**CLOUD COMPUTING**

**Unit-4**

**EVOLUTION OF CLOUD COMPUTING**

**INTRODUCTION TO MAINFRAME ARCHITECTURE**

In a mainframe System, all the processing is done by a single very powerful computer. Individual terminals are used to access the mainframe computer but don’t run by applications themselves.

**Mainframe (Host)**

**- Communication.**

**-User interface**

**-Dbms**

**-Os**

**-storage**

**Terminal**

**Terminal**

**Terminal**

**Fig : Mainframe Architecture.**

* Mainframe measured in millions of instructions per second
* Mainframe are built to be reliable for transaction processing.

**CLIENT –SERVER ARCHITECTURE**

Laptop

Internet

Mobile

SERVER

Desktop

**Fig: client server Architecture.**

Client-server Architecture is a computing model in which the server hosts ,delivers and manages most of the resources and services to be consumed by the client. This type of architecture has one or more client computers connected to a central server over a network . this system shares computing resources . It is a producer consumer computing architecture where the server acts as a producer and client as a consumer.

**CLUSTER COMPUTING**

Cluster computing is a form of computing in which a group of computers are linked together so that they can act like a single computer.

**Front End Node**

**NIC (Network Interface Card)**

**Public network**

NIC

NIC

**Switch**

**Node1 Node2 Node3 Node4**

**Fig cluster computing architecture**

BENEFITS OF CLUSTER COMPUTING

* High availability – The ability to provide end users with access to a service for a high percentage of time.
* High reliability – The ability of a system to reduce frequency of system failure.

DISADVANTAGES

* With respect to software it is difficult to develop software for distributed systems.
* With respect to Network it shows lossy transmissions.
* With respect to security easy access to secret data.

**GRID COMPUTING**

Grid computing is the collection of computer resources from multiple locations to reach a common goal. Grid computers have each node set to perform a different task or application. Grid computer also tend to be more heterogeneous and geographically dispersed than cluster computers . Single grid can be dedicated to a particular application.

BENEFITS

* Exploit under utilized resources.
* Resource load balancing.
* Virtualize resources across an enterprise.
* Enable collaboration for virtual organization .

Control Node

**Fig : Grid computing architecture.**

**PROS AND CONS OF GRID COMPUTING**

Pros cons

Time saving Resource management

(Who is Prior?)

Resource saving Security Problem

(data is remote)

Space saving schedule problem

APPLICATIONS

1. Used in inventory control.
2. Used in climate forecasting.
3. Enterprise computing.

**PARALLEL COMPUTING**

Parallel computing is the **simultaneous** use of multiple computing resources to solve a computation problem.

* A problem is broken into discrete parts that can be solved concurrently.
* Each part is further broken down to a series of instructions.
* Instruction from each part execute simultaneously on different processors.
* Co-ordinator mechanism is employed.

**Problems**  **Instruction**

**Processor**

**Processor**

**Tn................T1**

**Fig parallel computing.**

ADVANTAGES

* Saves time
* Cost is saved
* Solve larger and complex problems
* Provide concurrency
* Make better use of underlying parallel hardware.

DISADVANTAGES

* Portability
* Resource requirements
* Scalabilit

**DISTRIBUTED COMPUTING**

A distributed system is a collection of independent computers, interconnected via a network, capable of collaborating on a task. Distributed computing is computing performed in a distributed system.

**Network host**

**Internet**

**Work station**

Fig distributed computing.

ADVANTAGES

* The affordability of computers and availability of network access
* Resource sharing
* Scalability
* Fault tolerance

DISADVANTAGES

* Multiple points of failures
* Security concerns

**EVOLUTION OF SHARING ON THE INTERNET**

Service sharing cloud computing. Everything as a service.

Resource grid computing.

Sharing std’s / s/w for sharing remote resources.

Information www.

Sharing HTML,HTTP,doc exchange

Network inter – networking and internet

Sharing inter networking of regional networks with TCP/IP.

Networking multiple regional networks linking computer

network

INTRODUCTION OF CLOUD COMPUTING

Cloud computing is the delivery of computing services over the internet.cloud services allow individuals and businesses to use software and harsdware that are managed by third parties of remote locations.

**DEFINITION OF CLOUD**

NIST defines “ cloud computing is a model for enabling ubiquitous , convenient on demand network access to a shared pool of configurable computing resources(eg networks ,servers ,storage ,applications and services )that can be rapidly provisioned and released with minimal management effort or service provider interaction .

**CLOUD DEPLOYMENT MODELS**

A cloud deployment model represents a specific type of cloud environment , primarily distinguished by ownership, size and access.

Four common cloud deployment models

* Public clouds
* Community clouds
* Private clouds
* Hybrid clouds

**PUBLIC CLOUDS**

A public cloud is a publicly accessible cloud environment owned by a third party cloud provider. The cloud provider is responsible for the creation and ongoing maintenance of public cloud and its IT resources.

**Sales force**

**Microsoft**

**Yahoo**

**Amazon**

**Google**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Fig- organizations acts as cloud consumers when accessing cloud services and IT resources made available by different cloud providers.

**COMMUNITY CLOUDS**

A community cloud is similar to a public cloud except that its access is limited to specific community of cloud consumers. the community cloud may be jointly owned by the community members or by a third party cloud provider that provisions a public cloud with limited access .

Community cloud

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Fig : an example of a community of organizations accessing IT resources from a community cloud.

PRIVATE CLOUD

A private cloud is owned by a single organization .private clouds enable an organization to use cloud computing technology as a means of centralising access to IT resources by different parts , location or department of organization.

Cloud Service

Consumer

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

**organization**

Fig : A cloud service consumer in the organization’s premise environment to access a cloud service hosted on the same organization’s private cloud via a virtual private network.

**HYBRID CLOUDS**

A hybrid cloud is a cloud environment comprised of two or more different cloud deployment models.

Eg. A cloud consumer may choose to deploy cloud services processing sensitive data to a private cloud and other less sensitive cloud services to a public cloud. The result of this combination is a hybrid deployment model.

Public

data



Cloud services consumer

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Fig : An organization using a hybrid cloud architecture that utilizes both a private and public cloud.

**OTHER DEPLOYMENT MODELS**

Virtual private cloud : also called as “dedicated cloud” or “hosted cloud” . this model results in a self contained cloud environment hosted and managed by a public cloud provider and made available to a cloud consumer.

Inter cloud: this model based on architecture comprised of two or more inter connected clouds.

**CLOUD SERVICES**

Infrastructure as a service (IaaS) it includes

* Processing
* Storage
* Network

Ex- Amazon elastic compute cloud EC2.

Platform as a service (PaaS)

The PaaS model includes services that build an IaaS services. They add value to the IaaS services by providing a platform in which cloud users can provision their own applications. The user does not need to manage the underlying cloud infrastructure (N/W , storage, and O.S). services provided in PaaS models

* Middle ware
* Application servers
* Database servers
* Development routine environment

Example- Microsoft windows Azure

Software as a service (SaaS)

SaaS is a software distribution model in which applications are hosted by a vendor or a service provider and made available to customers over a network, typically the internet.

Benefits of SaaS model include:

* Easier administration
* Easier collaboration
* Global accessibility

**Key characteristics of cloud computing**

* On demand self service : users are able to use cloud computing resources without human interaction , mostly done through web based service.
* Broad network access: cloud computing resources are accessible over the network, supporting heterogeneous client platforms such as mobile devices and work stations.
* Resource pooling: service multiple customers from the same physical resources by securely separating the resources on logical level.
* Rapid elasticity : resources are used and released on- demand and/or automated based on triggers and parameters. This will make sure your application will have exactly the capacity it needs at any time.
* Measured service: resources usage are monitored , measured and reported (billed) transparently based on utilization ,in short pay for use .

**BENEFITS AND RISKS IN CLOUD COMPUTING**

Benefits

* Lower capital costs: organization can provide unique services using large scale computing services and paying for actual capacity used.
* Lower IT operation costs: the flexibility to host their virtual IT infrastructure in locations offering the lowest cost.
* No hardware or software installation or maintenance.
* Optimized IT infrastructure provides quick access to needed computing services.

Risks

* Environment security
* Data privacy and security
* Data availability
* Record retention requirements
* Disaster recovery

**Data Center**

A data center is a facility that centralizes an organization’s shared IT operations and equipment for the purposes of storing, processing, and disseminating data and applications. Because they house an organization's most critical and proprietary assets, data centers are vital to the continuity of daily operations. Consequently, the security and reliability of data centers and their information are among any organization’s top priorities.

In the past, data centers were highly controlled physical infrastructures, but the public cloud has since changed that model. Except where regulatory restrictions require an on-premises data center without internet connections, most modern data center infrastructures have evolved from on-premises physical servers to virtualized infrastructure that supports applications and workloads across multi-cloud environments.

The Role of the Data Center

Data centers are an integral part of the enterprise, designed to support business applications and provide services such as:

Data storage, management, backup and recovery

Productivity applications, such as email

High-volume e-commerce transactions

Powering online gaming communities

Big data, machine learning and artificial intelligence

Today, there are reportedly more than 7 million data centers worldwide. Practically every business and government entity builds and maintains its own data center or has access to someone else's, if not both models. Many options are available today, such as renting servers at a colocation facility, using data center services managed by a third party, or using public cloud-based services from hosts like Amazon, Microsoft, Sony and Google.

The Core Components of a Data Center

Data center architectures and requirements can differ significantly. For example, a data center built for a cloud service provider like Amazon satisfies facility, infrastructure and security requirements that significantly differ from a completely private data center, such as one built for a government facility that is dedicated to securing classified data.

Regardless of classification, an effective data center operation is achieved through a balanced investment in the facility and the equipment it houses. In addition, since data centers often house an organization's business-critical data and applications, it's essential that both facility and equipment are secured against intruders and [cyberattacks](https://www.paloaltonetworks.com/network-security/data-center).

The primary elements of a data center break down as follows:

Facility – the usable space available for IT equipment. Providing round-the-clock access to information makes data centers some of the world’s most energy-consuming facilities. Design to optimize space and environmental control to keep equipment within specific temperature/humidity ranges are both emphasized.

Core components – equipment and software for IT operations and storage of data and applications. These may include storage systems; servers; network infrastructure, such as switches and routers; and various information security elements, such as [firewalls](https://www.paloaltonetworks.com/network-security/next-generation-firewall).

Support infrastructure – equipment contributing to securely sustaining the highest availability possible. The Uptime Institute has defined four tiers of data centers, with availability ranging from 99.671% to 99.995%. Some components for supporting infrastructure include:

Uninterruptible Power Sources (UPS) – battery banks, generators and redundant power sources.

Environmental control – computer room air conditioners (CRAC); heating, ventilation and air conditioning (HVAC) systems; and exhaust systems.

Physical security systems – biometrics and video surveillance systems.

Operations staff – personnel available to monitor operations and maintain IT and infrastructure equipment around the clock.

**UNIT-5 Virtualization & Cloud Services.**

* **IaaS :**

|  |
| --- |
| Application services |
| Platform services |
| Infrastructure |

* Provides of Iaas offer computers, physical or more often virtual machines and other resources.
* A hypervisor such as Valware,XEW, runs an virtual machines as guests.
* Pool of hypervisors within the cloud operational system can support large number of virtual machines and the ability to scale services up and down by customer’s varying requirements

**PaaS**

Provides platform allowing customers to develop, run and manage web applications without the complexity of building and maintaining the infrastructure.

Advantages

* Allows for higher level programming with dramatically reduced complexity.
* Useful in situations where developers are working on a single project involving parties who are not located nearby.

Disadvantage

* Possibility of being locked into a certain platform.

**SaaS**

Saas is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.used in CRM,ERP collaboration.

Advantages

* Configuration and customization
* Accelerated feature delivery
* Collaboration functionality

Disadvantages

* Difficult task of transferring very large data files over internet.

**Communication as a Service(CaaS)**

Communications as a service is an outsources enterprise communications solution that can be leased from a single vendor. Such communications can include voice over IP, instant messaging. Caas is responsible for hardware and software management and offers guarantee QoS. Caas offers flexibility and expandability, allowing for addition of services.

Example AWS- SNS.

**Monitoring as a service(MaaS)**

Maas is one of many cloud delivery models under Xaas. It is a framework that facilitates the deployment of monitoring functionalities for various other services and application within the cloud. The most common application for Maas is online state monitoring, which continuously tracks certain state of applications, network, system, instances of any element that may be deployable within the cloud.

Example AWS-Cloud Watch

**Storage as a service**

Storage as a service is a business model in which a large company needs space in their infrastructure to a smaller company or individual. Storage as a service is generally seen as a good alternative for a small or midsized business that lacks the capital budget and or technical personnel to implement and maintain their own storage infrastructure .Storage as a service is also being promoted for business to mitigate risk in disaster recovery, provide long term retention for records and enhance both business continuity and availability.

Traditional storage versus cloud

* Performance : no SQL, low latency,
* Maintenance: focus on main application/ feature
* Support: quick, accurate and efficient
* Reliability is good
* Security is good

**Amazon EC2**

Amazon Elastic computer cloud EC2 is a web services that provides compute capacity in the cloud. It is a web simple web service interface allows you to obtain and configure capacity with universal function. It provides complete control of computing resources , with quick scale capacity and less failure.

Feature of Amazon EC2:

* Virtual computing environment known as instances.
* Preconfigured template for your instances known as Amazon Machine images.
* Various configurations of CPU, memory, storage and networking capacity for your instances known as instance types.
* secure login info for your instances using key pairs.
* virtual networks you can create that are logically isolated from the rest of cloud, and that you can optionally connect to your own network known as virtual private clouds(VPC).

**Virtualization**

Refers to act of creating a virtual (rather than actual) version of something. Including virtual computer hardware platform, OS, storage devices and computer n/w resources.

Virtualization introduction

Virtualization is a framework or methodology of dividing the resources of computer into multiple execution environments, by applying one or more concepts or technologies such as H/W and S/W partitioning, time sharing, partial or complete machine simulation,gos,others

In multitasking

AP3

AP2

AP1

OS

CPU

OS3

AP3

AP2

AP1

VIRTUAL CPU3

OS2

AP3

AP2

AP1

VIRTUAL CPU2

OS1

AP3

AP2

AP1

VIRTUAL CPU1

Fig virtualization

**Why to virtualize ?**

* Flexibility – more than one instance.
* Availability – temporary migration , if physical node is down.
* Scalability- very easy to insert a physical node with the basic cluster
* Hardware utilization – virtual machines utilize hardware resources that are left idle.
* Security: using multiple virtual machines, it is possible to separate services by running one service on each virtual machine . this approach is also called jailing of services.

Definition

Virtual machines

A representation of real machine using S/W. that provides an O.S environment which can run or host a guest O.S, virtual machines are created and managed by V.M.M

Guest O.S

O.S which is running inside the created virtual machine.

Hypervisor

A thin layer of software that generally provides virtual partitioning capabilities which runs directly an hardware, referred to as “bare metal” approach.

VMM

S/W that runs in a layer between host O.S and one or more virtual machines that provides virtual machine abstraction to guest O.S.

Types of virtualization

* Hosted: when VMM runs in O.S.
* Bare metal approach runs on VMM on top of n/w directly.

Full virtualization

* Native virtualization
* It is designed to simulate the underlying network which is physically available.
* It gives flexibility to more user virtual machines from one host to another host very easily. But at the cost of performance due to overhead. Ex VMWare.

Para virtualization

* The hypervisor exports a modified version of the underlying physical network.
* It provides better performance than full virtualization.

Ex : Xen.

OS level virtualization

* No requirement of virtual machine monitor software
* Single OS image handles all the guest images in different isolated containers.

Ex : linux Vserver.

Application virtualization

* Referred as process virtualization
* It is the approach of running applications inside a virtual execution environment.
* The virtual execution environment provides standard API for cross platform execution and manages consumption of applications local resources.

Ex: environment variables, objects.

Pros and cons of virtualization

Pros

* Lower overall capital expenditures by hosting multiple virtual servers on a single physical machine, you can reduce cost.
* Automated tasks: virtualization lets you automate a number of significant roujtine IT tasks
* Greater redundancy: provides greater safety and security.
* Faster deployment: deploying a virtual machine is simpler than deploying a physical machine.

Cons

* High upfront expenditures
* Not all applications are ready for virtualization.
* The danger of server sprawl.

Virtualization application inenterprises

Server virtualization

* It is a masking of server resources
* Divide one physical server into multiple isolated virtual environments.
* The virtual environments are sometimes called virtual private servers , also called as guests instaces , containers, emulations.
* Virtual machine model.
* Para virtual machine model
* Virtualization at OS layer.

VMM 🡪 users hypervisor to coordinate instructions to CPU.

PVM🡪modifies guest O.S code is called porting.

Virtualization at OS level, the hosts runs a single OS kernel as its core and exports O.S functionality to each of the guests.

Advantages

* Disaster recovery
* Reduces CPU overhead
* Reduces S/w calls.

Desktop virtualization

It is the concept of isolating a logical O.S instance from the client. That is used to access it.

* Needs remote display protocol.
* Uses both a machine virtualization

Layer for hosting PC VM’s on a server and presentation virtualization for remote access of those virtual machines from the desktop.

* A full instance of desktop O.S runs as an virtual machine that is hosted on a server and remote accessed from a client device.
* For the end user, the experience of virtual desktop should be same as using local PC.
* Access is managed through connection broker software.

Ex : VMware view, Citrix Xen desktop.

Application virtualization

Application virtualization is software technology that encapsulates application software from the underlying system in which it is executed.

Benefits

Allows applications to run an environments that do not suit the native application

Storage virtualization

Storage virtualization is the process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device. Storage virtualization is also known as cloud storage. Storage virtualization aggregates the function and hides the actual complexity of SAN.

Advantages

* Improved storage management in a heterogeneous IT environment.
* Better availability and estimation of down time with automated management.
* Better storage utilization.

Network virtualization

Network virtualization is the process of combining hardware and software network resources and network functionality into a single , software based administrative entity , a virtual network.

Advantages

* Flexibility
* Manageability
* Scalability
* Security
* Privacy and isolation
* Heterogeneity and Programmability.

**SECURITY IN THE CLOUD**

Cloud security is an evolving sub domain of information security, it refers to a broad set of policies, technologies, controls deployed to protect data, applications and associated infrastructure of cloud computing.

Dimensions of cloud security

Identity management – to control access to information and computing resources.

Physical security – secure the IT hardware (servers, routers,cable etc)

Personnel security – service level agreement , code of conduct , policies etc.

Availability – cloud providers help ensure that customers can rely on access to their data and applications

Privacy – providers ensure that all critical data are masked or encrypted.

Cloud security challenges

* Data protection
* User authentication
* Disaster and data breach

Data protection

Here placing critical data in the hands of third party, data needs to be encrypted at all times.

User authentication – companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data.

Disaster and data breach refered as contingency planning – a comprehensive security assessment from a neutral third part is strongly recommended as well.

Other challenges

* Loss of control
* Lack of trust
* Multi-tenancy

Infrastructure security

Network security

Network components are shared by different tenants due to resource pooling. Sharing resources allows attackers to launch cross-tenant attacks. Virtual networks increases virtual machines inter connectivity , an important security challenge in cloud computing. The most secure way is to look each virtual machine with its host by dedicated physical channels. Most hypervisors use virtual networks to link virtual machines to communicate more directly and efficiently. Most virtualization platforms such as Xen provide two ways to configure virtual networks bridged and routed. But these techniques increase the possibility to perform some attacks such as sniffing and spoofing.

Host and application level security

The applications such as SaaS are typically delivered via the internet through a web browser. Flaws in web applications may create vulnerabilities for SaaS applications . attackers having been using the web to compromise user’s computer and perform malicious activities such as steal sensitive data .

* Multi-tenancy
* Data security
* Accessibility

Storage security

* Traditional security problems
* Law issue
* Third party issue
* Authentication
* Encryption
* Segmentation
* Metadata based storage model
* Multi-cloud architecture model

Security management in cloud

* Ensure effective governance , risk.
* Audit operational and business processes.
* Manage people , roles and identities.
* Ensure proper protection of data and information.
* Ensure privacy policies
* Assess the security provisions for cloud application
* Ensure cloud network and connections are secure
* Evaluate security controls on physical infrastructure and facilities
* Manage security terms in cloud SLA
* Understand the security requirements of the exit process

data privacy

data privacy questions about how safe is your data in the cloud ?

Issues

* Data segregation and ownership
* Location of data
* Security procedures/ standards
* Access protocols.
* Audit rights
* Notifications of security breaches

Life cycle of data in cloud

Create

Store

Use

Share

Archive

Destroy

In create phase

* Data classi9fication
* Assignments of rights to create
* Integer creation

In store phase

* Access management
* Data integrity and confidentiality
* Encryption in REST
* Data recovery