Unit-II: Cloud Enabling Technology

Primary technology components that collectively enable key features & characteristics associated with cloud computing are:

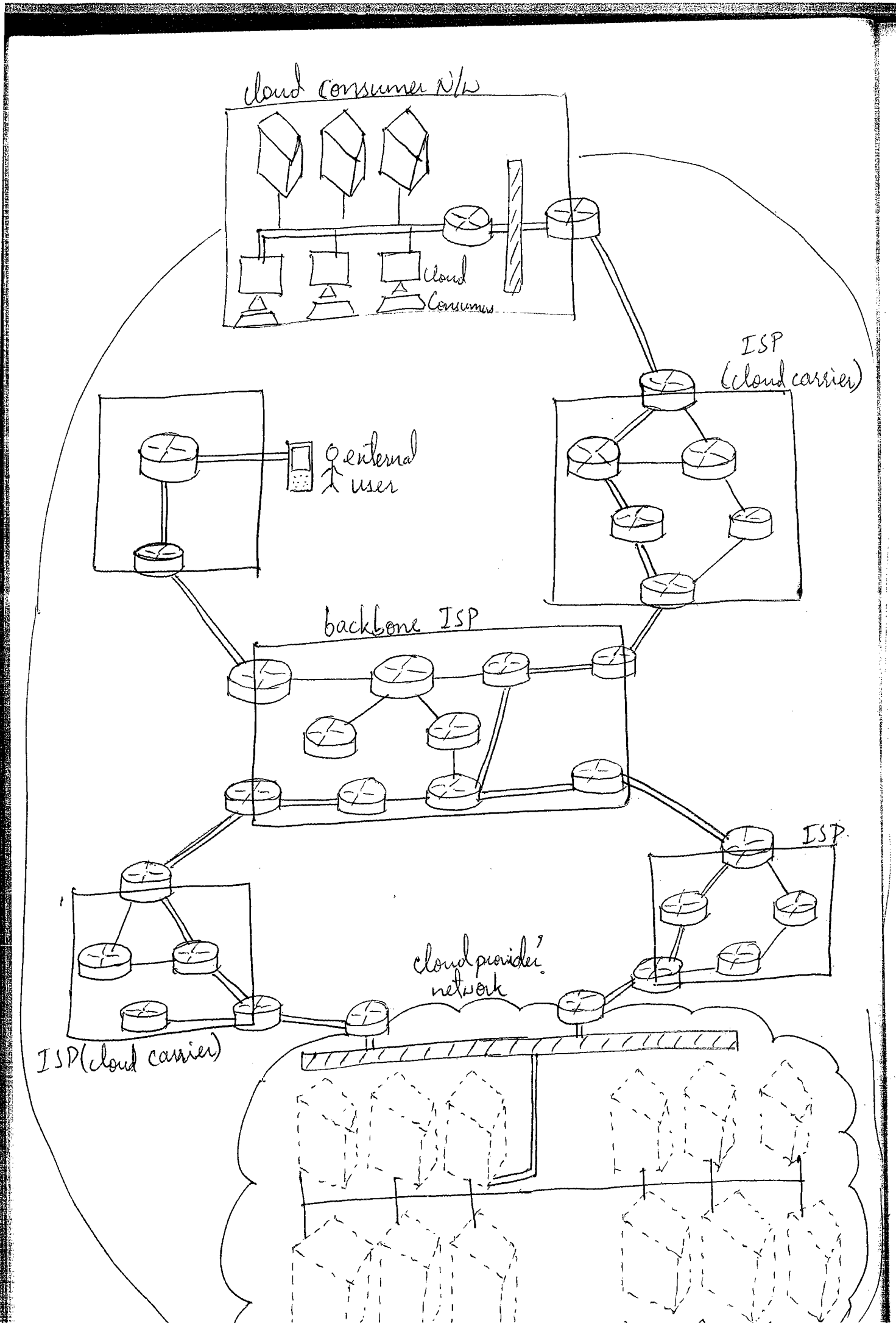
- Broadband Networks & Internet Architecture
- Virtualization Technology
- Data Center Technology
- Web Technology
- Multitenant Technology
- Service Technology

Broadband Networks and Internet Architecture

- Internetworks, or the Internet, allows for the remote provisioning of IT resources & are directly supportive of ubiquitous network access.

Internet Service Providers (ISPs)

- Established & deployed by ISPs, the Internet's largest backbone networks are strategically interconnected by core routers that connect the world's multinational networks.


cloud consumer N/w
Cloud Consumers
ISP (cloud carrier)
external user
backbone ISP
ISP
cloud provider's network
ISP (cloud carrier)

- ISPs can freely deploy, operate, & manage their networks & select partner ISPs for interconnection.
- Internet Corporation for Assigned Names & Numbers (ICANN) supervise & coordinate Internet Communication
- The Internet's topology has become a dynamic & complex aggregate of ISPs that are highly interconnected via its core protocols.
- Smaller branches extend from these major nodes of interconnection, branching outwards through smaller networks until eventually reaching every Internet-enabl electronic device.

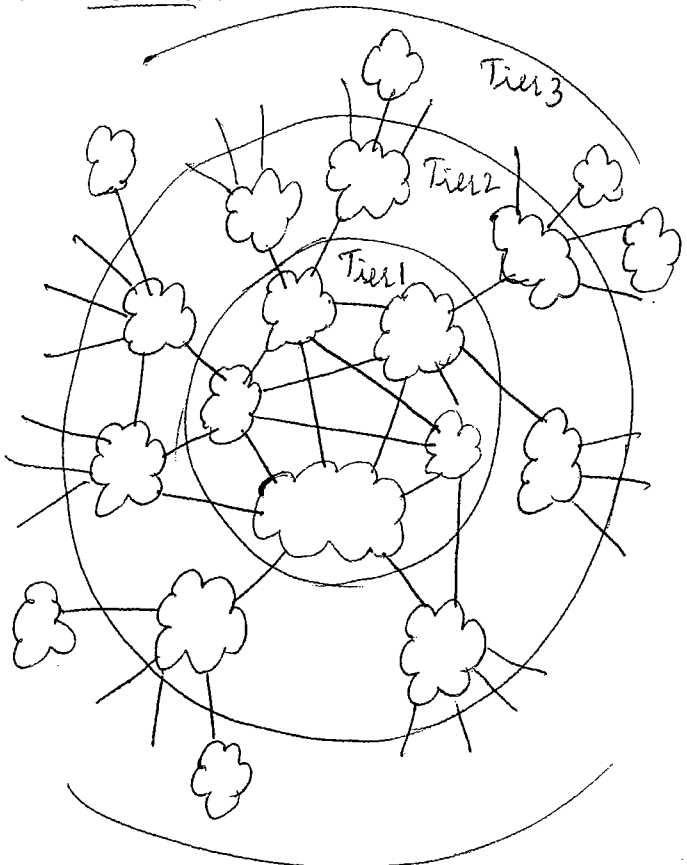


Fig: An abstraction of the internetworking structure of the internet.

- Worldwide connectivity is enabled through a hierarchical topology composed of Tiers 1, 2 and 3.
- Core Tier 1 is made of large-scale, international cloud providers that oversee massive interconnected global networks, which are connected to Tier 2's large regional providers.
- The interconnected ISPs of Tier 2 connect with Tier 1 providers, as well as local ISPs of Tier 3.
- Cloud consumers & cloud providers can connect directly using a Tier 1 provider.
- The communication links & routers of Internet & ISP networks are IT resources that are distributed among countless traffic generation paths.

Two fundamental components used to construct the internetworking architecture are:

- connectionless packet switching (datagram networks)
- router-based interconnectivity.

Connectionless Packet Switching (Datagram Networks)

- End-to-end (sender-receiver pair) data flows are divided into packets of a limited size that are received & processed through network switches & routers, then queued & forwarded from one intermediary node to the next.

- Each packet carries the necessary location information, such as Internet Protocol (IP) or Media Access Control (MAC address.

Router-Based Interconnectivity

- A router is a device that is connected to multipl networks through which it forwards packets.
- Router maintains the network topology information that locates the next node on communication path between the source & destination nodes
- Routers manage network traffic & gauge the most efficient hop for packet delivery.

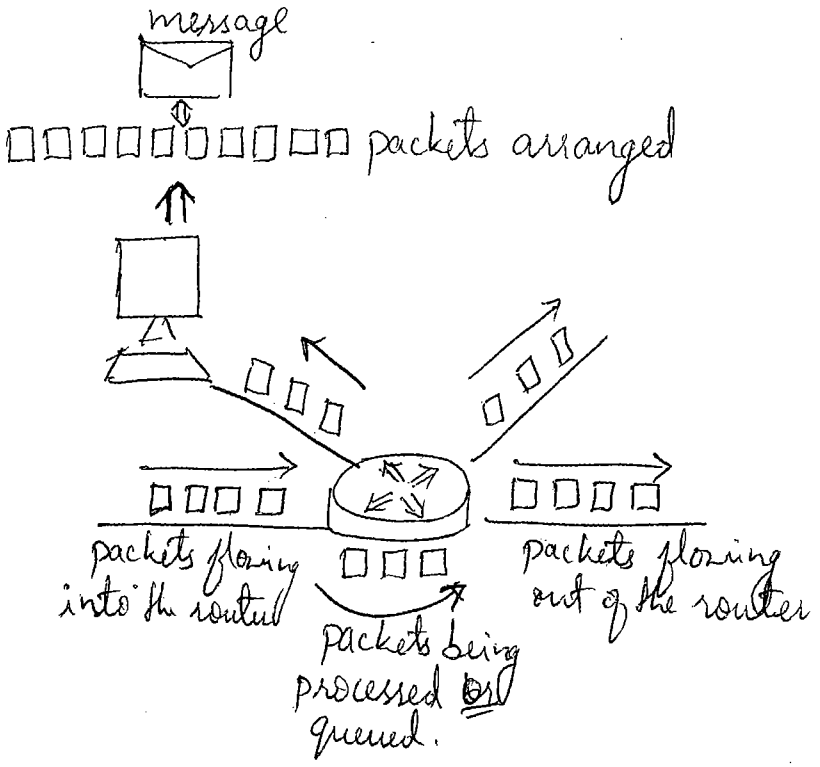


Fig: Packets traveling through the Internet are directed by router that arranges them into a message.

- The Internet's mesh structure connects Internet hosts using multiple alternative network routes that are determined at runtime.

Physical Network

- IP packets are transmitted through underlying physical networks that connect adjacent nodes, such as Ethernet, ATM (Asynchronous transfer mode) network & 3G mobile HSDPA (High Speed Downlink Packet Access).
- Physical Networks comprise a data link layer that controls data transfer between neighboring nodes, & a physical layer that transmits data bits through both wired & wireless media.

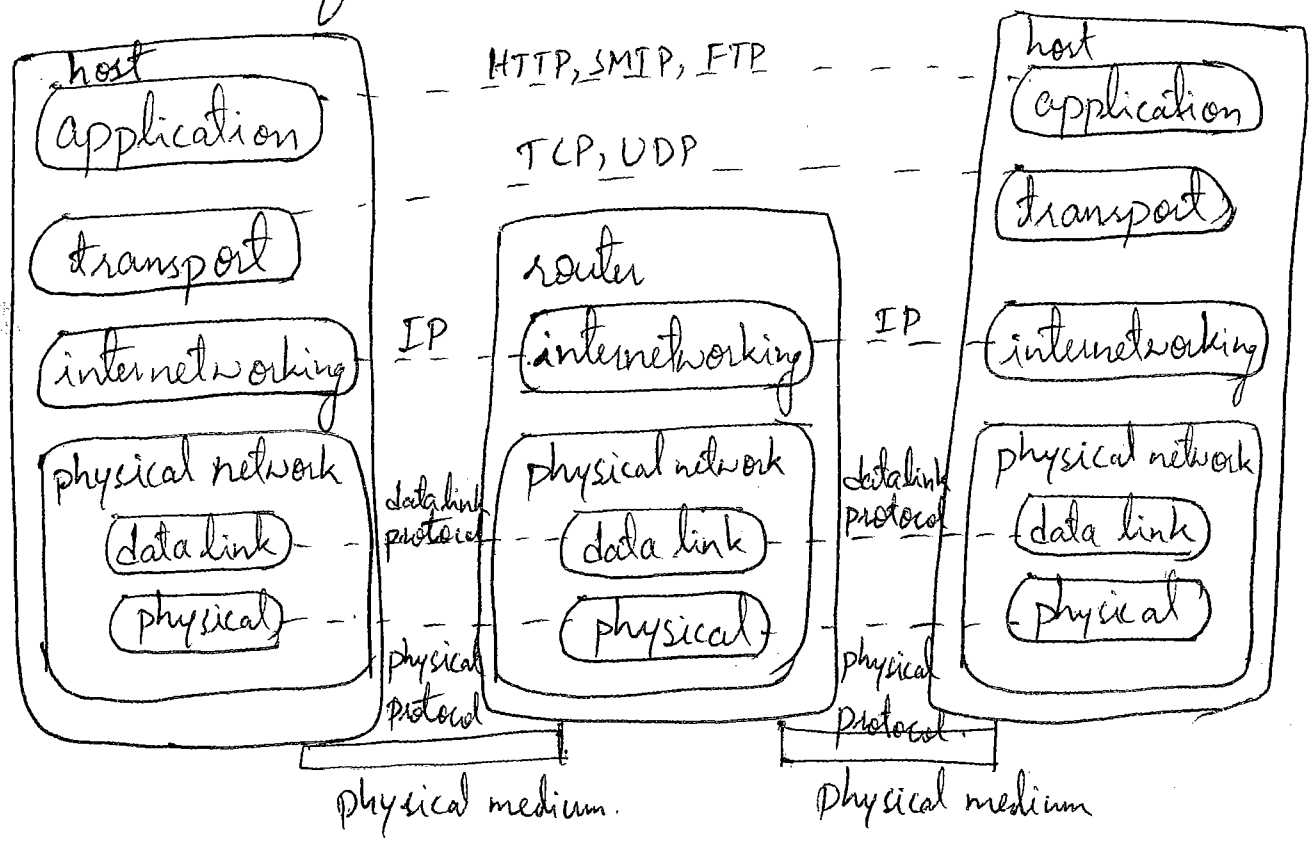
Transport Layer Protocol

- Transport layer protocols, such as Transmission Control Protocol (TCP) & User Datagram Protocol (UDP), use the IP to provide standardized, end-to-end communication support that facilitates the navigation of data packets across the Internet.

Application Layer Protocol

- Protocols such as HTTP, SMTP for e-mail, BitTorrent for P2P, and SIP for IP telephony use transport layer protocols

Internet Reference Model & the protocol stack



Technical and Business Considerations

Connectivity Issues

- In On premise deployment models, enterprise applications & various IT solutions are commonly hosted on centralized server & storage devices residing in organization's own data center.
- End-user devices, like smartphones & laptops, access the data center through corporate network.

- TCP/IP facilitates both Internet access & on-premise data exchange over LANs.
- Organizations using this deployment model have complete control over & can safeguard their corporate network using firewalls & monitoring software
- Organization is responsible for deploying, operating & maintaining their IT resources & Internet connectivity

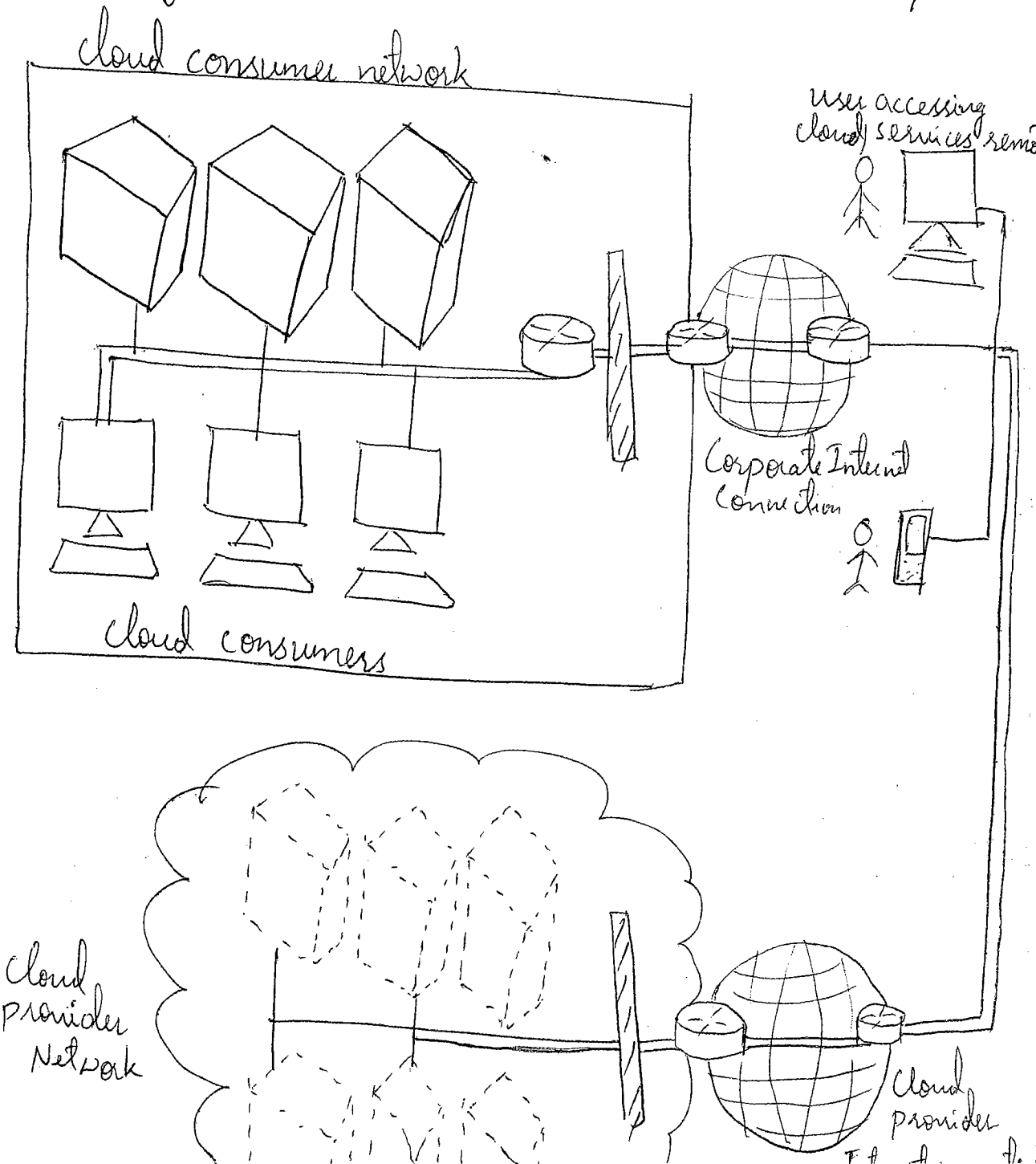


Fig. The internetworking architecture of an Internet-based cloud deployment model. The Internet is the connecting agent between non-proximate cloud consumers, roaming end-users, and the cloud provider's own network.

A salient cloud feature that applies to end-user functionality is how centralized IT resources can be accessed using the same network protocols regardless of whether they reside inside or outside of a corporate network.

A comparison of on-premise & cloud-based internetworking

On-Premis IT Resources	Cloud-Based IT Resources
- internal end-user devices access corporate IT services through the corporate network.	- internal end user devices access corporate IT services through an Internet connection
- internal users access corporate IT services through the corporate Internet connection while roaming in external networks.	- internal users access corporate IT services while roaming in external networks through the cloud provider's Internet connection
- external users access corporate IT Services through the corporate Internet connection	- external users access corporate IT services through the cloud provider's Internet connection.

Network Bandwidth and Latency Issues

- End-to-end bandwidth is determined by transmission capacity of the shared data links that connect intermediary nodes.
- ISPs need to use broadband network technology which is constantly increasing, as Web acceleration technologies, such as dynamic caching, compression, and pre-fetching, continue to improve end-user connectivity.
- Latency is the amount of time it takes a packet to travel from one data node to another.
- Latency increases with every intermediary node on the data packet's path.

Cloud Carrier & Cloud Provider Selection

- QoS management across multiple ISPs is difficult to achive in practice, requiring collaboration of the cloud carriers on both sides.

Organizational Agility

- it is the measure of an organization's responsiveness to change

Technology Innovations

- Clustering.
  - A cluster is a group of independent IT resources that are interconnected & work as a single system.
  - availability & reliability are increased
  - cluster components should have reasonably identical hardware & operating system to provide similar performance.
  - Component devices that form a cluster are kept in synchronization through dedicated, high-speed communication link

Grid Computing.

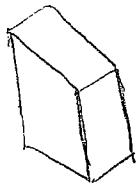
- Grid computing provides a platform in which computing resources are organized into one or more logical pools.
- high performance.
- more loosely coupled & distributed.
- heterogeneous & geographically dispersed.
- based on middleware layer that is deployed on computing resources
- workload distribution & coordination functions.
- middle tier contains - load balancing logic, failover controls autonomic configuration management.

Virtualization.

- Technology Innovations vs. Enabling Technologies.
  - Broadband N/w & Internet Architecture
  - Data Centre Tech.
  - Virtualizat° Tech
  - Web Tech
  - Service Tech.

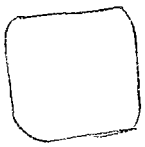
3.2 Basic Concepts & Terminology

- Cloud
- IT Resource

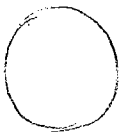


Physical Server

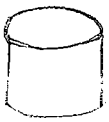
Virtual server



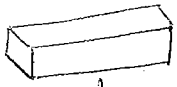
Software Program



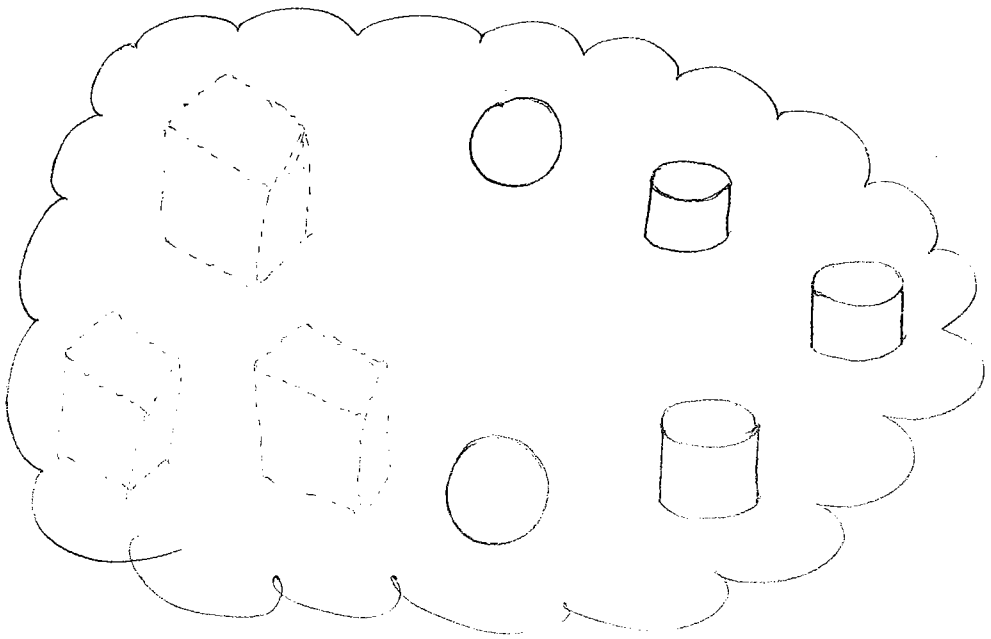
Service



Storage device

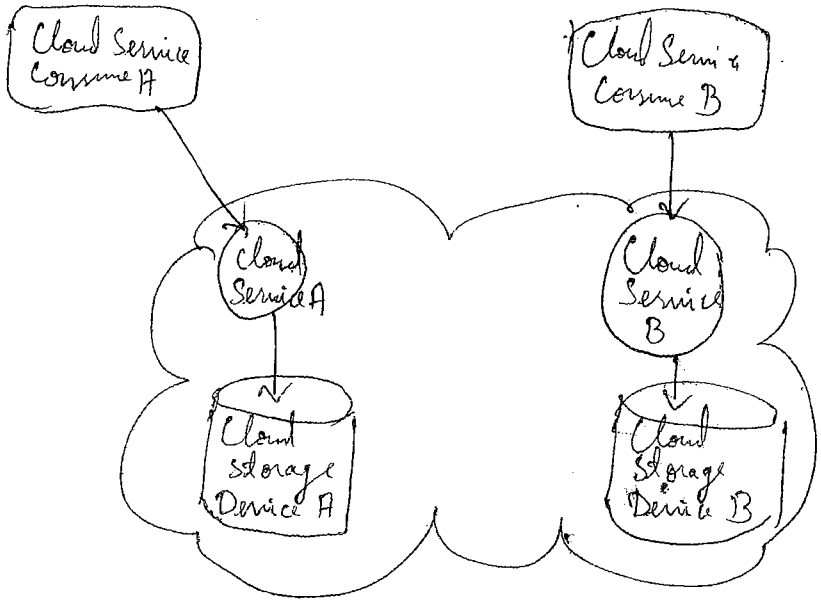


N/w device.

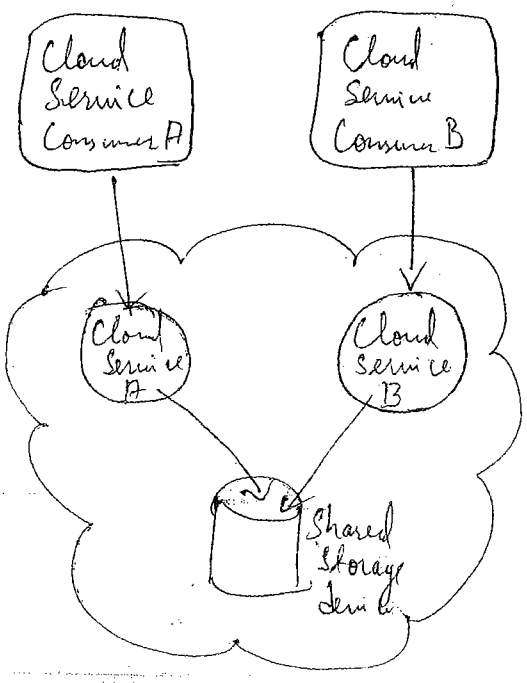


Multitenancy (& Resource Pooling)

- an instance of prog to serve different consumers (tenants).
- isolated from other
- rely on the use of virtualizat°.
- dynamically assigned & reassigned, according to demand.
- pool large-scale IT resources to serve multiple cloud consumers.



In Single-tenant environment, each cloud consumer has separate IT resource instance.

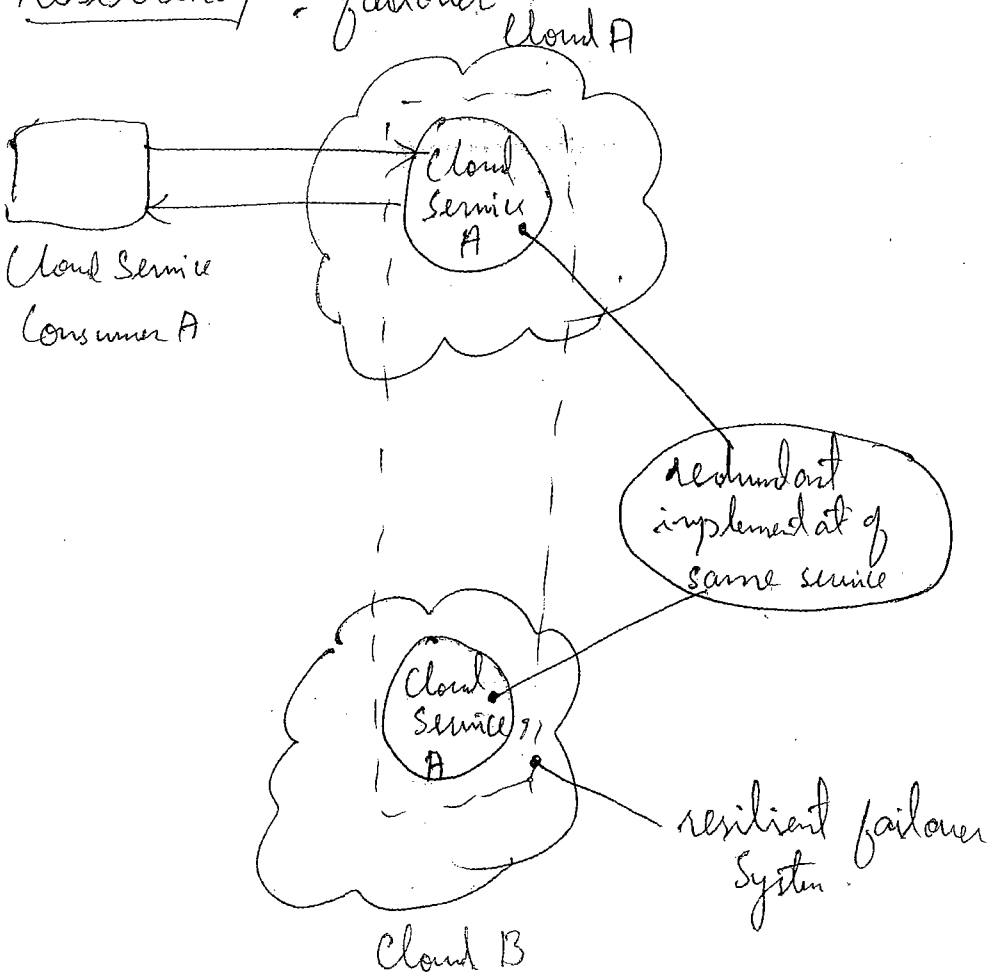


In multitenant environment, a single instance of an IT resource, such as a cloud storage device, serves multiple consumer

) Elasticity - ability to scale IT resources during runtime condit=
- Reduced investment & Proportional Costs benefit

5) Measured Usage
- keep track of the usage of its IT resources
- charged for resource for timeframe during which access to IT resources was granted.
- billing
- monitoring.

6) Resiliency - failover



Combining Cloud Delivery Models

IaaS + PaaS

- PaaS environment will be built upon an underlying ~~environment~~ infrastructure provided by IaaS environment.
- PaaS envit provider may lease an IaaS from different cloud provider

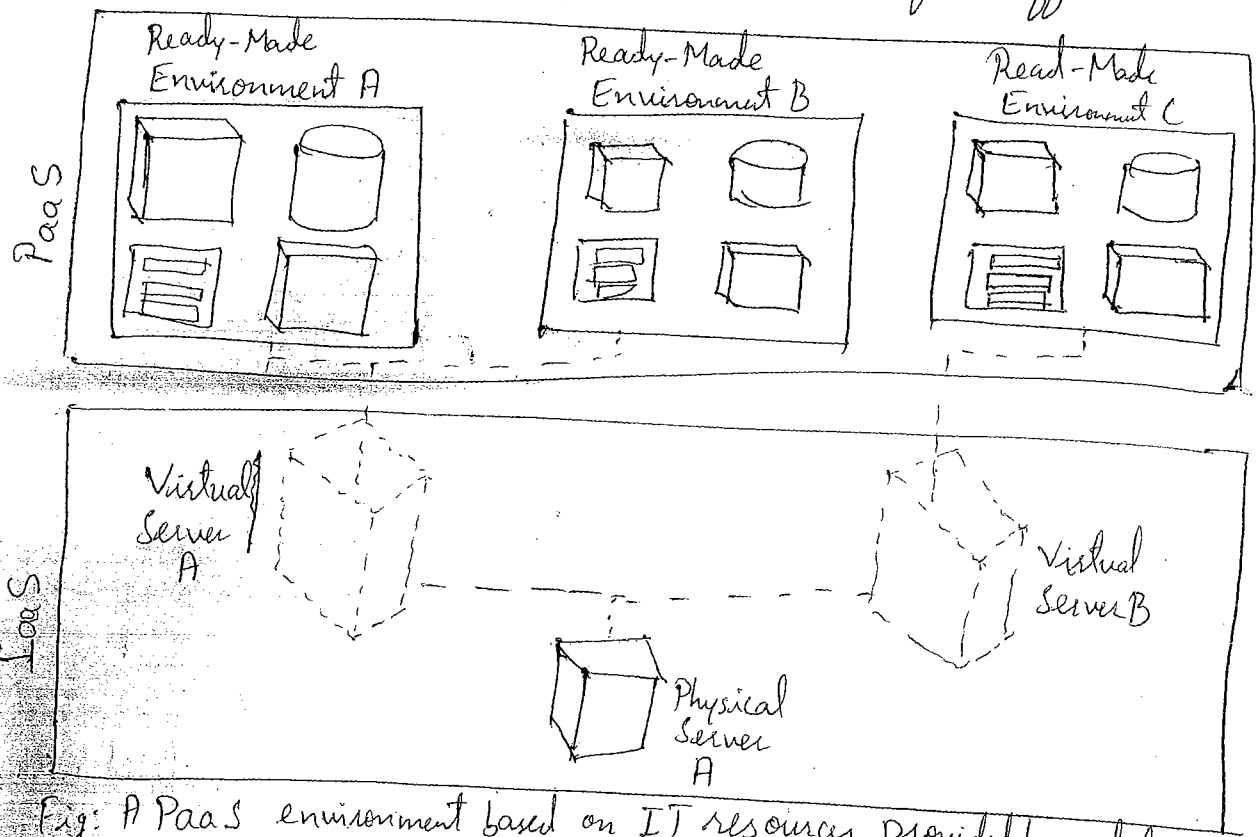
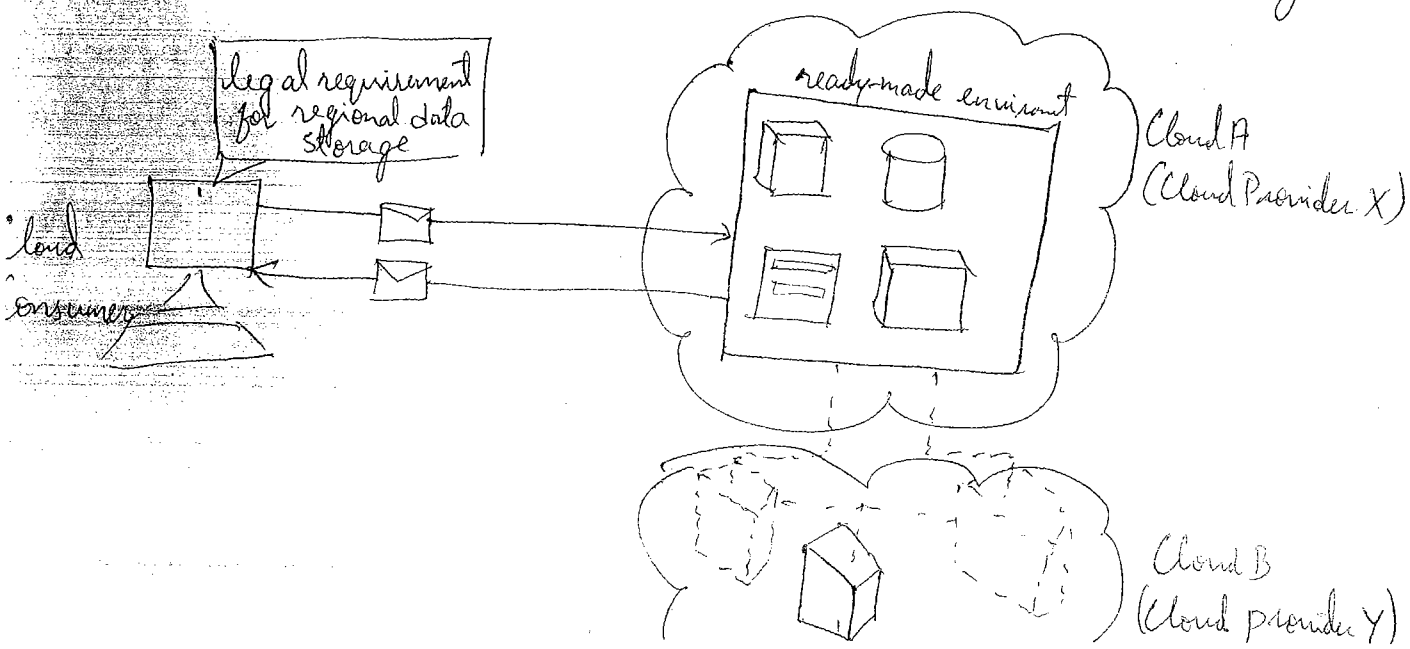


Fig: A PaaS environment based on IT resources provided by underlying IaaS envir



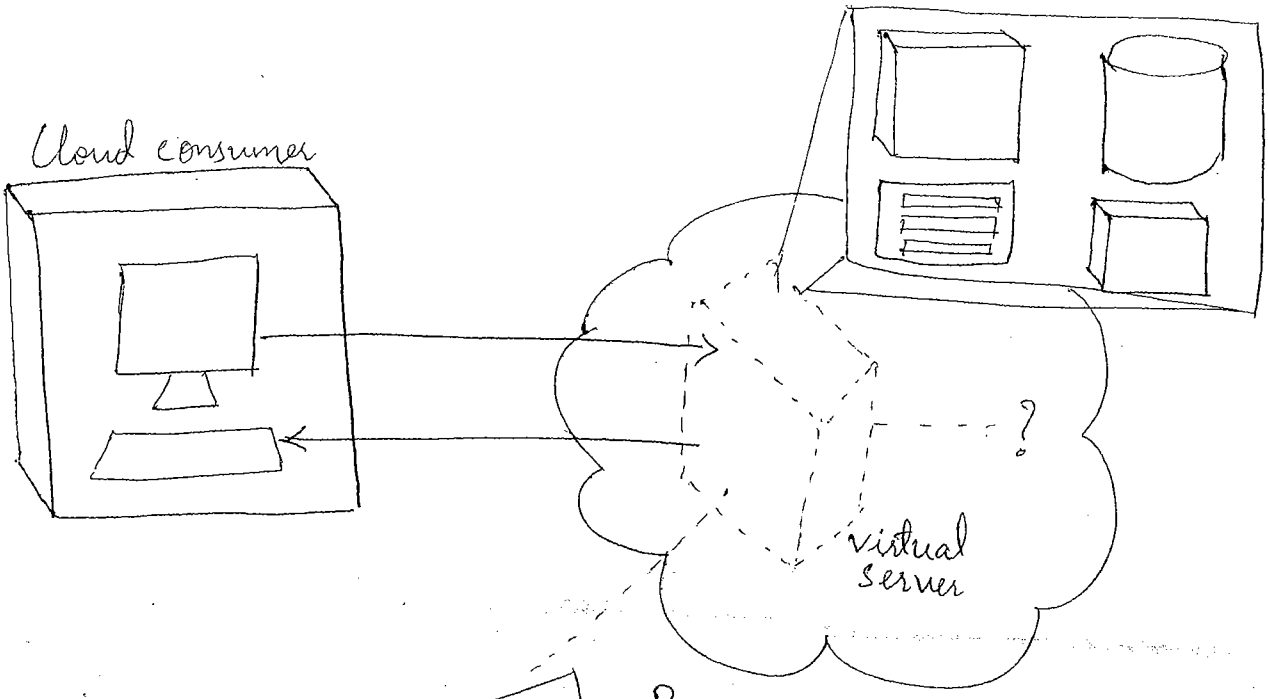
Comparing Cloud Delivery Models

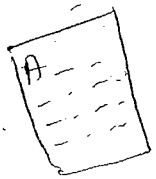
Cloud Delivery Model	Typical Level of Control Granted to cloud Consumer	Typical Functionality Made Available to Cloud Consumer
SaaS	usage & usage-related configuration	access to frontend user-interface
PaaS	limited administrative	moderate level of administrative control over IT resources relevant to cloud consumer's usage of platform
IaaS	full administrative	full access to virtualized infrastructure related IT resources & possibly, to underlying physical IT resources

A comparison of typical cloud delivery model control levels.

Cloud Delivery Model	Common Cloud Consumer Activities	Common Cloud Provider Activities
SaaS	uses & configures cloud service	implements, manages and maintains cloud service monitors usage by cloud consumers
PaaS	develops, tests, deploys and manages cloud services & cloud-based solutions	-pre-configures platform & provisions underlying infrastructure, middleware and other needed IT resources, as necessary -monitors usage by cloud consumers
IaaS	sets up & configures bare infrastructure, and installs, manages, & monitors any needed software	provisions & manages the physical processing, storage, networking & hosting required -monitors usage by cloud consumers.

Typical activities carried out by cloud consumer & provider

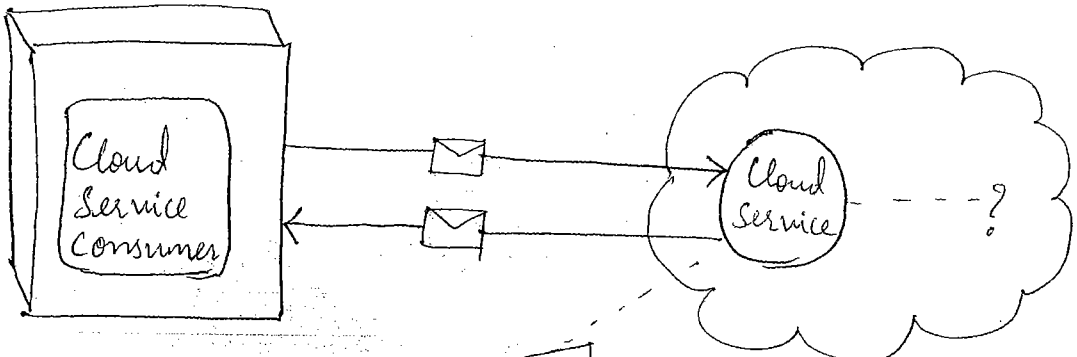


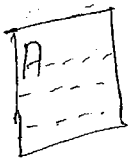


PaaS Cloud Service Contract
Product: application server + DMBS platforms
SLA: availability = 99.5 %, auto-scaling
Price: $0.45 per hour (500,000 requests)

Ex: Google App Engine
Java, Python.

Software-as-a Service (SaaS)





SaaS Cloud Service Contract
SLA: response time = 0.5ms
Price: $0.05 per 100 requests.

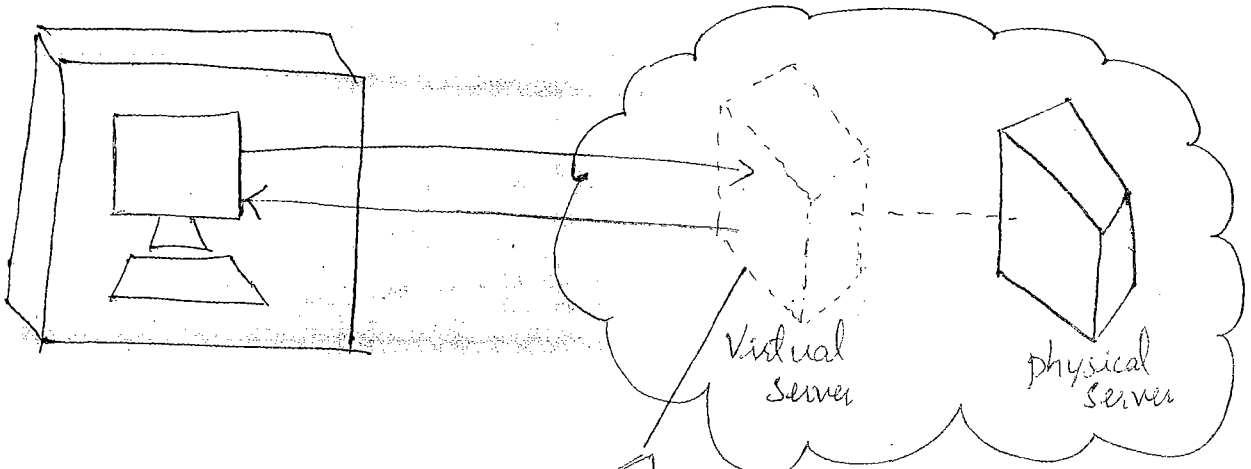
Ex: Office 365, Box
Google Apps,

Product or generic utility.
commercially.
limited administrative control over SaaS implementation.

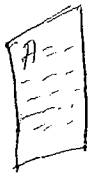
Ex: Amazon Web Services.

1) Infrastructure-as-a Service (IaaS)

- Self-contained IT environment, infrastructure-centric IT resources accessed & managed thru service-based interfaces & tools.
- hardware, network, connectivity, operating systems & 'raw' IT resources.
- high level of control & responsibility over its configuration & utilizat°.
- central & primary IT resource - virtual server.



Eg: Microsoft Azure
Linode, Rackspace



IaaS Cloud Service Contract
Product: Virtual Server, 32GB RAM, 4GB local stor
SLA: availability = 99.5%, no failover
Price: $0.95 per hour, $0.05 per GB transfered out of cloud

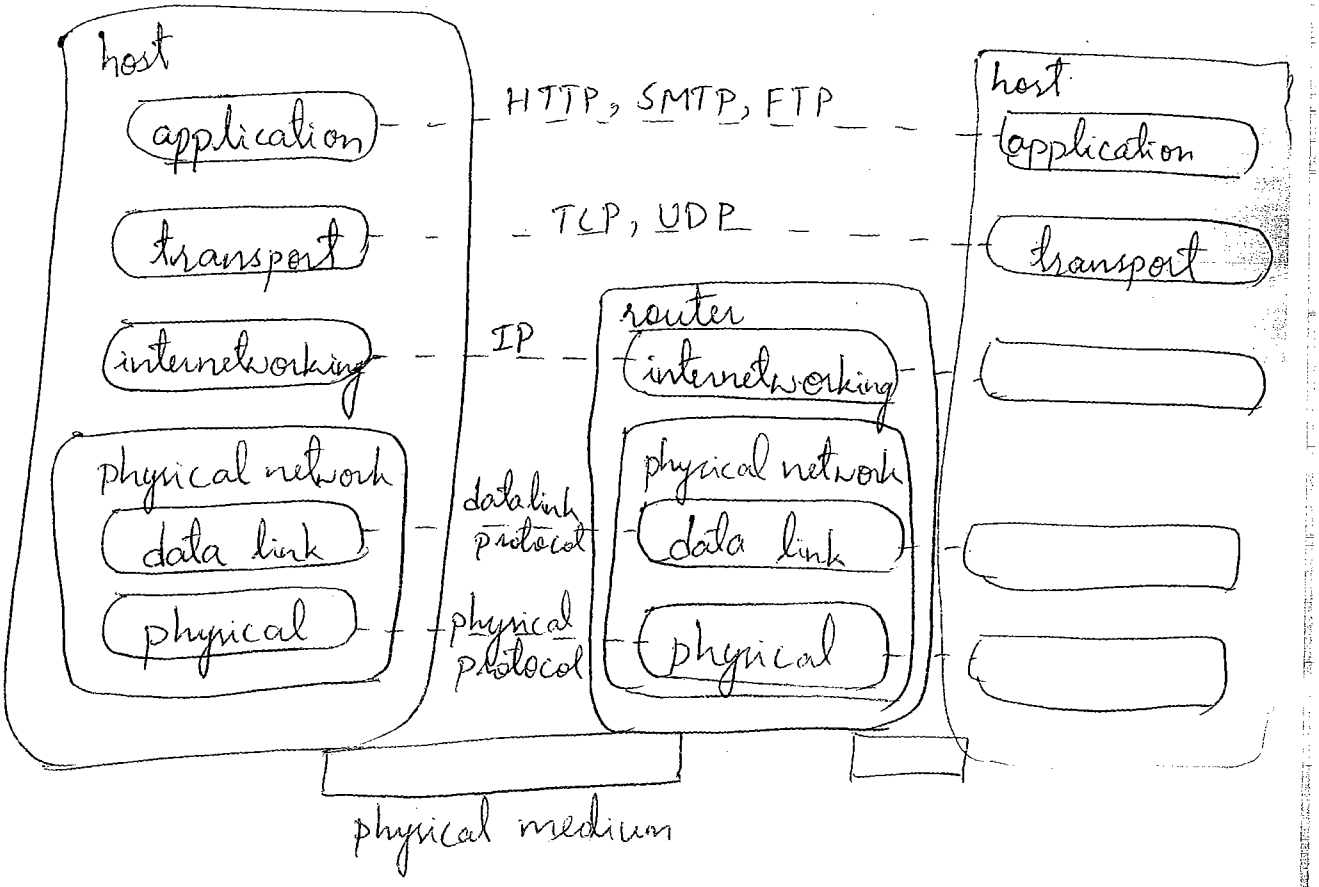
2) Platform-as-a-Service (PaaS)

- pre-defined "ready-to-use" environment comprised of already deployed and configured IT resources.
- pre-packaged products & tools used to support entire delivery lifecycle of custom applications.

Common reasons a cloud consumer would use & invest in PaaS

- Cloud consumer wants to extend on-premise environment into the cloud for scalability & economic purpose
- ready-made environment that entirely substitute an on-premise environme
- Cloud consumer wants to become a cloud provider & deploys its own cloud service to be made available to

REVA ITM
Department of Computer Science and Engineering



Physical Network

- Ethernet, ATM network, & 3G mobile HSDPA (High Speed Downlink Packet Access)
- Data bits transmits thr both wired & wireless media.

Transport Layer Protocol:

- Transmission Control Protocol (TCP), User Datagram Protocol (UDP) facilitates the navigation of data packets across the Internet.

Application Layer protocol

- HTTP, SMTP, FTP

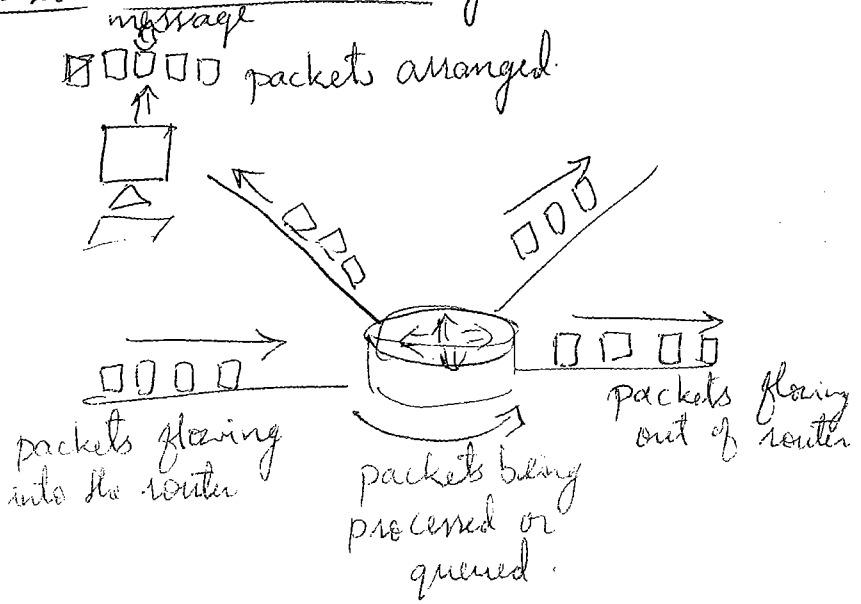
Two fundamental components used to construct the internetworking architecture are

- Connectionless packet switching
- Router-based interconnectivity.

Connectionless packet switching.

- End-to-end (sender-receiver pair) data flows are divided into packets.
- Each packet has info like IP or Media Access Control (MAC) address.
- Processed & routed at every source, intermediary & destination node.

Router-Based Interconnectivity



Broadband Nw & Internet Architecture

Internetworks or Internet, allow remote provisioning of IT resources & ubiquitous Nw access. Cloud consumer access thr private & dedicated LAN or cloud.

Internet Service Providers (ISPs)

- ISPs establishes & deploy internet, strategically interconnected by core routers that connect worlds multinational networks.
- Internet concept is decentralized provisioning & management model.
- ISPs can freely deploy, operate & manage their network & select partener ISP for interconnect.
- Internet Corporation for Assigned Names & Numbers (ICANN) - supervise & coordinate

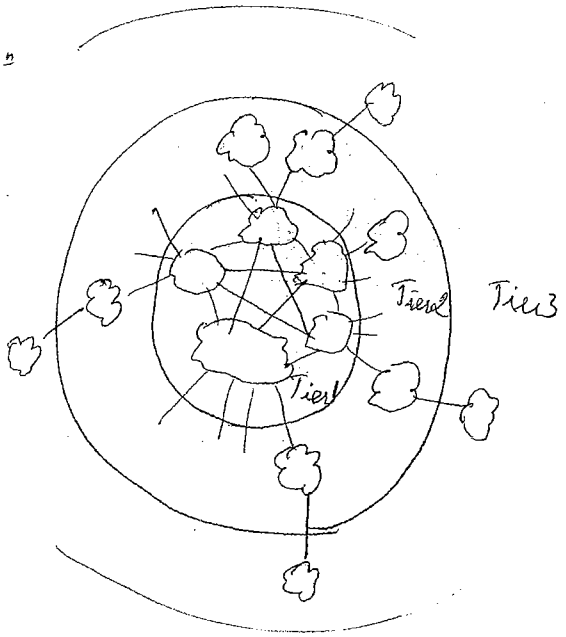


Fig: Analysis of internetworking structure of Internet

8/6/17 PL

126, 128, 144,
145, 146, 158,
165, 171, 172, 173,

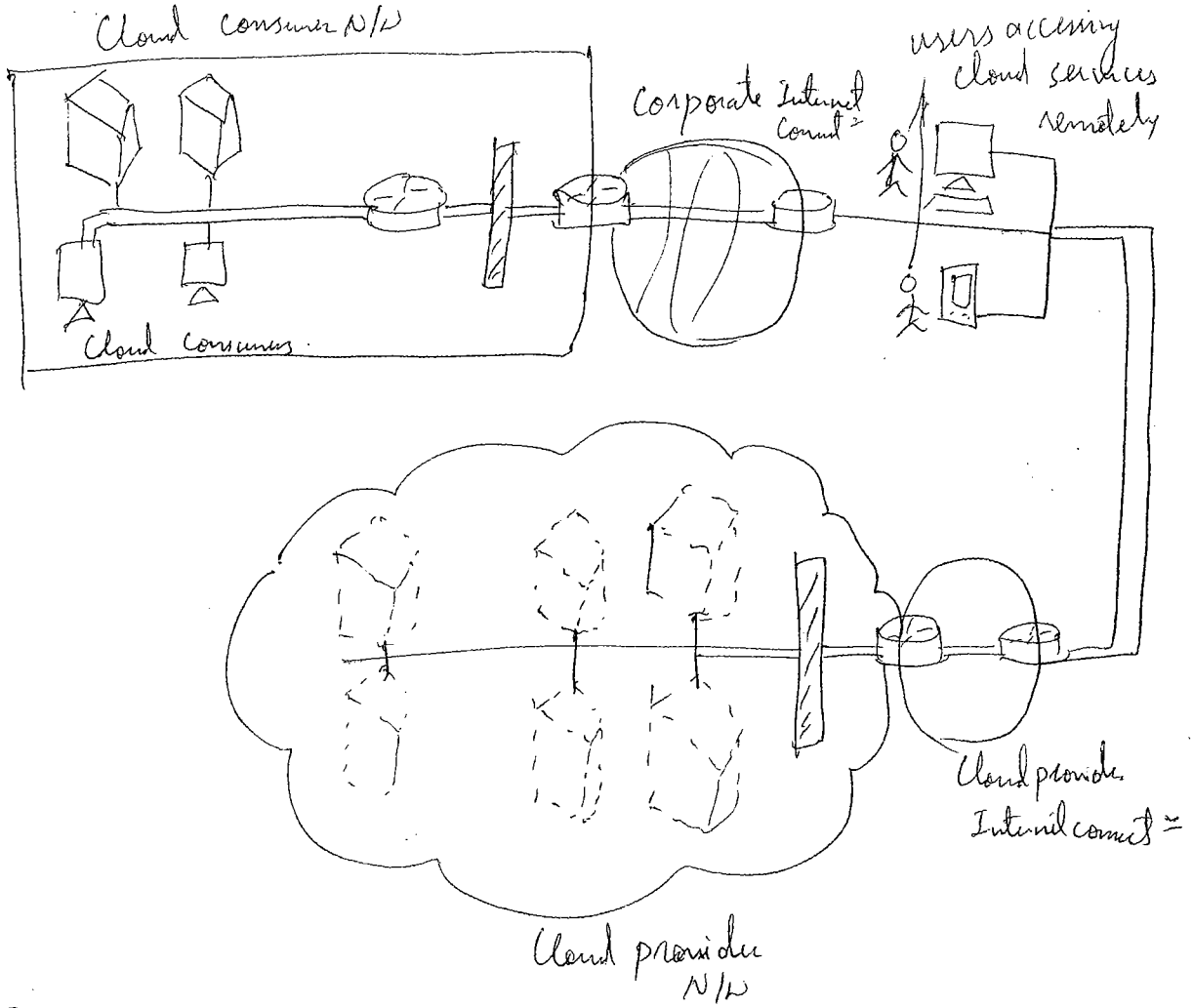


Fig - interworking architecture of an Internet-based cloud deployment model

Technical & Business Considerations

1. Connectivity Issues

On Premise IT Resources	Cloud-Based IT Resources
- Internal end-user devices access corporate IT services through the corporate network.	- internal end-user devices access corporate IT services through an Internet connection.
- internal users access corporate IT services through the corporate Internet connection while roaming in external n/ws.	- internal users access corporate IT services while roaming in external networks thr' the cloud provider's internet connect=.
- external users access corporate IT services through the corporate Internet connect=	- external users access corporate IT services thr' the cloud provider's internet connect=.

Storage Hardware

- Storage systems are containers housing numerous hard disks that are organized into arrays.

Storage system involve following technologies

- Hard Disk Arrays - inherently divide & replicate data among multiple physical drives, & increase performance & redundancy by including spare disks.
- Redundant Arrays of Independent Disks (RAID) - realized thru hardware disk array controllers.
- I/O Caching - done by hard disk array controllers, enhances disk access times & performance by data caching.
- Hot-swappable Hard Disks -
- Storage Virtualization - realized thru virtualized hard disks & storage sharing.
- Fast Data Replication Mechanisms -
  - snapshotting: - saving a virtual machine's memory into a hypervisor-readable file for future reloading.
  - Volume cloning - copying virtual or physical hard disk volumes & partitions.

Tertiary redundancies - such as robotized tape libraries, which are used as backup & recovery systems that rely on removable media.

- Networked IT resources
- Direct-Attached storage (DAS) - directly connected to computing IT resource using host bus adapter (HBA).

Networked storage devices fall into one of following categories

- Storage Area Network (SAN) - dedicated network & provide block-level data storage access using industry standard protocols - Small Computer System Interface (SCSI)

- Network-Attached Storage (NAS) - Hard drive arrays are contained & managed by this dedicated device, - access thr' file-centric data access protocols like the Network File System (NFS) or Server Message Block (SMB)

Network Hardware

1) Carrier & External Network Interconnection - backbone routers - provide routing betⁿ external WAN & data centers LAN. firewalls & VPN gateways.

2) Web-Tier Load Balancing & Acceleration - web acceleration devices, such as XML preprocessors, encryption/decryptⁿ appliances & layer 7 switching devices that perform content-aware routing.

3) LAN Fabric - internal LAN & provides high-performance & redundant connectivity. - multiple network switches that facilitate network communicatⁿ & operate speeds of up to ten gigabits per second. Switches perform virtualizatⁿ functⁿ - LAN segregation into VLAN, link aggregation, controlled routing betⁿ N/w. load balancing & failover

4) SAN Fabric - connects betⁿ servers & storage systems. SAN is implemented thr' Fibre channel (FC), Fibre Channel over Ethernet (FCoE)

5) NAS Gateways - Data transmission betⁿ SAN & NAS devices.

Cloud Infrastructure Mechanisms

Cloud infrastructure mechanisms are foundational building blocks of cloud environment that establish primary artifacts to form the basis of fundamental cloud technology architecture.

Following are the cloud infrastructure mecha

- Logical Network Perimeter
- Virtual Server
- Cloud Storage Device
- Cloud Usage Monitor
- Resource Replication
- Ready-Made Environment.

Logical Network Perimeter

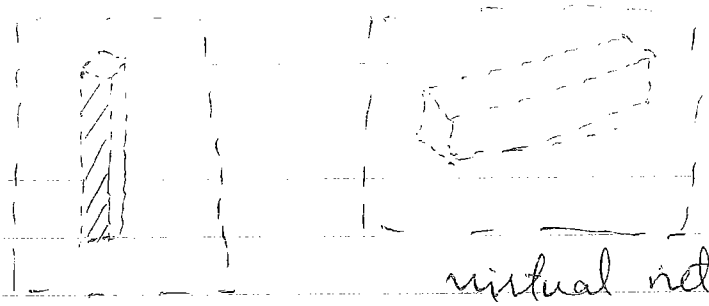
The isolation of a network environment from the rest of a communications network, the logical network perimeter establishes a virtual network boundary that can encompass & isolate a group of related cloud-based IT resources that may be physically distributed.

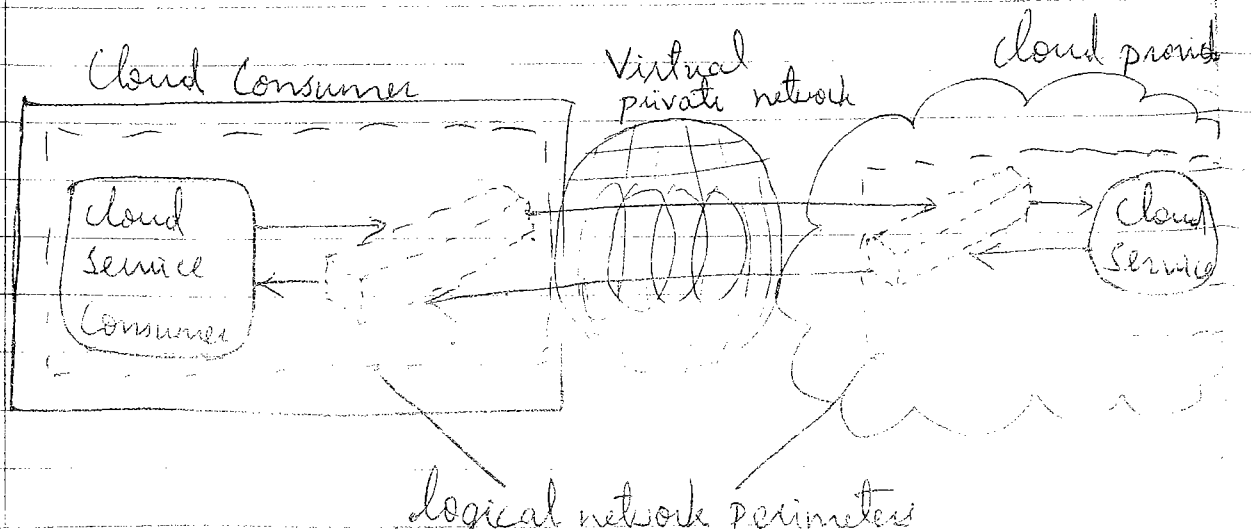
This mechanism can be implemented to:
- isolate IT resources in a cloud from non-authorized users
- isolate IT resources in a cloud from non-users
- isolate IT resources in a cloud from cloud consumer
- control the bandwidth that is available to isolated IT resources.

Logical network perimeters are typically established via network devices that supply & control the connectivity of a data center & are commonly deployed as virtualized IT environment that include:

- Virtual Firewall - An IT resource that actively filters network traffic to & from the isolated network while controlling its interactions with the internet.

- Virtual Network - Usually acquired through VLANs, this IT resource isolates the network environment within the data center infrastructure.



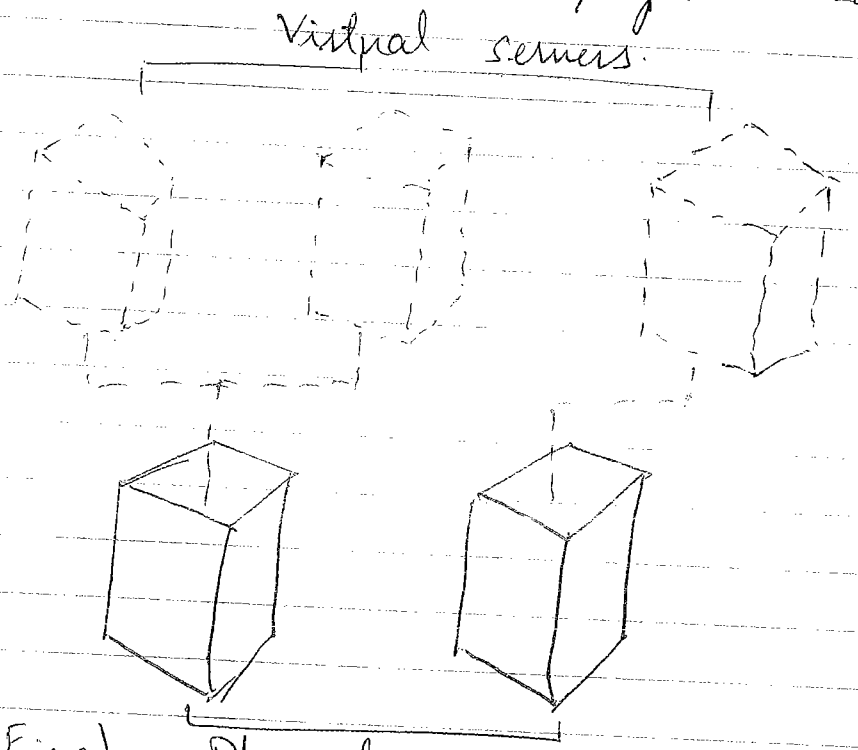


In above fig. depicts a scenario in which perimeters are connected through a VPN that protects

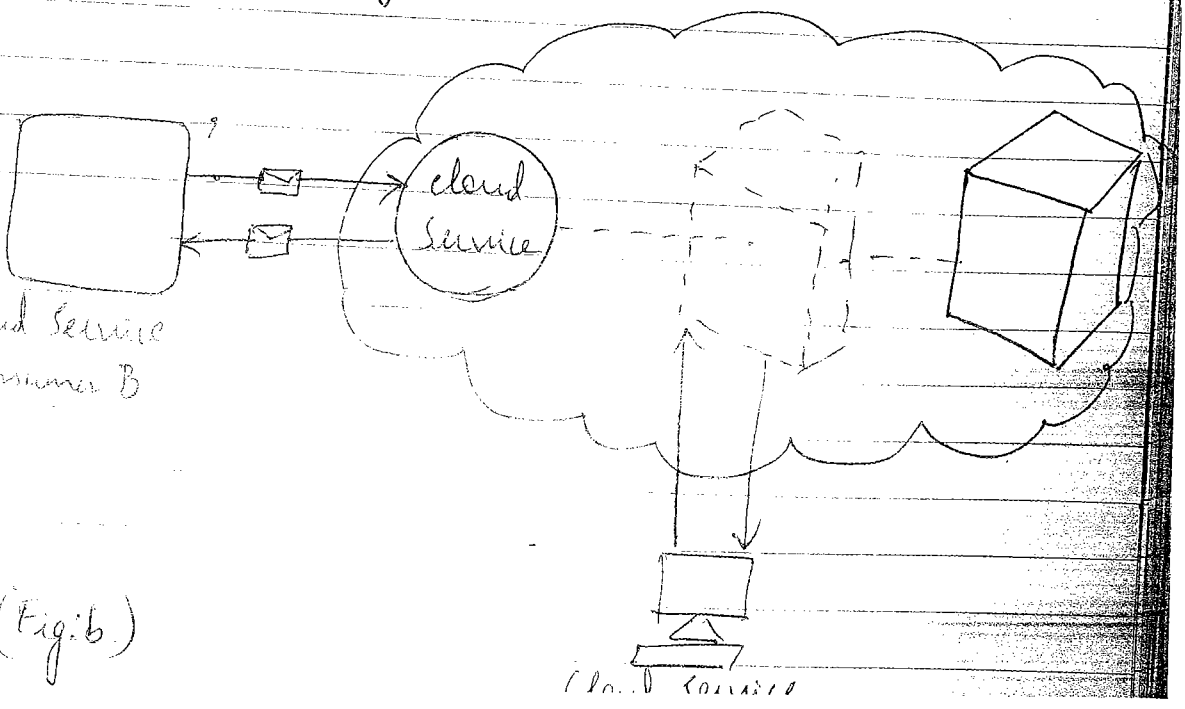
communications, since VPN is implemented by point-to-point encryption of the data packets sent between the communicating endpoints.

Virtual Server

- A virtual server is a form of virtualization software that emulates a physical server.



(Fig a)



(Fig: b)

Cloud Storage Device

The cloud storage device mechanism represents storage devices that are designed specifically for cloud-based provisioning.

Cloud storage devices are commonly able to provide fixed-increment capacity allocation in support of the pay-per-use mechanism.

A primary concern related to cloud storage is the security, integrity & confidentiality.

Cloud Storage Levels

Cloud storage device mechanisms provide common logical units of data storage, such as

- Files - Collections of data are grouped into files that are located in folders.
- Blocks - The lowest level of storage & the closest to the hardware, a block is the smallest unit of data that is still individually accessible.
- Datasets - Sets of data are organized into a table-based, delimited, or record format.
- Object - Data & its associated metadata are organized as Web-based resources.

Each of these data storage levels is commonly associated with a certain type of cloud storage device & cloud storage service used to expose its API.

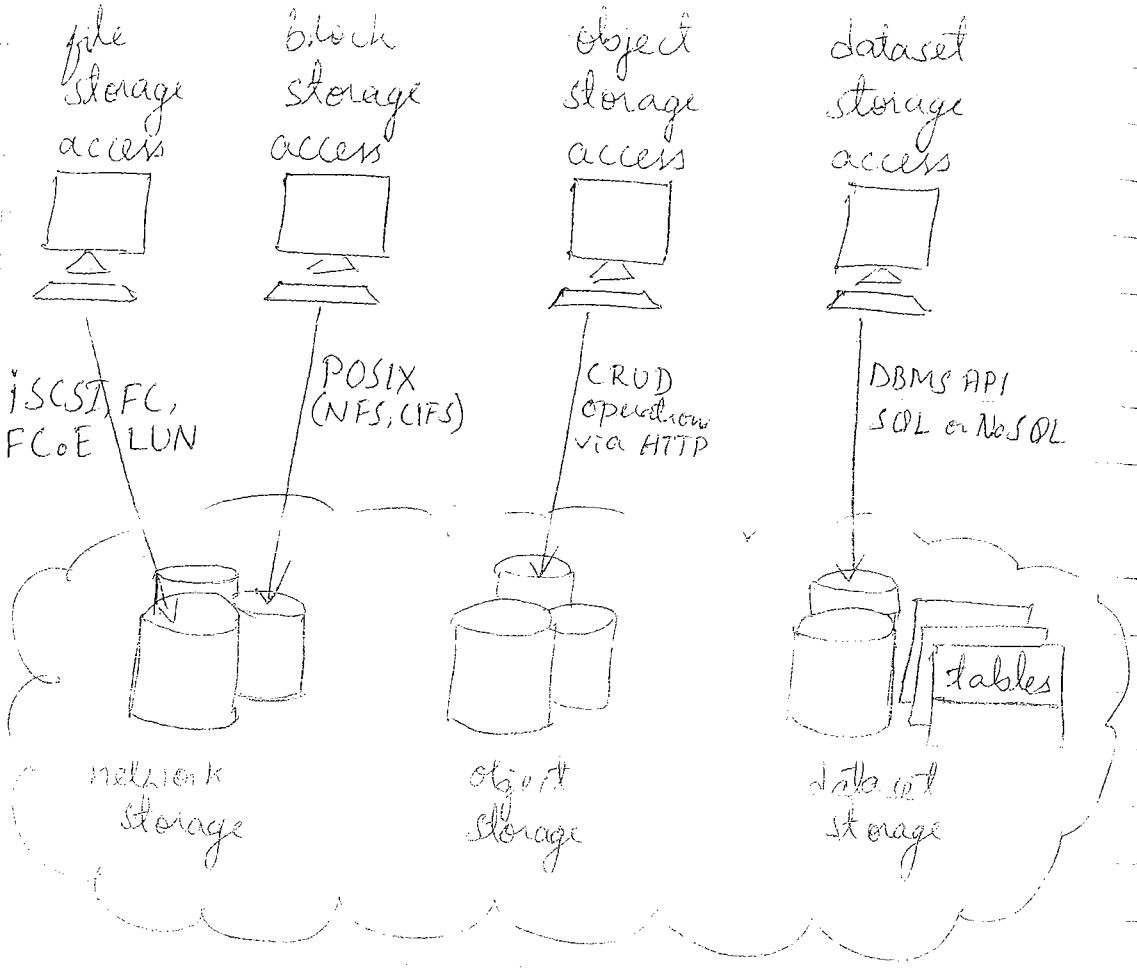


Fig: Different cloud service consumers utilize different technologies to interface with virtualized cloud storage device.

Network Storage Interfaces.

It includes storage devices in compliance with industry standard protocols, such as SCSI for storage blocks & the server message block (SMB), common Internet file system (CIFS) & network file system (NFS) for file & network storage.

Data storage entails storing units of data in separate file that can be different size & format & organized into hierarchical subdirectories.

- When a cloud storage device mechanism is based on this type of interface, its data searching & extraction preformance is suboptima

- Block storage requires data to be in a fixed format, i.e. data block, smallest unit that can be stored & accessed.

- Using either the logical unit number (LUN) or virtual volume block-level storage have better peformance than file-level storage.

Object Storage Interfaces

- Various types of data can be referenced & stored as Web resources, referred as object storag

- Cloud Storage Device mechanisms that implement this interface can be accessed via REST or Web service-based cloud services using HTTP.

- The Storage Networking Industry Association's Cloud Data Management Interface (SNIA CDMI) supports the use of object storage interfaces.

Data Storage Interfaces.

- This support a query language.
  The storage interface is divided into two categories according to storage structure
  - Relational Data Storage
  - Non-Relational Data Storage

Relational Data Storage

- Relational database rely on tables to organize similar data into rows & columns.
- Tables can have relationships with each other to give the data increased structure, to protect data integrity & to avoid data redundancy.

- A cloud storage device mechanism is implemented using number of commercially available database products, such as IBM DB2, Oracle Database, Microsoft SQL Server, & MySQL.

- Challenges with cloud-based relational databases are scaling & performance.
- Scaling a relational cloud storage device vertically is more complex & cost-ineffective than horizontal scaling.
- Database with complex relationships and/or containing large volumes of data can (be afflicted) have higher processing overhead & latency.

Non-Relational Data Storage

Non-relational storage establishes a "looser" structure for stored data with less emphasis on defining relationships & realizing data normalization.

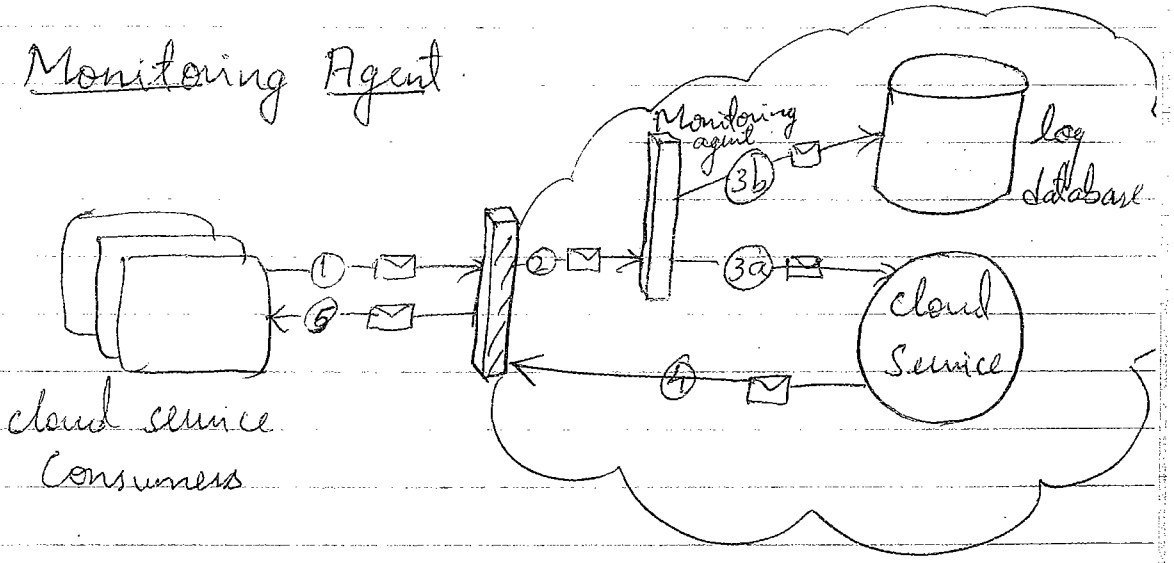
- Cloud providers often offer non-relational storage that provides scalability & availability of stored data over multiple server environments.

Cloud Usage Monitor

The cloud usage monitor mechanism is a lightweight & autonomous s/w prog responsible for collecting & processing IT resource usage data.

Depending on the type of usage metrics they are designed to collect & the manner in which usage data needs to be collected, cloud usage monitors can exist in different formats.

Monitoring Agent



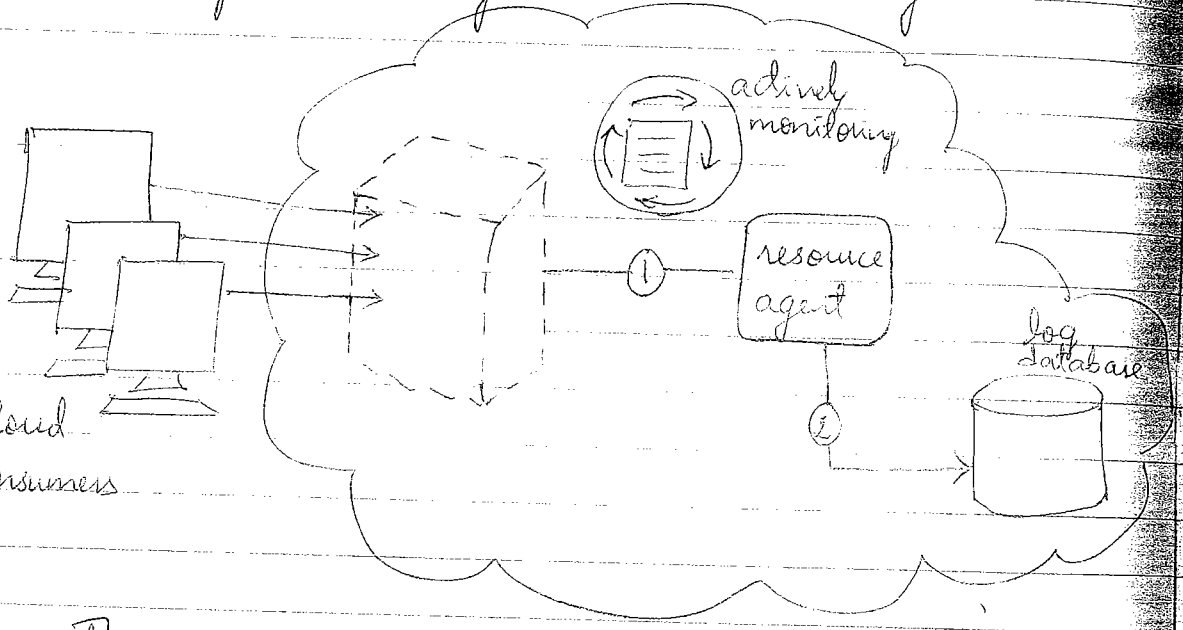
A monitoring agent is an intermediary, event-driven program that exists as a service agent & resides along existing communication paths to transparently monitor & analyze dataflows.

- This type of cloud usage monitor is used to measure network traffic & message metrics.

Resource Agent.

A resource agent is a processing module that collects usage data by having event-driven interactions with specialized resource software.

- This module is used to monitor usage metrics based on pre-defined, observable events at the resource software level, such as initiating, suspending, resuming, & vertical scaling.

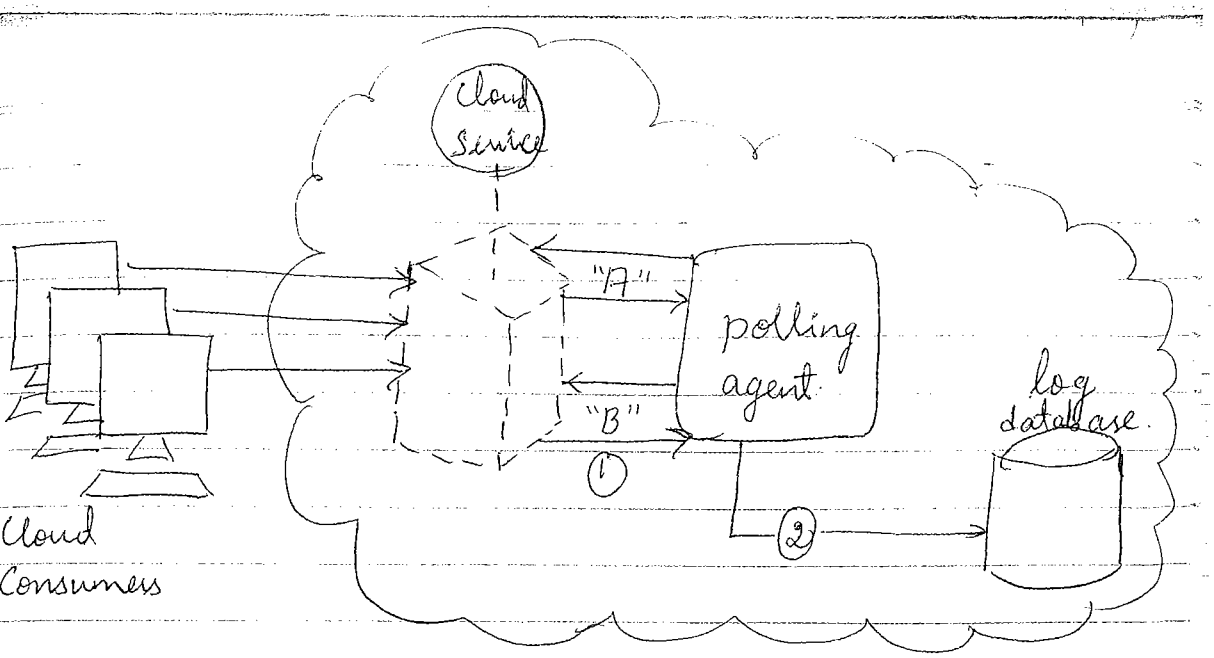


① → The resource agent receives a notification from the underlying resource management program that the virtual server is being scaled up & stores the collected usage data in a log database, as per its monitoring metrics ②.

Polling Agent.

A polling agent is a processing module that collects cloud service usage data by polling IT resources.

This type of cloud service monitor is commonly used to periodically monitor IT resource status, such as uptime & down time.



A polling agent monitors the status of a cloud service hosted by a virtual server by sending periodic polling request messages & receiving polling response messages that report usage status "A" after a number of polling cycles, until it receives a usage status of "B" (1), upon which the polling agent records the new usage status in the log database (2).

Resource Replication

- The creation of multiple instances of the same IT resources, when an IT resource's availability & performance need to be enhanced.
- Virtualization technology is used to implement the resource replication mechanism.

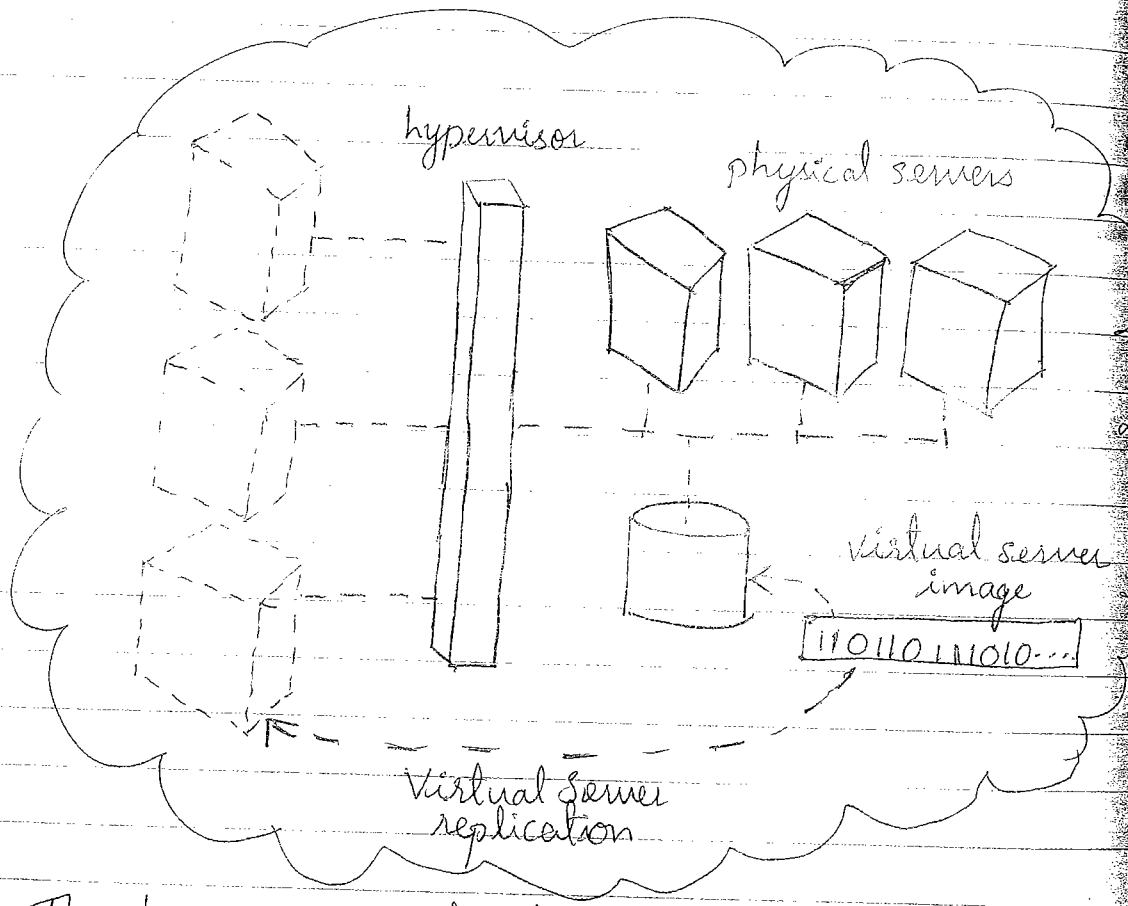


Fig: The hypervisor replicates several instances of a virtual server, using a stored virtual server image.

Other common types of replicated IT resources include cloud service implementations & various forms of data & storage device replication.

Ready-Made Environment

The ready-made environment mechanism is a defining component of the PaaS cloud delivery model that represents a pre-defined, cloud-based platform comprised of a set of already installed IT resources, ready to be used & customized by a cloud consumer.

- Cloud consumers remotely develop & deploy their own services & applications within a cloud environment.
- Ready-made environments include pre-installed IT resources, such as databases, middleware, development tools & governance tool.

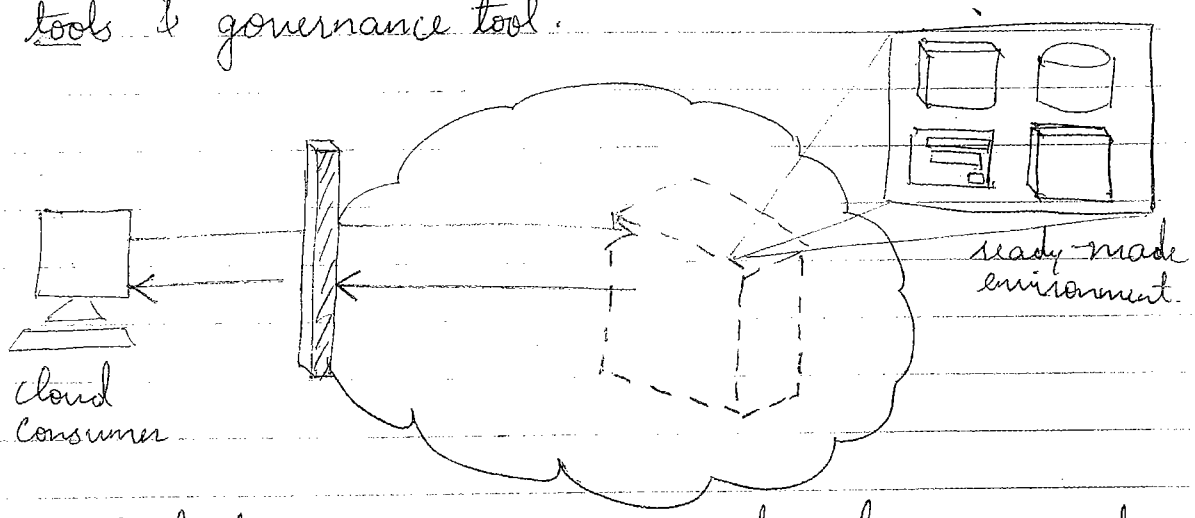


Fig: A cloud consumer accesses a readymade environment hosted on a virtual server.

- A ready-made environment is equipped with complete software development kit (SDK) with programmatic access to development technologies.
- Middleware is available for multitenant platforms to support the development & deployment of Web applications.