

Emerging Technologies

Basic Concepts

1. Cloud Computing: Cloud computing simply means the use of computing resources as a service through networks, typically the Internet. 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.

With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software. Cloud computing is of benefit to small and medium-sized business systems, who wish to completely outsource their data-center infrastructure; or large companies, who wish to get peak load capacity without incurring the higher cost of building larger data centers internally. In both the instances, service consumers use *'what they need on the Internet'* and *pay only for 'what they use'*.

2. Cloud v/s Grid Computing: Some pertinent similarities and differences are:

- Cloud Computing and Grid Computing both are scalable.
- Both computing types involve multi-tenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances.
- While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
- A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

3. Goals of Cloud Computing: The core goal of utilizing a cloud-based IT ecosystem is to pool available resources together into a highly efficient infrastructure whose costs are aligned with what resources are actually used to make the services accessible and available from anywhere at any time.

4. Cloud Computing Architecture: The Cloud Computing Architecture (CCA) of a cloud solution is the structure of the system, which comprises of on-premise and cloud resources,

services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them. Cloud architecture typically involves multiple cloud components communicating with each other over a loose coupling mechanism, such as a messaging queue. This is depicted in Fig. 8.1, which is given as follows:

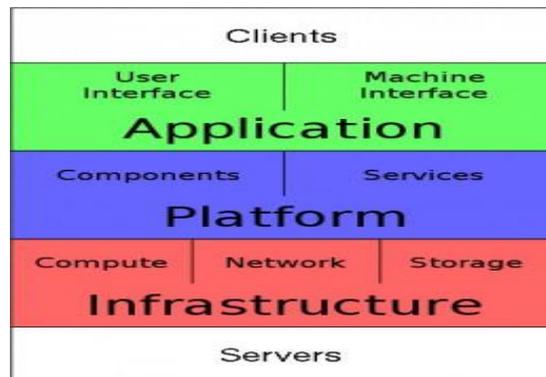


Fig. 8.1: Cloud Computing Architecture

5. Cloud Computing Environment/Deployment Models: The cloud computing environment can consist of multiple types of clouds based on their deployment and usage. These are:

- (a) **Public Clouds:** This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called provider clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.
- (b) **Private Clouds:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization. Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud).
- (c) **Hybrid Clouds:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

(d) **Community Clouds:** The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations.

6. Cloud Computing Service Models: These are as follows:

(a) **Infrastructure as a Service (IaaS):** IaaS providers offer computers, more often virtual machines and other resources as service. It provides the infrastructure / storage required to host the services ourselves i.e. makes us the system administrator and manage hardware/storage, network and computing resources. The different instances of IaaS are as follows:

- **Network as a Service (NaaS):** It is a category of cloud services where the capability provided to the cloud service user is to use network/transport connecting services. NaaS involves optimization of resource allocation by considering network and computing resources as a whole.
 - **Storage as a Service (STaaS):** STaaS, an instance of IaaS, provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term.
 - **Database as a Service (DBaaS):** This is also related to IaaS and provides users with seamless mechanisms to create, store, and access databases at a host site on demand.
 - **Backend as a Service (BaaS):** It is a type of IaaS, that provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.
 - **Desktop as a Service (DTaaS):** It is an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure.
- **Platform as a Service (PaaS):** PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider. Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server. **For** example- Google AppEngine, Windows Azure Compute etc.

(c) **Software as a Service (SaaS):** SaaS provides users to access large variety of applications over internet that are hosted on service provider's infrastructure. Thus, the end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure. SaaS changes the way the software is delivered to the customers.

- **Testing as a Service (TaaS):** This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.
- **API as a Service (APIaaS):** This allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.
- **Email as a Service (EaaS):** This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

(e) **Other Cloud Service Models:**

- **Communication as a Service (CaaS):** CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vendor. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates large capital investments.
- **Data as a Service (DaaS):** DaaS provides data on demand to a diverse set of users, systems or application. The data may include text, images, sounds, and videos. Data encryption and operating system authentication are commonly provided for security.
- **Security as a Service (SECaaS):** It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats.
- **Identity as a Service (IDaaS):** It is an ability given to the end users; typically an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed and provided by the third party service provider.

7. Characteristics of Cloud Computing: Major characteristics are: High Scalability, Agility, High Availability and Reliability, Multi-sharing, Services in Pay-Per-Use Mode, Virtualization, Performance, and Maintenance.

8. Advantages of Cloud Computing: Major advantages of Cloud Computing are: Cost Efficiency, Almost Unlimited Storage, Backup and Recovery, Automatic Software Integration, Easy Access to Information, and Quick Deployment.

9. Challenges to Cloud Computing: Major challenges are: Confidentiality, Integrity, Availability, Governance, Trust, Legal Issues and Compliance, Privacy, Audit, Data-Stealing, Architecture, Identity Management and Access control, Incident Response, Software Isolation and Application Security.

10. Mobile Computing: It refers to the 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 for the biggest problem of business people on the move i.e. mobility.

Various companies design and develop several wireless applications and solutions for Blackberry, iPhone, Google Android G1, iPad, Windows Mobile, Symbian, Brew devices, PDA, Palm & Pocket PC. Mobile Computing Services allow mobile workforces to access a full range of corporate services and information from anywhere, at any time and it improves the productivity of a mobile workforce by connecting them to corporate information systems and by automating paper-based processes.

11. BYOD: BYOD (Bring Your Own Device) 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.

12. Emerging BYOD Threats: Overall, these can be classified into four areas as outlined below:

- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network.
- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information.
- **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software.

- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy.

13. Social Media: A social network is usually created by a group of individuals, who have a set of common interests and objectives. There are usually a set of network formulators followed by a broadcast to achieve the network membership. This happens both in public and private groups depending upon the confidentiality of the network.

14. Web 2.0: 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. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users.

Components of Web 2.0 for Social Networks: Major components that have been considered in Web 2.0 include the following: Communities, **RSS-generated Syndication**, Blogging, Wikis, **Usage of Ajax and other new technologies**, Folksonomy, File Sharing/Podcasting, and Mash-ups.

15. Web 3.0: 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. 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.

An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence.

16. Green IT: Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way. Green computing is the environmentally responsible use of computers and related resources.

It is largely taken as the study and practice of designing, manufacturing, using, and disposing of computers, servers, associated subsystems and peripheral devices efficiently and effectively with highly mitigated negative impact on the environment. The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.

Question 1

What is Cloud Computing? Explain some pertinent similarities and differences between Cloud and Grid computing.

8.7 Information Systems Control and Audit

Answer

Cloud Computing: Cloud computing simply means the use of computing resources as a service through networks, typically the Internet. With Cloud Computing, users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. The best example of cloud computing is *Google Apps* where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.

Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service. With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software.

Some pertinent similarities and differences between cloud and grid computing are highlighted as follows:

- Cloud computing and grid computing both are scalable. Scalability is accomplished through load balancing of application instances running separately on a variety of operating systems and connected through Web services. CPU and network bandwidth is allocated and de-allocated on demand. The system's storage capacity goes up and down depending on the number of users, instances, and the amount of data transferred at a given time.
- Both computing types involve multi-tenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances. Sharing resources among a large pool of users assists in reducing infrastructure costs and peak load capacity. Cloud and grid computing provide Service-Level Agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. If the service slides below the level of the guaranteed uptime service, the consumer will get service credit for not receiving data within stipulated time.
- While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
- A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

Question 2

Discuss the major goals of Cloud Computing in brief.

Answer

Major goals of cloud computing are as follows:

- To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;
- To access services and data from anywhere at any time;
- To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- To consolidate IT infrastructure into a more integrated and manageable environment;
- To reduce costs related to IT energy/power consumption;
- To enable or improve “Anywhere Access (AA)” for ever increasing users; and
- To enable rapid provision of resources as needed.

Question 3

Describe Front End and Back End architecture with reference to Cloud Computing.

Answer

A Cloud computing architecture consists of two parts - a Front End and a Back End that connect to each other through a network, usually the Internet. A central server is established to be used for administering the whole system.

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. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.

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. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.

Question 4

What do you understand by Public cloud? Also discuss its major advantages and limitations in brief.

Answer

Public Clouds: This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administered by third parties or vendors over the Internet, and the services are offered on pay-per-use basis.

8.9 Information Systems Control and Audit

These are also called provider clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.

The Advantages of public cloud include the following:

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- There is no need for establishing infrastructure for setting up and maintaining the cloud.
- Strict SLAs are followed.
- There is no limit for the number of users.
- Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen. Further, privacy and organizational autonomy are not possible.

Question 5

What is Private cloud? Also explain its major advantages and limitations in brief.

Answer

Private Clouds: This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

The advantages of private clouds include the following:

- They improve average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies; thus, reducing the costs that a greater number of servers would otherwise entail.
- It provides a high level of security and privacy to the user.
- It is small and controlled and maintained by the organization.

Moreover, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently. Budget is a constraint in private clouds and they also have loose SLAs.

However, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently.

Question 6

Explain the characteristics of the following regarding cloud computing:

- (i) *Infrastructure as a Service (IaaS)*
- (ii) *Platform as a Service (PaaS)*
- (iii) *Software as a Service (SaaS)*

Answer

- (i) Characteristics of Infrastructure as a Service (IaaS) are as follows:
 - **Web access to the resources:** The IaaS model enables the IT users to access infrastructure resources over the Internet. When accessing a huge computing power, the IT user need not get physical access to the servers.
 - **Centralized management:** The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.
 - **Elasticity and Dynamic Scaling:** Depending on the load, IaaS services can provide the resources and elastic services where the usage of resources can be increased or decreased according to the requirements.
 - **Shared infrastructure:** IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensure high resource utilization.
 - **Metered Services:** IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.
- (ii) Characteristics of Platform as a Service (PaaS) are as follows:
 - **All in One:** Most of the PaaS providers offer services like programming languages to develop, databases, test, deploy, host and maintain applications in the same Integrated Development Environment (IDE).
 - **Web access to the development platform:** PaaS provides web access to the development platform that helps the developers to create, modify, test, and deploy different applications on the same platform.
 - **Offline Access:** To enable offline development, some of the PaaS providers allow the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.

8.11 Information Systems Control and Audit

- **Built-in Scalability:** PaaS services provide built-in scalability to an application that is developed using any particular PaaS. This ensures that the application is capable of handling varying loads efficiently.
- **Collaborative Platform:** To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.
- **Diverse Client Tools:** PaaS providers offer a wide variety of client tools like Web UI, API etc. to help the developers to choose the tool of their choice.

(iii) Characteristics of Software as a Service (SaaS) are as follows:

- **One to Many:** SaaS services are delivered as one-to-many models where a single instance of the application can be shared by multiple customers.
- **Web Access:** SaaS services allow the end users to access the application from any location of the device is connected to the Internet.
- **Centralized Management:** Since SaaS services are hosted and managed from the central location, the SaaS providers perform the automatic updates to ensure that each customer is accessing the most recent version of the application without any user-side updates.
- **Multi-device Support:** SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smartphones, and thin clients.
- **Better Scalability:** Most of the SaaS services leverage PaaS and IaaS for its development and deployment and ensure a better scalability than traditional software.
- **High Availability:** SaaS services ensure 99.99% availability of user data as proper backup and recovery mechanisms are implemented.
- **API Integration:** SaaS services have the capability of integrating with other software or service through standard APIs.

Question 7

Explain, in brief, the characteristics of Cloud Computing.

Answer

Major characteristics of cloud computing are given as follows:

- **High Scalability:** Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
- **Agility:** The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).

- **High Availability and Reliability:** Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
- **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
- **Services in Pay-Per-Use Mode:** SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.
- **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- **Performance:** It is monitored and consistent and its loosely coupled architecture constructed using web services as the system interface enables high level of performance.
- **Maintenance:** The cloud computing applications are easier, because they are not to be installed on each user's computer and can be accessed from different places.

Question 8

Briefly discuss the advantages of Cloud Computing.

Answer

Major advantages of Cloud Computing are given as follows:

- **Cost Efficiency:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot in terms of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned. The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
- **Almost Unlimited Storage:** Storing information in the cloud gives us almost unlimited storage capacity. Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.
- **Backup and Recovery:** Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle

8.13 Information Systems Control and Audit

recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

- **Automatic Software Integration:** In the cloud, software integration is usually something that occurs automatically. This means that we do not need to take additional efforts to customize and integrate the applications as per our preferences. This aspect usually takes care of itself. Not only that, cloud computing allows us to customize the options with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her particular enterprise.
- **Easy Access to Information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.
- **Quick Deployment:** Lastly and most importantly, cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes. Of course, the amount of time taken here will depend on the exact kind of technology that we need for our business.

Question 9

Discuss any four challenges to Cloud computing in brief.

Answer

Four challenges to cloud computing are given as follows:

- **Confidentiality:** Prevention of unauthorized disclosure of data is referred to as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control).
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be ensured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.

- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete. Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability. One of the major Cloud service provider, AWS had a breakdown for several hours, which led to data loss and access issues with multiple Web 2.0 services.
- **Architecture:** In the architecture of Cloud computing models, there should be control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework.

Question 10

Explain some of the tangible benefits of mobile computing.

Answer

Major tangible benefits of mobile computing are given as follows:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.
- It enables us to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

Question 11

Write short notes on the following:

- (i) *Hybrid Cloud*
- (ii) *Mobile Computing*
- (iii) **BYOD and its advantages**
- (iv) *Web 2.0*
- (v) *Green IT*

(vi) *Major components of Web 3.0*

Answer

- (i) **Hybrid Cloud:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.
- (ii) **Mobile Computing:** It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. 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 of the biggest problem of business people on the move i.e. mobility.
- (iii) **BYOD:** BYOD (Bring Your Own Device) 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. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, challenging the long-standing policy of working on company-owned devices. Though it has led to an increase in employees' satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

Advantages of Bring Your Own Device (BYOD) are as follows:

- **Happy Employees:** *Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as organization provided devices.*
- **Lower IT budgets:** *The employees could involve financial savings to the organization since employees would be using the devices they already*

possess, thus reducing the outlay of the organization in providing devices to them.

- ***IT reduces support requirement: IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.***
- ***Early adoption of new Technologies: Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.***
- ***Increased employee efficiency: The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.***

(iv) **Web 2.0:** Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability of people to collaborate and share information online. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information. Over the time, Web 2.0 has been used more as a marketing term than a Computer Science based term. Blogs, wikis, and Web services are all seen as components of Web 2.0. Web 2.0 tries to tap the power of humans connected electronically through its new ways at looking at social collaboration. The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner. In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mash-ups, and Tagging. The power of Web 2.0 is the creation of new relationships between collaborators and information.

(v) **Green IT:** Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient, environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle. It is largely taken as the study and practice of designing, manufacturing, using, and disposing of computers, servers, associated subsystems and peripheral devices efficiently and effectively with highly mitigated negative impact on the environment. The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.

8.17 Information Systems Control and Audit

(vi) The two major components of Web 3.0 are as follows:

- (i) **Semantic Web:** This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines can take contextual decisions on their own by finding, combining and acting upon relevant information on the web.
- (ii) **Web Services:** It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr to search for images.
To conclude, Web 3.0 helps to achieve a more connected open and intelligent web applications using the concepts of natural language processing machine learning, machine reasoning and autonomous agents.

Question 12

'The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment'. Discuss some of such steps, which can be followed for Green IT.

Or

Discuss best practices of Green IT.

Answer

Some of such steps for Green IT include the following:

Develop a sustainable Green computing plan

- Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;
- Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
- On-going communication about and campus commitment to green IT best practices to produce notable results.
- Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans; and
- Use cloud computing so that multiple organizations share the same computing resources thus increasing the utilization by making more efficient use of hardware resources.

Recycle

- Dispose e-waste per central, state and local regulations;
- Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;
- Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and
- Recycle computers through manufacturer's recycling services.

Make environmentally sound purchase decisions

- Purchase of desktop computers, notebooks and monitors based on environmental attributes;
- Provide a clear, consistent set of performance criteria for the design of products;
- Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and
- Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

Reduce Paper Consumption

- Reduce paper consumption by use of e-mail and electronic archiving;
- Use of "track changes" feature in electronic documents, rather than redline corrections on paper;
- Use online marketing rather than paper based marketing; e-mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste; and
- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

Conserve Energy

- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;
- Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;

8.19 Information Systems Control and Audit

- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;
- Power-up and power-down energy-intensive peripherals such as laser printers according to need;
- Employ alternative energy sources for computing workstations, servers, networks and data centers; and
- Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

Question 13

Discuss some of the pertinent objectives to achieve the goals of Cloud Computing.

Answer

Some of the pertinent objectives to achieve the goals of Cloud Computing are as follows:

- To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are used;
- To access services and data from anywhere at any time;
- To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- To consolidate IT infrastructure into a more integrated and manageable environment;
- To reduce costs related to IT energy/power consumption;
- To enable or improve "Anywhere Access" (AA) for ever increasing users; and
- To enable rapidly provision resources as needed.

Question 14

Discuss the Security and Implementation issues in using Cloud Computing technology for running the new web application.

Answer

Major challenges in Cloud Computing Technology for running new Web application are as follows:

(A) Security Issues: Security is a major issue relating to cloud computing. Some of the major security issues are discussed below:

- **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. With the use of encryption and physical isolation, data can be kept secret.
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible.
- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure and natural calamities are all threats to availability.
- **Governance:** Due to the lack of control over the employees and services, there is problem relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization.
- **Trust:** Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.
- **Legal Issues and Compliance:** There are various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements.
- **Privacy:** The privacy issues are embedded in each phase of the Cloud design that includes both the legal compliance and trusting maturity.
- **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'.
- **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. Some of the Cloud providers use server/s from other service providers and thus there is a probability that the data is less secure and is more prone to the loss from external server.
- **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The reliability and scalability of architecture is dependent on the design and implementation to support the overall framework.

8.21 Information Systems Control and Audit

- **Identity Management and Access control:** A robust federated identity management architecture and strategy internal in the organization provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.
- **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
- **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture and evaluate the risks required for the organization.
- **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have the complete access to the server with all rights for monitoring and maintenance of server.

(B) Implementation/Adaptation Issues: Some of the well-identified implementation issues are as follows:

- **Threshold Policy:** This involves the checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de-allocated and turned over to other work needs to work out in the context.
- **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary Application Programming Interfaces (APIs) and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors.
- **Hidden Costs:** Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another instance of incurring network costs, companies, who are far from the location of cloud providers, could experience latency, particularly when there is heavy traffic.
- **Unexpected Behavior:** Let's suppose that credit card validation application works well at our company's internal data centre. It is important to test the application in the cloud with a pilot study to check for unexpected behavior. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If

the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud.

Instead of waiting for an outage to occur, consumers should do security testing on their own checking how well a vendor can recover data. Apart from the common testing practices, what one needs primarily to do is to ask for old stored data and check how long it takes for the vendor to recover. If it takes too long to recover, ask the vendor why and how much service credit we would get in different scenarios. Moreover, in such cases, verifying the checksums match with the original data is a requisite. Another area of security testing is to test a trusted algorithm to encrypt the data on the local computer, and then try to access data on a remote server in the cloud using the decryption keys. If we can't read the data once we have accessed it, the decryption keys are corrupted, or the vendor is using its own encryption algorithm. We may need to address the algorithm with the vendor. Another issue is the potential for problems with data in the cloud. To protect the data, one may want to manage his/her own private keys. Checking with the vendor on the private key management is no longer a simple as it appears so.

- **Software Development in Cloud:** To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud. The cost associated with each cloud type may differ from one another. The cost per hour or usage with the development cloud is most likely lower than the production cloud, as additional features, such as SLA and security, are allocated to the production cloud. The managers can limit projects to certain clouds. For instance, services from portions of the production cloud can be used for the production configuration. Services from the development cloud can be used for development purpose only. To optimize assets at varying stages of the project of software development, the managers can get cost-accounting data by tracking usage by project and user.
- **Environment Friendly Cloud Computing:** One incentive for cloud computing is that it may be more environment friendly. First, reducing the number of hardware components needed to run applications on the company's internal data centre and replacing them with cloud computing systems reduces energy for running and cooling hardware. By consolidating these systems in remote centers, they can be handled more efficiently as a group.

Question 15

List major advantages and limitations of Hybrid Cloud, in brief.

8.23 Information Systems Control and Audit

Answer

The Advantages of Hybrid Cloud include the following:

- It is highly scalable and gives the power of both private and public clouds.
- It provides better security than the public cloud.

The limitation of Hybrid Cloud is that the security features are not as good as the public cloud and complex to manage.

Question 16

What is Community Cloud? Discuss its advantages and limitations in brief.

Answer

Community Cloud: The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations.

Advantages of Community Clouds are as follows:

- It allows establishing a low-cost private cloud.
- It allows collaborative work on the cloud.
- It allows sharing of responsibilities among the organizations.
- It has better security than the public cloud.

The limitation of the community cloud is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the cases where there is no collaboration.

Question 17

Discuss the components of Mobile Computing.

Answer

The key components of Mobile Computing are as follows:

- **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.
- **Mobile Hardware:** This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers,

Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS or a wireless gateway embedded in wireless carrier's network. The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.

- **Mobile Software:** Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

Question 18

Discuss security issues of Mobile Computing.

Answer

Security Issues: Wireless networks have relatively more security requirements than wired network. Several approaches have been suggested and also the use of encryption has been proposed.

- **Confidentiality:** Preventing unauthorized users from gaining access to critical information of any user.
- **Integrity:** Ensures unauthorized modification, destruction or creation of information cannot take place.
- **Availability:** Ensuring authorized users getting the access they require.
- **Legitimate:** Ensuring that only authorized users have access to services.
- **Accountability:** Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked when necessary.

Question 19

Describe the major components of Web 2.0 for social networks.

Answer

Major components that have been considered in Web 2.0 include the following:

- **Communities:** These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are several tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.
- **Blogging:** Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.

8.25 Information Systems Control and Audit

- **Wikis:** A Wiki is a set of co-related pages on a subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.
- **Folksonomy:** Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.
- **File Sharing/Podcasting:** This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.
- **Mashups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps to find the exact information of a cell phone device from the internet, just by entering the cell number.

Question 20

Write a short note on the services provided by the SaaS model of Cloud Computing.

Answer

The services provided by Software as a Service Model of Cloud Computing are:

- **Business Services:** *SaaS providers provide a variety of business services to startup companies that include ERP, CRM, billing, sales, and human resources.*
- **Social Networks:** *Since the number of users of the social networking sites is increasing exponentially, cloud computing is the perfect match for handling the variable load.*
- **Document Management:** *Most of the SaaS providers provide services to create, manage, and track electronic documents as most of the enterprises extensively use electronic documents.*
- **Mail Services:** *To handle the unpredictable number of users and the load on e-mail services, most of the email providers offer their services as SaaS services.*

Exercise

1. *Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are two of the three main categories of cloud computing. What's the third category? Explain in brief.*
2. *Explain components of Web 3.0 for Social Networks.*
3. *Discuss limitations of Mobile Computing.*
4. *Discuss pertinent issues of Mobile Computing.*
5. *Discuss advantages of Bring your own Device (BYOD).*