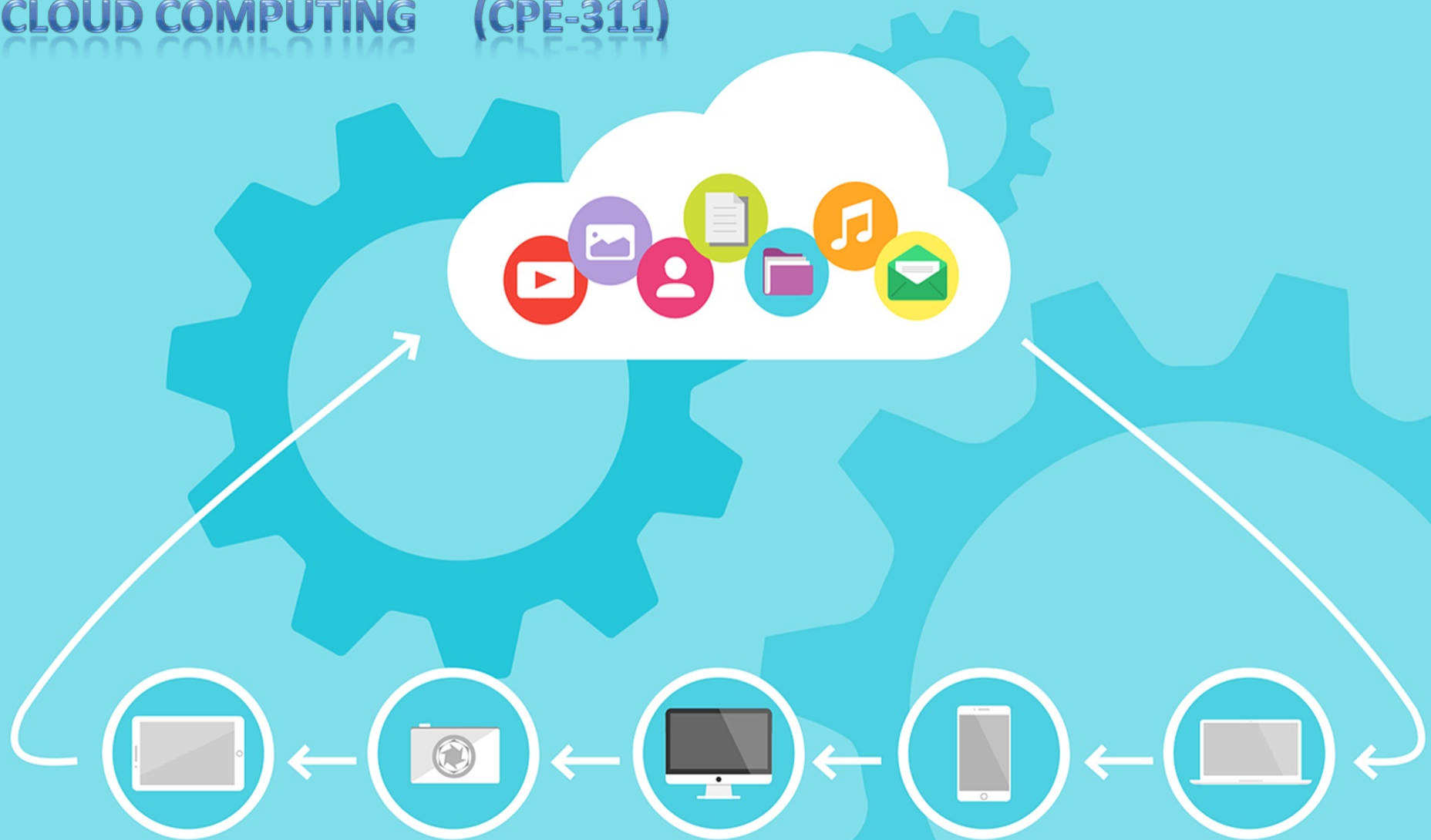


# CLOUD COMPUTING (CPE-311)



**GURJIT SINGH BHATHAL**  
**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**  
**PUNJABI UNIVERSITY**  
**2021-22**

# Section-A (Part-I)

**Overview of Computing Paradigm-** Recent trends in Computing: Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud computing; Evolution of cloud computing Business driver for adopting cloud computing

# Computing Paradigm

- It is the technique of linking two or more computers into a network (Usually through a local area network) in order to take advantage of the parallel processing power of those computers.
- Over the years different computing paradigms have been developed and used. In fact different computing paradigms have existed before the cloud computing paradigm.

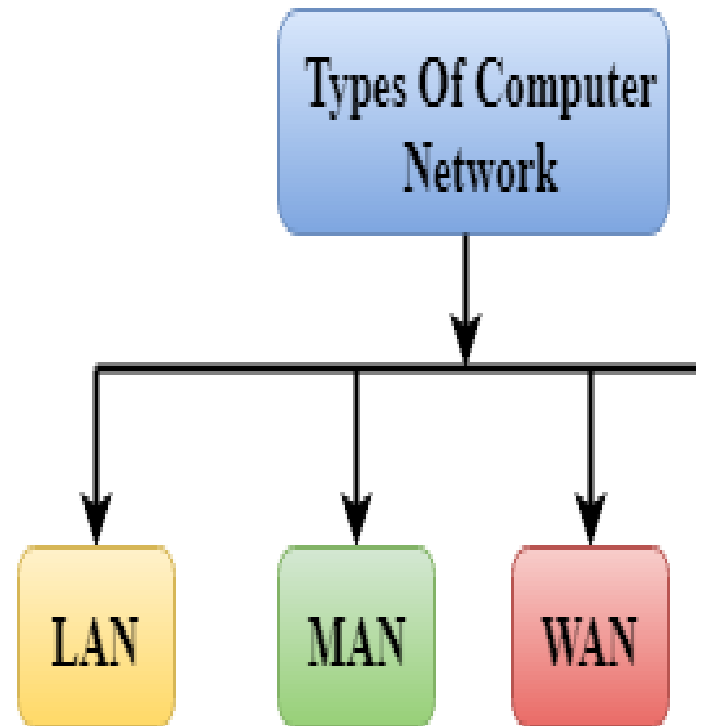
# Types of Computer

- Supercomputer
- Mainframe Computer (Server)
- Minicomputer
- Microcomputer (PC)

# Computer Network Types

A **computer** connected together for the purpose of sharing resources.

- LAN(Local Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)



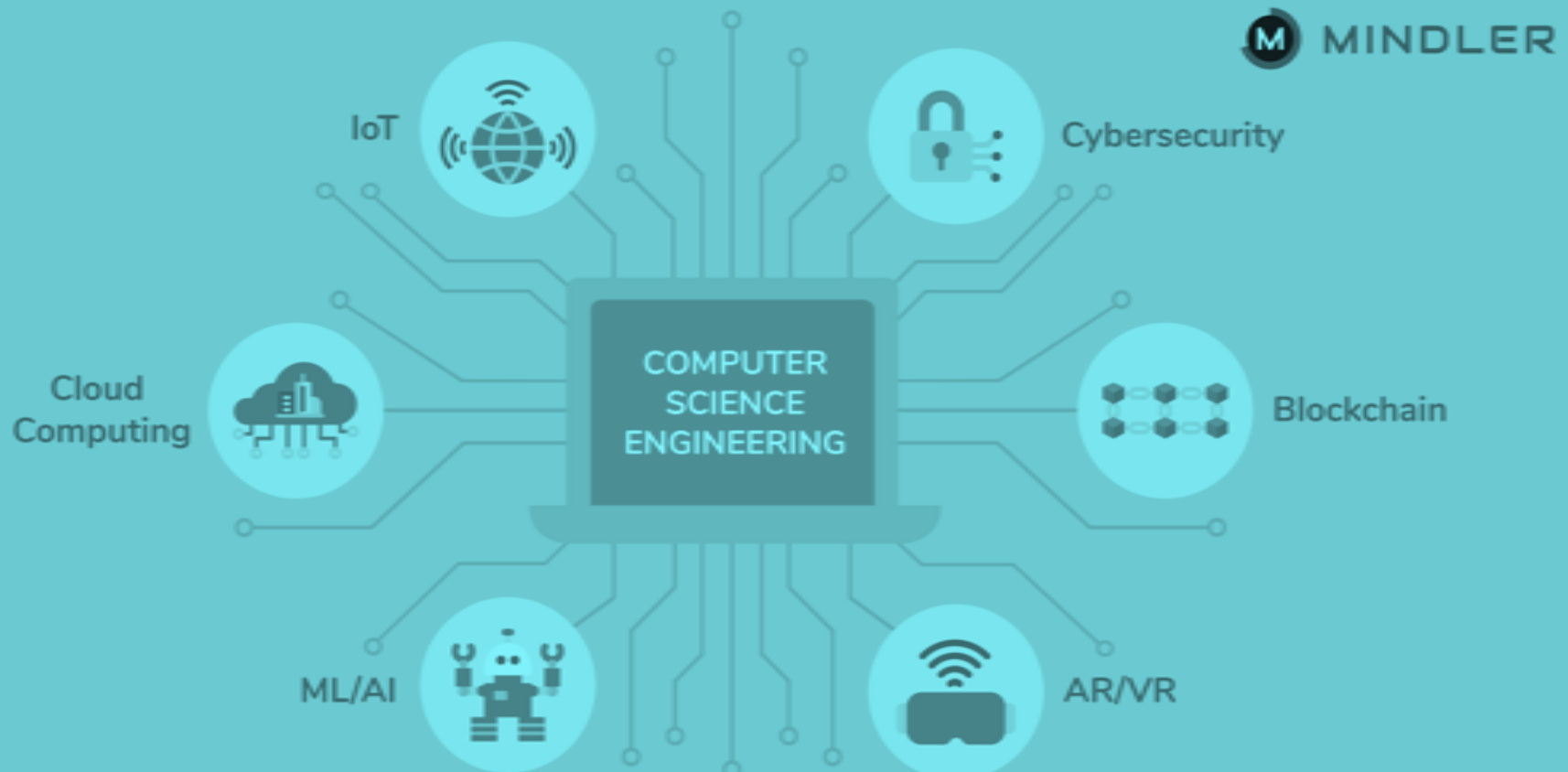
# Computing Paradigm

Nowadays computing is moved away from personal computers or an individual application server to a “CLOUD” of computers.

# Recent Trends in Computing

The latest computer science trends include **artificial intelligence, edge computing, and quantum computing**. IT professionals are also knowledgeable about developments in robotics and cyber-security.

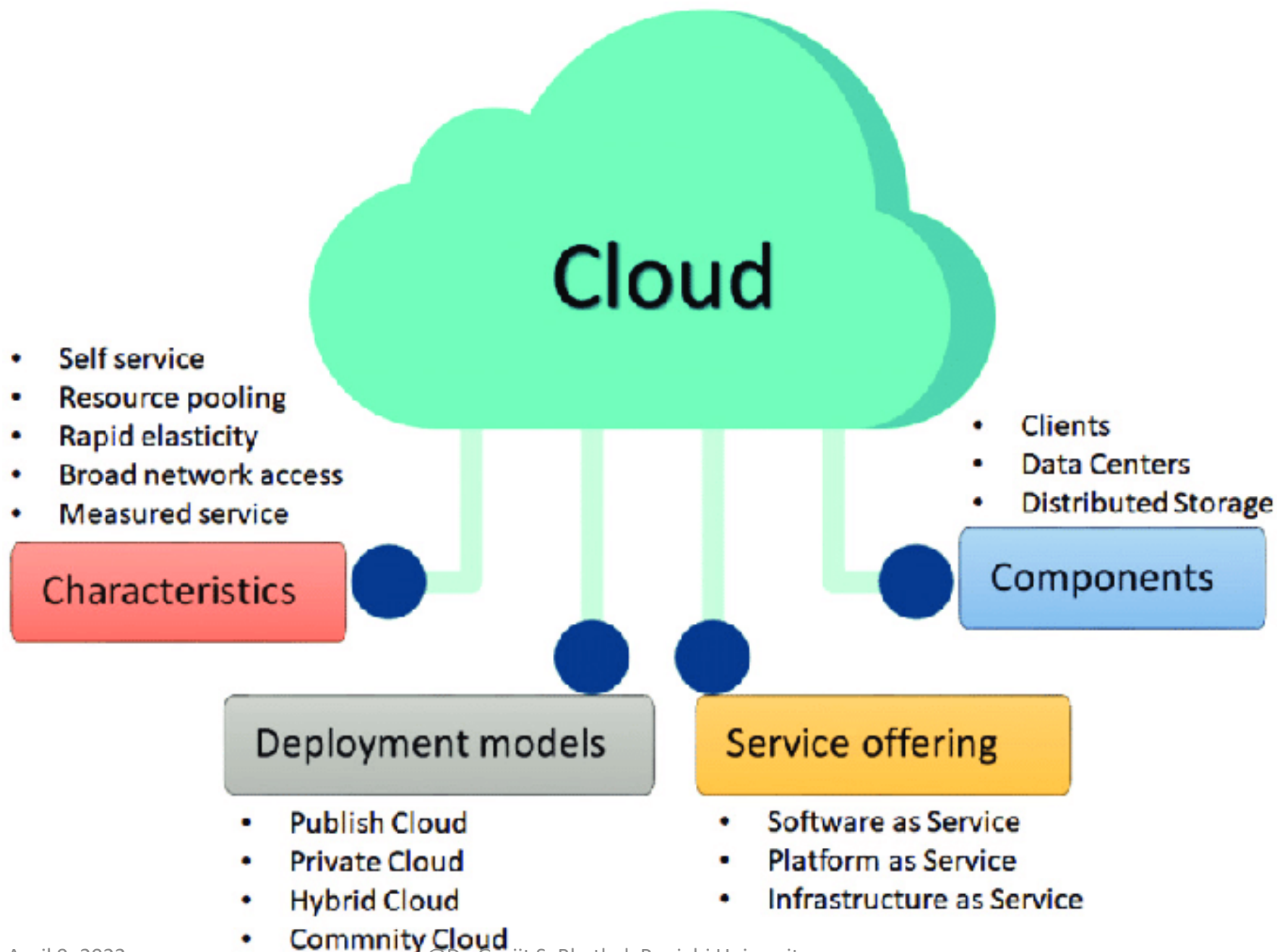
# Recent Trends in Computing





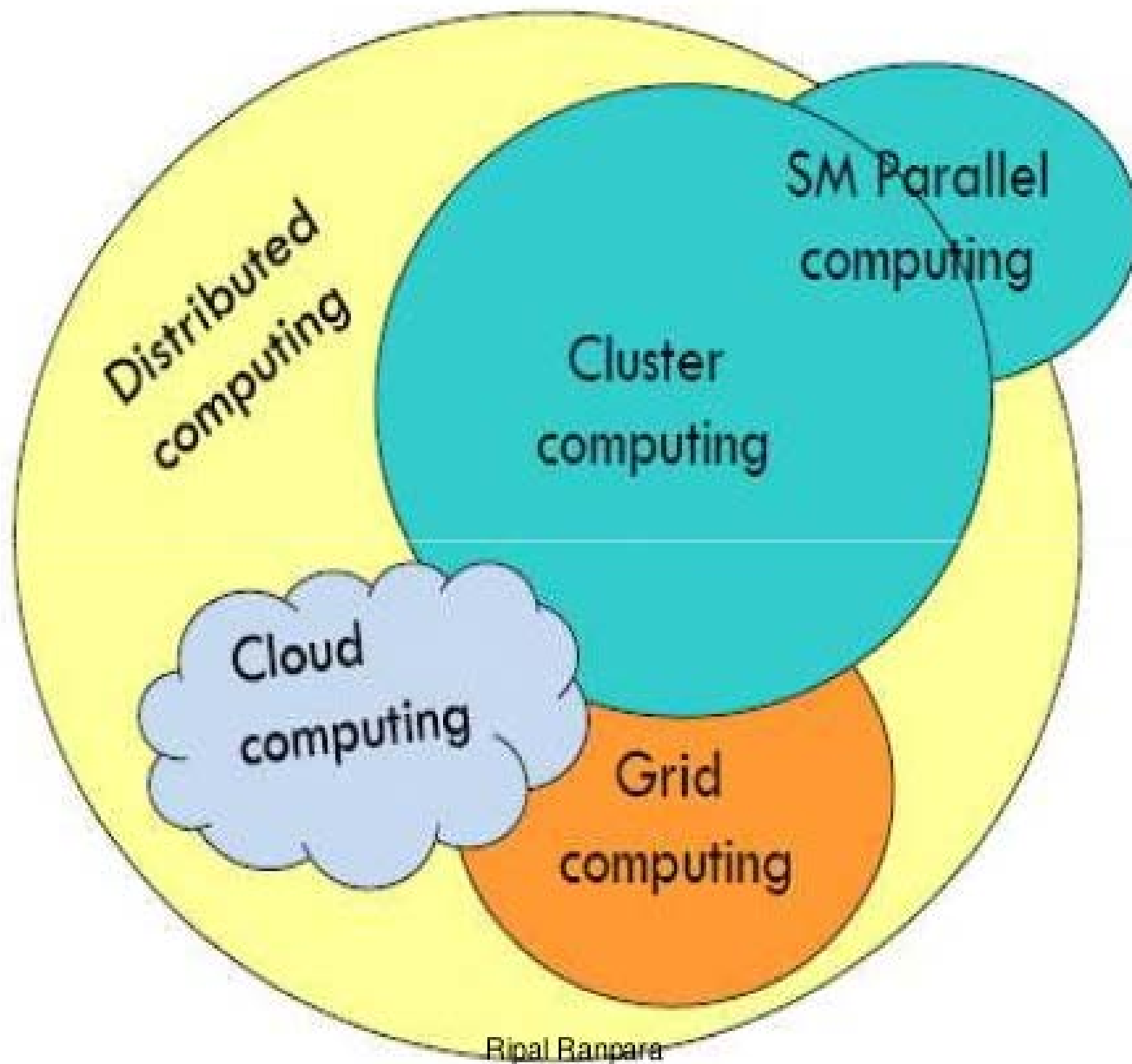
# Cloud Computing Paradigm

**Cloud Computing** is defined as the type of computing where it is the delivery of **on-demand computing services** over the internet on a **pay-as-you-go** basis. It is widely distributed, network-based and used for storage.



# Types of Computing

- Distributed Computing
- Grid Computing
- Utility Computing
- Cluster Computing
- Cloud Computing

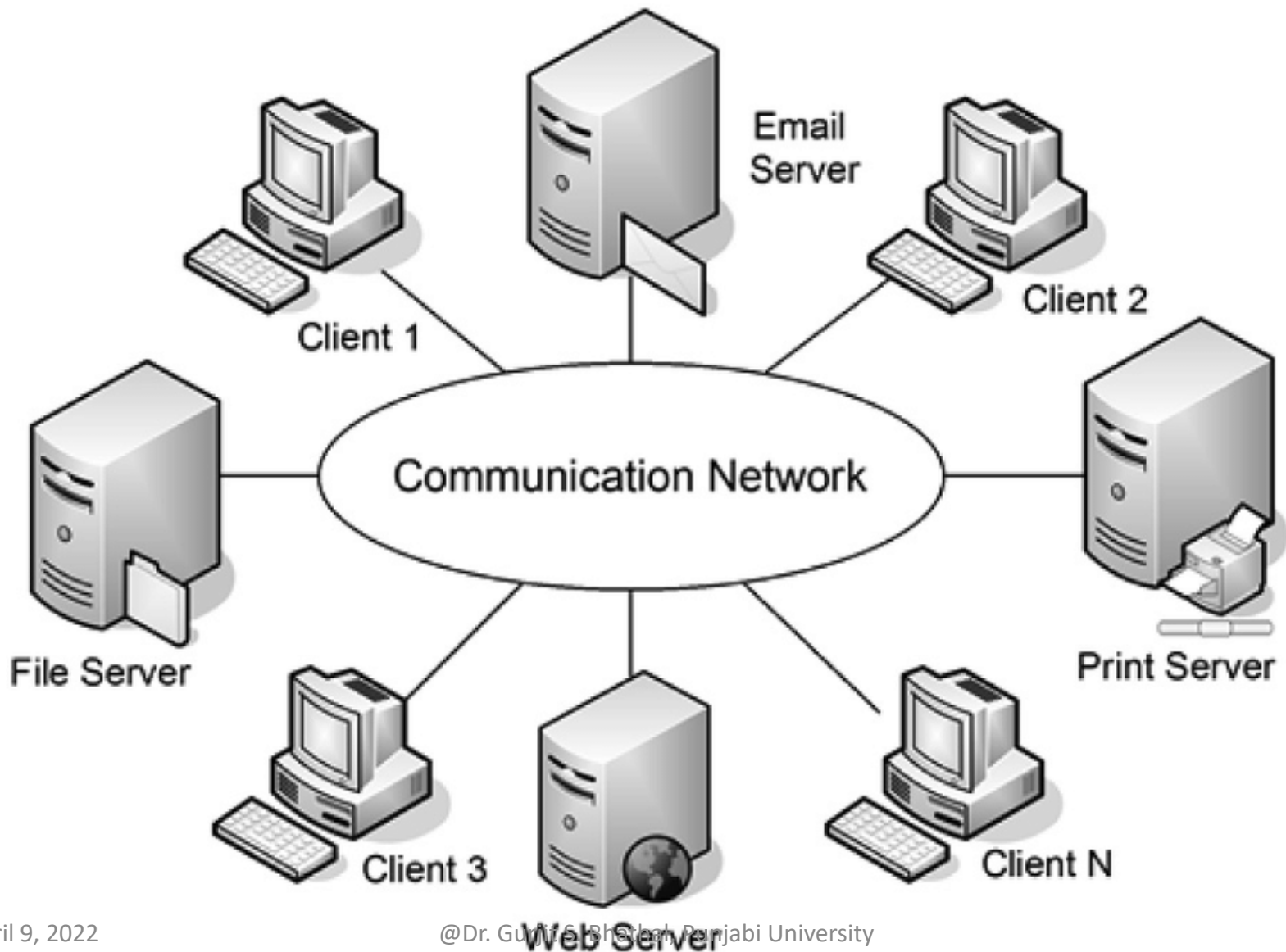


Ripal Banpara

# Distributed Computing

A distributed computer system **consists of multiple software components that are on multiple computers, but run as a single system.** The computers that are in a distributed system can be physically close together and connected by a local network, or they can be geographically distant and connected by a wide area network.

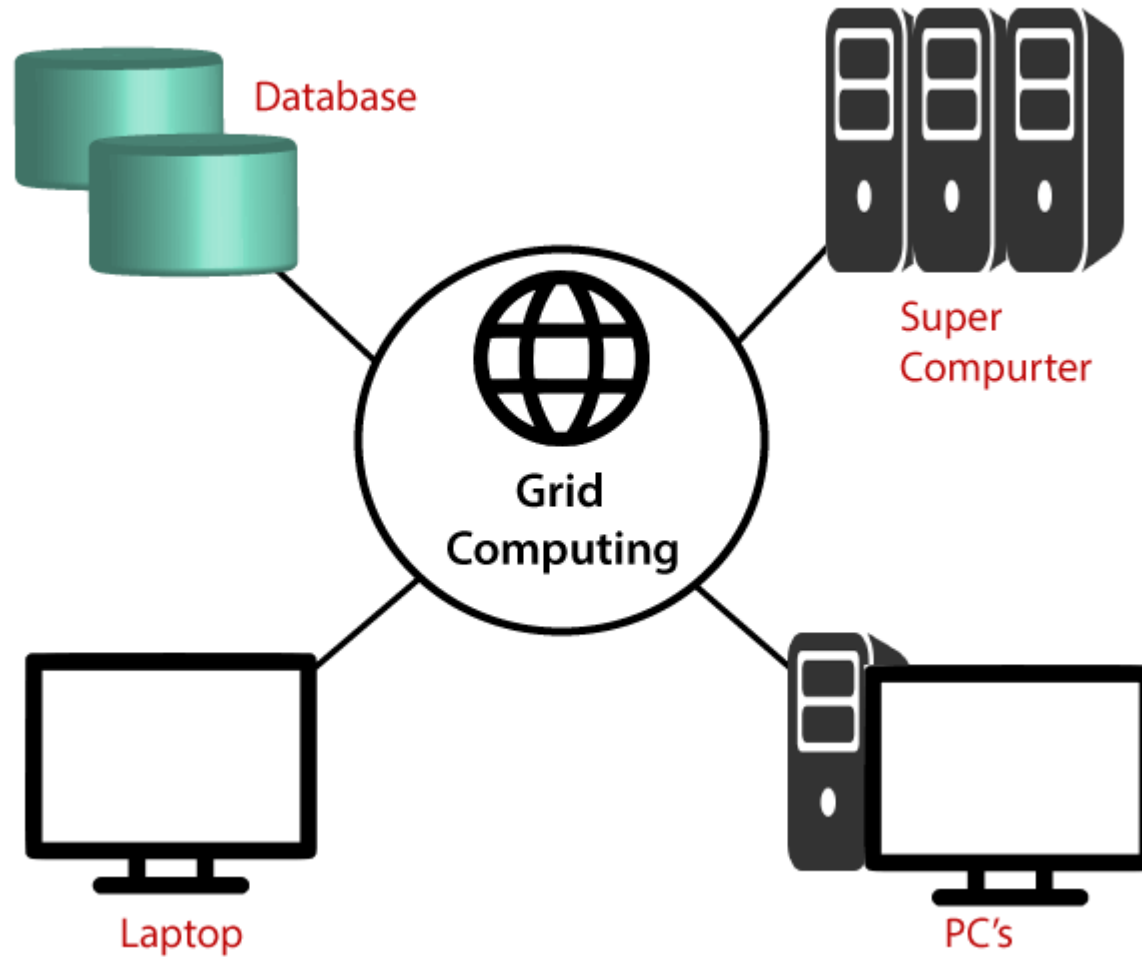
# Distributed Computing



# Grid Computing

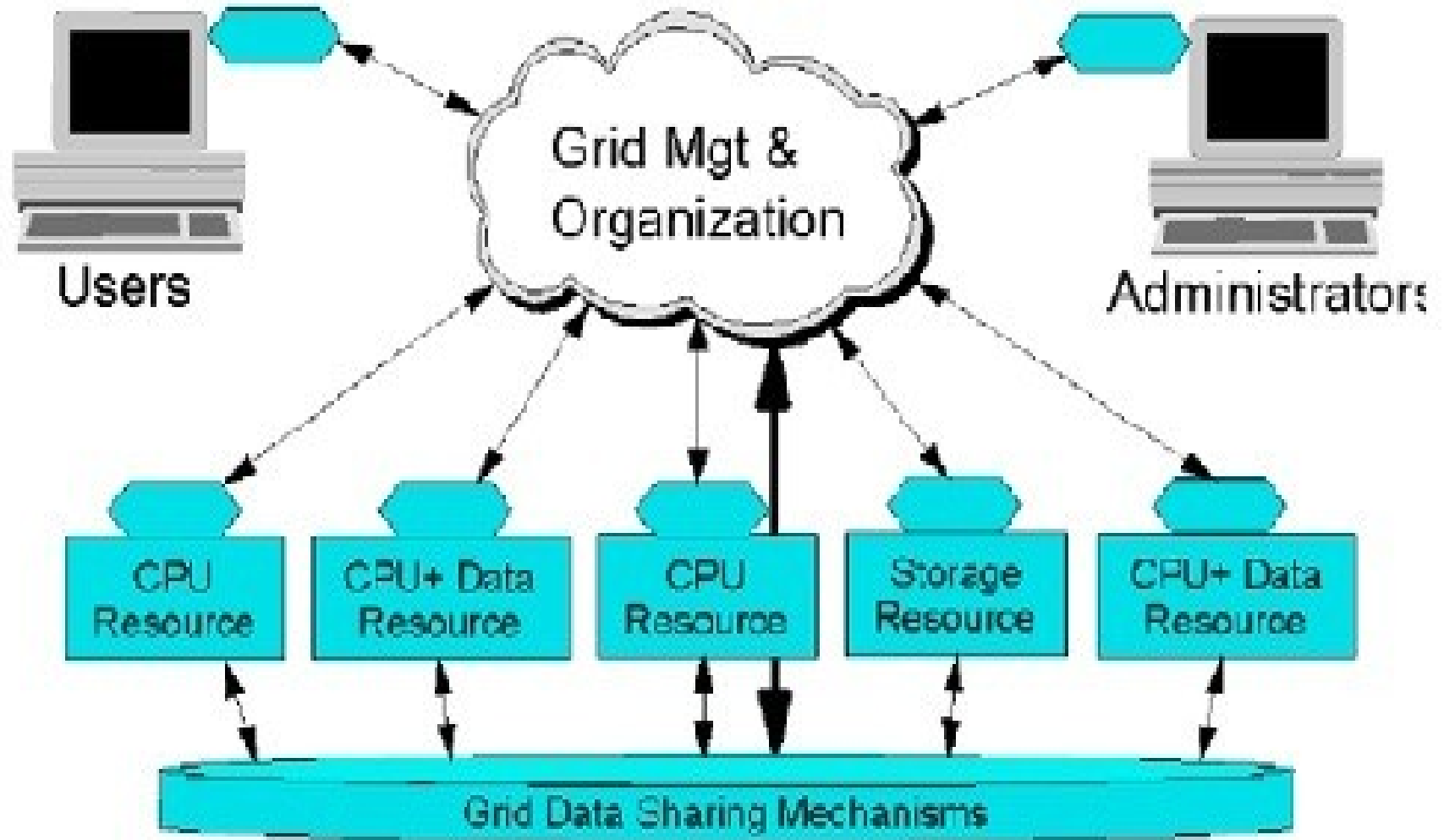
Grid computing is the practice of leveraging multiple computers, often geographically distributed but connected by networks, to work together to accomplish joint tasks. It is typically run on a “data grid,” a set of computers that directly interact with each other to coordinate jobs

# Grid Computing





# Grid Computing



# Utility Computing

Utility computing is a model in which computing resources are provided to the customer based on specific demand. The service provider charges exactly for the services provided, instead of a flat rate.

# Utility Computing

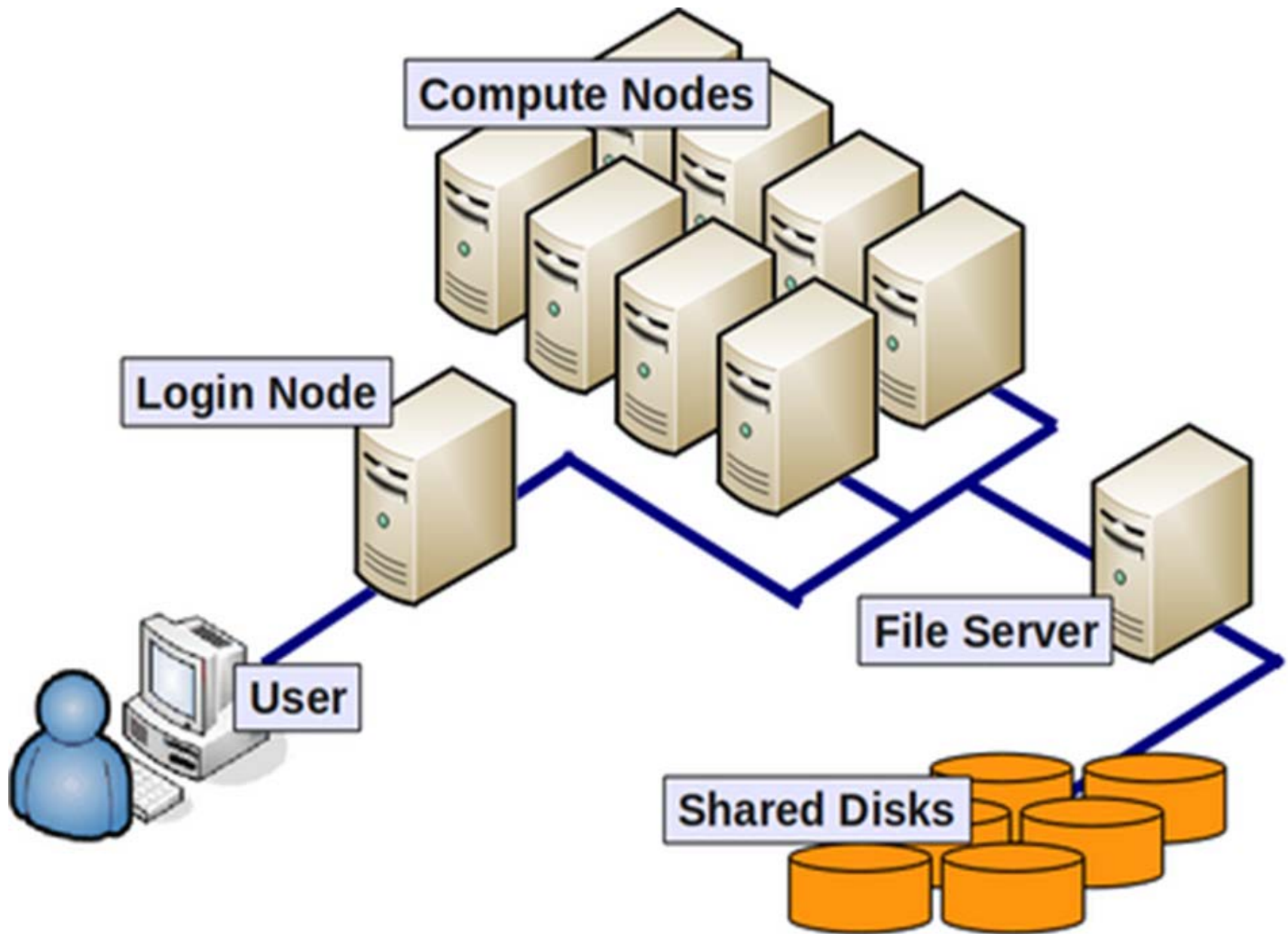
## UTILITY COMPUTING

The word **utility** is used to make an analogy to other services, such as electrical power; **pay-per-use** or **metered service**.



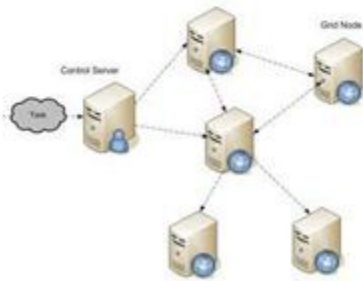
# Cluster Computing

Cluster computing **defines several computers linked on a network and implemented like an individual entity.** Each computer that is linked to the network is known as a node. Cluster computing provides solutions to solve difficult problems by providing faster computational speed, and enhanced data integrity



## Grid Computing

- Solving large problems with parallel computing
- Made mainstream by Globus Alliance



## Utility Computing

- Offering computing resources as a metered service
- Introduced in late 1990s



## Software as a Service

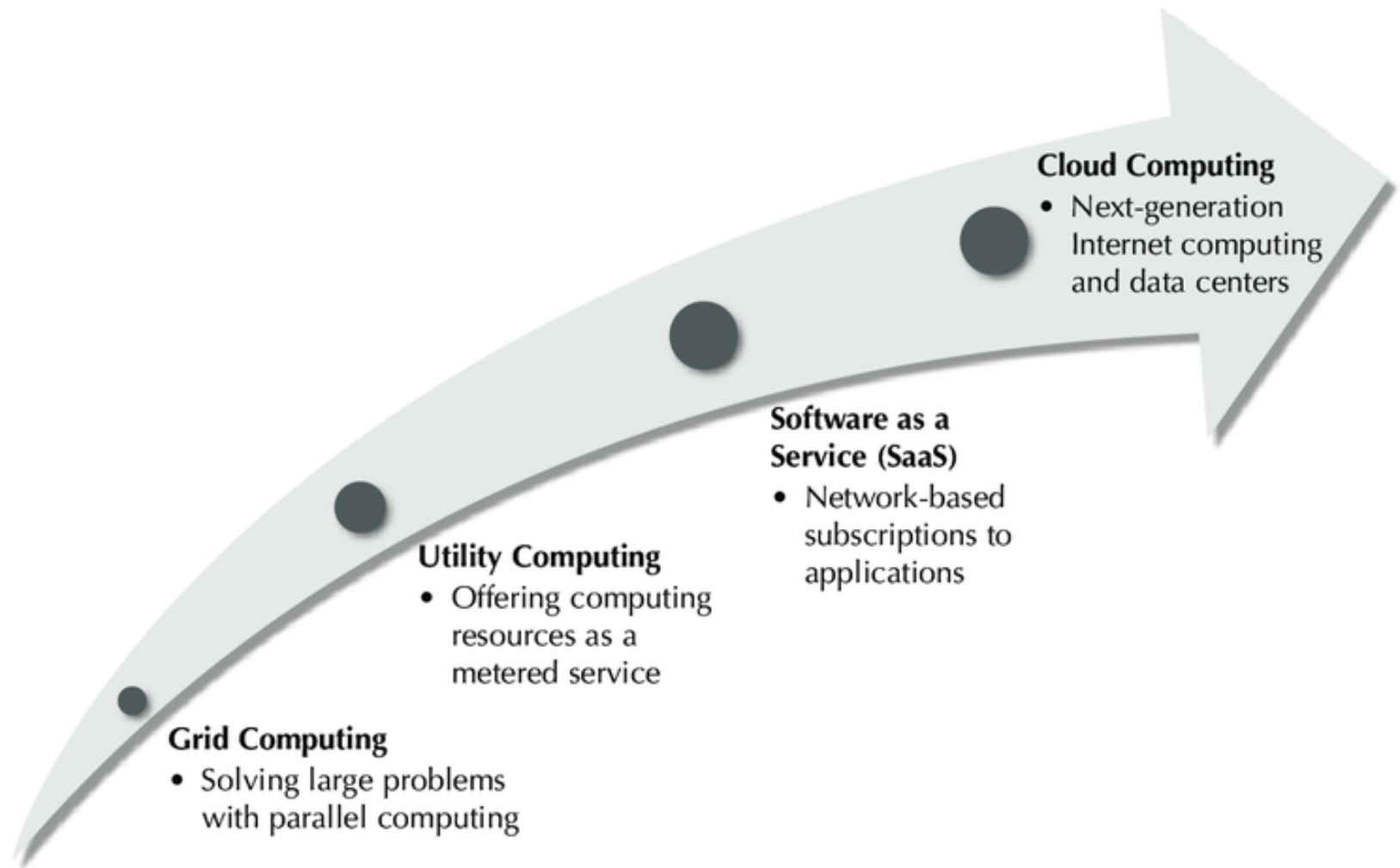
- Network-based subscription to applications
- Gained momentum in 2001



## Cloud Computing

- Next-Generation Internet computing
- Next Generation Data Centers





# COMPARISON OF COMPUTING

Grid Computing	Utility Computing	Cluster Computing	Cloud Computing
Loosely coupled	On-demand pricing	Tightly coupled systems	On-demand self-service
Diversity and Dynamism	Standardized Utility Computing Services.	Single system image	Broad network access
Distributed Job Management & scheduling	Share the web & other resources in the shared pool of machines	Centralized Job management & scheduling system	Resources pooling & Rapid elasticity
High-end computers (servers, clusters)	High-end computers (servers)	Commodity computers	Commodity computers and high-end servers and network attached storage



# Cloud Computing

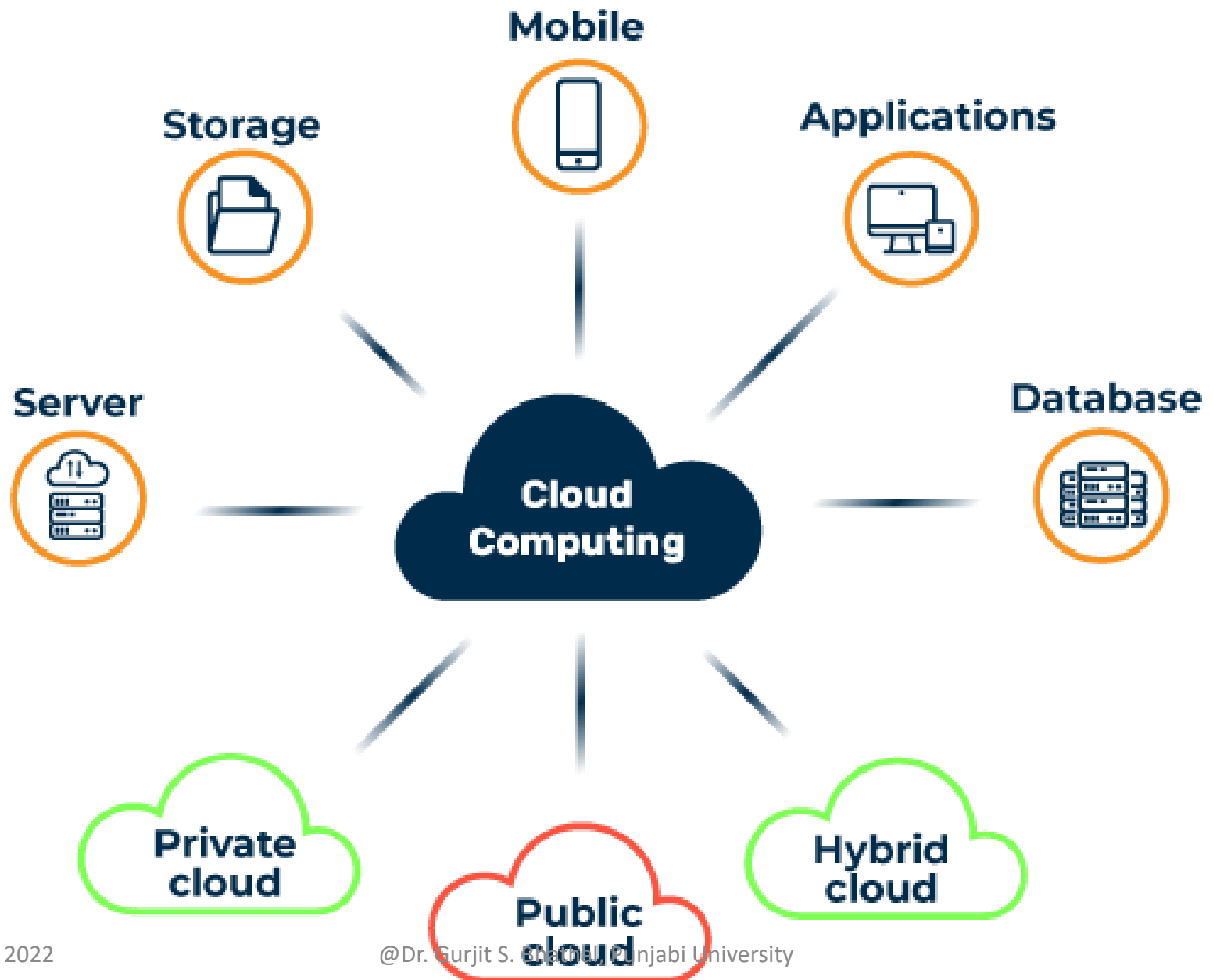
It is the on-demand availability of computer services like servers, data storage, networking, databases, etc. The main purpose of cloud computing is to give access to data centers to many users. Users can also access data from a remote server. Examples of Cloud Computing Services: AWS, Azure, Google Cloud.

# Basic Definition of Cloud Computing

- Cloud Computing is the use of various services, such as software development platforms, servers, storage and software, over the internet, often referred to as the "cloud."

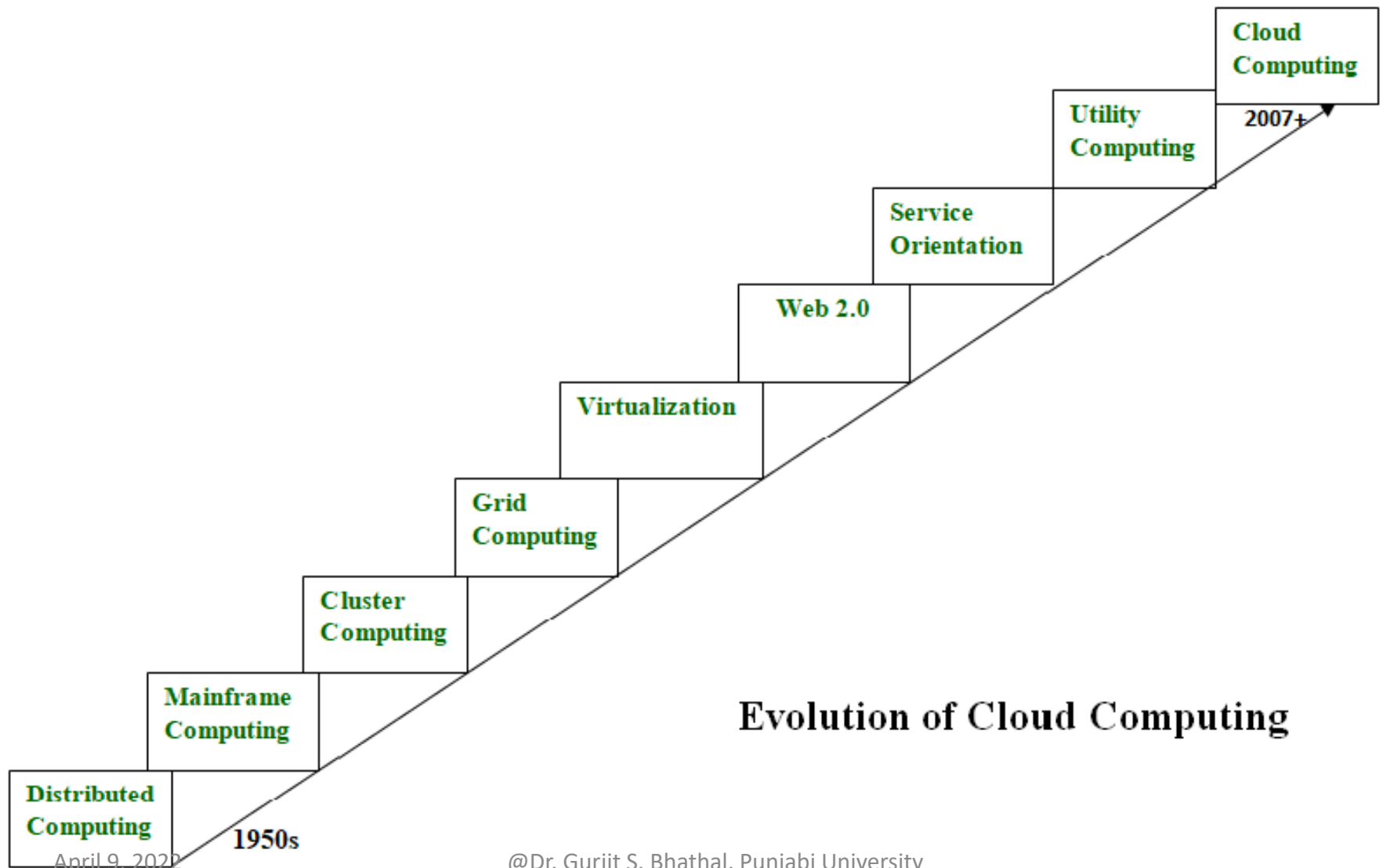
**or**

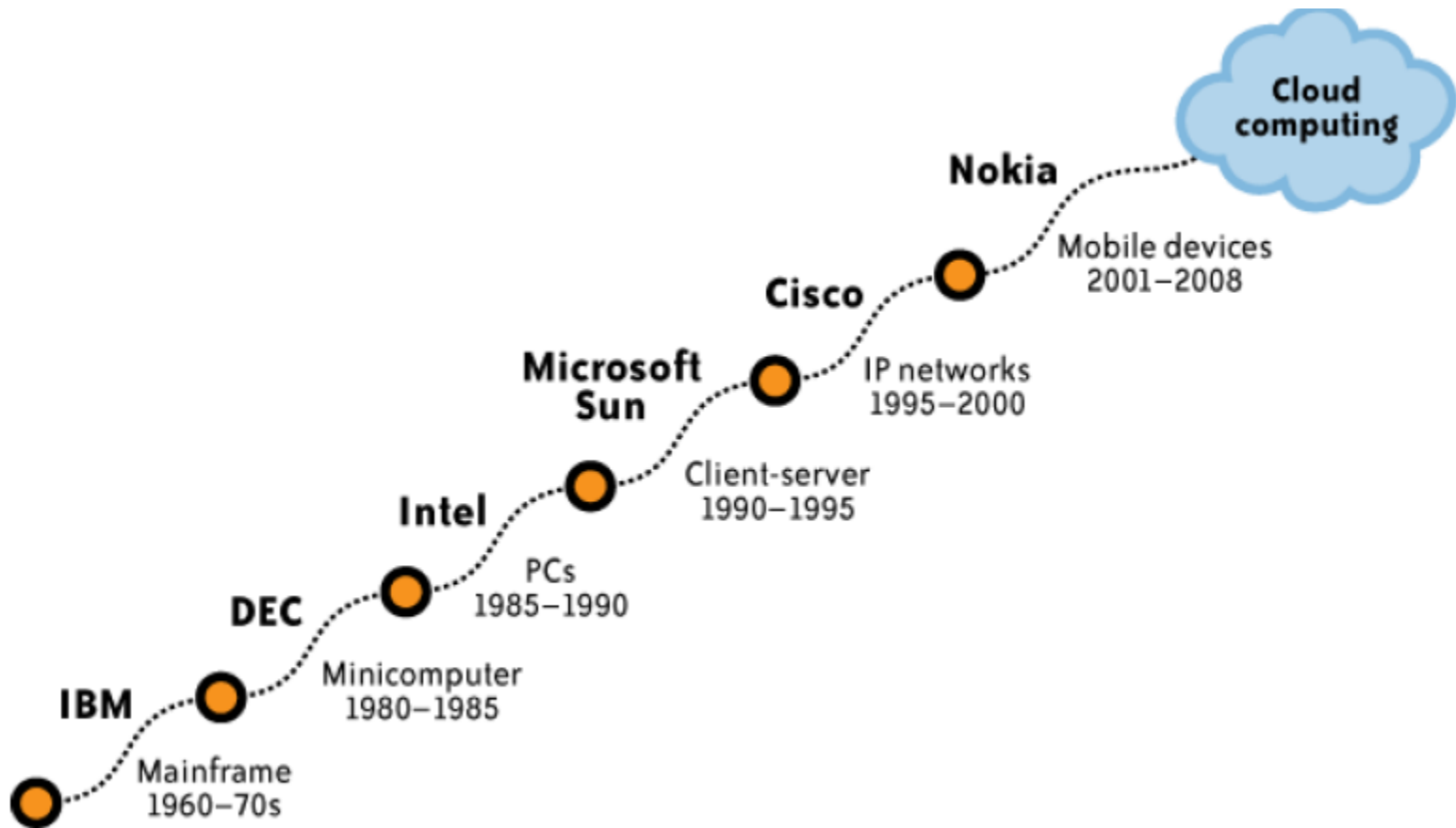
- The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.



# Evolution of Cloud Computing

Cloud computing is all about renting computing services. This idea first came in the 1950s. In cloud computing five technologies played a vital role. These are **Distributed Systems** and its **Peripherals**, **Virtualization**, **Web 2.0**, **Service Orientation**, and **Utility Computing**.





# Business Drivers for Cloud Computing

Business drivers are the key inputs that drive a business operationally and financially. Business drivers for cloud computing are cost, security, flexibility for cloud adoption.

# Business Drivers for Adoption Cloud Computing

- Cost Savings with Cloud Storage
- Cloud Storage Provides Convenience
- Flexibility and Scalability
- Cutting-Edge Security
- Suited to Your Unique Needs and Budget
- Rapid Disaster Recovery
- Improve Collaboration Among Teams

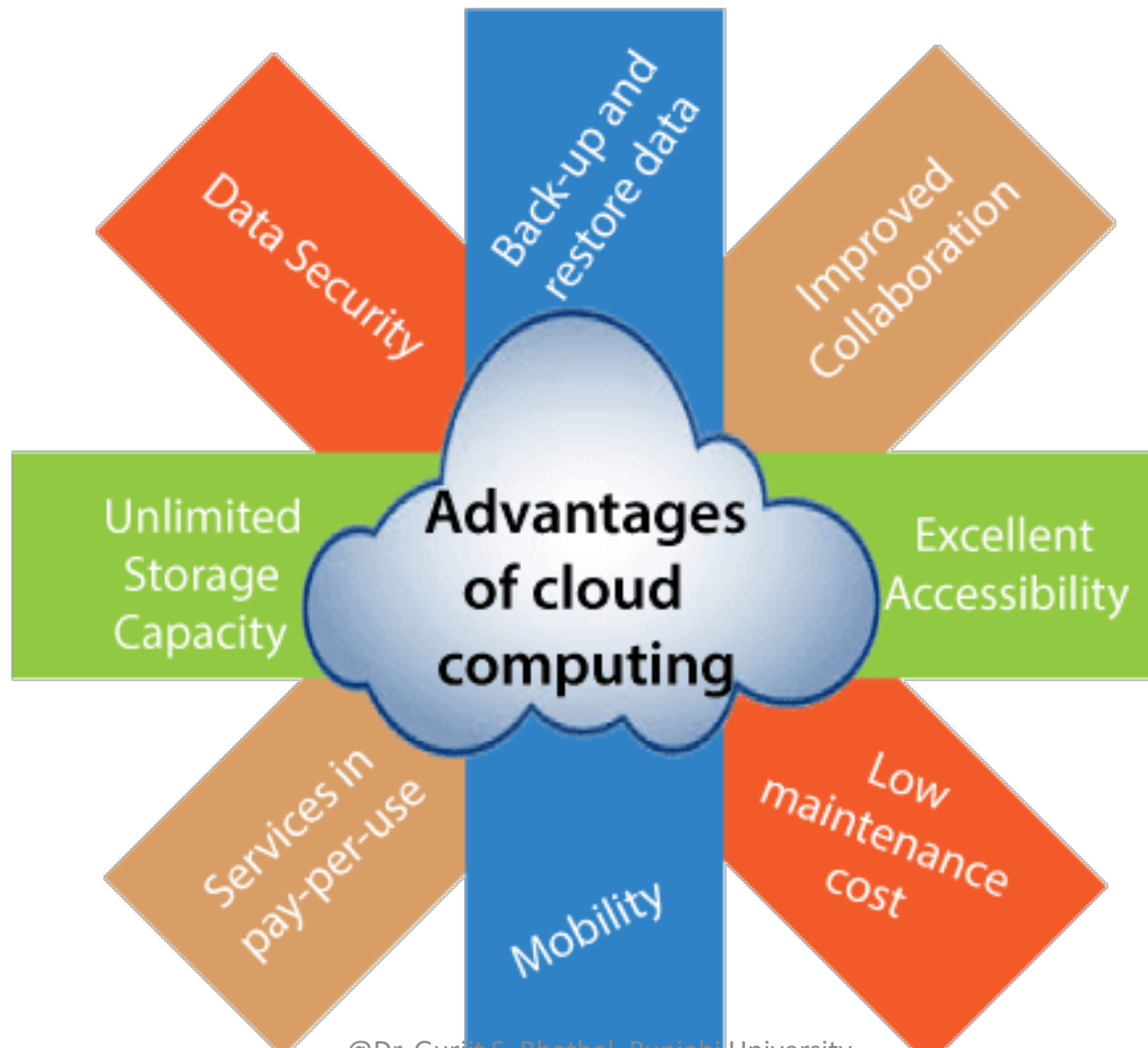
.



# Business Drivers for Cloud Computing



# Business Drivers for Cloud Computing



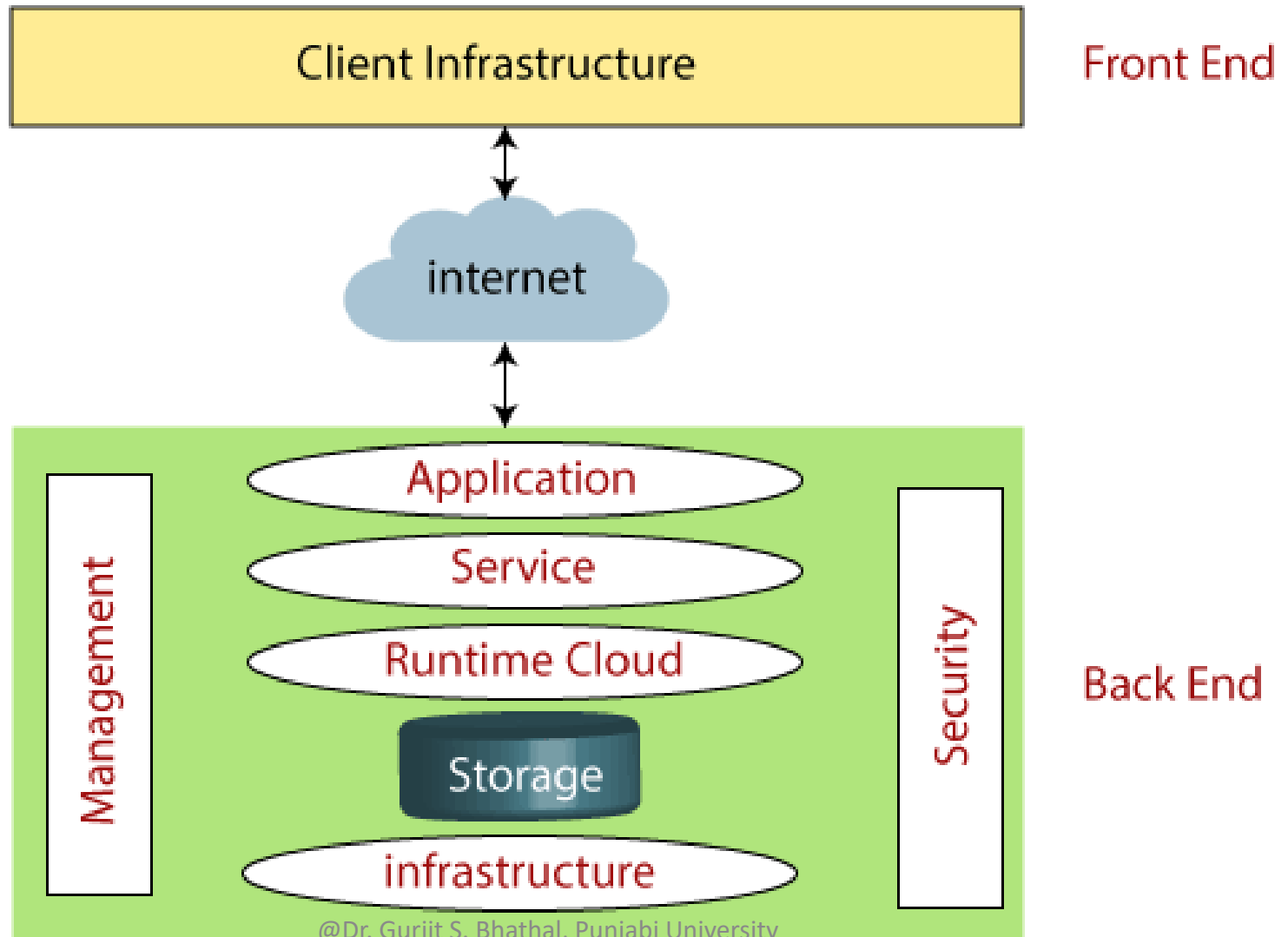
# Section-A (Part-II)

**Cloud Computing Architecture-** Cloud computing stack: Comparison with traditional computing architecture (client/server), Services provided at various levels, How Cloud Computing Works, Role of Networks in Cloud computing, protocols used, Role of Web services; Service Models (XaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Deployment Models: Public cloud, Private cloud, Hybrid cloud, Community cloud

# Cloud Computing Architecture

Architecture of cloud computing is **the combination of both SOA (Service Oriented Architecture) and EDA (Event Driven Architecture)**. Client infrastructure, application, service, runtime, storage, infrastructure, management and security all these are the components of cloud computing architecture.

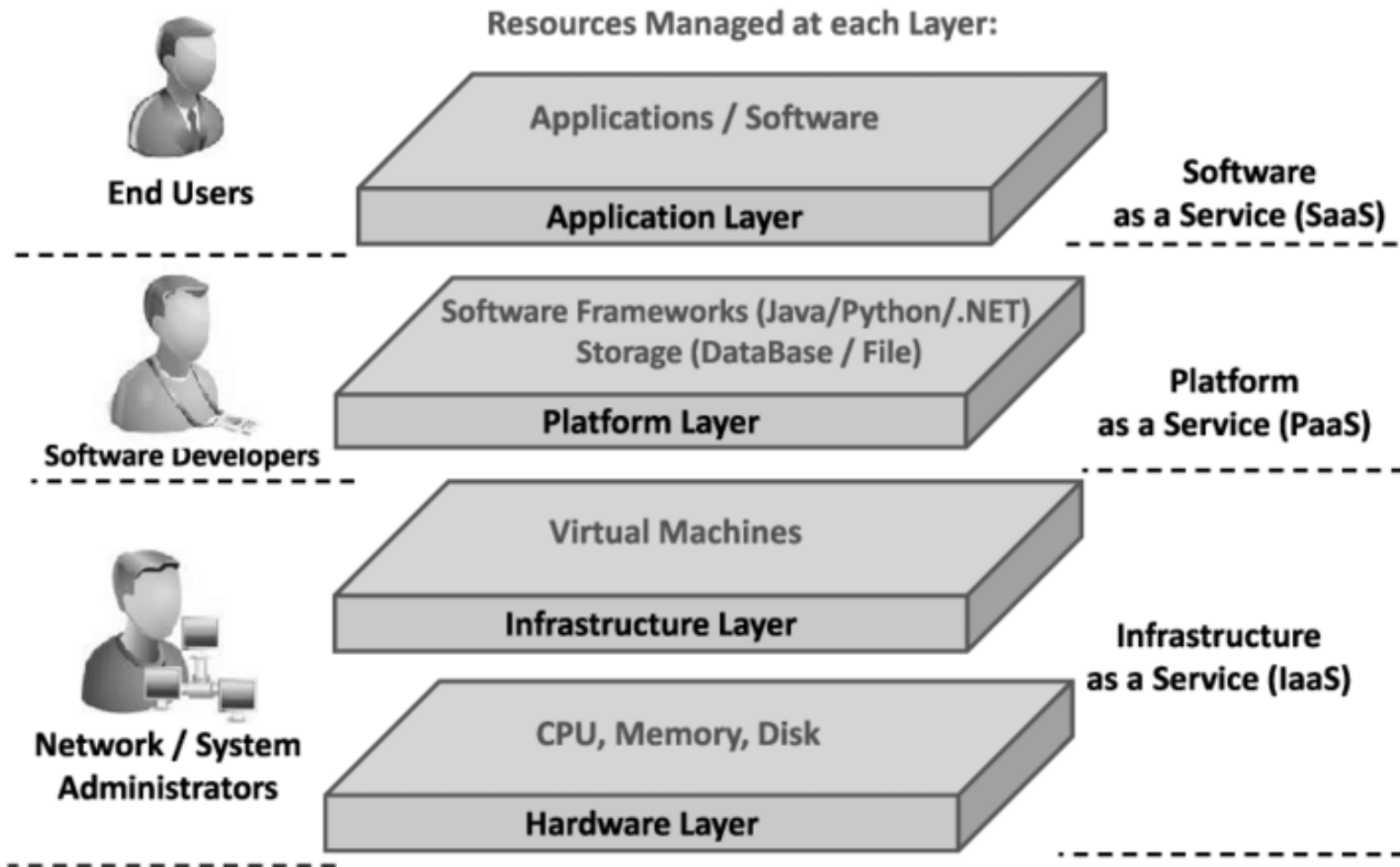
# Cloud Computing Architecture



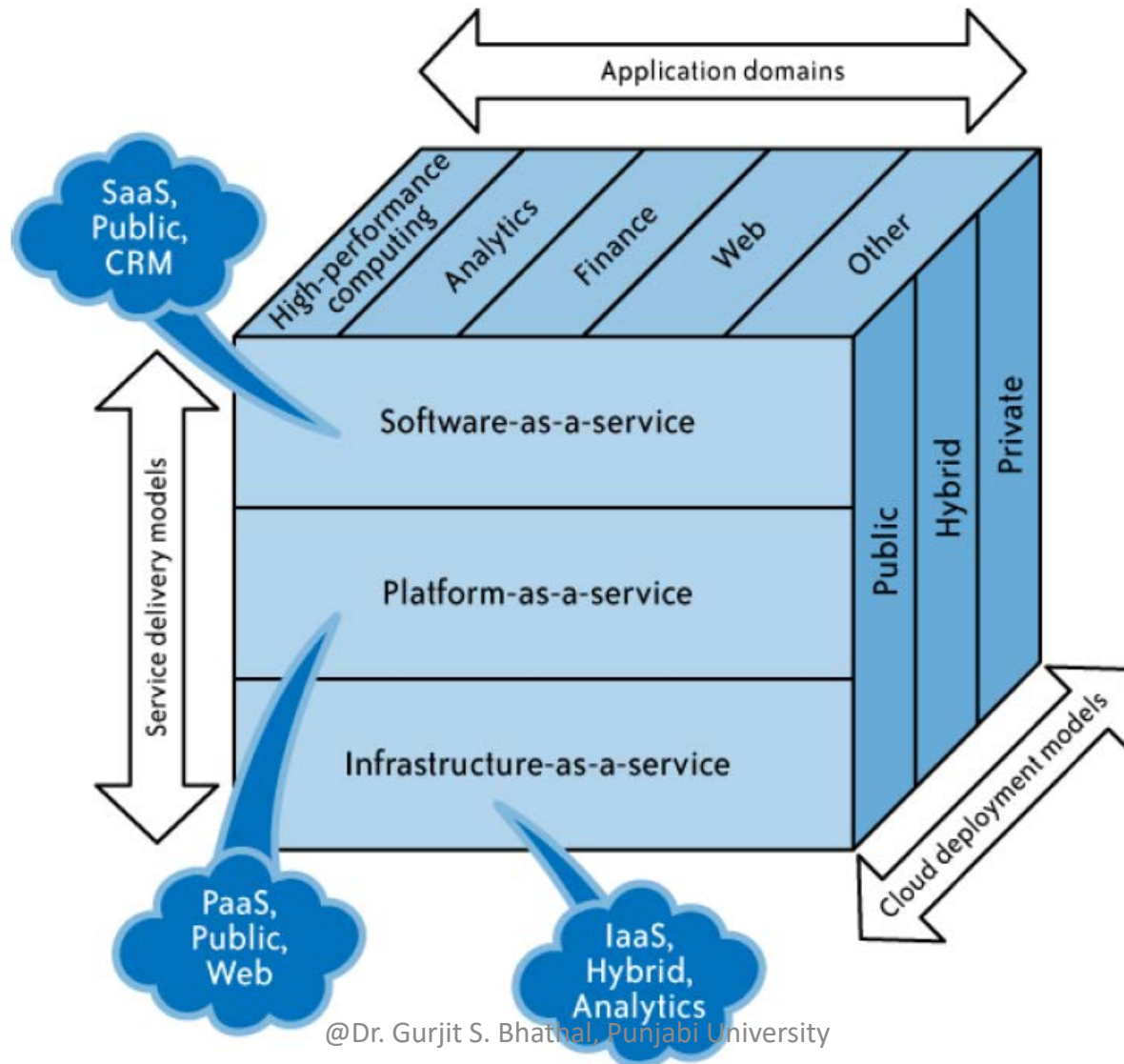
# Cloud Computing Stack

Cloud computing can be described as **a stack that is formed by layers**. Those layers will be built using cloud computing services, servers, and components, which can leverage several different clouds forming a single application stack.

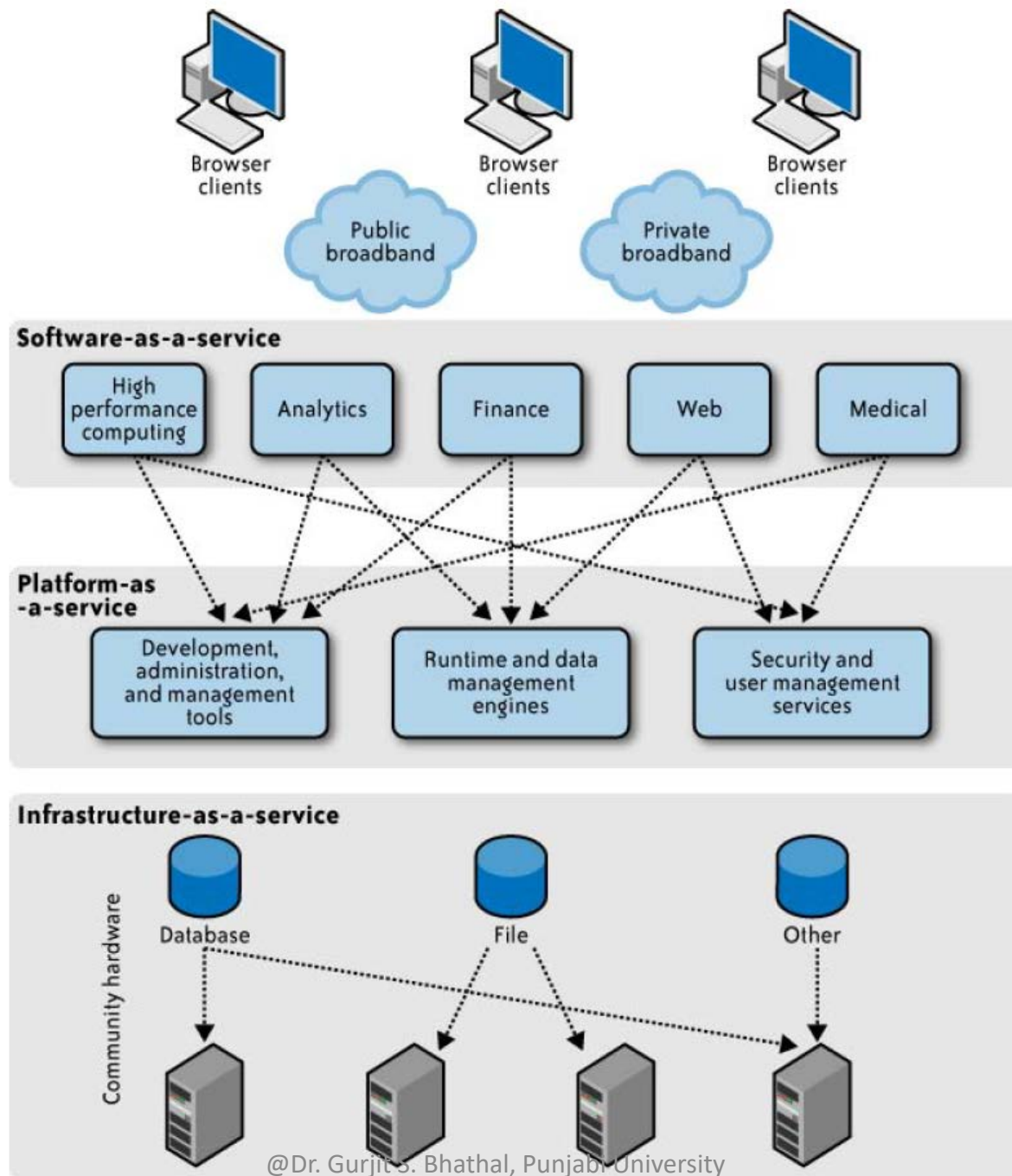
# Cloud Computing Stack



# The SPI Framework for Cloud Computing







# Cloud Computing and Traditional Client Server

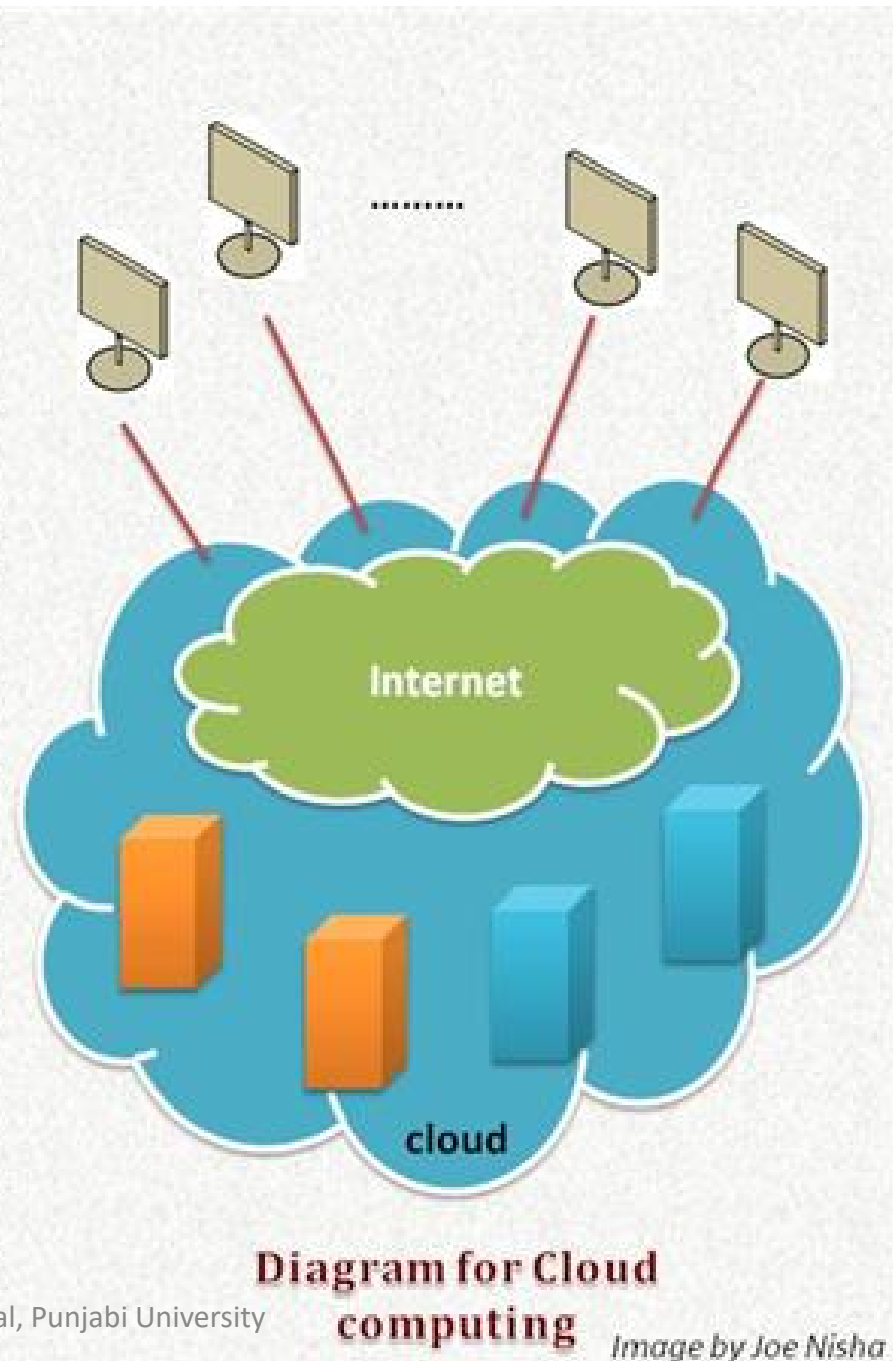
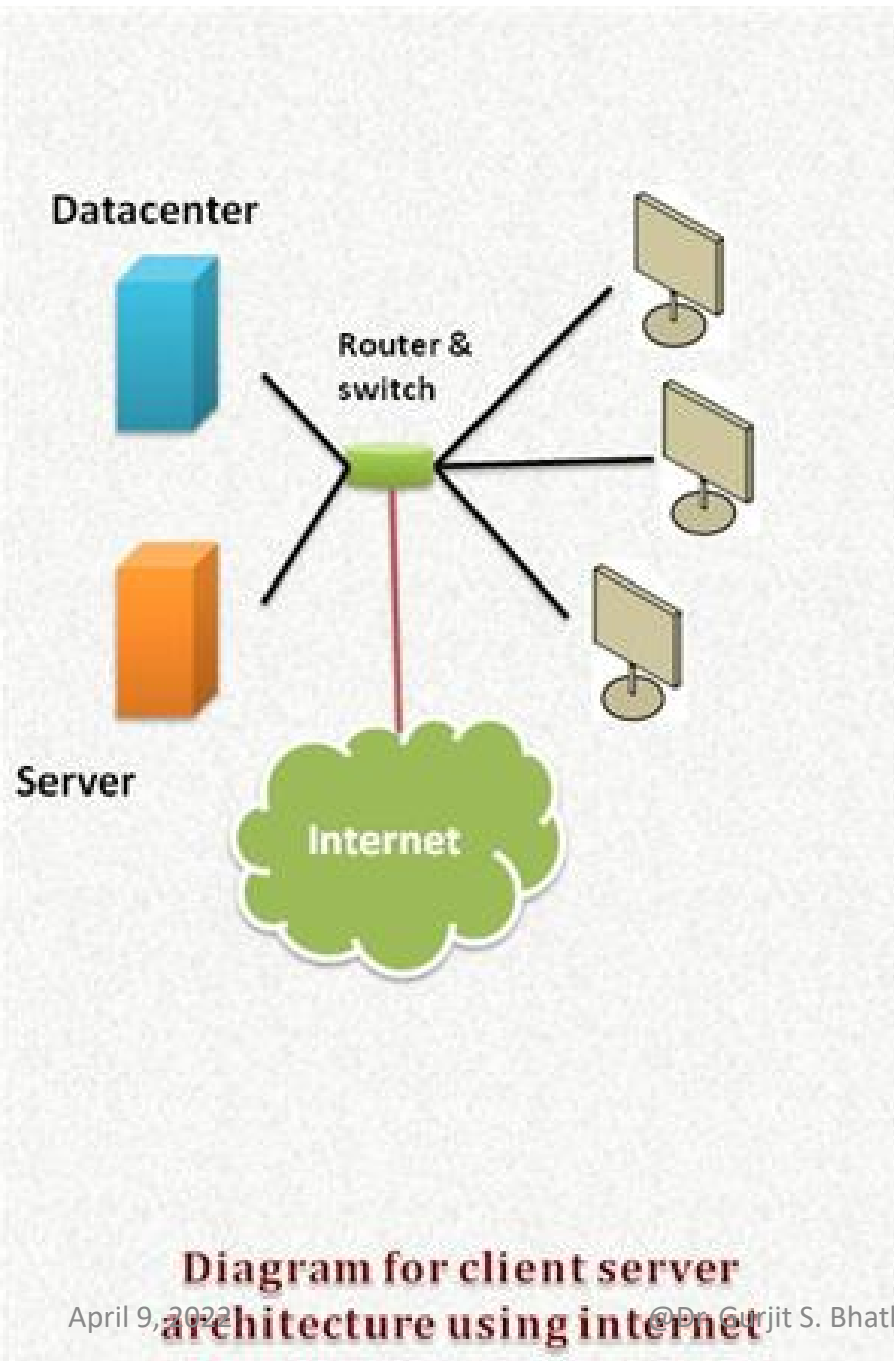
**Client-Server system, including hardware and software, is based and maintained in-house, whereas cloud-based storage is off-site in an infrastructure maintained by a third-party vendor and is accessible via the Internet.**



## TRADITIONAL HOSTING

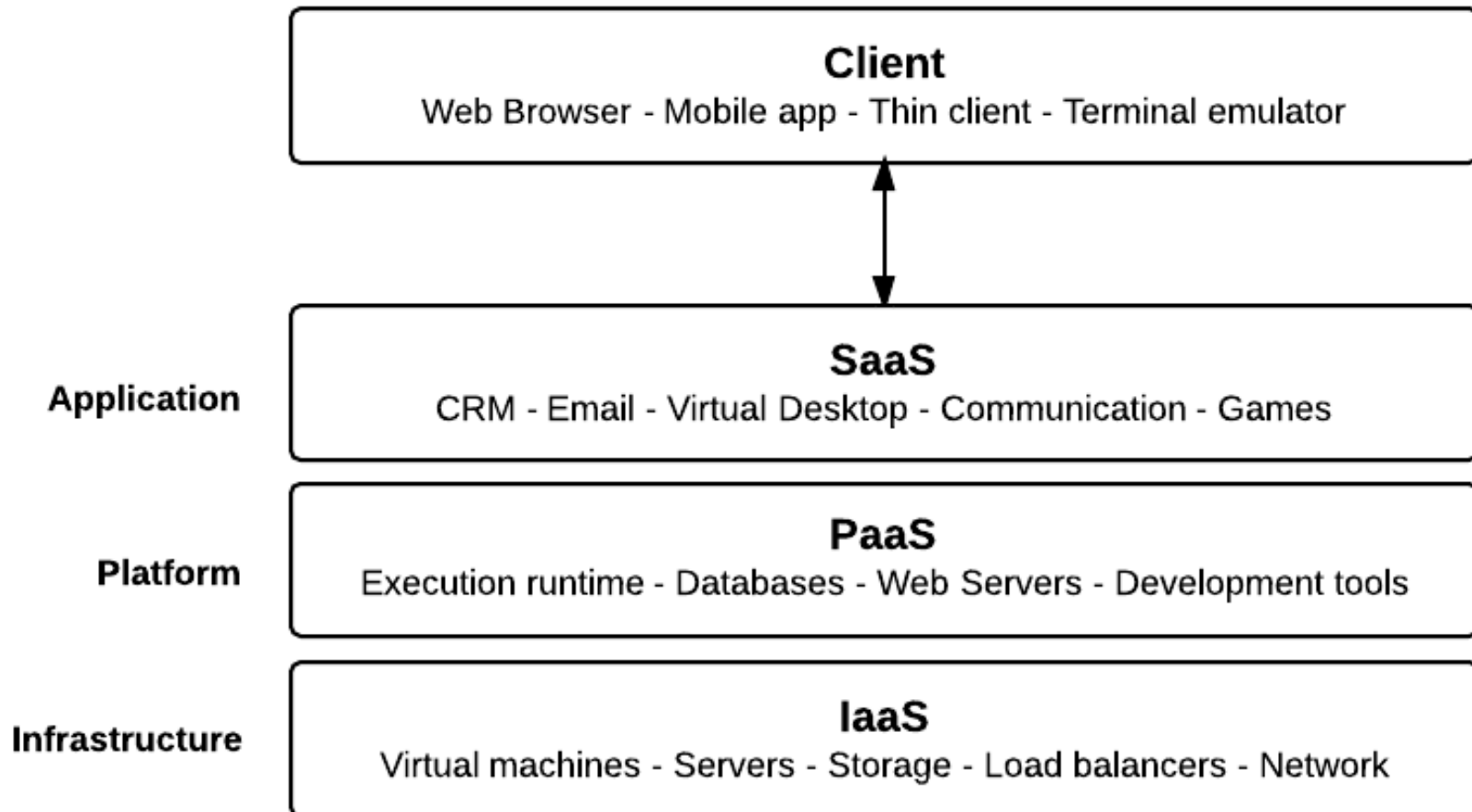





## CLOUD HOSTING



<b>Model</b>	<b>Traditional Computing</b>	<b>Cloud Computing</b>
Acquisition	<ul style="list-style-type: none"> <li>• Buy Assets</li> <li>• Build Technical Architecture</li> </ul>	<ul style="list-style-type: none"> <li>• Buy Service</li> <li>• Architecture Included</li> </ul>
Business	<ul style="list-style-type: none"> <li>• Pay for Assets</li> <li>• Administrative Over Head</li> </ul>	<ul style="list-style-type: none"> <li>• Pay for use</li> <li>• Reduce admin function</li> </ul>
Access	<ul style="list-style-type: none"> <li>• Internal Networks</li> <li>• Corporate Desktops</li> </ul>	<ul style="list-style-type: none"> <li>• Over the internet</li> <li>• Any device</li> </ul>
Technical	<ul style="list-style-type: none"> <li>• Single Tenant, Non Shared</li> <li>• Static</li> </ul>	<ul style="list-style-type: none"> <li>• Multi-tenant, scalable, elastic</li> <li>• Dynamic</li> </ul>
Delivery	<ul style="list-style-type: none"> <li>• Costly, lengthy deployments</li> <li>• Land and Expand Staffing</li> </ul>	<ul style="list-style-type: none"> <li>• Reduce deployment time</li> <li>• Fast ROI</li> </ul>

# Cloud Services on Different Levels



Service Class	Main Access & Management Tool	Service content
 SaaS	Web Browser	<b>Cloud Applications</b> Social networks, Office suites, CRM, Video processing
 PaaS	Cloud Development Environment	<b>Cloud Platform</b> Programming languages, Frameworks, Mashups editors, Structured data
 IaaS	Virtual Infrastructure Manager	<b>Cloud Infrastructure</b> Compute Servers, Data Storage, Firewall, Load Balancer

17

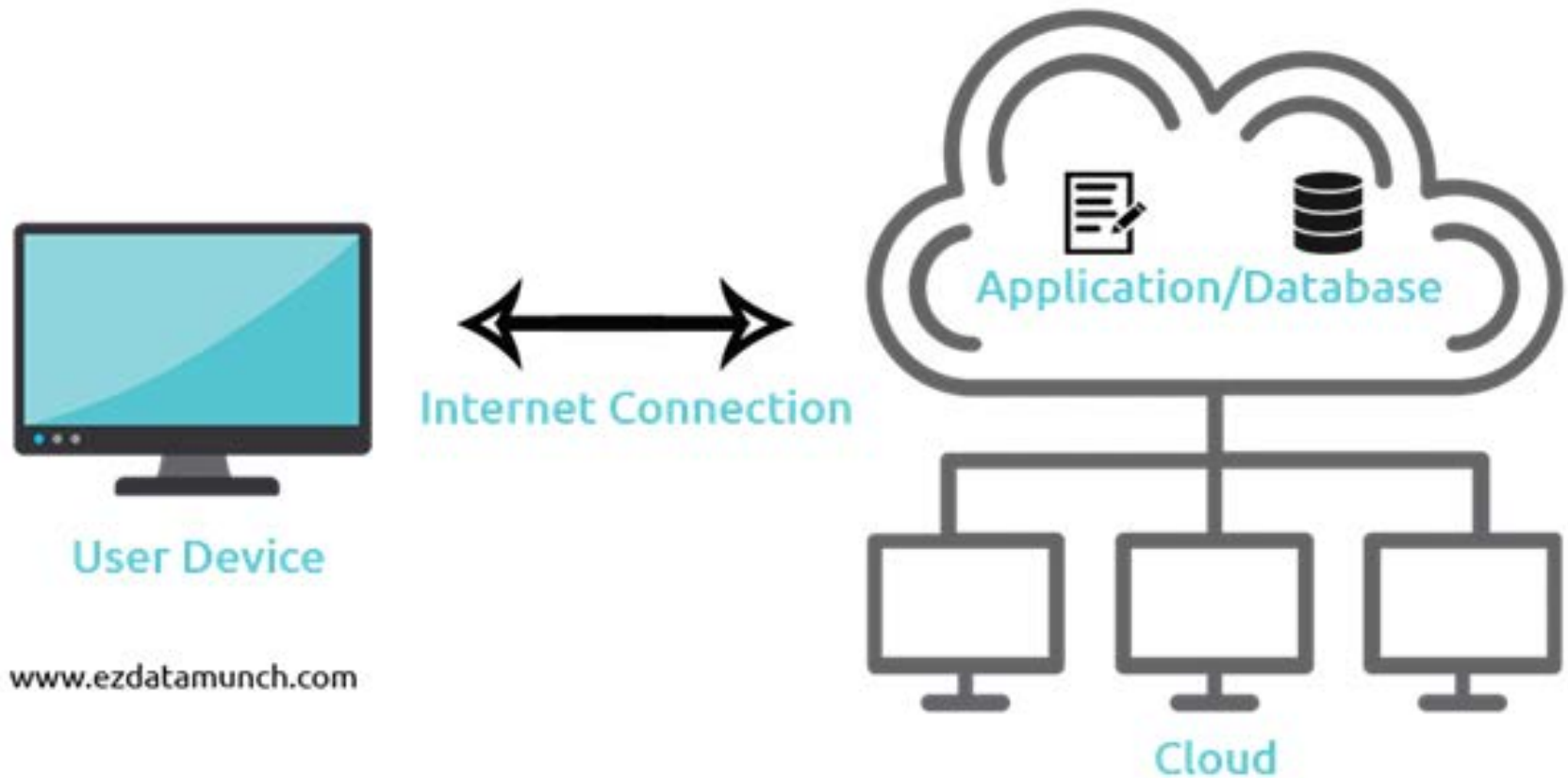
**FIGURE 1.3.** The cloud computing stack.

# Cloud Computing Working

cloud computing means storing and accessing data and programs over the internet instead of your computer's hard drive. Ultimately, the "cloud" is just a metaphor for the internet.



# Cloud Computing Working



[www.ezdatamunch.com](http://www.ezdatamunch.com)

# Network Role in Cloud Computing

The network plays a key role in the delivery of cloud-based services as it **provides a means to connect every IT system and has the ability to provision and scale these resources to meet application and end-user requirements**

# Network Protocols

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- Post office Protocol (POP)
- Simple mail transport Protocol (SMTP)
- File Transfer Protocol (FTP)
- Hyper Text Transfer Protocol (HTTP)
- Hyper Text Transfer Protocol Secure (HTTPS)

# Cloud Computing Protocols

- Secure Shell protocol (SSH)
- State Routing Protocol (SRP)
- Gossip Protocol.
- Connection-less n/w protocol (CLNP)
- Coverage Enhanced Ethernet Protocol (CEE)
- Internet Group Management Protocol (IGMP)
- Media Transfer Protocol (MTP)

# Web Server Definition

A web server is a computer that runs websites. It's a computer program that distributes web pages as they are requisitioned. The basic objective of the web server is **to store, process and deliver web pages to the users**. This intercommunication is done using Hypertext Transfer Protocol (HTTP).

# Web Services

A web service is a software module that is intended to **carry out a specific set of functions**.

Web services in cloud computing can be found and invoked over the network. The web service would be able to deliver functionality to the client that invoked the web service.

# Web Services Definition

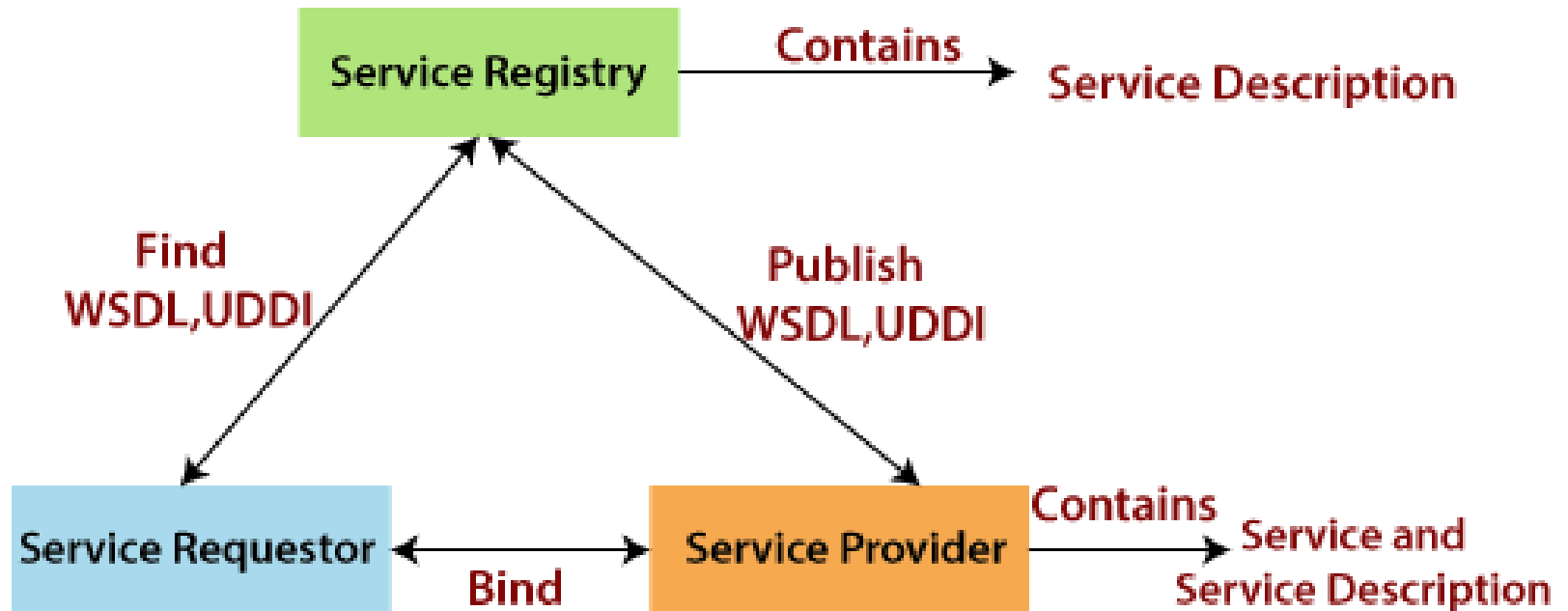
A web service is a standardized communication medium between a server and the client on the internet. Being a software module, it performs specific kinds of tasks. In cloud computing, web services are used to **provide various functionalities when invoked by a client.**

# Web Services

The architecture of web service interacts among three roles: **service provider, service requester, and service registry.** The interaction involves the three operations: publish, find, and bind.



# Web Services



Web Service Roles, Operations and Artifacts

# Cloud Computing Architecture

- Service Models
  - SaaS
  - PaaS
  - IaaS
- Deployment Models
  - Public Cloud
  - Private Cloud
  - Hybrid Cloud
  - Community Cloud

# Cloud Computing Services

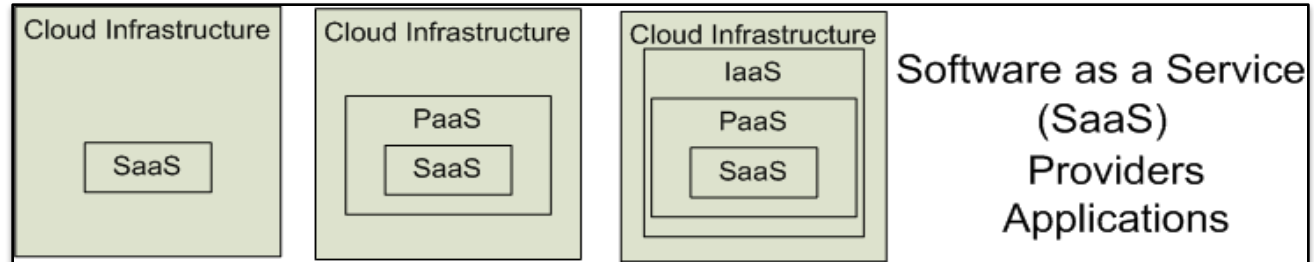
- **Infrastructure as a Service (IaaS):** This service provides the infrastructure like Servers, Operating Systems, Virtual Machines, Networks, and Storage on rent basis.  
Amazon Web Service, Microsoft Azure
- **Platform as a Service (PaaS):** This service is used in developing, testing and maintaining of software. PaaS is same as IaaS but also provides additional tools like DBMS and BI service.  
Apprenda, Red Hat OpenShift
- **Software as a Service (SaaS):** This service makes the users connect to the applications through the Internet on a subscription basis.  
Google Applications, Salesforce

# Cloud Service Models

Software as a  
Service (SaaS)

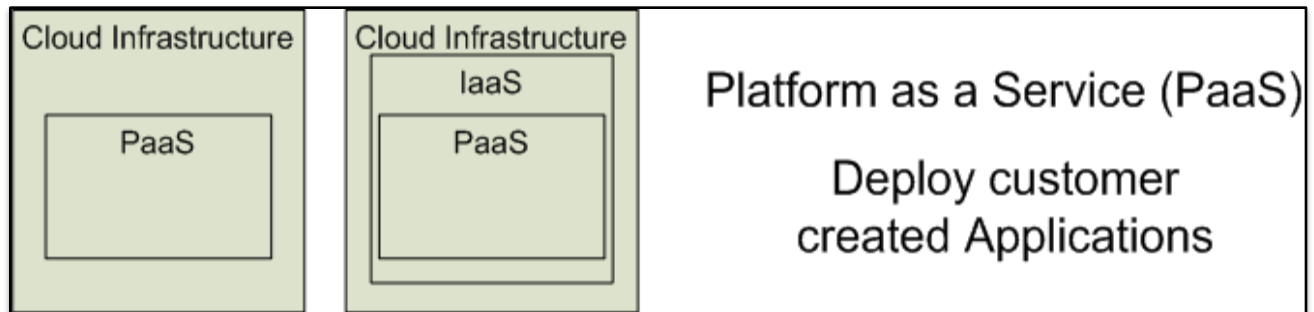
Platform as a  
Service (PaaS)

Infrastructure as a  
Service (IaaS)



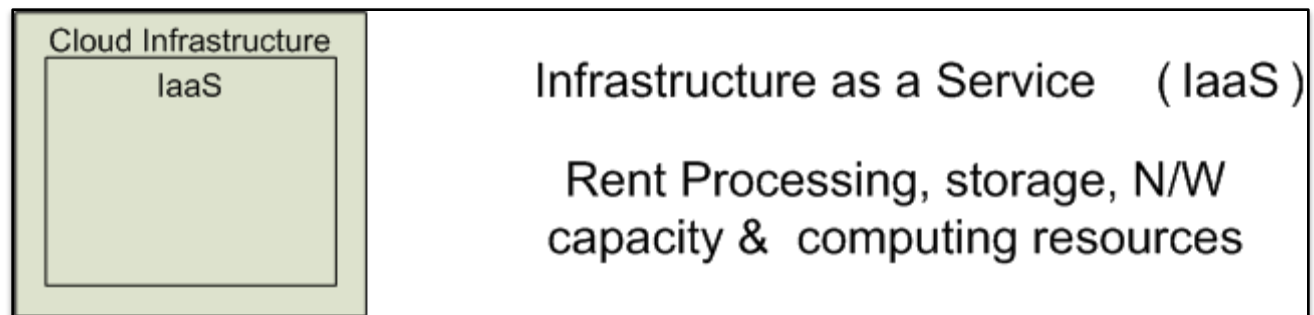
SalesForce CRM

Lotus Live



Google App  
Engine

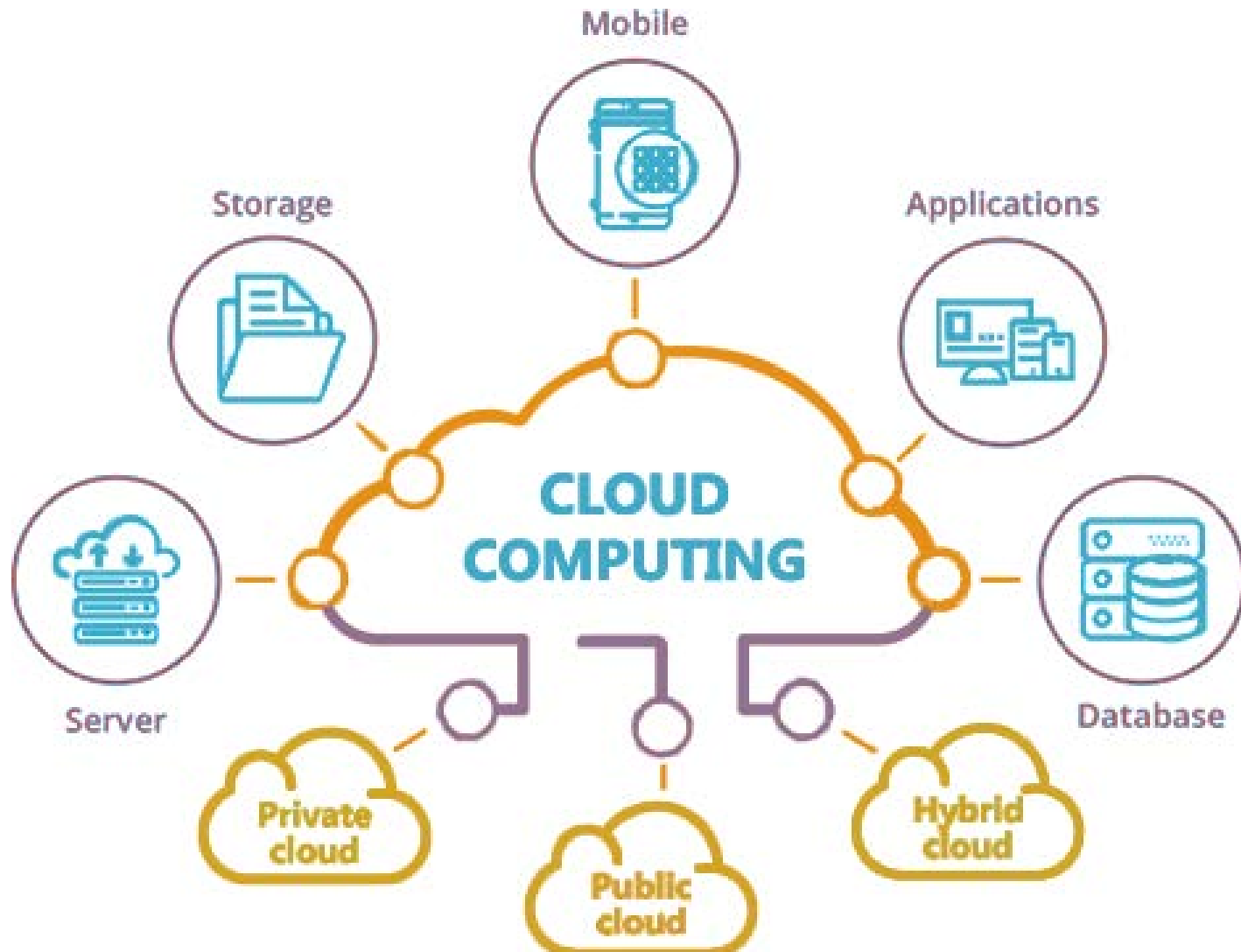
Windows Azure  
The Future Made Familiar



amazon  
web services™

rackspace®  
HOSTING

# Cloud Deployment Model and Services



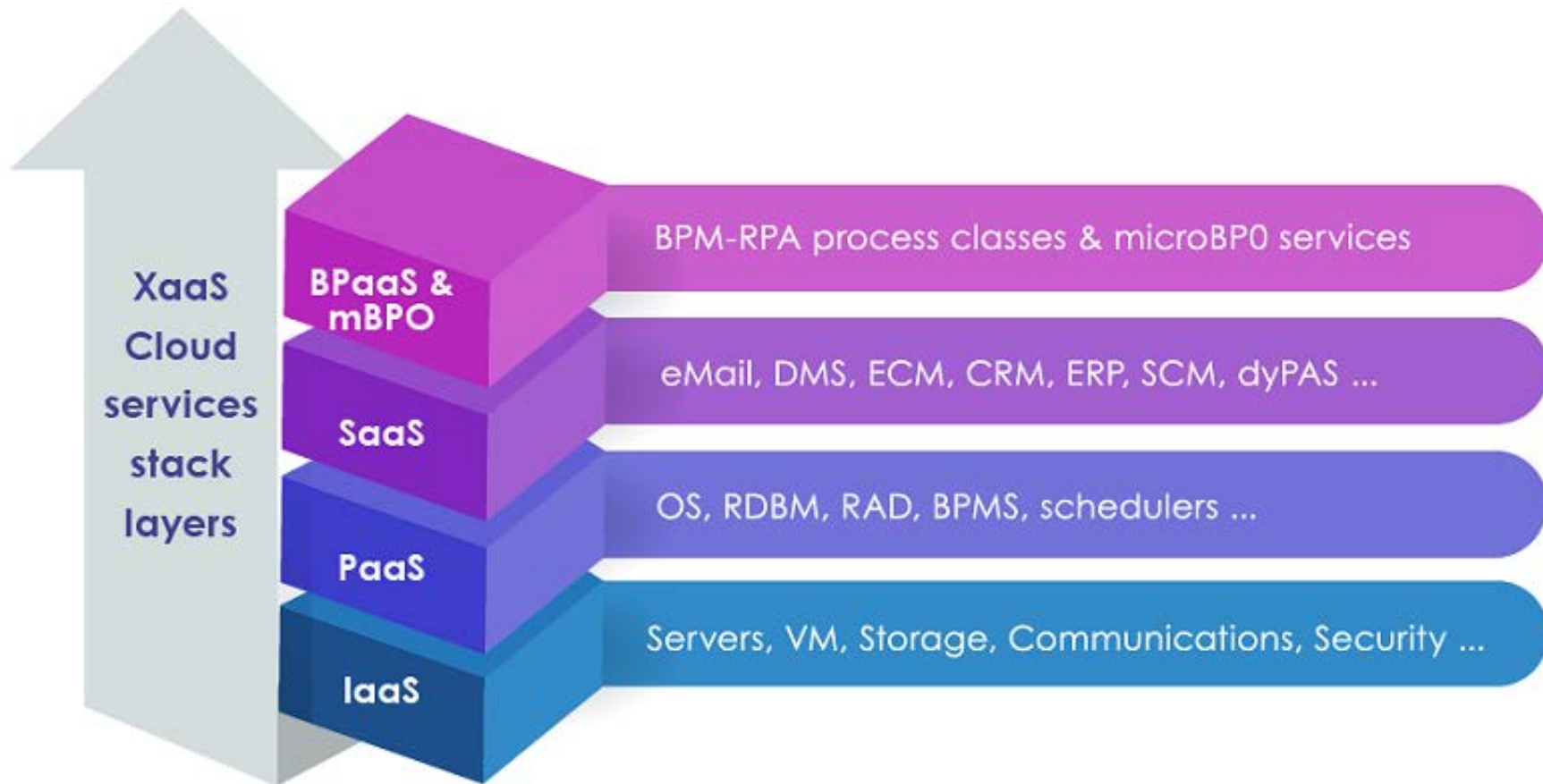
# XaaS Model

**XaaS is a general, collective term that refers to the delivery of anything as a service. It recognizes the vast number of products, tools and technologies that vendors now deliver to users as a service over a network**

# XaaS Model

- Network as a Service (NaaS)
- *Disaster Recovery as a Service (DRaaS)*
- Communications as a Service (CaaS)
- MaaS (Malware as a Service)
- DBaaS (Database as a Service)
- StaaS (Storage as a Service, also denoted as SaaS)

# XaaS Model





# Cloud Service Provider

- Amazon Web Services.
- Microsoft Azure.
- Google Cloud Platform.
- Adobe.
- VMware.
- IBM Cloud.

# Some Commercial Cloud Offerings



Amazon Elastic Compute Cloud (Amazon EC2) - Beta



TAP INTO THE  
**POWER OF NETWORK.COM**



info@3tera.com (44) 305-0050

CAREERS | SU

APPLIC | UTILITY COMPUTING | TECHNOLOGY | PARTNERS | GRID UNIVERSITY | COMPANY

Cloud Computing

Cloudware - Cloud Computing Without Compromise



**MOSSO**  
the hosting cloud



**VERIO**  
An NTT Communications Company

# Cloud Taxonomy

## Infrastructure Services

### Storage

- Amazon S3
- Amazon EBS
- CTERA Portal
- Mosso Cloud Files
- Nirvanix

### Compute

- Amazon EC2
- Serve Path GoGrid
- Elastra
- Mosso Cloud Servers
- Joyent Accelerators
- AppNexus
- Flexiscale
- ElasticHosts
- Hosting.com CloudNine
- Terramark
- GridLayer
- ITRICITY
- LayeredTech

### Services Management

- RightScale
- enStratus
- Scalr
- CohesiveFT
- Kaavo
- CloudStatus
- Ylastic
- Dynect
- CloudFoundry
- NewRelic
- Cloud42

## Cloud Software

### Data

- 10Gen MongoDB
- Oracle Coherence
- Gemstone Gemfire
- Apache CouchDb
- Apache HBase
- Hypertable
- TerraCotta
- Tokyo Cabinet
- Cassandra
- memcached

### Appliances

- PingIdentity
- Symplified
- rPath
- Vordel

### Compute

- Globus Toolkit
- Xeround
- Beowulf
- Sun Grid Engine
- Hadoop
- OpenCloud
- Gigaspace
- DataSynapse
- Xeround

### File Storage

- EMC Atmos
- ParaScale
- Zmanda
- CTERA

### Cloud Management

- 3Tera App Logic
- OpenNebula
- Open.ControlTier
- Enomaly Enomalism
- Altor Networks
- VMware vSphere
- OnPathTech
- CohesiveFT VPN Cubed
- Hyperic
- Eucalyptus
- Reductive Lbs Puppet
- OpenQRM
- Appistry

## CLOUD TAXONOMY

## Platform Services

### General Purpose

- Force.com
- Etelos
- LongJump
- AppJet
- Rollbase
- Bungee Labs Connect
- Google App Engine
- Engine Yard
- Caspio
- Qrimp
- MS Azure Services Platform
- Mosso Cloud Sites

### Business Intelligence

- Aster DB
- Quantivo
- Cloud9 Analytics
- Blink Logic
- K2 Analytics
- LogiXML
- Oco
- Panorama
- PivotLink
- Sterna
- ColdLight Neuron
- Infobright
- Vertica

### Integration

- Amazon SQS
- MuleSource Mule OnDemand
- Boomi
- SnapLogic
- OpSource Connect
- Cast Iron
- Microsoft BizTalk Services
- gnip
- SnapLogic SaaS Solution Packs
- Appian Anywhere
- HubSpan
- Informatica On-Demand

### Development & Testing

- Keynote Systems
- Mercury
- SOASTA
- SkyTap
- Aptana
- LoadStorm
- Collabnet
- Dynamsoft

### Database

- Google BigTable
- Amazon SimpleDB
- FathomDB
- Microsoft SDS

## Software Services

### Billing

- Aria Systems
- eVapt
- OpSource
- Redi2
- Zuora

### Financials

- Concur
- Xero
- Workday
- Beam4d

### Legal

- DirectLaw
- Advologix
- Fios
- Sertifi

### Sales

- Xactly
- LucidEra
- StreetSmarts
- Success Metrics

### Desktop Productivity

- Zoho
- IBM Lotus Live
- Google Apps
- Desktoptwo
- Parallels
- ClusterSeven

### Human Resources

- Taleo
- Workday
- iCIMS

### Content Management

- Clickability
- SpringCM
- CrownPoint

### Backup & Recovery

- JungleDisk
- Mozy
- Zmanda Cloud Backup
- OpenRSM
- Synclplicity

### CRM

- NetSuite
- Parature
- Responsys
- Rightnow
- Salesforce.com
- LiveOps
- MSDynamics
- Oracle On Demand

### Document Management

- NetDocuments
- Questys
- DocLanding
- Aconex
- Xythos
- Knowledge TreeLive
- SpringCM

### Collaboration

- Box.net
- DropBox

### Social Networks

- Ning
- Zemby
- Amityive

# Section-A (Part-III)

**Service Management in Cloud Computing:** Service Level Agreements (SLAs), Billing and Accounting, Comparing Scaling Hardware: Traditional vs. Cloud, Economics of scaling: Benefitting Enormously, Managing Data: Looking at Data, Scalability & Cloud Services, Database & Data Stores in Cloud, Large Scale Data Processing.

# Service Management in Cloud

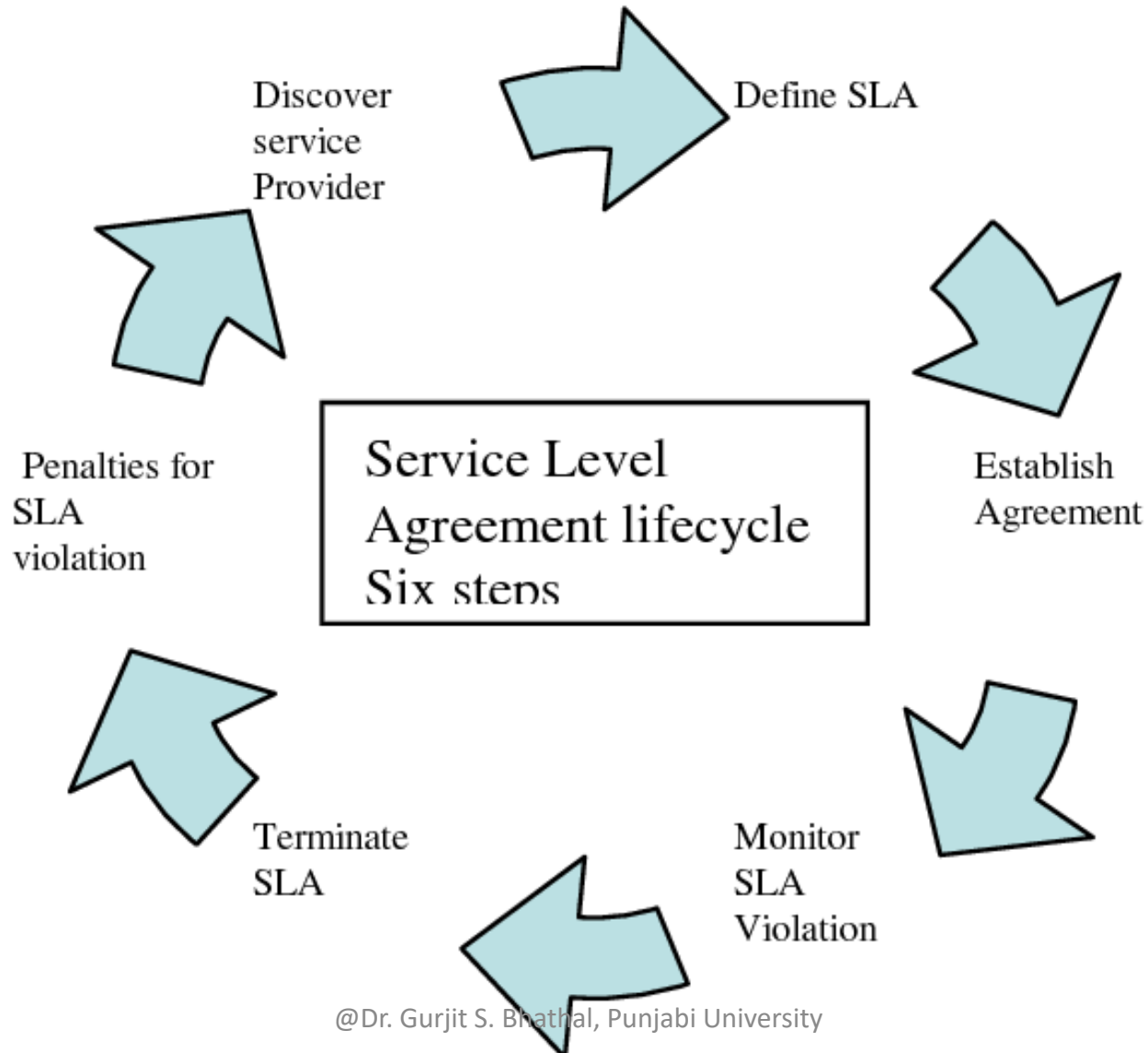
- Cloud Service Management (CSM) is the cloud version of Information Technology Service Management (ITSM). Traditionally, IT departments have had to manage both hardware and software in order to deliver IT services in an efficient and cost-effective manner.
- IT services moves toward remote resources started off with the centralization. Remote IT administration has enabled businesses to remove the need for IT experts to be present on every site.

# Service Level Agreement (SLA)

A cloud SLA (cloud service-level agreement) is an agreement between a cloud service provider and a customer that ensures a minimum level of service is maintained. Particular aspects of the service, such as quality, availability, responsibilities are agreed upon between the service provider and the service user.

- Customer-based SLA
- Service-based SLA
- Multilevel SLA

# SLA Life Cycle



# Billing and Accounting

- In metered-billing pricing model, the cloud-based application must be able to track your usage level and automatically calculate a price that matches your usage level.
- Cloud accounting gives you access to your key business numbers 24/7, from any location where you can access the internet, removing the need to work from one central office-based computer. Log in via a web browser from your laptop, or use your provider's mobile app to access your accounts from your phone or tablet.



# Scalability Vs Elasticity

Scalability is used to meet the static increase in the workload. Elasticity is used to meet dynamic changes, where the resources need can increase or decrease.

# Scalability Vs Elasticity

Cloud Elasticity	Cloud Scalability
Elasticity is used just to meet the sudden up and down in the workload for a small period of time.	Scalability is used to meet the static increase in the workload.
Elasticity is used to meet dynamic changes, where the resources need can increase or decrease.	Scalability is always used to address the increase in workload in an organization.
Elasticity is commonly used by small companies whose workload and demand increases only for a specific period of time.	Scalability is used by giant companies whose customer circle persistently grows in order to do the operations efficiently.
It is a short term planning and adopted just to deal with an unexpected increase in demand or seasonal demands.	Scalability is a long term planning and adopted just to deal with an expected increase in demand.

# Hardware Scaling

Traditional computing is done on physical hard drive and website servers. Cloud Computing runs on third-party server which are hosted by third-party hosting companies.

	Traditional IT Infrastructure	Cloud Based Infrastructure
hardware, networking, storage	Organization will have to acquire large number of servers, setup networking with proper security and acquire large number of storage devices to store user data and setup databases.	All the hardware, networking, storage is provided by the cloud service provider. All these resources are available on rental basis or short or long terms and no need to acquire any physical hardware.
security and fault tolerance	Organization will have to setup proper security and ensure proper security measures are being taken to protect user data at all times. Fault tolerance mechanisms have to be deployed to prevent any loss of critical data in case of a failure.	Security of the infrastructure is provided by the cloud service provider but security of the services such as access to server from the web is the responsibility of the organization acquiring the hardware on the cloud. Fault tolerance mechanisms are provided by the cloud service provider to ensure zero downtime in case of failure on vendor side.
maintenance	Organization will have to do regular checkups of their hardware. Replace any malfunctioned hardware with minimal downtime. They will also have to ensure software being used are regularly updated.	Regular maintenance of the hardware is handled by the cloud service provider. Cloud service provider also handles software updates for services managed by the service provider. However, any software deployed by the customer have to be managed by the customer himself.
disaster recovery	Organization will have to do necessary backups of data and setup fall back mechanisms so in case of a disaster such as earthquake, fire, power outages not only the data is preserved, the users don't face any downtimes.	Cloud service providers have global infrastructure with multiple data centers within one region to ensure in case of any disaster services are uninterrupted and user data saved all the times.
IT staff	A team of trained IT professionals had to be hired to operate and monitor the entire infrastructure 24/7.	Cloud service providers have highly trained IT staff that work 24/7 to ensure best service to their customers. Customers just need to use the services they would like. They also provide customer support for any queries or troubleshooting at customer's end.
space	Some viable geographical space had to be acquired either on rental or permanent basis to setup and run the entire infrastructure.	No operational concerns for the customers since all the resources are virtually provided by the cloud service providers.
flexibility and scaling	To handle increasing workloads, more and powerful hardware has to be acquired and setup so users get a seamless service even with increased burdens.	One of the most prominent features of cloud is its flexibility and scaling up or down depending upon workloads. With virtually infinite resources, any spike up or down in workloads can easily be handled and customers need not buy any additional hardware for that and just pay for the time additional resources were used.
automation	Most of the processes of scaling up or down, making the hardware more powerful, backups, monitoring etc are manual and time consuming	Everything over the cloud is automated. From deploying the infrastructure, monitoring and sending alerts to customers and taking necessary actions in case of failures, all can be automated.
cost of running and miscellaneous costs	Requires a lot of capital to acquire the necessary hardware, licenses, IT team, operational space in addition to other costs such as power supply, cooling costs, maintenance costs.	Cloud service providers just charge for the time resources are used, or the amount of storage being used or the data movement in and out of the cloud. Any resource can be released or acquired again whenever wanted with no additional costs. With most service providers using the pay as you go pricing model.

# Scalability

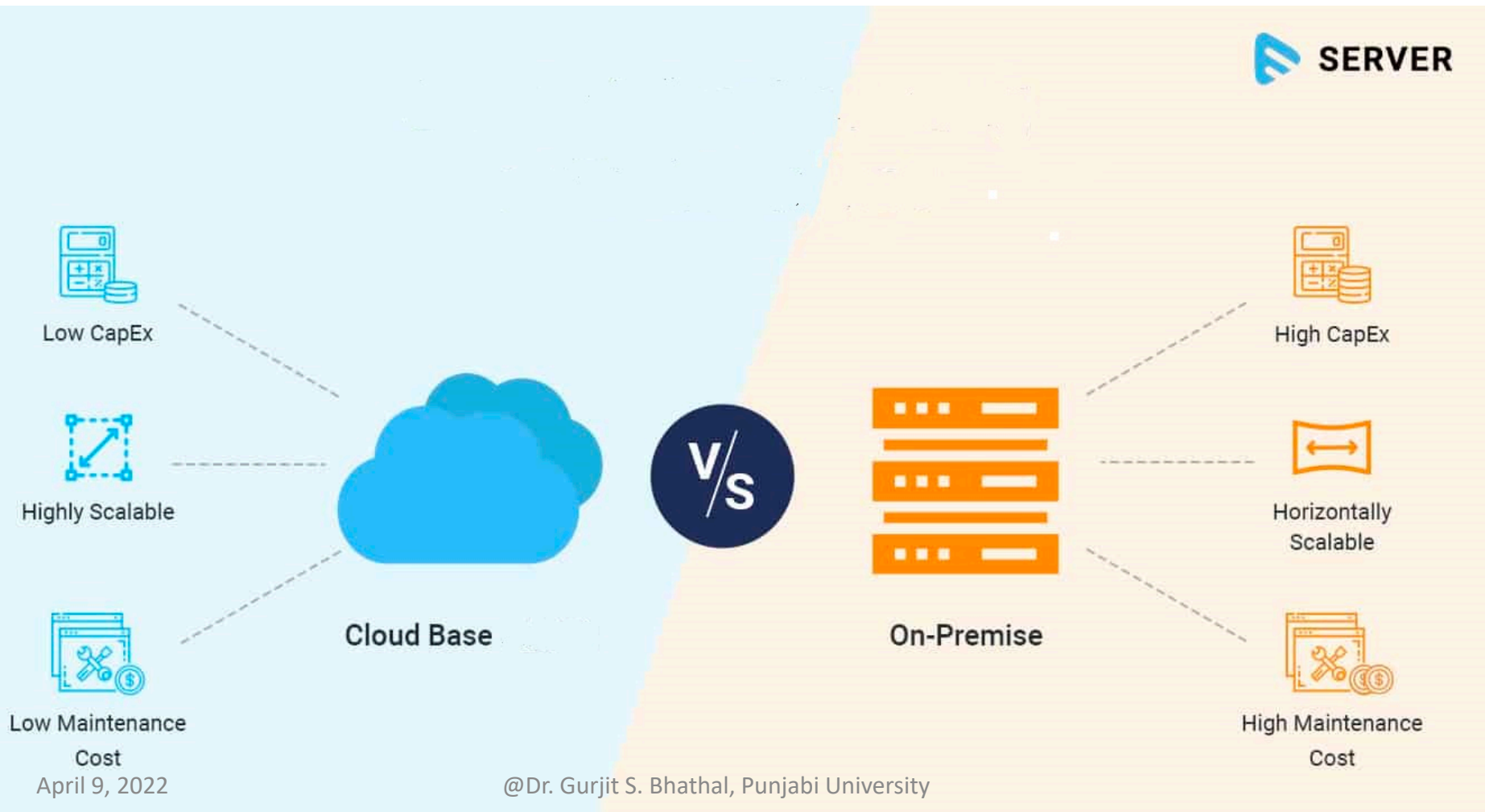
Scalability refers to the idea of a system in which every application or piece of infrastructure can be expanded to handle increased load.

- Vertical scaling
- Horizontal scaling

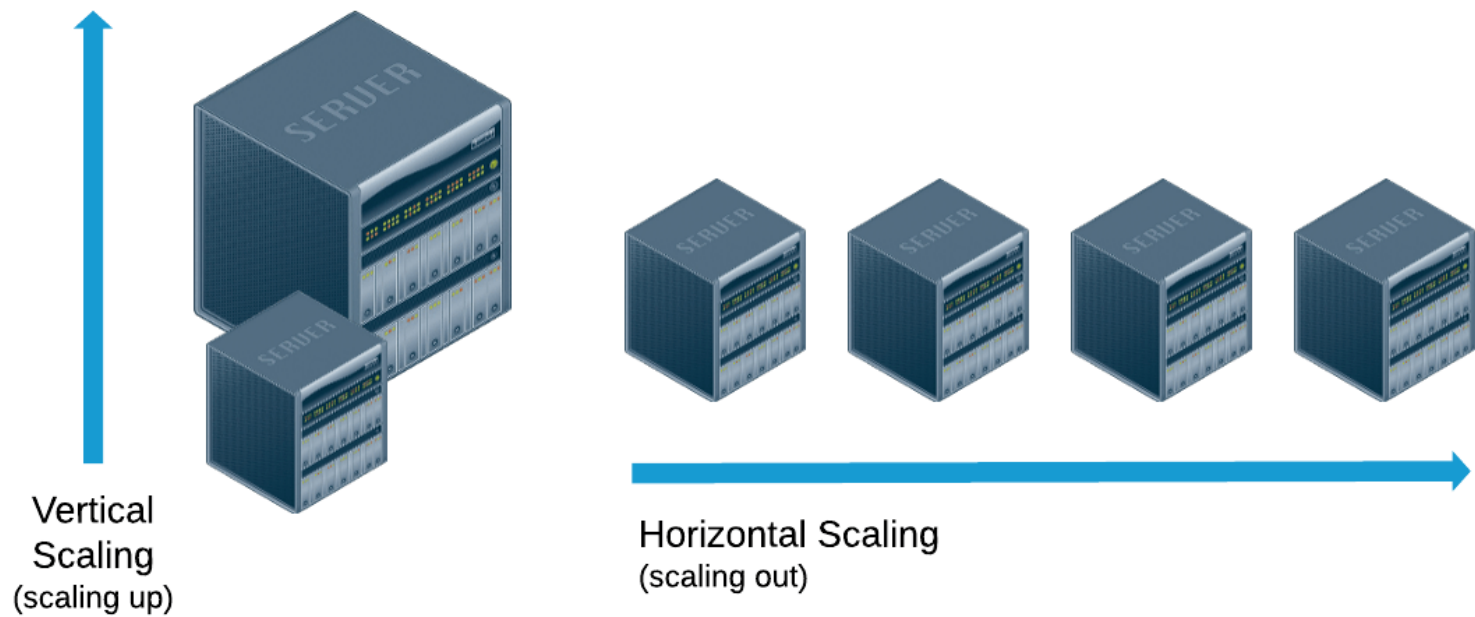
# Cloud Scalability

Scalability is one of the driving reasons to migrate to the cloud. Whether traffic or workload demands increase suddenly or grow gradually over time, a scalable cloud solution **enables organizations to respond appropriately and cost-effectively to increase storage and performance.**

# Scalability Cloud vs Traditional



# Scalability





# Economies of Scale

Through economies of scale, **cloud providers save organizations money because they purchase computing resources in massive quantities at lower costs.** When companies utilize these shared resources, they avoid the substantial up-front Capital expenditures (CapEx) costs of purchasing their own expensive infrastructure.

# Data Management

Data management is **the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively.**

# Database

**A database is an organized collection of structured information, or data, typically stored electronically in a computer system. A database is usually controlled by a database management system (DBMS).**

# Datastore

**Datastore is a schemaless database, which allows you to worry less about making changes to your underlying data structure as your application evolves.** Datastore provides a powerful query engine that allows you to search for data across multiple properties and sort as needed.

# Datastore on cloud

Datastore is a highly scalable NoSQL database for your applications. Datastore automatically handles sharding and replication, providing you with a highly available and durable database that scales automatically to handle your applications' load.

# Cloud Database

- **A cloud database is a database service built and accessed through a cloud platform.** It serves many of the same functions as a traditional database with the added flexibility of cloud computing. Users install software on a cloud infrastructure to implement the database.

# Cloud Database

- A cloud database is a database that typically runs on a cloud computing platform and access to the database is provided as-a-service. There are two common deployment models: users can run databases on the cloud independently, using a virtual machine image, or they can purchase access to a database service, maintained by a cloud database provider. Of the databases available on the cloud, some are SQL-based and some use a NoSQL data model.

# Large-Scale Data Processing

- Large-scale data processing **enables the use of diverse types of big data in a cloud environment in order to create mash-up services.**
- Large scale data processing **brings together technologies like Distributed Systems, Machine Learning, Statistics, and Internet of Things together.** It's include use cases like targeted advertising, fraud detection, product recommendations, and market surveys.



# Section-A (Part-IV)

**Cloud Security-** Infrastructure Security, Network level security, Host level security, Application level security, Data security and Storage, Data privacy and security Issues, Jurisdictional issues raised by Data location, Identity & Access Management, Access Control, Trust, Reputation, Risk Authentication in cloud computing, Client access in cloud, Cloud contracting Model, Commercial and business considerations

# Overview of Security

- Goals of IT Security – CIA Triad

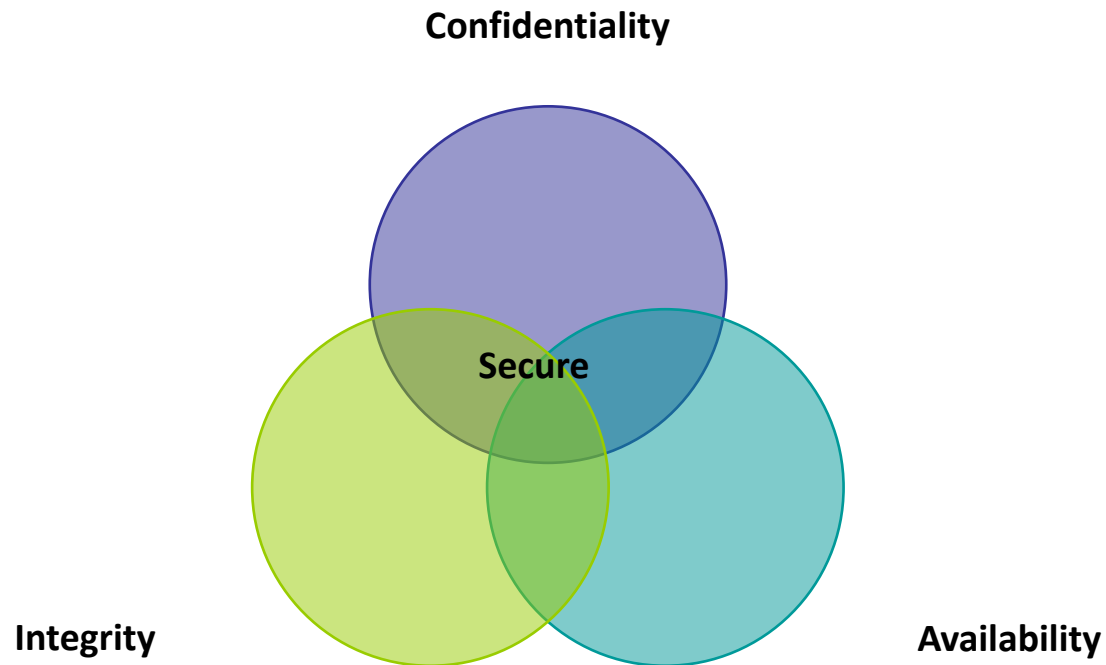
- ☐ Confidentiality

- ☐ Integrity

- ☐ Availability



# CIA Triad



# Risks

- Types Of Risk
  - Legal Risks
    - Fines, liability lawsuits, criminal prosecution
  - Financial Risks
    - Numerous costs involved including losing customer's trust, legal fees, fines
  - Reputational Risks
    - Loss of trust
  - Operational Risks
    - Failed internal processes – insider trading, unethical practices, etc.
  - Strategic Risks
    - Financial institutions future, mergers, etc.

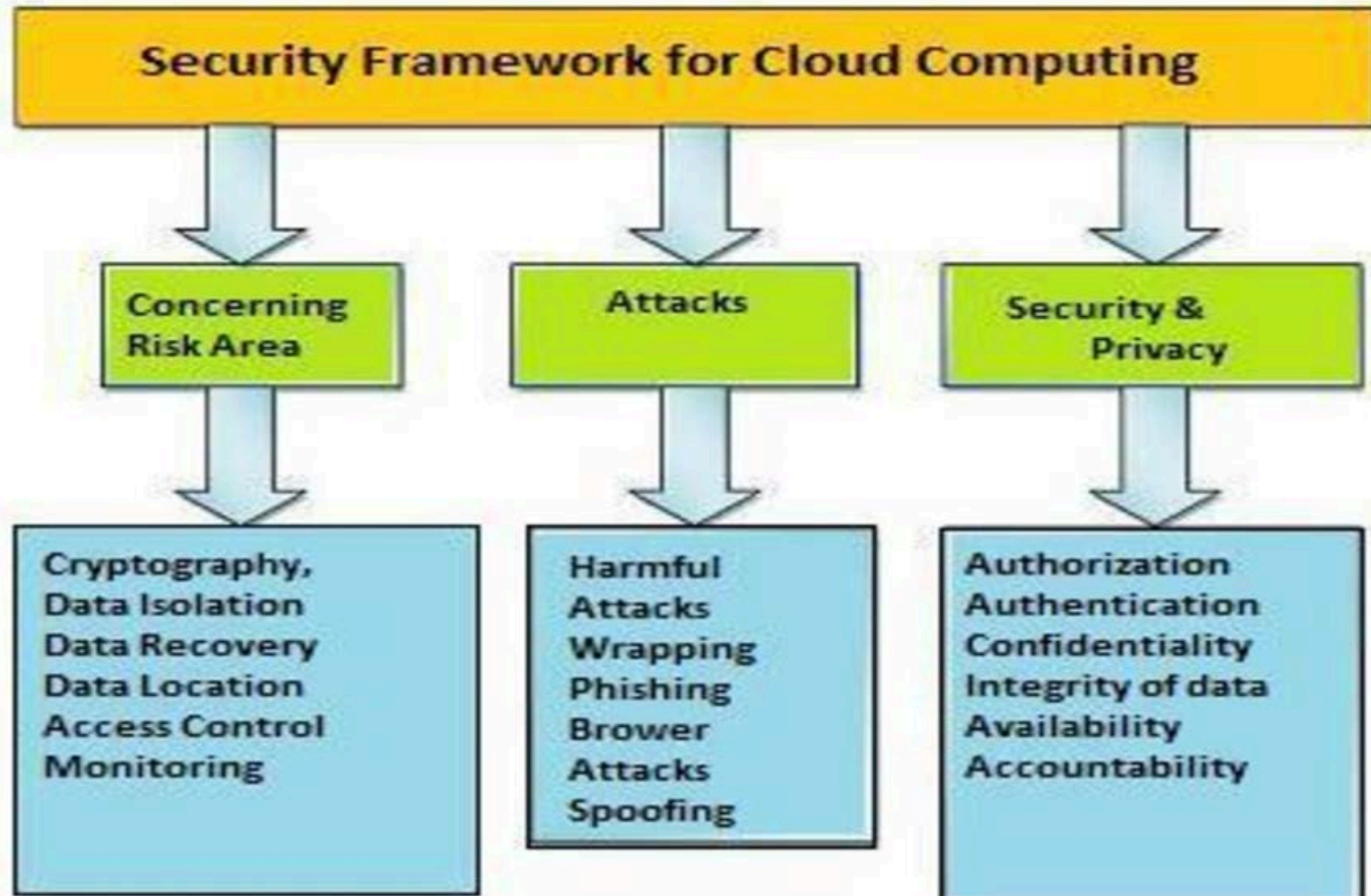
# Cloud Security

Cloud security is a set of policies, methods, and technologies that protects the infrastructure, data, and applications that are cloud-based, whether the cloud be private, public, or a hybrid

# Cloud Security

- Safe from theft, unauthorized deletion, and data leakage
- Protected from cyber attacks and unauthorized access
- Private and secure to support regulatory compliance requirements

# Cloud Security



# Cloud Security

axiom

## PROACTIVE PRACTICES

Proactive practices are grouped together into individual blocks following the main architectural layers of any cloud hosted application.





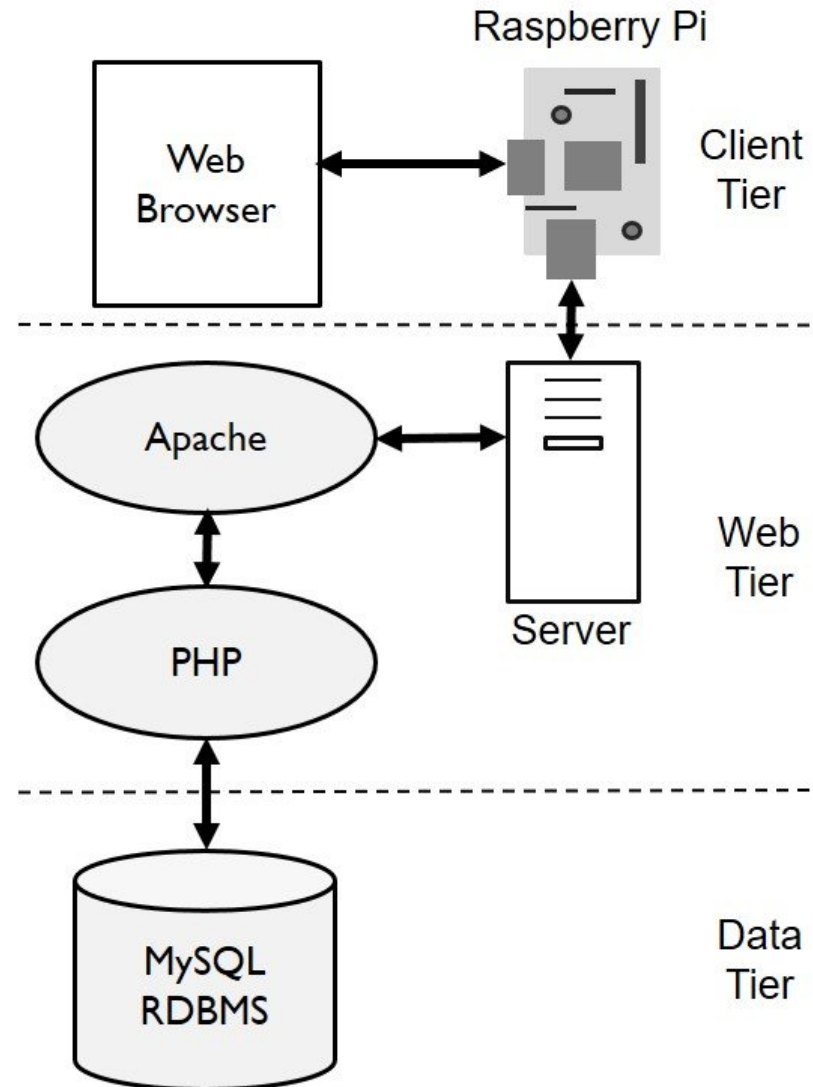
# Cloud Infrastructure Security

- **Infrastructure Security**
  - Network level
  - Host level
  - Application level

# Network Level

- **Confidentiality and integrity of data-in-transit**
  - Amazon had security bugs with digital signature on SimpleDB, EC2, and SQS accesses (in 2008)
- **Less or no system logging /monitoring**
  - Only cloud provider has this capability
  - Thus, difficult to trace attacks
- **Reassigned IP address**
  - Expose services unexpectedly
  - spammers using EC2 are difficult to identify
- **Availability of cloud resources**
  - Some factors, such as DNS, controlled by the cloud provider.
- **Physically separated tiers become logically separated**
  - E.g., 3 tier web applications

# 3 Tier Web Applications



# Network Level

*TABLE 3-1. Security controls at the network level*

<b>Threat outlook</b>	<b>Low (with the exception of DoS attacks)</b>
Preventive controls	Network access control supplied by provider (e.g., firewall), encryption of data in transit (e.g., SSL, IPSec)
Detective controls	Provider-managed aggregation of security event logs (security incident and event management, or SIEM), network-based intrusion detection system/intrusion prevention system (IDS/IPS)

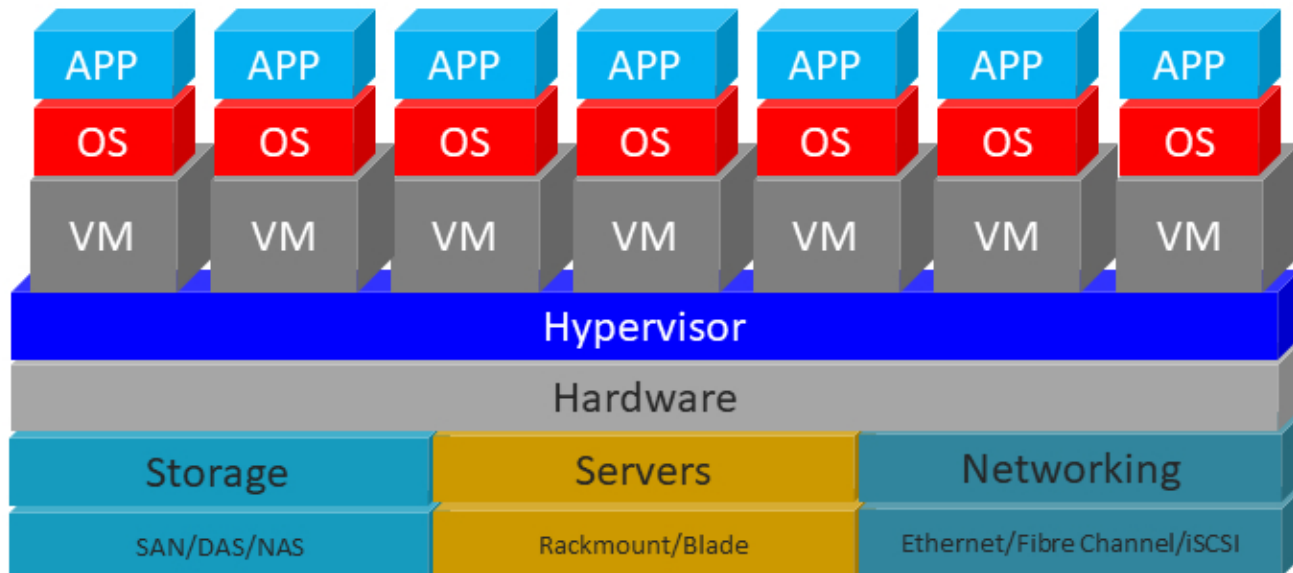
# Host Level (IaaS)

- **Hypervisor security**
  - Virtual machine security “zero-day vulnerability” in VM
- **Virtual Machine Security**
  - SSH private keys (if mode is not appropriately set)
  - VM images (especially private VMs)
  - Vulnerable Services

# Hypervisor

- A hypervisor, also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.

## How does a hypervisor work?



# Host Level (IaaS)

*TABLE 3-2. Security controls at the host level*

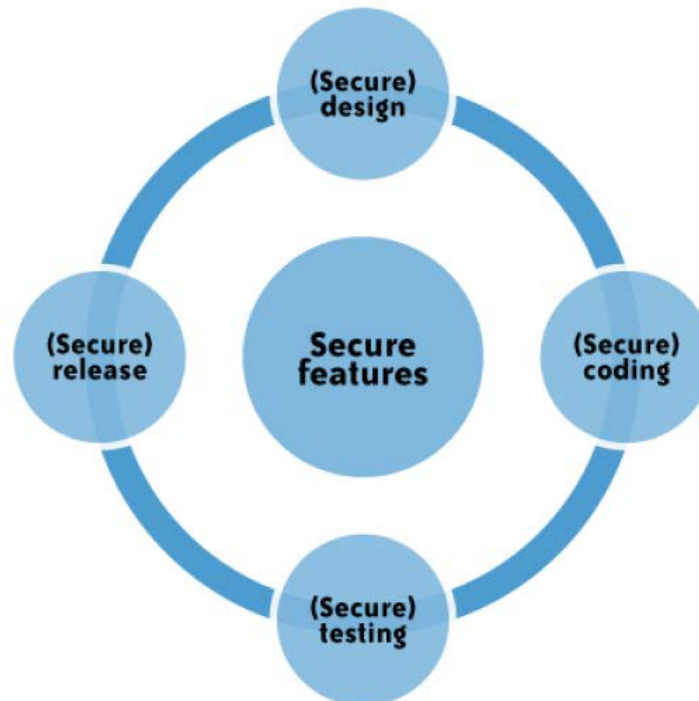
<b>Threat outlook</b>	<b>High</b>
<b>Preventive controls</b>	Host firewall, access control, patching, hardening of system, strong authentication
<b>Detective controls</b>	Security event logs, host-based IDS/IPS

---

# Application Level

- **SaaS application security**

- In an accident, Google Docs access control failed. All users can access all documents





**TABLE 3-5. Security controls applicable to IaaS applications**

<b>Threat outlook</b>	<b>High</b>
Preventive controls	Application developed using security-embedded SDLC process, least-privileged configuration, timely patching of application, user authentication, access control, account management, browser hardened with latest patches, endpoint security measures including antivirus, IPS, host-based IDS, host firewall, and virtual private network (VPN) for administration
Detective controls	Logging, event correlation, application vulnerability scanning and monitoring

**TABLE 3-4. Security controls applicable to PaaS applications**

<b>Threat outlook</b>	<b>Medium</b>
Preventive controls	User authentication, account management, browser hardened with latest patches, endpoint security measures including antivirus and IPS
Detective controls	Application vulnerability scanning

**TABLE 3-3. Security controls at the application level**

<b>Threat outlook</b>	<b>Medium</b>
Preventive controls	Identity management, access control assessment, browser hardened with latest patches, multifactor authentication via delegated authentication, endpoint security measures including antivirus and IPS
Detective controls	Login history and available reports from SaaS vendors

# Cloud Data Security

- **Data security**
  - Data-in-transit
  - Data-at-rest
  - Data processing
  - Data Provenance

# Cloud Data Security

- **Data-in-transit**

- Ensure that a protocol provides Confidentiality as well as Integrity (SFTP, HTTPS)
- The Amazon digital signature problem

- **Data-at-rest & Processing data**

- Encryption to protect data-at-rest for static storage
- Cannot be encrypted for most PaaS and SaaS (such as Google Apps) Prevent indexing or searching
  - Research on indexing/searching encrypted data
  - Fully homomorphic encryption?

# Homomorphic Encryption

Homomorphic encryption is **a form of encryption with an additional evaluation capability for computing over encrypted data without access to the secret key.** The result of such a computation remains encrypted. Homomorphic encryption can be viewed as an extension of public-key cryptography.

# Cloud Data Security

- **Data provenance**

- Origin/ownership of data

- Verify the authority of data
    - Trace the responsibility
    - e.g., financial and medical data

- Difficult to prove data provenance in a cloud computing

# Cloud Data Security

- **Data lineage**
  - Definition: tracking and managing data
  - For audit or compliance purpose
  - Data flow or data path visualization
  - Time-consuming process even for inhouse data center
  - The Amazon digital signature problem
    - Not possible for a public cloud

# Cloud Identity and Access Management (IAM)

- **Authentication**

- Authentication is the process of verifying the identity of a user or system

- **Authorization**

- Authorization is the process of determining the privileges the user or System is entitled to once the identity is established-in other words, authorization is the process of enforcing policies.

- **Auditing**

- In the context of IAM, auditing entails the process of review and examination of authentication, authorization records, and activities to determine the adequacy of IAM system controls, to verify compliance with established security policies and procedures and to recommend any changes that are indicated for countermeasures.

# Cloud Identity and Access Management (IAM)

- **Traditional trust boundary reinforced by network control**
  - Secure Access including VPNs, IDSs, IPSs and multifactor authentication
  - **Loss of network control in cloud computing**
- **Have to rely on higher-level software controls**
  - Application security
  - User access controls



# Access Control

- User access management controls, including strong authentication, single sign-on (SSO), privilege management, and logging and monitoring of cloud resources, play a significant role in protecting the confidentiality and integrity of your information in the cloud.

# Access Control

- **Who should have access to what resource?**
- **Why should the user have access to the resource?**
- **How should you access the resource?**
- **Who has access to what resource?**

# Access Control

The following are the six control statements:

- Control access to information.
- Manage user access rights.
- Encourage good access practices.
- Control access to network services.
- Control access to operating systems.
- Control access to applications and systems.

# TRUST CSP

Trust based on the service provider: by trust in performance, **a user trusts a cloud service with respect to performance, security, and privacy, based on the identity of the provider.** If the user trusts that the provider gives trustworthy cloud services, then the cloud service is trusted.

# Reputation CSP

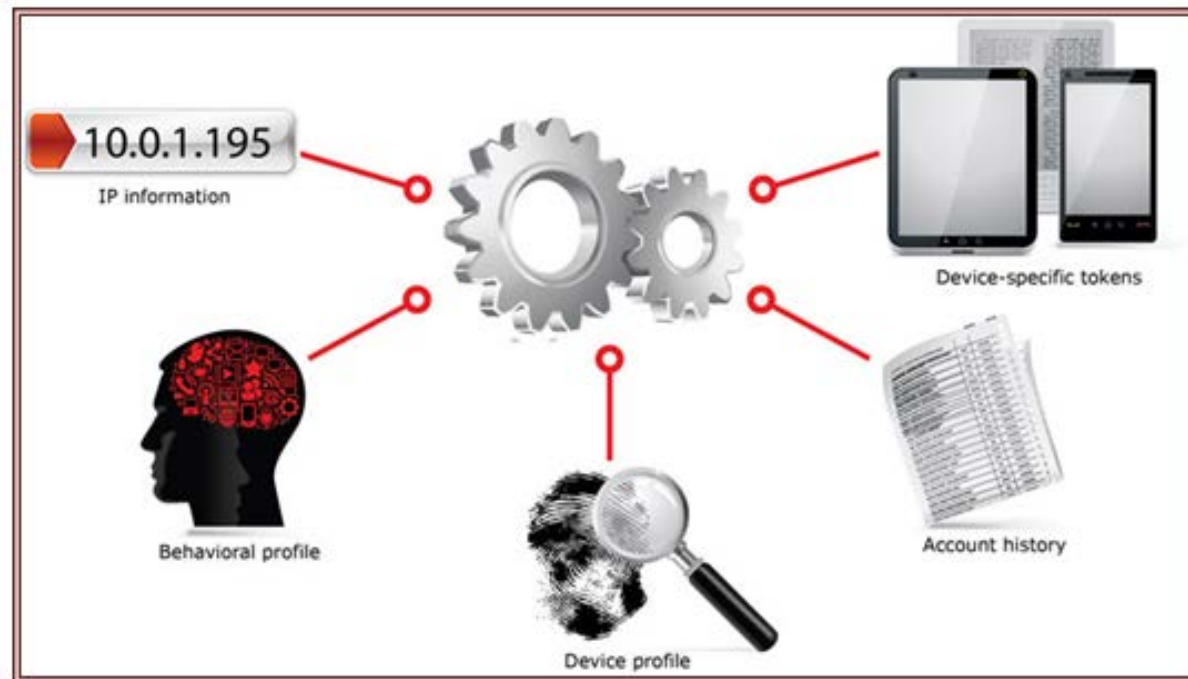
Reputation is the assessment of the tasks which ensures the derived trust based services in cloud. Cloud users basically require the reputed system to guarantee the security in cloud services.

# Risk Based Authentication in CC

Risk Based authentication provides an additional level of authentication for your cloud applications. It is a dynamic method of applying levels of protection to the system, based on various factors. It is a multi step procedure to prevent any unauthorized access to sensitive data.

# Risk Based Authentication in CC

The risk based authentication uses elements such as location based, role based, activity based and changes in the usual usage patterns



# Client Access in Cloud

A cloud client is a **hardware device or software used to access a cloud service**. Computer systems, tablets, navigation devices, home automation devices, mobile phones and other smart devices, operating systems, and browsers can all be cloud clients.



# Cloud Contracting Model

Cloud computing contracts differ significantly from typical IT outsourcing agreements. Cloud computing can be perceived as **a new type of outsourcing, in which IT infrastructure and software are made available in a form of a continuous service.**

# BUSINESS CONSIDERATIONS FOR CLOUD COMPUTING

- Improving disaster recovery
- Increasing computer resources
- Minimizing performance issues
- Optimizing application or hardware upgrades
- Meeting compliance requirements
- Increasing efficiency or flexibility