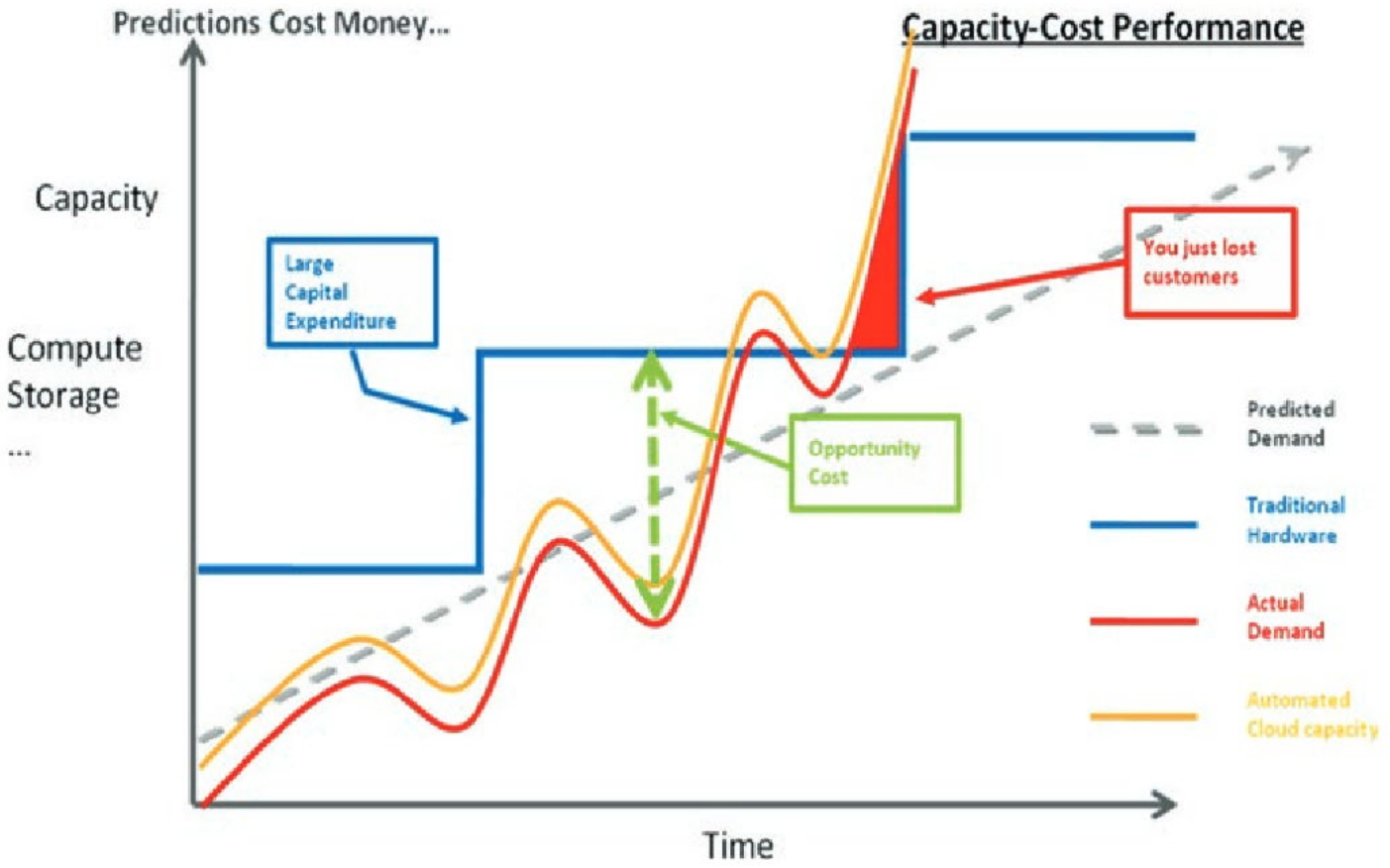


Top-Level Cloud Workload Categorization

- Cloud Computing users have a variety of needs and wants.
- Cloud Computing platform (or services) suppliers have resource choices for allocation, planning, purchasing, and pricing.
- Workload categories can be split in two ways:
  - Static architecture
  - Dynamic behavior
- Also:
  - Interactive
  - Batch-mode jobs

Top-Level Cloud Workload Categorization

- Considerations:



Cloud Workload Categories

Big Streaming Data	Big Database Calculation	Big Database Access	Big Data Storage	Many Tiny Tasks (ants)
Tightly coupled calculation intensive HPC	Highly Interactive Single Person Tasks	Highly interactive multi-person jobs	Single compute intensive jobs	Private local tasks
Slow communication	Real-time local tasks	Real-time geographically dispersed tasks,	Access Control	Voice or Video over IP

Computing Resources

Persistent Storage

Compute power/Computational Capability

Network bandwidth

Broadcast transmission receivers

Data buses within a server

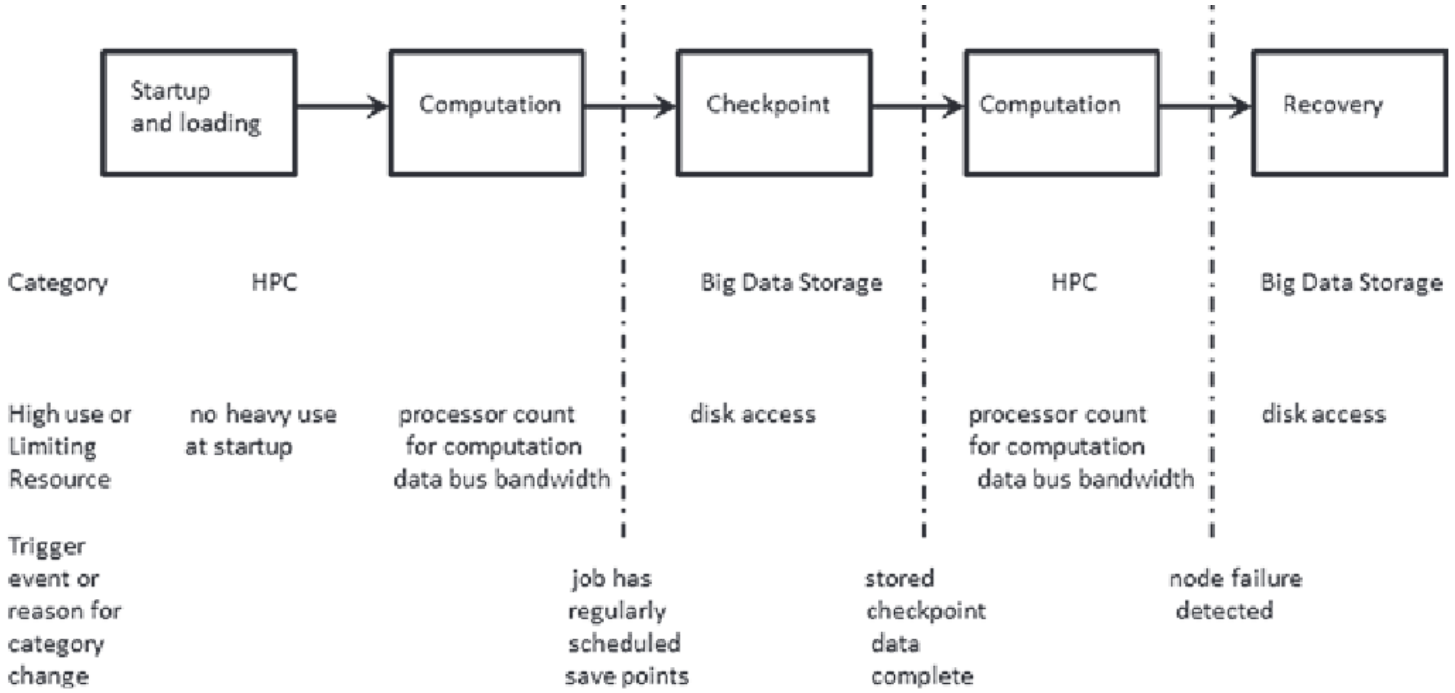
- USB
- Network Types
- Cache memory
- Software capability
- Main Memory

Temporal Variability of Workloads

- There are two different cases in which the workload category would change.
  - when a job's next step or phase is a different category than the current one.
  - when the job is incorrectly categorized.

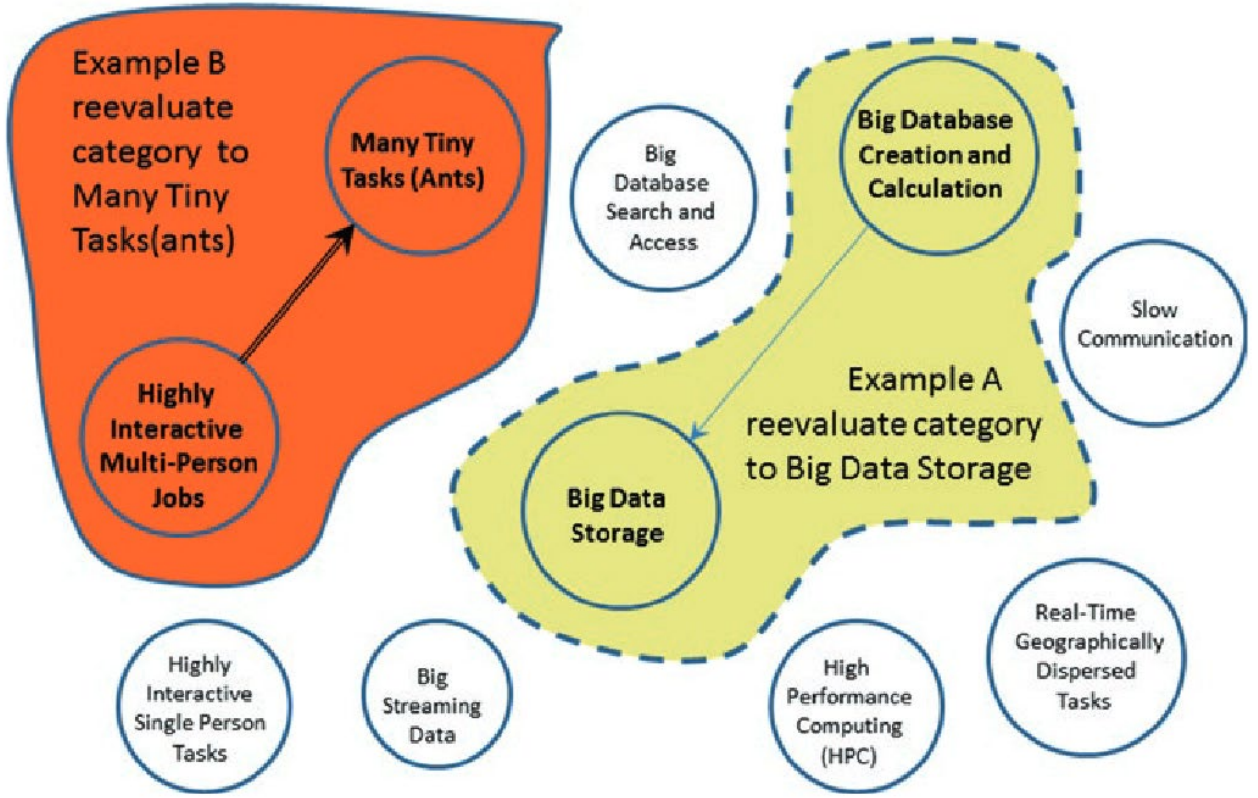
Temporal Variability of Workloads

Example of the changing Cloud Workload categories for HPC Job



Temporal Variability of Workloads

Example of miscategorized workloads



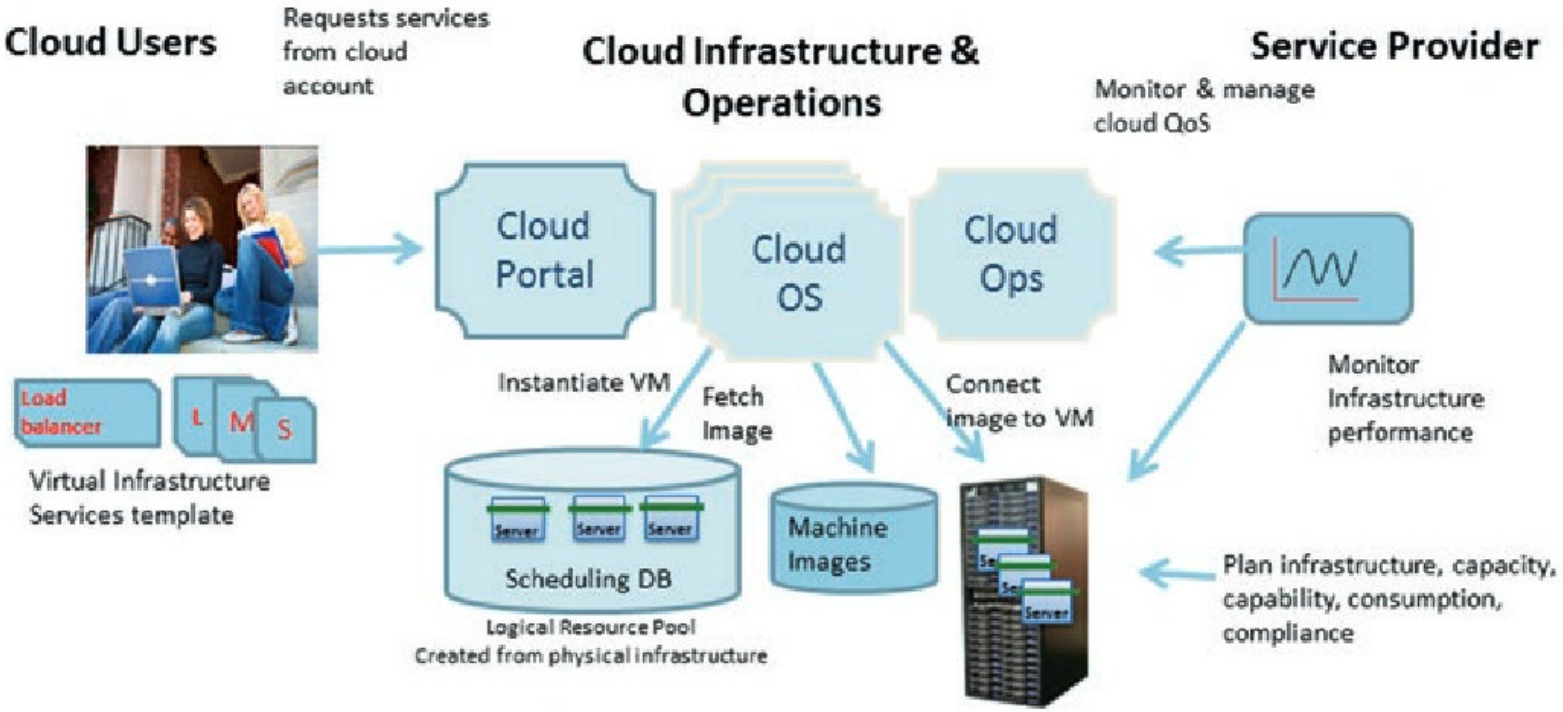
Low-Level or Hardware Metrics of Computer Utilization

Intel's VTune Amplifier XE documentation provides a fair amount of details about performance counters:

- Instruction per Cycle (IPC)
- LLC misses
- L1 data cache misses
- Cycles for which Instruction Queue is Full
- L1 Instruction Cache Misses
- Cycles during which reservation stations are full
- Number of lines fetched from memory

Benefits to Cloud Service Providers

SLA and QoS in IaaS Cloud. Cloud OS can benefit from fine-grained platform resource monitoring and controls to assure predictable performance and efficient and secure operations



Cloud Management Requirements

- Cloud management tools can be of two types: in-band (IB) or out-of-band (OOB).
  - In-band refers to an agent that typically runs in an OS or VM, collects data, and reports for monitoring purposes. However, it may interfere with other processes running in that VM, slowing it down or creating additional resource contentions.
  - OOB refers to monitoring tools that typically use a baseboard management controller with a processor and memory system to observe the main server's health metrics.

Monitoring Metrics

Metrics name	Description	Units
CPUUtilization	The percentage of allocated compute units	*Percent*
DiskReadOps	Completed read operations from all disks available to the VM	*Count*
DiskWriteOps	Completed write operations to all disks available to the VM	*Count*
DiskReadBytes	Bytes read from all disks available to the VM	*Bytes*
DiskWriteBytes	Bytes written to all disks available to the VM	*Bytes*
NetworkIn	The number of bytes received on all network interfaces by the VM	*Bytes*
NetworkOut	The number of bytes sent out on all network interfaces by the VM	*Bytes*

Monitoring Metrics

Frequency

Monitored resources	Frequency
VM instance (basic)	Every 5 minutes
VM instance (detail)	Every 1 minute
Storage volumes	Every 5 minutes
Load balancers	Every 5 minutes
DB instance	Every 1 minute
SQS queues	Every 5 minutes
Network queues	Every 5 minutes

Some Example of Monitoring Tools

Amazon Cloud Watch

Nagios

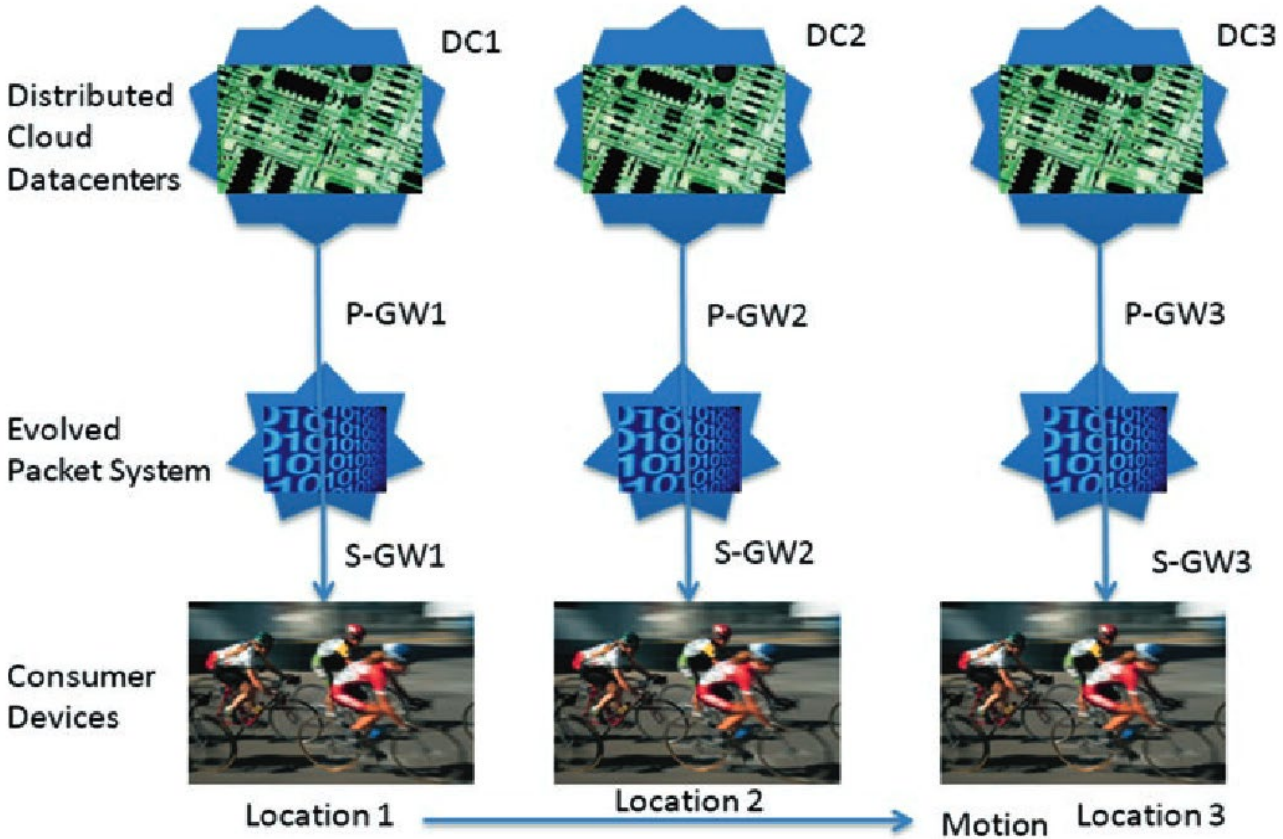
New relic

Follow-ME Cloud

- Major consumers of Public Cloud services are the numerous mobile user devices, with their needs of live video calls and always-connected social networks, with minimal latency requirements.
- However, these users are not stationary. A need to provide them with continuous IP (Internet Protocol)-based services while optimizing support from the nearest data center is nontrivial.
- The ability to smoothly migrate a mobile user from one data center to another in response to the physical movement of a user's equipment without any disruption in the service, is called Follow-ME Cloud (FMC)

Follow-ME Cloud

- Migration of a user's with changes in location




thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
merci
obrigado
dziękuję
bedankt
спасибо
sukriya
kop khun krap
go raibh maith agat
mochchakkeram
tapadh leat
arigatō
takk
dakujem
grazie
terima kasih
감사합니다
ευχαριστώ
мерси
sagolun
mauruuru
hvala
dank je
рахмат
Баярлалаа
ありがとう
хвала
blagodaram
faafetai lava
kiitos
dankie
misaotra
matondo
paldies
asante
manana
djiere dieuf
mamnun
tanemirt
rahmet
dhanyavadagalu
shukriya
xiexie
diolch
trugarez
enkosi
sobodi
dekuji
mesi
najis tuke
gracies
sulpay
taiku
spas
tack
welalin
barka
mersi
vinaka

Cloud Computing dan Keamanan Informasi.

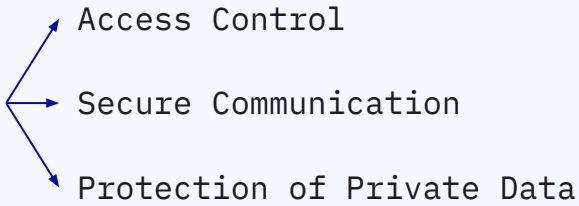
Kelompok G:
Edgrant H. S. (2206025016)
Andikha Wisanggeni (2106731503)
Fayza Nirwasita (2106635700)
Fairuz Muhammad (2206814324)

Table of contents

01

Information Security

Information Security



Access Control

- Memastikan akses yang sah ke sistem atau data.
- Diimplementasikan pada perangkat keras (misalnya, dongle USB) atau perangkat lunak (misalnya, sistem login, cookie).

Secure Communication

- Melindungi transfer informasi di antara para peserta.
- Sangat bergantung pada enkripsi (manajemen kunci sangat penting).

Protection of Private Data

- Melibatkan pengamanan perangkat penyimpanan, unit pemrosesan, dan memori.

Aspek umum: Kerahasiaan, Integritas, Ketersediaan (CIA keamanan).

Security Challenges

Weak Points

Ditentukan oleh faktor teknis (panjang kata sandi) dan penerimaan pengguna (autentikasi yang rumit).

Private Data Protection

- Menyeimbangkan ketersediaan dan integritas: Data harus dapat diakses oleh pengguna yang berwenang dengan tetap menjaga keakuratannya.
- Tingkat keamanan bervariasi berdasarkan sensitivitas data (misalnya, membaca iklan vs. aplikasi nuklir).

Cloud Security

Membutuhkan keamanan multi-level karena sumber daya yang digunakan bersama dan beragam aplikasi dengan kebutuhan yang berbeda.

Security Challenges

Environmental Factors Affecting Security

- **Daya komputasi:**
  Peningkatan kapasitas mempercepat kemampuan defensif dan ofensif.
- **Kebutuhan yang terus meningkat:**
  Semakin banyak industri yang membutuhkan data yang aman, termasuk keuangan dan perawatan kesehatan.
- **Berbagi informasi:**
  Penggunaan komputasi awan yang meluas meningkatkan kepentingan keamanan.

02

EVOLUTION OF SECURITY CONSIDERATIONS

Timeline Evolusi

Early Computer Security

- Keamanan fisik adalah metode utama (akses yang besar dan terbatas ke perangkat).
- Perangkat terhubung langsung ke mainframe; kontrol akses masih bersifat dasar (berbasis fisik dan terminal).

Access Control Evolution

- Transisi dari terminal ke PC individual; muncul sistem berbasis ID pengguna dan kata sandi.
- Pengenalan komunikasi melalui saluran telepon dan kontrol akses jarak jauh.

Move to Cloud Computing

- Enkripsi informasi menjadi lebih standar.
- Batas-batas fisik memudar karena pengguna dapat mengakses sumber daya cloud dari mana saja.
- Komputasi awan bertujuan untuk memisahkan penyampaian layanan dari implementasi yang mendasarinya.

Security Challenges

in Cloud Computing

Denial-of-Services (DoS)

Pengguna yang tidak sah dapat membebani layanan secara berlebihan, sehingga menyebabkan kerusakan (misalnya, permintaan web yang berlebihan)

Privacy Concerns

Informasi akses harus dilindungi dari pengungkapan atau penyalahgunaan yang tidak sah.

Security Trade-offs

- Biaya kinerja tinggi untuk enkripsi data penuh, penting untuk data sensitif di Awan Publik.
- Kontrol akses dan kata sandi mungkin cukup untuk perangkat pengguna tunggal.
- Teknik seperti VPN dan pengecekan hash dapat mengamankan koneksi perangkat pribadi ke awan.

Balancing Act

Mempartisi data dan kode sensitif agar dapat berjalan di lingkungan yang aman di dalam Public Cloud untuk menyeimbangkan keamanan dan kinerja.

03

Security Concerns in Cloud Operating Models

Security Concerns in Cloud Operating Models

Varied Security Levels:

Langkah-langkah keamanan bergantung pada tingkat sumber daya pengguna di tingkat Cloud.

Data Security Requirement:

Persyaratan baru memastikan pengguna tidak mengetahui alokasi sumber daya mereka.

Cloud Service Models

Software as a Service (SaaS):

- Tingkat abstraksi tertinggi, berfokus pada replikasi data di beberapa pengguna.
- Memastikan informasi yang dibagikan terlindungi dengan akses layanan tak terbatas.
- Mengelola kapasitas instance aplikasi melalui sumber daya server host.

Platform as a Service (PaaS):

- Menargetkan pengembang aplikasi, menyediakan akses layanan yang ditingkatkan.
- Memanfaatkan inti CPU yang dialokasikan ke server host.
- Mendukung akses utilitas dan komponen, memastikan operasi inti yang aman.
- Memungkinkan desain hosting dan tautan untuk penyedia Public Cloud, memfasilitasi analitik skala besar dan kepuasan sistem berbiaya rendah.

04

Identity Authentication

Identity Authentication in Information Security

Traditional Authentication Elements:

What You Know: Passwords, PINs, personal information (e.g., birthday).

What You Have: Item fisik seperti smart card atau token.

What You Are: Biometric data (e.g., fingerprints, facial recognition).

Password Challenges

- Rentan terhadap serangan brute force.
- Meningkatnya kompleksitas menyebabkan praktik pengguna seperti menuliskan kata sandi, sehingga mempertaruhkan keamanan.

Identity Authentication in Information Security

Information Security Functions:

Access Control: User IDs, encryption, secure communication.

Data Protection: Encryption data pada saat diam dan transit, secure logging.

Metadata Management: Menjamin secure access dan handling metadata.

		Access control	Secure communications	Data protection	Monitoring
Software	User application	Some login, usually relies on lower levels [1]	Usually relies on lower levels of implementation	Encrypt or disguise data [5]	Access logs
	Operating system (OS)	Login [1]	In-memory transactions	[1, 5]	Special processes as watchdogs
	Virtual machine layer (VM)	[1, 5]		[1, 5]	[1]
	Hypervisor layer	[1]		[1]	[1]
	Software drivers	From OS	Encryption, security handshake	Encrypt data	
	BIOS/ FW-based system management layer	Privileged execution		Privileged access to certain memory locations	Log files

Hardware	CPU	From OS	Port and bus encryption, secure caches	Separate secure registers and memory	
	Memory cache/main RAM	Encrypted busses, hash checking tables	Data encryption	Partitioning and encryption	Interrupt logs
	Memory disk	Hash, checking tables [5–8]	USB data encryption	Encrypt disk storage, removable devices	Error logs [9, 10]
	I/O	Verify access ID, such as Internet IP address	Encrypt transmissions; trust keyboard, mouse, and audio	Security handshake, coding, encryption	Watchdog processes in hardware and software

Pertimbangan keamanan bagi para profesional IoT di lingkungan cloud

Keamanan Konten:
Memastikan perlindungan data dan konten di dalam perangkat IoT dan platform cloud.

Keahlian Profesional:
Pentingnya pengetahuan khusus dalam keamanan IoT dan cloud untuk mengatasi tantangan yang unik.

05

Keamanan Transmisi

Enkripsi Data dan Trade-off Keamanan dan Efisiensi

Pentingnya Keamanan Transmisi

- Seberapa aman pun data di dalam sistem, jika data tersebut harus **dipindahkan** ke sistem lain, data tersebut dapat **terancam keamanannya**.
- Saat data dipindahkan, data berada pada lingkungan publik yang **diluar kontrol sistem; keamanan tidak lagi terjamin**.
- Solusinya adalah dengan **mengenkripsi data**.

Trade-off Keamanan dan Efisiensi

Keamanan

Keamanan data tergantung pada enkripsinya. Namun, **bukan berarti kita harus menggunakan enkripsi yang paling kuat**. Enkripsi yang kuat membutuhkan waktu dan **sumber daya yang besar untuk dipecahkan**.

Efisiensi

Keputusan **trade-off** antara keamanan dan efisiensi harus dilakukan dengan mempertimbangkan nilai dan "umur" data.

Contoh Trade-off

Contoh 1

- Pengumuman diplomatik yang akan diumumkan pada **hari berikutnya**.
- Data tersebut memiliki **"umur" yang terbatas**, hanya perlu diamankan selama 2 hari.
- Sehingga, enkripsi yang digunakan **tidak perlu terlalu kuat.**

Contoh 2

- Deskripsi investasi jangka panjang yang memiliki nilai **jangka panjang**.
- Data tersebut memiliki **"umur" yang panjang**, sehingga **enkripsi** yang digunakan harus sangat **kuat**.

06

Penyimpanan dan Komputasi Aman

Trade-off Keamanan dan Efisiensi

Trade-off Keamanan dan Efisiensi

- Konsep trade-off antara keamanan dan efisiensi juga berlaku untuk penyimpanan dan komputasi.
- Sistem dapat memiliki **enkripsi ringan** dan **cepat** untuk data atau enkripsi yang kuat.
- Jenis enkripsi **tergantung dengan keperluan data**.
- Data harus dienkripsi, terutama jika disimpan di **3rd party** storage provider.

Trade-off Keamanan dan Efisiensi

Keamanan

Data yang memiliki "umur" yang **panjang**, seperti film copyright, memerlukan enkripsi yang **kuat**.

Efisiensi

Data yang memiliki "umur" yang **pendek**, seperti data yang disimpan di memori, dapat menggunakan enkripsi yang ringan, memprioritaskan read-write **speed**.

Trade-off Keamanan dan Efisiensi

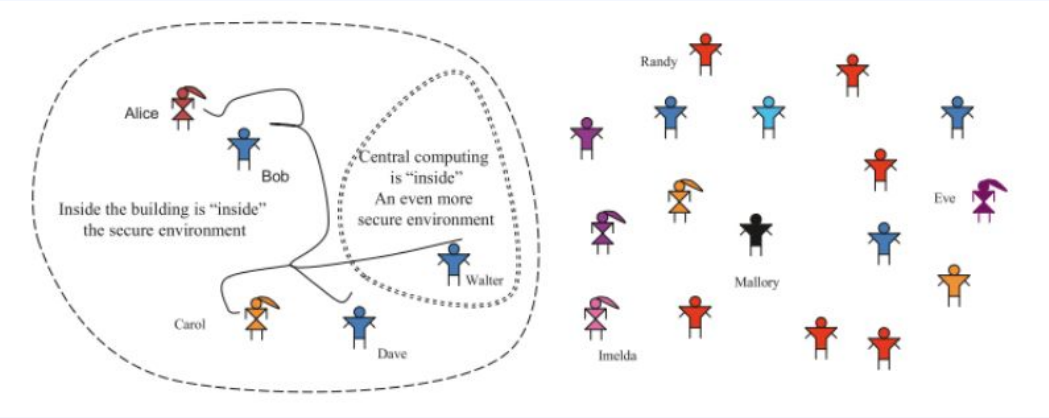
- HSMs adalah **perangkat fisik** yang berfungsi sebagai "brankas" untuk menyimpan dan **mengelola kunci digital** untuk dekripsi data.
- HSMs dapat berupa kartu **plug-in** atau **perangkat eksternal** yang terhubung ke server jaringan.
- Data yang paling sensitif dapat disimpan dengan metode **dekripsi yang hanya ada pada HSM**.

07

Pemain Keamanan

Peran dan Nickname dalam Sistem Keamanan

Pemain Keamanan



- Deskripsi sistem keamanan dan partisipannya dapat membingungkan. Untuk memudahkan, pemain dalam sistem keamanan diberi nickname.
- Nickname adalah sebagai berikut
  - **Alice, Bob, Carol, Dave:** Pengguna dalam sistem (Legitimate Users)
  - **Walter:** Administrator sistem
  - **Eve:** Penyerang eveasdropping (menguping komunikasi)
  - **Mallory:** Penyerang yang mencoba mengubah data (Malicious Attacker)
  - **Randy:** Pengguna atau entitas yang secara tidak sengaja menyebabkan masalah keamanan (Accidental Attacker).
  - **Imelda:** Penyerang yang melakukan serangan Denial-of-Service (DoS) untuk mengganggu layanan sistem.

Tipe Serangan

Lapisan	Jenis Serangan	Perubahan Data atau Program Tidak Sah (Mallory dan Randy [Accidental])	Pengamatan dan Penyalinan Tidak Sah (Eve dan Randy [Accidental])	Serangan Denial-of-Service (DoS) (Imelda dan Randy [Accidental])
Perangkat Lunak	Aplikasi Pengguna	Login palsu, atau akses tidak langsung	Biasanya bergantung pada lapisan implementasi yang lebih rendah	Enkripsi atau penyamaran data
	Sistem Operasi (OS)	Login palsu, instruksi tingkat rendah	Transaksi dalam memori	
	Lapisan Mesin Virtual (VM)	Komunikasi antar-VM	Kebocoran informasi	
	Lapisan Hypervisor			
	Driver Perangkat Lunak	Dari sistem operasi (OS)	Enkripsi, keamanan handshake	Enkripsi data
Perangkat Keras	BIOS/Lapisan manajemen sistem berbasis firmware	Manipulasi stempel waktu dan tanggal	Lokasi memori yang aman	Autentikasi untuk eksekusi
	CPU	Kebocoran informasi	Kebocoran informasi	
	Memori cache/ RAM utama	Kebocoran informasi		
	Disk Memori	Hak akses	Hak akses	

08

Pemain Keamanan

Peran dan Nickname dalam Sistem Keamanan

Keamanan Tradisional

- Pendekatan keamanan tradisional bergantung pada **penghalang fisik**.
- **Akses** ke pusat komputasi hanya tersedia untuk **personil terperaya**.
- Aktivitas dan **akses** hardware dan jaringan **terkontrol** dan dipantau.

Keamanan Internet

- Dengan internet, admin sistem memiliki **akses** melalui **channel transmisi yang tidak terkontrol**.
- **Identitas** asli pengguna **tidak diketahui**.
- **Intruder** memiliki **kesempatan tak terbatas** untuk mencoba **akses**.
- Kebijakan **keamanan** yang **ketat** dapat **mengganggu pengguna** yang sah seperti menyebabkan serangan Denial-of-Service (DoS).

09

Keamanan Menggunakan Kunci Enkripsi

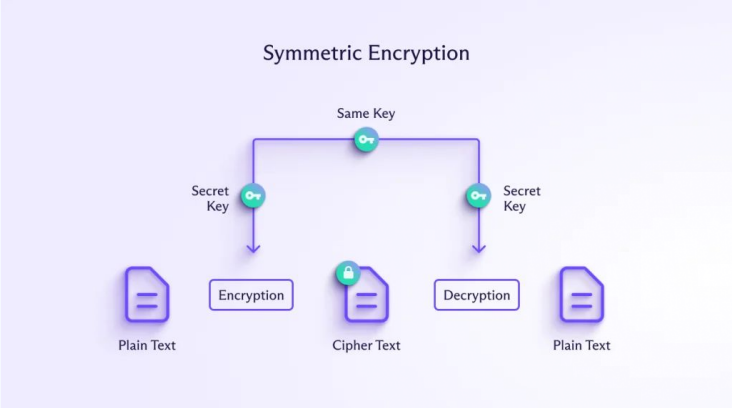
Keamanan dalam Cloud

Enkripsi

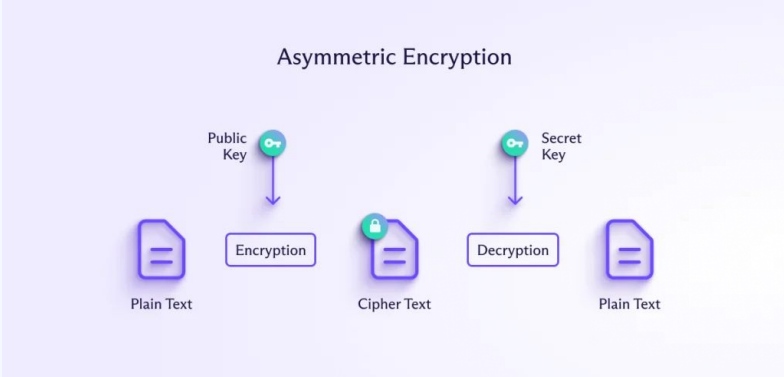
Enkripsi digunakan untuk melindungi data dari akses tidak sah dengan mengonversi informasi menjadi bentuk yang hanya dapat dibaca oleh pihak yang berwenang.

Jenis Enkripsi

Enkripsi Simetris: Menggunakan satu kunci yang sama untuk enkripsi dan dekripsi (contoh: AES, DES).



Enkripsi Asimetris: Menggunakan pasangan kunci publik dan privat (contoh: RSA, ECC).

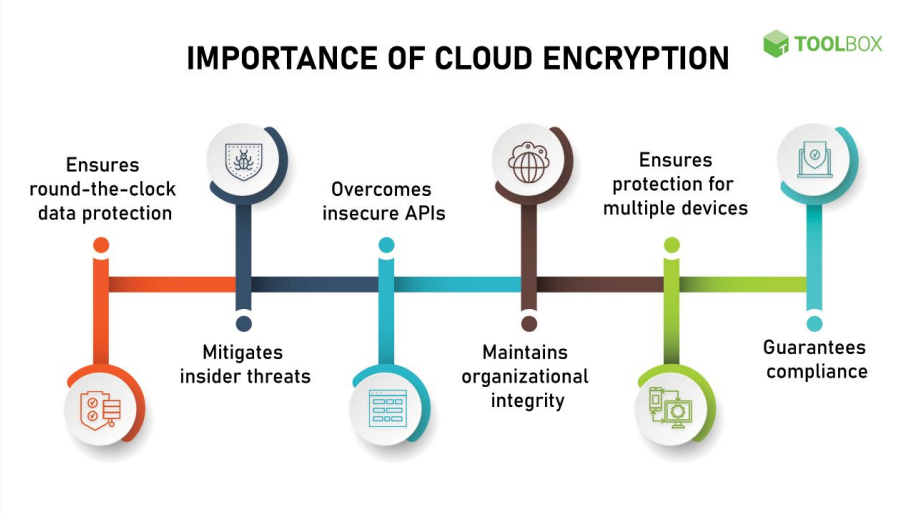


Perbandingan Enkripsi Simetris dan Asimetris

Aspek	Enkripsi Simetris	Enkripsi Asimetris
Kunci yang Digunakan	Satu kunci yang sama untuk enkripsi dan dekripsi	Pasangan kunci publik dan privat
Keamanan	Kurang aman jika kunci bocor	Lebih aman karena kunci privat tidak dibagikan
Kecepatan	Lebih cepat	Lebih lambat karena kompleksitas kriptografi

Penerapan dalam Cloud

- Melindungi data saat transit dan saat disimpan.
- Digunakan dalam layanan seperti TLS/SSL, VPN, dan penyimpanan terenkripsi.



10 Tantangan dalam Menggunakan Algoritma Keamanan Standar

Tantangan yang dihadapi dalam Cloud

Efisiensi, Performa, Tantangan

- Algoritma keamanan yang lebih kuat seringkali membutuhkan sumber daya komputasi yang lebih besar.
- Tantangan utama dalam penyimpanan dan distribusi kunci yang aman.
- Algoritma konvensional seperti RSA dan ECC bisa menjadi rentan jika komputer kuantum berkembang.

11

Variasi dan Kasus Khusus dalam Keamanan Cloud Computing

Kasus Khusus dalam Keamanan Cloud

- **Keamanan Multi-Tenant**: Pengguna berbagi infrastruktur yang sama.
- **Proteksi DDoS**: Serangan dapat mengganggu layanan berbasis cloud.
- **Keamanan API**: API yang lemah dapat membuka celah keamanan.
- **Isolasi Data**: Data harus dipisahkan dengan baik antara pengguna.

12

Tantangan Utama dalam Cloud Computing dan Virtualisasi

Tantangan Utama dalam Cloud Computing dan Virtualisasi

- **Manajemen Identitas:** Verifikasi pengguna dan kontrol akses.
- **Isolasi Sumber Daya:** Memastikan keamanan antar lingkungan virtual.
- **Privasi dan Kepatuhan:** Mematuhi regulasi seperti GDPR dan HIPAA.
- **Ancaman Insider:** Risiko dari pengguna internal yang memiliki akses ke sistem.

13

Some Suggested Security for Cloud Computing

You can enter a subtitle here if you need it

Best Practices

Continuous Monitoring

Pemantauan terus-menerus diperlukan untuk mendeteksi pola penggunaan yang tidak biasa atau perubahan dalam sumber daya cloud.

Attack Surface Management

Mengelola dan membatasi titik akses yang bisa dimanfaatkan oleh pihak tidak berwenang untuk mengakses data penting.

No Residual Footprints

Menghapus jejak digital dari memori atau disk setelah penggunaan cloud, sehingga data yang tersisa tidak dapat dieksploitasi oleh pihak lain.

Strong Access Control

Mengelola kontrol akses dengan baik untuk mencegah serangan melalui titik masuk yang tidak terduga, seperti sistem HVAC yang kurang aman.

Damage Control

Menyusun strategi mitigasi untuk mengurangi dampak jika terjadi serangan, misalnya dengan menonaktifkan akun yang terancam atau mematikan server yang terinfeksi.

Keamanan Cloud

Email	Application
• Antivirus • Anti-spam • Information Leakage Control • Kemampuan membuat aturan untuk blokir konten • Email Traffic Monitoring	• Intrusion Detection Tools • Application Firewall • Firewall generasi terbaru • Alat Mitigasi Serangan DDoS • Log Correlation • CDN (Content Delivery Network

*** Persyaratan keamanan ini dapat dimasukkan dalam SLA (Service-Level Agreement) antara penyedia cloud dan penggunanya untuk memastikan tanggung jawab dan alat keamanan yang tersedia.**

14

Side Channel Security Attacks in the Cloud

You can enter a subtitle here if you need it

Kategori Side Channel Attack

Cache Side Channel Attack

- Serangan ini menargetkan cache memori yang digunakan oleh berbagai proses dalam sistem berbagi sumber daya.

- Jika dua proses menggunakan cache yang sama, penyerang bisa mengamati pola penggunaan cache untuk menebak informasi dari proses lain.

Timing Attacks

- Penyerang mengukur waktu eksekusi operasi tertentu untuk mendapatkan informasi terkait algoritma atau data yang digunakan.

- Contohnya adalah calculation timing attacks, di mana perbedaan kecepatan operasi tertentu membantu penyerang menebak bagian dari kunci enkripsi.

Power Analysis Attacks

- Serangan ini menggunakan pola konsumsi daya dari prosesor untuk menebak data yang sedang diproses.

- Contohnya, variasi konsumsi daya saat transistor berpindah antara 1 dan 0 bisa memberikan informasi tentang bit dalam sebuah kunci enkripsi.

Serangan Side Channel Lain

Electromagnetic Radiation	Photon Attack	Acoustic Attack
Menganalisis sinyal elektromagnetik yang dipancarkan oleh chip untuk mendapatkan informasi tentang data yang diproses.	Mengamati chip menggunakan teknik optik untuk memahami operasi internalnya.	Menggunakan pola suara yang dihasilkan oleh perangkat keras, seperti getaran dari keyboard atau disk drive.

15

An Introduction to Block Chain for Security

You can enter a subtitle here if you need it

Blockchain

Blockchain adalah basis data terdistribusi yang mencatat semua transaksi digital yang terjadi di dalam jaringan. Teknologi ini bersifat desentralisasi, artinya data tidak tersimpan di satu tempat tetapi didistribusikan ke semua peserta jaringan, sehingga sulit untuk diretas atau dimanipulasi.

Tiga komponen utama:

1. Block → berisi daftar transaksi yang terjadi dalam periode tertentu
2. Chain → blok-blok ini ditandai dengan timestamp dan dihubungkan secara kriptografis, sehingga membentuk rantai yang aman
3. Distributed Ledger → setiap peserta dalam jaringan memiliki salinan data transaksi yang selalu diperbarui

Keuntungan:

1. Menghilangkan perantara dalam transaksi, sehingga lebih cepat dan hemat biaya.
2. Meningkatkan keamanan, karena transaksi dienkripsi dan tidak bisa diubah.
3. Mengurangi risiko kejahatan siber dan penipuan.

Aplikasi Blockchain

Cryptocurrency	Smart Contracts	Trusted Computing
• Digunakan untuk menyimpan dan mentransfer nilai tanpa otoritas pusat. • Menggunakan enkripsi kuat (misalnya SHA-256) untuk melindungi dari manipulasi data. • Setiap peserta jaringan memiliki salinan transaksi sehingga tidak bisa dipalsukan.	• Kontrak yang dijalankan secara otomatis tanpa perantara. • Bisa melibatkan dua atau lebih pihak dengan aturan yang telah disepakati. • Memungkinkan pembayaran otomatis setelah syarat terpenuhi. • Menerapkan sanksi jika aturan tidak dipenuhi.	• Meningkatkan keamanan dalam berbagi sumber daya dan transaksi. • Menggabungkan blockchain, desentralisasi, dan smart contracts untuk menciptakan sistem yang lebih aman.

Cara Kerja Transaksi Keuangan

1. Setiap blok memiliki input, amount, dan output
   - Input → Sumber dana yang digunakan dalam transaksi
   - Amount → Jumlah yang ingin dikirimkan
   - Output → Alamat penerima transkasi
2. Transaksi baru dibuat dalam bentuk blok dan dikirim ke jaringan.
3. Setiap node dalam jaringan memperbarui ledger-nya.
4. Konsensus terjadi untuk memvalidasi transaksi baru.
5. Blok baru ditambahkan ke rantai blockchain.

16

Summary

You can enter a subtitle here if you need it

Pertumbuhan Internet meningkatkan risiko keamanan informasi, terutama dengan penerapan Cloud Computing. Bab ini membahas tantangan keamanan spesifik Cloud Computing dan perlunya keseimbangan antara keamanan dan kinerja sistem. Solusi keamanan harus mencakup berbagai lapisan dan fungsi. Pembahasan ini bertujuan mendorong diskusi lebih lanjut mengenai model keamanan Cloud Computing, mencakup ancaman nyata maupun persepsi risiko.

—Summary

Thanks!

Do you have any questions?

Tugas Individu Piramida Komputasi Awan

Edgrant Henderson Suryajaya
2206025016

I. Sejarah

Pada tahun 1990-an, perusahaan telekomunikasi menyediakan layanan jaringan komputer yang disebut dengan Virtual Private Network (VPN) yang memungkinkan banyak user menggunakan hardware yang sama. Ini merupakan awal dari konsep cloud computing. Lalu, konsep seperti grid computing, utility computing, dan Software as a Service (SaaS) muncul sebagai cikal bakal dari cloud computing.

- *Grid computing*: Masalah komputasi dibagi menjadi beberapa bagian dan dikerjakan oleh beberapa komputer yang berbeda
- *Utility computing*: menjual layanan komputasi
- *Software as a Service (SaaS)*: menyediakan *software* pada user melalui internet

  "*Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction*."

Itulah definisi *Cloud Computing* oleh NIST. Dalam kata lain, cloud computing memberikan layanan sumber daya komputasi *sharing* yang mudah dikonfigurasi.

II. Roots of Cloud Computing

Menurut NIST (*National Institute of Standards and Technology*), *Cloud Computing* memiliki 5 karakteristik utama, 3 model layanan, dan 5 model implementasi.

A. Model Layanan Cloud Computing

- *Software as a Service (SaaS)*: menyediakan aplikasi yang sudah jadi. Pelanggan hanya perlu menggunakan aplikasi tersebut tanpa perlu mengurus infrastruktur atau pembuatan aplikasi. (Contoh: Google Docs, Microsoft Office 365)
- *Platform as a Service (PaaS)*: menyediakan platform untuk pengembangan aplikasi. Pelanggan dapat membuat aplikasi mereka sendiri tanpa perlu mengurus infrastruktur. (Contoh: Vercel, Heroku, Wordpress)
- *Infrastructure as a Service (IaaS)*: menyediakan infrastruktur komputasi, seperti server, jaringan, dan penyimpanan. Pelanggan dapat mengelola infrastruktur tersebut sesuai kebutuhan mereka. (Contoh: Amazon Web Services, Microsoft Azure)

Saas adalah layanan yang *High Level*, user hanya perlu menggunakan aplikasi dan tidak perlu memikirkan implementasi dibaliknya. PaaS adalah layanan yang *Middle Level*, user dapat mengembangkan aplikasi mereka sendiri tanpa perlu memikirkan infrastruktur. IaaS adalah layanan yang *Low Level*, user dapat mengelola infrastruktur sesuai kebutuhan mereka.

B. Model Implementasi Cloud Computing

- *Public Cloud*: layanan cloud yang disediakan oleh penyedia layanan cloud dan dapat diakses oleh publik. (Contoh: AWS, Azure, Google Cloud)
- *Private Cloud*: layanan cloud yang disediakan oleh perusahaan sendiri untuk kebutuhan internal biasanya digunakan oleh perusahaan besar.
- *Hybrid Cloud*: gabungan dari public dan private cloud. Perusahaan menggunakan private cloud untuk data sensitif dan public cloud untuk data yang tidak sensitif.
- *Community Cloud*: layanan cloud yang digunakan oleh beberapa organisasi yang memiliki kepentingan yang sama. Contohnya kluster perumahan besar yang menggunakan layanan cloud khusus untuk kluster tersebut.
- *Virtual Private Cloud*: layanan cloud yang mengsimulasikan private cloud, tetapi sebenarnya menggunakan public cloud. Contohnya sebuah organisasi memberikan layanan cloud khusus untuk karyawan mereka tetapi sebenarnya data di-*host* pada AWS.

Model implementasi cloud yang paling sering digunakan pada zaman sekarang adalah *Public Cloud* dan *Hybrid Cloud*. *Public Cloud* digunakan oleh banyak perusahaan karena lebih murah dan mudah digunakan. *Hybrid Cloud* digunakan oleh perusahaan besar yang memiliki data sensitif, tetapi juga ingin menggunakan layanan cloud yang murah.

C. Characteristics of Cloud Computing

- *Rapid Elasticity*: kemampuan untuk menambah atau mengurangi sumber daya komputasi sesuai kebutuhan.
- *Measured Service*: penggunaan sumber daya komputasi diukur dan dilaporkan. Pengguna hanya membayar sumber daya yang digunakan.
- *On-demand Self-service*: sumber daya komputasi dapat digunakan tanpa perlu interaksi dengan penyedia layanan.
- *Ubiquitous Network Access*: sumber daya komputasi dapat diakses dari mana saja dan kapan saja.
- *Resource Pooling*: sumber daya komputasi disediakan secara bersamaan untuk beberapa pengguna. Sumber daya ini dapa dialokasikan sesuai kebutuhan.

III. Virtualisasi

Tidak ada aplikasi yang menggunakan 100% sumber daya komputasi yang ada pada server setiap saat, sehingga penyedia layanan cloud menggunakan teknologi virtualisasi untuk

membagi sumber daya komputasi tersebut ke beberapa user. Virtualisasi memungkinkan satu server fisik digunakan oleh beberapa user secara bersamaan.

Virtualisasi adalah teknologi yang memungkinkan satu server fisik untuk menjalankan beberapa sistem operasi secara bersamaan yang masing-masing berjalan secara independen dan terisolasi. Terdapat beberapa tipe virtualisasi yang digunakan pada cloud, beberapa antaranya adalah *Hypervisor-based Virtualization* dan *Container-based Virtualization*.

A. Hypervisor-based Virtualization

Hypervisor adalah software yang menjalankan beberapa sistem operasi secara bersamaan pada satu server fisik. Terdapat dua tipe *Hypervisor*, yaitu *Type 1 Hypervisor* dan *Type 2 Hypervisor*.

- *Type 1 Hypervisor*: *Hypervisor* berjalan langsung pada hardware server. Contoh dari *Type 1 Hypervisor* adalah VMware ESXi, Microsoft Hyper-V, dan Xen.
- *Type 2 Hypervisor*: *Hypervisor* berjalan di atas sistem operasi yang sudah ada. Contoh dari *Type 2 Hypervisor* adalah VMware Workstation, Oracle VirtualBox, dan Parallels Desktop.

Hypervisor-based Virtualization memungkinkan user untuk menjalankan sistem operasi yang berbeda pada satu server fisik. Setiap sistem operasi yang berjalan di-*host* oleh *Hypervisor* disebut dengan *Virtual Machine*. *Virtual Machine* memiliki sumber daya komputasi yang terisolasi dari *Virtual Machine* lainnya yang ditentukan saat pembuatan *Virtual Machine* tersebut.

B. Container-based Virtualization

Container-based Virtualization adalah teknologi yang memungkinkan user untuk menjalankan aplikasi dan dependensinya dalam wadah yang terisolasi dari aplikasi lainnya. *Container* berbagi kernel dari sistem operasi yang sama. Contoh dari *Container-based Virtualization* adalah Docker, Kubernetes, dan LXC.

Perbedaan utama antara *Hypervisor-based Virtualization* dan *Container-based Virtualization* adalah pembagaian sumber daya komputasi. *Hypervisor-based Virtualization* membagi sumber daya komputasi secara fisik seperti RAM, CPU, dan storage *Virtual Machine* dibuat, sedangkan *Container-based Virtualization* dapat membagi sumber daya komputasi secara dinamis sesuai kebutuhan aplikasi.

IV. Concern of Cloud Players

Dalam penggunaan layanan cloud, terdapat banyak *stakesholder* yang memiliki kepentingan masing-masing. *Stakeholder* tersebut adalah manajer fasilitas, penyedia layanan, pengguna layanan, manajer IT, dan *End User*. Kepentingan dari *stakeholder* tersebut adalah berbeda-beda

- *Manajer fasilitas*: memastikan infrastruktur *data center* (DC) berjalan dengan baik dan aman. Memaksimalkan performa, meminimalkan biaya operasional.
- *Penyedia layanan*: memastikan layanan cloud yang disediakan aman, handal, dan tidak terputus. Memaksimalkan utilisasi peralatan, merencanakan kapasitas dengan mengkonsiderasi kemungkinan pertumbuhan.
- *Pengguna layanan*: memastikan *End User* dapat menggunakan layanan mereka dengan baik.
- *End User*: mementingkan data mereka aman, privasi terjaga, dan layanan yang mereka gunakan dapat diakses kapan saja.
- *Manajer IT*: IT dari sisi pengguna layanan, memastikan layanan yang digunakan oleh *End User* dapat diakses kapan saja, aman, dan privasi terjaga. Selain itu, merencanakan kemungkinan pertumbuhan layanan.

Kelima *stakeholder* tersebut memiliki kepentingan yang berbeda-beda, tetapi terdapat beberapa kepentingan yang sama, yaitu keamanan data, privasi, dan ketersediaan layanan. Teknologi *Cloud Computing* yang digunakan harus memenuhi kepentingan dari kelima *stakeholder* tersebut.

V. Considerations for Data Centers

A. Migration

DC harus mempertimbangkan migrasi data dari satu DC ke DC lainnya. Kemungkinan terjadinya *downtime* harus diminimalkan. DC harus memastikan data yang di-*migrate* aman, tidak terjadi kehilangan data, dan data dapat diakses kapan saja.

B. Performence

DC harus memastikan performa layanan yang diberikan kepada pengguna layanan. DC harus memastikan sumber daya komputasi yang digunakan oleh pengguna layanan optimal, tidak terjadi *overload* atau *underload* pada sumber daya komputasi. DC harus memastikan layanan yang diberikan dapat diakses kapan saja dengan performa yang baik.

C. Security

Public cloud sering menjadi target serangan *cyber*. Tergantung dengan model layanan yang digunakan, tangung jawab keamanan data dapat berbeda-beda. Sebagai contoh, pada model *Infrastructure as a Service (IaaS)*, penyedia layanan hanya bertanggung jawab untuk keamanan infrastruktur, sedangkan pengguna layanan bertanggung jawab untuk keamanan data mereka. DC harus memastikan data yang disimpan aman, tidak terjadi kebocoran data, dan data tidak diakses oleh pihak yang tidak berhak. Namun, pada model *Software as a Service (SaaS)* atau *Platform as a Service (PaaS)*, penyedia layanan bertanggung jawab untuk keamanan data dan aplikasi (hanya pada SaaS) yang disimpan oleh pengguna layanan.

References

[1] N. K. Sehgal, V. Chandra Joshi, A. Aggarwal, A. Mathur, and G. S. Tomar, "Chapter 3," in *Cloud Computing with Security*. Springer Nature Switzerland AG, 2020. doi: 10.1007/978-3-030-24612-9_3.

[2] Amazon Web Services, "What is a hypervisor?," Available: https://aws.amazon.com/what-is/hypervisor/. [Accessed: Feb. 20, 2025].

[3] Amazon Web Services, "The difference between Docker and VMs," Available: https://aws.amazon.com/id/compare/the-difference-between-docker-vm/. [Accessed: Feb. 20, 2025].