

DHISHAN COMMERCE ACADEMY
PRESENTS



Second Edition



SUMMARY ISCA NOTES

FOR MAY 2020 EXAMS

First Edition Notes
2018 edition

**10,000**
DOWNLOADS



9953209955

AUTHORED BY
CA AKHIL MITTAL

contactus@dcacademy.co.in

www.dcacademy.co.in

Buy Full
Notes



Chapter 8: Emerging Technologies

8.1 Introduction:

Emerging Technologies are contemporary advances and innovation in various fields of technology. Various converging technologies have emerged in the technological convergence of different systems evolving towards similar goals. Emerging technologies are those technical innovations which represent progressive developments within a field for competitive advantage.

8.2 Cloud computing:

Cloud Computing is both, a combination of software and hardware based computing resources delivered as a networked service. This model of IT-enabled services enables anytime access to a shared pool of applications and resources. These applications and resources can be accessed using a simple front-end interface such as a Web browser, and thus enabling users to access the resources from any client device including notebooks, desktops and mobile devices.

ARCHITECTURE	CHARACTERISTICS V- P.M. – M.A.R.S.	ADVANTAGES I. - C.A.R.D.S.
• FRONT END ARCHITECTURE: The front end of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. • BACK END ARCHITECTURE: Back end refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system.	• VIRTUALISATION • PERFORMANCE • MAINTENANCE • MULTI-SHARING • AGILITY • REALIBILITY AND AVAILABILITY • SCALABILITY	• INTEGRATION OF SOFTWARE • COST EFFICIENT • ACCESS TO INFORMATION • RECOVERY • DEPLOYMENT • STORAGE

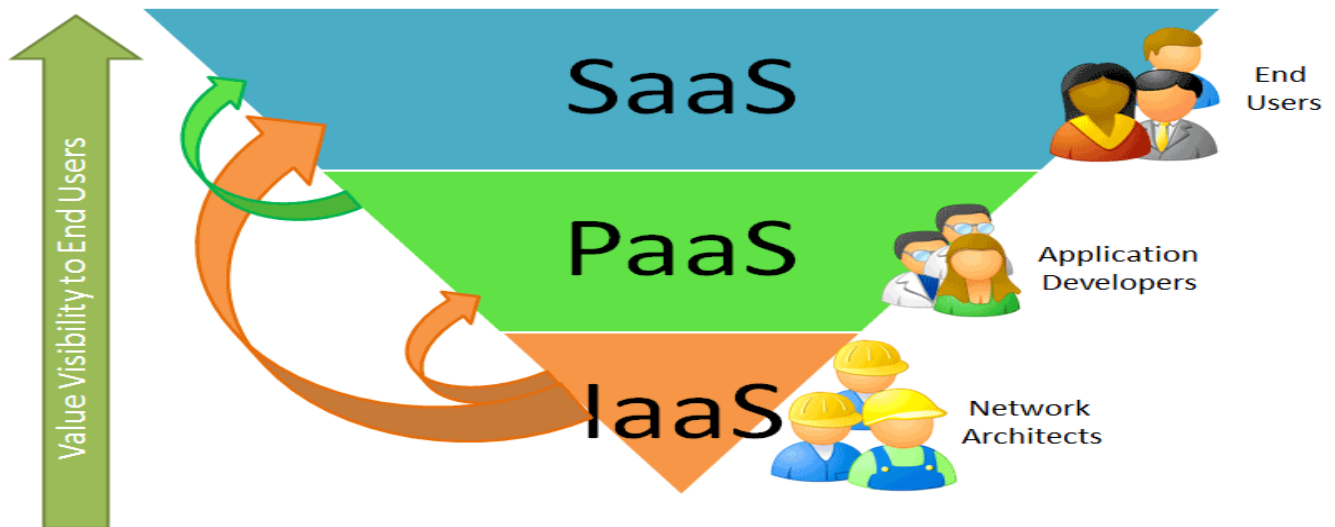
8.3 Cloud computing environment / Types of Cloud:

Cloud computing environment			
PUBLIC CLOUD	PRIVATE CLOUD	COMMUNITY CLOUD	HYBRID CLOUD
A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider). Public cloud services may be free or offered on a pay-per-usage model. This environment can be used by general public.	A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. These are typically deployed within an organization's own internal ecosystem, often leveraging the organization's own private data center. Private clouds typically rely on the organization having trained IT staff onsite to manage the private cloud ecosystem.	Here the cloud is being shared by person(s) of one community and hence the name. In this type of cloud infrastructure is provisioned by a specific community	A hybrid storage cloud uses a combination of public and private storage clouds. Hybrid storage clouds are often useful for archiving and backup functions, allowing local data to be replicated to a public cloud.

8.4 Advantages Characteristics of type of cloud:

ADVANTAGES	THE MAIN BENEFITS OF USING A PUBLIC CLOUD:
	(a) Easy & inexpensive set-up due to hardware, application & bandwidth costs are covered by provider. (b) Scalability to meet needs. (c) No wasted resources because you pay for what you use.
CHARACTERISTICS	THE MAIN BENEFITS OF USING A PRIVATE CLOUD:
	(a) Improves the average server utilization, usage of low cost servers & hardware. (b) Small in size...Controlled and maintained by the organization. (c) Provides high level of security and privacy to the users.
	CHARACTERISTICS OF PUBLIC CLOUD: (S.A.L.S.A.)
	(a) Scalable: Resources and the users in the public code are large and service provider has to grant all the requests. Hence public clouds are considered to be scalable. (Able to be changed in size or scale.) (b) Affordable: In this case, user pays for that only for what he or she is using and this don't involve any cost related to the deployment Less Secure: Since it is offered by third party and they have full control over the cloud, as such it is less secured as compared to on-premises public cloud. (c) Stringent SLAs: Since there is Service level agreement between the service provider and users, and reputation of the service provider is dependent on that, they follow the SLA very strictly. (d) Available: It is highly available since anyone can link to the public cloud with the proper permission.
	CHARACTERISTICS OF PRIVATE CLOUD:
	(a) Secure: Private cloud is being managed by organization itself, hence less chance of data being stolen and leaked out. (b) Central Control: Private cloud is managed by organization itself so there is no need of relying on the outside agency hence results in central control by the entity. (c) Weak Service-level Agreement: SLAs are agreement between user and the service provider. However, in case of private cloud the SLA is weak since this type of networking is between the organizations & user of the same organization.
	CHARACTERISTICS OF HYBRID CLOUD:
	(a) Scalable: Hybrid has the property of public cloud hence scalable. (b) Partly Secure: Public cloud is more vulnerable and is subject to high risk of security breach. AS such hybrid is not fully secure, hence partly. (c) Stringent SLAs: Since there is Service level agreement between the service provider and users, and reputation of the service provider is dependent on that, they follow the SLA very strictly. (d) Complex Cloud Management: Since hybrid model comprises of one or more deployment models & users are also very large.
	CHARACTERISTICS OF COMMUNITY CLOUD:
	(a) Cost effective: Since community cloud is shared by several organizations, the community cloud is cost effective too (b) Collaborative & Distributive Maintenance: Since there is sharing of the cloud among various organization, as such the control is distribute and hence better cooperation provides better results.

8.5 Cloud computing service models:



Now explaining each of the services in detail:

INFRASTRUCTURE AS A SERVICE (IaaS)	MEANING OF IaaS:	
	Infrastructure-as-a-Service providers provide an alternative to buy and install the software and the equipment which are needed to support the business operations. The servers and the networks that are required to provide the storage, server functions and networks are provided by this IaaS vendor. Example of IaaS provider includes Amazon, EC2, Dyn DNS, Google chrome engine etc. IaaS provides you the computing infrastructure, physical or (quite often) virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc.	
	CHARACTERISTICS OF IaaS: (M. - W.I.S.E.)	
	M	Management is centralized: Resources distributed across different places to be controlled from any management console that ensure effective resource management
	W	Web access to the resources: IaaS enables the users to access the infrastructure resources over the internet.
	I	Infrastructure Sharing: In IaaS, different users share same physical infrastructure and thus ensure high resource utilization.
	S	Metered Services: IaaS allows the user not to buy the computing resources but to rent them. The user will be charged as per the usage.
	E	Elasticity & dynamic Scaling: IaaS service provider can increase or decrease the usage of the resources depending on the load.
	DIFFERENT INSTANCE OF IaaS:	
	• Network-As-A-Service (NaaS) • Storage as a Service (STaaS) • Database as a Service (DBaaS) • Backend as a Service (BaaS) • Desktop as a Service (DTaaS)	

PLATFORM AS A SERVICE (PaaS)	MEANING OF PaaS:	
	(a) PaaS is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. (b) Platform as a Service allows users to create software applications using tools supplied by the provider. (c) PaaS services can consist of preconfigured features that customers can subscribe to; they can choose to include the features that meet their requirements while discarding those that do not.	
	CHARACTERISTICS OF PaaS:	
	W	Web access to development platform: PaaS provides helps the developer to create, modify, test & deploy different applications.
	S	Scalability: PaaS ensure that applications built are capable of handling the varied loads efficiently.
	C	Collaborative Platform: To enable collaboration among developers, most of PaaS provider provides tools for project planning and communication.
	O	Metered Services: IaaS allows the user not to buy the computing resources but to rent them. The user will be charged as per the usage.
	E	Elasticity & dynamic Scaling: IaaS service provider can increase or decrease the usage of the resources depending on the load.

SOFTWARE AS A SERVICE (SaaS)	MEANING OF SaaS:	
	Software-as-a-Service is cloud service where consumers are able to access software applications over the internet. The programs which are developed by the software developers are accessed by the customers through the browser and pay the fees for their usage. Users don't have to worry about the installation, setup and running of the application. Service provider will do that.	
	CHARACTERISTICS OF SaaS: (W.O. – C.A.M)	
	W	Web access: User can use application from any location of device is connected to internet.
	O	One to many: Single application can be used by multiple users.
	C	Centralized Management: SaaS services are managed from a single location as such there is centralized control.
	A	Availability: SaaS ensures almost 100% availability of data..
	M	Multi-device Support: SaaS can be accessed from any devices e.g. desktop, mobile, laptop etc.

8.6 Challenges to cloud computing: (D. – L.A.S.T. – I.C.A.I. – G.A.A.P)

D	Data Stealing: In cloud computing, data is accessible by everyone and from anywhere. There may be the chances where the cloud provider uses infrastructure of some other service provider. As such, data is less secured and is prone to concept of “data stealing”.
L	Legal Issues And Compliances There are various data, security laws that to be complied with by the entity. There is need to understand various types of rules and laws that imposes security and privacy duties on the organization.

A	Audit: It emphasis on “What is happening in the cloud environment”. It is being hosted on the virtual machine to watch “what is happening in the system”. The context of use of clouds, time consuming audits seriously detains the key gain of cloud agility.
S	Software Isolation: Software isolation is a way to understand virtualization and other techniques that the cloud owner employs in software architecture and evaluate the risks required for the organization.
T	Trust: Deployment model provide a trust to cloud environment. An entity has direct control over its security issue. Trust is an important issue in the cloud. Trust ensures that service arrangements are sufficient to allow visibility into security and privacy controls.
I	Incident Response: It ensures to meet the organization’s requirement during an incident. It ensures that cloud provider has a transparent response process in proper place. Affected network, applications, exposed intrusion helps to understand an incident response.
C	Confidentiality: Prevention of data access from unauthorized disclosure referred to as confidentiality. Cloud works on public network therefore it is imperative to keep the data confidential. This can be done through encryption of data or by way of physically secure at separate location.
A	Architecture: In cloud computing model, there should be control over security and privacy of the system. Its reliable and scalable infrastructure depends on design and implementation to support the overall framework.
I	INTEGRITY: Integrity means prevention of data from unauthorized modification of data and ensures that data is of high quality, correct, accessible and correct. On cloud network it should be ensured that data is not changed. Redundant Array of Independent Risks (RAID) is one of the way to preserve integrity on the cloud computing.
G	Governance: Since on cloud computing there is no control over the employees and services, it creates problems like design, implementation, testing etc. So there is need to put up governance model that will control the standards, policies and procedures of the entity.
A	Application security: It applies when application moves to cloud platform. Service provider should have complete access to server with all rights to ensure protection of the application. Infected application need to be monitored and recovered by the cloud security drivers.
A	Availability: The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. It ensures back up of data through BCP, DRP. Cloud computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the Cloud Computing systems.
P	Privacy: It is one of the important issue in the cloud computing. The privacy issues are embedded in each phase of cloud design. The cloud should be designed in such a way that it decreases the privacy risks.

8.7 Mobile Computing:

A technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution to the biggest problem of business people on the move – mobility.

CODE	Issue in Mobile Computing	CODE	Limitations of Mobile Computing
C	<u>Challenges of Business</u> This is due to lack of trained professionals to bring mobile technology to general people.	B	<u>Bandwidth insufficient:</u> It is slower than direct cable connections
S	<u>Security Issues:</u> Wireless networks have more security requirement then that of wired networks	S	<u>Security standards:</u> When mobile connects, one is dependent on public network
B	<u>Bandwidth:</u> The same can be improved by logging and compression of data before transmission	P	<u>Power consumption:</u> a mobile is dependent on the battery inbuilt in it. expensive batteries are used.
P	<u>Power consumption:</u> In case of mobile, without power a mobile is dependent on the battery inbuilt in it.	H	<u>Health Hazards:</u> Use of phone while driving which is a major cause of accidents.
P	<u>Performance:</u> Since mobile computing involves multiple networks and applications, end-to-end technical compatibility, server capacity and network response time are difficult to achieve.	H	<u>Human interface with the device:</u> input device in mobile such as keyboard is small in size and as such hard to use
L	<u>Integration with Legacy mainframe:</u> IT focuses on mainframes, a huge inventory of applications using communication interface that are basically incompatible with mobile connectivity have been accumulated.	T	<u>Transmission Interface:</u> Any geographical conditions may hinder the good transmission for e.g. hilly areas, tunnel etc.
R	<u>Revising technical architecture:</u> Mobile users are demanding. So in order to provide complete connectivity among the users; the current communication must be revised to incorporate mobile connectivity.		

Components of Mobile Computing

- Mobile Communication:**
Refers to infrastructure put in place to ensure that seamless and reliable communication goes on.
- Mobile Hardware:**
This includes mobile devices/device components that range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA).
- Mobile Software:**
It is the actual program that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications.

8.8 Green Computing:



Green Computing or Green IT refers to the study and practice of environmentally sustainable computing or IT. In other words, it is the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way. Below are the best practices of green computing→

(a) Develop a sustainable green Computing plan

1. Involve stakeholders to include checklist, recycling policies for disposal of used components & equipment.
2. Involve power usage, reduction of consumption of papers, recycling old machines & equipment.
3. Use cloud computing so that multiple organizations share same computing resources.

(b) Recycle:

1. Dispose e-waste as per regulations.
2. Discard unwanted equipment in environmentally responsible manner.
3. Manufacturers must provide option how to dispose equipment when become unusable.

(c) Environment Sound Decisions:

1. Purchase of laptops, desktops based on environmental attributes.
2. Clear policy in respect of designing of the product.

(d) Reduced Paper Consumption:

1. More use of emails resulting in saving of papers.
2. For marketing, advertising on-line marketing is best and will reduce paper wastage.
3. Use both side of paper while printing any document.

8.9 BYOD:

This refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application.

Advantages	Threats
1. Happy employees: Employees use their own devices at work. It lowers the burden since they have to take only their device not the organizational device. 2. Lower IT budget: Since employee bring their own device, this result in decrease in outlay of the organization. (Organizations need not to purchase the devices for their employee). 3. IT reduces support requirement: Since, devices are of employee there is cost saving since IT doesn't have to provide and user support and maintenance activities. 2. Increased employee efficiency: In case of self-device, user is efficient in working on its own device. In case it works on other devices some learning phase is included.	1. Application risks: Employee's phone or smart devices that are connected to corporate network are not protected by security software. 2. Device risks: Lost or stolen computer device or mobile phones can result adverse impact on the company as these devices contains vital information about the company. 3. Implementation risks: A weak BYOD policy may result in failure of communication of employee expectations; thereby increase the chances of device misuse. 4. Network risks: As BYOD involves use of personal devices, IT is unaware of number of devices connected to the company network. For instance, any virus is detected in the network as such it is imperative to scan all connected devices. Since complete visibility is not there, it may be possible that some devices may not get covered under scanning program. This is hazardous for the company.

8.10 Web 2.0 & 3.0:



This refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application.

Web 2.0	Web 3.0
1. Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. 2. The two major contributors of Web 2.0 are the technological advances enabled by Ajax (Asynchronous JavaScript and XML) and other applications and other applications such as RSS (Really Simple Syndication) and Eclipse that support the user interaction and their empowerment in dealing with the web. 3. The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner.	1. Known as the Semantic Web, this describes sites wherein the computers will generate raw data on their own without direct user interaction 2. Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users. 3. Web 3.0 Technology uses the “Data Web” Technology, which features the data records that are publishable and reusable on the web through query-able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence. 4. Two major components of Web 3.0 are as follows: ■ Semantic Web ■ Web Services.

BENEFITS

1. Provide platform where users of the network need not to worry about the implementation or underlying technology at a very affordable cost and a very easy pickup time.
2. Concepts of Web 2.0 like blogging are some things that people do on a day to day basis and no new knowledge skills are required.
3. People are coming much closer to another and all social and geographical boundaries are being reduced at intense speed.
4. Increases the social collaboration to a very high degree and this in turn helps in achieving the goals for a social network

CHALLENGES

1. Provide platform Chances are there where there may be huge chance of data leak and confidentiality loss because there are usually no centrally mandated administrative services to take care of such things.
2. Malicious users somehow manage to perpetrate the social networks resulting in to penetration in privacy of individual users.