Roll No. _____ Section _____

National University of Computer and Emerging Sciences, Lahore Campus

	Course:	**Introduction to Cloud Computing**	**Course Code:**	**CS-499**
	Program:	**BS -Computer Science**	**Semester:**	**Fall 2017**
	Duration:	**60 Minutes**	**Total Marks:**	**40**
	Paper Date:	**18-Sep-17**	**Weight**	**15%**
	Section:	**N/A**	**Page(s):**	**1**
	Exam:	**Mid 1**	**Reg. No.**	

Instruction/Notes: Please answer all the questions on the answer book provided.

1-What are Warehouse Scale Computers? What is the difference between a data center and WSC?

Marks 10

ANS:

Datacenters are buildings where multiple servers and communication gear are co-located

because of their common environmental requirements and physical security needs, and for

ease of maintenance. In that sense, a WSC is a type of datacenter. Traditional datacenters, however,

typically host a large number of relatively small- or medium-sized applications, each running on

a dedicated hardware infrastructure that is de-coupled and protected from other systems in the

same facility. Those datacenters host hardware and software for multiple organizational units or

even different companies. Different computing systems within such a datacenter often have little

in common in terms of hardware, software, or maintenance infrastructure, and tend not to communicate

with each other at all.

WSCs currently power the services offered by companies such as Google, Amazon, Facebook,

and Microsoft's online services division. They differ significantly from traditional datacenters:

they belong to a single organization, use a relatively homogeneous hardware and system software

platform, and share a common systems management layer. Often, much of the application, middleware,

and system software is built in-house compared to the predominance of third-party software

running in conventional datacenters. Most importantly, WSCs run a smaller number of very large

applications (or Internet services), and the common resource management infrastructure allows

significant deployment flexibility. The requirements of homogeneity, single-organization control,

and enhanced focus on cost efficiency motivate designers to take new approaches in constructing

and operating these systems.

2-What are Cloud Characteristics, briefly describe each of them.

Marks 10

ANS: The following six specific characteristics are common to the majority of cloud environments:

• on-demand usage

• ubiquitous access

• multitenancy (and resource pooling)

• elasticity

• measured usage

• resiliency

On-Demand Usage

A cloud consumer can unilaterally access cloud-based IT resources giving the cloud consumer the

freedom to self-provision these IT resources. Once configured, usage of the self-provisioned IT

resources can be automated, requiring no further human involvement by the cloud consumer or cloud

provider. This results in an *on-demand usage* environment. Also known as “on-demand self-service

usage,” this characteristic enables the service-based and usage-driven features found in mainstream

clouds.

Ubiquitous Access

Ubiquitous access represents the ability for a cloud service to be widely accessible. Establishing

ubiquitous access for a cloud service can require support for a range of devices, transport protocols,

interfaces, and security technologies. To enable this level of access generally requires that the cloud

service architecture be tailored to the particular needs of different cloud service consumers.

Multitenancy (and Resource Pooling)

The characteristic of a software program that enables an instance of the program to serve different

consumers (tenants) whereby each is isolated from the other, is referred to as *multitenancy*. A cloud

provider pools its IT resources to serve multiple cloud service consumers by using multitenancy

models that frequently rely on the use of virtualization technologies. Through the use of multitenancy

technology, IT resources can be dynamically assigned and reassigned, according to cloud service

consumer demands.

Elasticity

Elasticity is the automated ability of a cloud to transparently scale IT resources, as required in

response to runtime conditions or as pre-determined by the cloud consumer or cloud provider.

Elasticity is often considered a core justification for the adoption of cloud computing, primarily due

to the fact that it is closely associated with the Reduced Investment and Proportional Costs benefit.

Cloud providers with vast IT resources can offer the greatest range of elasticity.

Measured Usage

The *measured usage* characteristic represents the ability of a cloud platform to keep track of the

usage of its IT resources, primarily by cloud consumers. Based on what is measured, the cloud

provider can charge a cloud consumer only for the IT resources actually used and/or for the

timeframe during which access to the IT resources was granted. In this context, measured usage is

closely related to the on-demand characteristic.

Resiliency

Resilient computing is a form of failover that distributes redundant implementations of IT resources

across physical locations. IT resources can be pre-configured so that if one becomes deficient,

processing is automatically handed over to another redundant implementation. Within cloud

computing, the characteristic of *resiliency* can refer to redundant IT resources within the same cloud

(but in different physical locations) or across multiple clouds. Cloud consumers can increase both the

reliability and availability of their applications by leveraging the resiliency of cloud-based IT

resources

3-How do Web Technologies enable us to provide Cloud Computing. Describe the Web Technologies used to provide cloud computing.

Marks 10

ANS:

Due to cloud computing's fundamental reliance on internetworking, Web browser universality, and

the ease of Web-based service development, Web technology is generally used as both the

implementation medium and the management interface for cloud services.

The World Wide Web is a system of interlinked IT resources that are accessed through the Internet.

The two basic components of the Web are the Web browser client and the Web server. Other

components, such as proxies, caching services, gateways, and load balancers, are used to improve

Web application characteristics such as scalability and security. These additional components reside

in a layered architecture that is positioned between the client and the server.

Three fundamental elements comprise the technology architecture of the Web:

• *Uniform Resource Locator (URL)* – A standard syntax used for creating identifiers that point to

Web-based resources, the URL is often structured using a logical network location.

• *Hypertext Transfer Protocol (HTTP)* – This is the primary communications protocol used to

exchange content and data throughout the World Wide Web. URLs are typically transmitted via

HTTP.

• *Markup Languages (HTML*, *XML)* – Markup languages provide a lightweight means of

expressing Web-centric data and metadata. The two primary markup languages are HTML

(which is used to express the presentation of Web pages) and XML (which allows for the

definition of vocabularies used to associate meaning to Web-based data via metadata).

For example, a Web browser can request to execute an action like read, write, update, or delete on a

Web resource on the Internet, and proceed to identify and locate the Web resource through its URL.

The request is sent using HTTP to the resource host, which is also identified by a URL. The Web

server locates the Web resource and performs the requested operation, which is followed by a

response being sent back to the client. The response may be comprised of content that includes HTML

and XML statements.

Web resources are represented as *hypermedia* as opposed to hypertext, meaning media such as

graphics, audio, video, plain text, and URLs can be referenced collectively in a single document.

Some types of hypermedia resources cannot be rendered without additional software or Web browser

plug-ins.

Roll No. _____ Section _____

4- What is a digital Signature and how is it implemented in the cloud.

Marks 10

ANS: The *digital signature* mechanism is a means of providing data authenticity and integrity through

authentication and non-repudiation. A message is assigned a digital signature prior to transmission,

which is then rendered invalid if the message experiences any subsequent, unauthorized

modifications. A digital signature provides evidence that the message received is the same as the one

created by its rightful sender.

Both hashing and asymmetrical encryption are involved in the creation of a digital signature, which

essentially exists as a message digest that was encrypted by a private key and appended to the

original message. The recipient verifies the signature validity and uses the corresponding public key

to decrypt the digital signature, which produces the message digest. The hashing mechanism can also

be applied to the original message to produce this message digest. Identical results from the two

different processes indicate that the message maintained its integrity.