Unit-5 Basics of Internet & Cloud Computing

LAN

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building. Early LAN (Local Area Network) networks were formed using coaxial cable, coax is an electric cable and it is used to carry radio signals. LAN (Local Area Network) setup is developed by connecting two or more than two computers with each other using a physical connection in order to share files and data overtime.

LAN Advantages:

- Workstations can share peripheral devices like printers. This is cheaper than buying a printer for every workstation.
- Workstations do not necessarily need their own hard disk or CD-ROM drives which make them cheaper to buy than stand-alone PCs.

Disadvantages of LAN or Local Area Network

- High Setup Cost. Although the LAN will save cost over time due to shared computer resources but the initial setup costs of installing Local Area Networks is high.
- Privacy Violations.
- Data Security Threat.
- LAN Maintenance Job.
- Covers Limited Area.

MAN

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). A metropolitan area network features a WAN that's built around a city or a section of a city. It connects all of the networks in the city into a single larger network. This network connects employees across the various agencies with shared resources. There are many advantages of the MAN network, some of them given below. Less expensive: It is less expensive to attach MAN with WAN. MAN gives you good efficiency of data.

Advantages of a metropolitan area network (MAN)

- Less expensive: It is less expensive to attach MAN with WAN.
- Sending local emails.
- High speed than WAN.
- Sharing of the internet.
- Conversion from LAN to MAN is easy.
- High Security.

Disadvantages of MAN

- **Difficult to manage:** If MAN becomes bigger then it becomes difficult to manage it. This is due to a security problem and other extra configuration.
- **Internet speed difference:** MAN cannot work on traditional phone copper wires. If MAN is installed on copper wires then there will be very low speed. So it required the high cost to set up fiber optics for the first time.
- **Hackers attack:** In MAN there are high chances of attacking hackers on the network compared to LAN. So data may be leaked. Data can be secured but it needs high trained staff and security tools.
- **Technical people required to set up:** To setup MAN it requires technical people that can correctly setup MAN. The technical people are network administrators and troubleshooters.
- **More wires required:** In MAN additional cables are required to connect two LAN which is another problem.

WAN

A wide area network (WAN) is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs). A LAN is a group of computers and network devices which are all connected to each other, typically from within a short relative geographical distance. In an enterprise or business, a WAN may consist of connections to a company's headquarters, branch offices, colocation facilities, cloud services and other facilities. Typically, a router or other multifunction device is used to connect a LAN to a WAN. Enterprise WANs allow users to share access to applications, services and other centrally located resources. This eliminates the need to install the same application server, firewall or other resources in multiple locations.

WAN connections can include wired and wireless technologies. Wired WAN services can consist of multiprotocol label switching, T1s, Carrier Ethernet and commercial broadband internet links. Wireless WAN technologies can include cellular data networks like 4G LTE, as well as public Wi-Fi or satellite networks.

Advantages of WAN include:

- Can cover a large geographical area
- Centralized infrastructure
- Security
- Increased bandwidth with the use of leased lines as opposed to broadband connections.

Disadvantages of WAN include:

- High set up cost
- Possibility for security gaps
- Needs antivirus software and firewalls

INTRODUCTION TO INTRNET

The Internet (portmanteau of interconnected network) is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. In general the Full Form of INTERNET is **International Network**. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

VPN

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, though not an inherent, part of a VPN connection.

VPN technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunnelling protocol and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN. In other applications, Internet users may secure their connections with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. However, some websites block access to known VPN technology to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these roadblocks.

Wi-Fi

Wi-Fi is a family of radio technologies commonly used for wireless local area networking (WLAN) of devices. It is based on the IEEE 802.11 family of standards. The false notion that the brand name "Wi-Fi" is short for "wireless fidelity" has spread to such an extent that even industry leaders have included the phrase wireless fidelity in a press release.

Wi-Fi uses multiple parts of the IEEE 802 protocol family and is designed to seamlessly interwork with its wired sibling Ethernet. Devices that can use Wi-Fi technologies include desktops and laptops, smartphones and tablets, smart TVs, printers, digital audio players, digital cameras, cars and drones. Compatible devices can connect to each other over Wi-Fi through a wireless access point as well as to connected Ethernet devices and may use it to access the Internet. Such an access

point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using overlapping access points.

Bluetooth

Bluetooth is a wireless technology standard for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in the industrial, scientific and medical radio bands, from 2.400 to 2.485 GHz, and building personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables.

A Bluetooth device works by using radio waves instead of wires or cables to connect with your cell phone, smartphone or computer. Bluetooth is a wireless short-range communications technology standard found in millions of products we use every day – including headsets, smartphones, laptops and portable speakers. Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 35,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks. A manufacturer must meet Bluetooth SIG standards to market it as a Bluetooth device. A network of patents applies to the technology, which are licensed to individual qualifying devices.

Switch

A network switch (also called switching hub, bridging hub, officially MAC Bridge) is networking hardware that connects devices on a computer network by using packet switching to receive, and forward data to the destination device.

A network switch is a multiport network bridge that uses media access control addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Switches for Ethernet are the most common form of network switch. The first Ethernet switch was introduced by Kalpana in 1990. Switches also exist for other types of networks including Fibre Channel, Asynchronous Transfer Mode, and Infini Band.

Internet Connectivity

Getting your computer connected to the Internet can happen in a variety of ways; taking the time to understand the benefits or drawbacks of each method will help you determine which is best for you. While there are exceptions, in general you can expect that most methods will require a subscription with an Internet service provider — or an ISP.

Dial-up modem: Connecting to the Internet with a dial-up modem is one of the oldest and simplest methods. It is used primarily in homes and by small businesses. It is the least expensive method, but with the low price comes very limited performance (in other words, it is slow). Dial-up connections require a modem (built right in to most new computers) and a phone line. The modems allow data to be transferred at a rate of 56 KB per second, which is very slow by today's standards. Many people dedicate a separate phone line for their modem so they don't have to share it with telephone calls. Any modem slower than 56 KB per second would be best upgraded to a faster one, as the cost is relatively low and the Internet access speed will increase significantly.

Digital subscriber line (DSL): A digital subscriber line (or DSL) connection is a widely used method of accessing the Internet for homes and small businesses; it provides faster download of files without the wait associated with dial-up. DSL runs over a telephone line, with the line split into three channels: voice (you can receive phone calls without disconnecting from the Internet), a faster download channel, and a moderately fast upload channel. The quality and speed of the DSL connection depends mainly on the quality of the phone line and the distance from your phone company's central office (the farther you are from the office, the slower the connection).

A DSL connection offers "always on" convenience, so there's no need to connect and disconnect every time you access the Internet. And DSL speeds are 25 to 100 times faster than 56K dial-up modems. One advantage DSL has over cable modems (see below) is consistent performance (or speed) because the connection is not shared with other users. A disadvantage is that you are vulnerable to hacking; however, investing in a personal firewall package can mitigate this risk. The cost is moderately more expensive than dial-up, but with greatly increased performance and convenience. Free equipment and installation deals are common.

Leased Line: A leased line is a service contract between a provider and a customer, whereby the provider agrees to deliver a symmetric telecommunications line connecting two or more locations in exchange for a monthly rent (hence the term lease). It is sometimes known as a "Private Circuit" or "Data Line" in the UK. Unlike traditional PSTN (public switched telephone network) lines it does not have a telephone number, each side of the line being permanently connected to the other. Leased lines can be used for telephone, data or Internet services. Some are ringdown services, and some connect two PBXes (private branch exchange).

Typically, leased lines are used by businesses to connect geographically distant offices. Unlike dial-up connections, a leased line is always active. The fee for the connection is a fixed monthly rate. The primary factors affecting the monthly fee are distance between end points and the speed of the circuit. Because the connection does not carry anybody else's communications, the carrier can assure a given level of quality.

An internet leased line is a premium internet connectivity product, delivered over fiber normally, which is dedicated and provides uncontended, symmetrical speeds, Full Duplex. It is also known as an Ethernet leased line, DIA line, data circuit or private circuit.

For example, a T-1 channel can be leased, and provides a maximum transmission speed of 1.544 Mbit/s. The user can divide the connection into different lines for multiplexing data and voice communication, or use the channel for one high speed data circuit. Increasingly, leased lines are being used by companies, and even individuals, for Internet access because they afford faster data transfer rates and are cost-effective for heavy users of the Internet.

MODEM: A modem (modulator-demodulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from light emitting diodes to radio. The most familiar example is a voice band modem that turns the digital data of a personal computer into modulated electrical signals in the voice frequency range of a telephone channel. These signals can be transmitted over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Modems are generally classified by the amount of data they can send in a given unit of time, usually expressed in bits per second (bit/s, or bps). Modems can alternatively be classified by their symbol rate, measured in baud. The baud unit denotes symbols per second, or the number of times per second the modem sends a new signal. For example, the ITU V.21 standard used audio frequency-shift keying, that is to say, tones of different frequencies, with two possible frequencies corresponding to two distinct symbols (or one bit per symbol), to carry 300 bits per second using 300 baud. By contrast, the original ITU V.22 standard, which was able to transmit and receive four distinct symbols (two bits per symbol), handled 1,200 bit/s by sending 600 symbols per second (600 baud) using phase shift keying.

Wi-Fi Router: A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.

E-mail

Electronic mail, commonly known as email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Some early email systems required that the author and the recipient both be online at the same time, in common with instant. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to an email server, for as long as it takes to send or receive messages.

An email message consists of three components, the message *envelope*, the message *header*, and the message *body*. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.

Originally a text-only (7-bit ASCII and others) communications medium, email was extended to carry multi-media content attachments, a process standardized in RFC2045 through 2049. Collectively, these RFCs have come to be called Multipurpose Internet Mail Extensions (MIME).

Advantages of Email:

1. It's free: Once you're online, there is no further expense.

2. Easy to reference: Sent and received messages and attachments can be stored safely, logically and reliably. It's a lot easier to organize emails than paper.

3. Easy to use: Once you're set up, sending and receiving messages is simple. That goes for a host of other email functions. Data storage and contacts can be accessed quickly and easily.

4. Easy to prioritize: Incoming messages have subject lines that mean you can delete without opening. How much time does that save compared to 'snail mail?'

5. Speed: Message to send? Done, under a second! Email is as fast a form of written communication as any.

6. Global: Web based email means you can access your messages anywhere online. Going overseas? Before you go, mail yourself a copy of your passport number, travel insurance details or your accommodation details.

7. Good for the planet: Actually the advantages and disadvantages of email are clear here. Computers themselves aren't 'green', but email offsets some of the damage by reducing the environmental cost of contact.

8. Info at your fingertips: Storing data online means less large, space taking file cabinets, folders and shelves. You can access information far quicker if you learn how to use email this way.

9. Leverage: Send the same message to any number of people. Adaptations are simple, too. If you have a product or service to sell, email is an effective medium to get your message out.

10. Send reminders to yourself: Do you use more than one account? Email yourself messages from work to home or vice versa. Does the idea of two or more accounts seem complicated? It's not if you know how to manage multiple accounts.

Disadvantages of Email:

1. Emotional responses: Some emails cause upset or anger. A reply in the heat of the moment can't be easily retracted, but it can cause lasting damage.

2. Information overload: Too many people send too much information. They cover their backs citing 'need to know' as the justification. Learn how to use email effectively and you'll reduce time wasted on this.

3. Lacking the Personal Touch: Some things are best left un-typed. Email will never beat a hand written card or letter when it comes to relationships.

4. Misunderstandings: Emails from people who don't take the time to read what they write before clicking 'send'. Time is wasted, either to clarify or, worse, acting on a misinterpretation of the message.

5. No Respite: Your email inbox is like a garden; it needs to be constantly maintained. Leave it and will continue to grow. Ignore it at your peril!

6. Pressure to Reply: Once it's in your inbox, you feel an ever increasing obligation to act on it. Procrastinating doesn't making it go away. Do it, dump it or delegate it.

7. Spam: Having to deal with spam and spoofs is one of the worst avoidable time wasters online. Use some anti-spam software.

8. Sucks up Your Time: Over checking messages are so common, but it is time wasted on a low value, passive activity. Better to check once or twice a day.

9. Too Long: How long is too long? It's hard to say exactly, but the longer it goes on, the harder it is to take in. Email is suited to brevity - keep it short and sweet.

10. Viruses: A virus could seriously affect your computer. If you want to know how to use email effectively, it's worth learning how to deal with these.

Voice Mail

A voicemail system (also known as voice message or voice bank) is a computer-based system that allows users and subscribers to exchange personal voice messages; to select and deliver voice information; and to process transactions relating to individuals, organizations, products, and services, using an ordinary telephone. The term is also used more broadly to denote any system of conveying a stored telecommunications voice messages, including using an answering machine. Most cell phone services offer voicemail as a basic feature; many corporate private branch exchanges include versatile internal voice-messaging services, and *98 vertical service code subscription is available to most individual and small business landline subscribers.

Newsgroup

A newsgroup is an online discussion forum accessible through Usenet. Each newsgroup contains discussions about a specific topic, indicated in the newsgroup name. You can browse newsgroups and post or reply to topics using a newsreader program. Access to newsgroups also requires a Usenet subscription. Most Usenet providers offer monthly access for around $10 USD per month.

Newsgroups may be either moderated or unmoderated. In a moderated newsgroup, a moderator must approve posts in order for them to become part of the discussion. In an unmoderated group, everything posted is included in the discussion. Some newsgroups may also use bots to moderate the content, automatically eliminating posts that are deemed offensive or off topic.

While many people now use web forums and online chat instead of newsgroups, the service is still popular around the world. In fact, there are estimated to be over 100,000 newsgroups in existence. While many newsgroups host traditional text-based discussions, a large number of newsgroups are now used for file sharing. These newsgroups, which primarily provide links to files, often have the term "binaries" in their name.

Chat (Text & Voice)

Online chat may refer to any kind of communication over the Internet, that offers an real-time direct transmission of text-based messages from sender to receiver, hence the delay for visual access to the sent message shall not hamper the flow of communications in any of the directions. Online chat may address point-to-point communications as well as multicast communications from one sender to many receivers and voice and video chat or may be a feature of a Web conferencing service.

Voice chat is a modern form of communication used on the Internet. The means of communicating with voice chat is through any of the messengers, mainly Skype, Yahoo! Messenger, AOL Instant Messenger, or Windows Live Messenger.[*citation needed*] Voice chat has led to a significant increase in distant communications where two or more people from opposite ends of the world can talk almost free of cost.

Video Conferencing

Videoconferencing is the conduct of a videoconference (also known as a video conference or video teleconference) by a set of telecommunication technologies which allow two or more locations to communicate by simultaneous two-way video and audio transmissions. It has also been called 'visual collaboration' and is a type of groupware.

Videoconferencing differs from videophone calls in that it's designed to serve a conference or multiple locations rather than individuals.[1] It is an intermediate form of video telephony, first deployed commercially in the United Arabs by AT&T during the early 1970s as part of their development of phone technology.

With the introduction of relatively low cost, high capacity broadband telecommunication services in the late 1990s, coupled with powerful computing processors and video compression techniques, videoconferencing usage has made significant inroads in business, education, medicine and media.

FTP

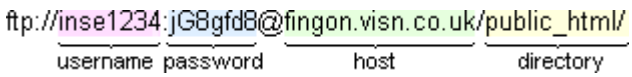
File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. It is often used to upload web pages and other documents from a private development machine to a public web-hosting server. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that hides (encrypts) your username and password, as well as encrypts the content, you can try using a client that uses SSH File Transfer Protocol.

The first FTP client applications were interactive command-line tools, implementing standard commands and syntax. Graphical user interfaces have since been developed for many of the popular desktop operating systems in use today,[2][3] including general web design programs like Microsoft Expression Web, and specialist FTP clients such as Cute FTP.

What is FTP? FTP stands for File Transfer Protocol and it's generally used as a means of uploading files to web sites. There are many different FTP clients (programs) on the market and it's very much up to personal preference which one you choose.

Using Windows Explorer to upload your website

The easiest way to get your site uploaded without paying extra money for an FTP client is to use Microsoft Windows Explorer. You would typically enter a URL in the format of ftp://Username:Password@Host/directory/ into the address bar. It's then possible to drag and drop any files you want to upload into this window. For example:-



WWW

The World Wide Web (abbreviated as WWW or W3, and commonly known as the Web) is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks.

Using concepts from his earlier hypertext systems like ENQUIRE, British engineer and computer scientist Sir Tim Berners-Lee, now Director of the World Wide Web Consortium (W3C), wrote a proposal in March 1989 for what would eventually become the World Wide Web. At CERN, a European research organization near Geneva situated on Swiss and French soil, Berners-Lee and Belgian computer scientist Robert Cailliau proposed in 1990 to use hypertext "... to link and access information of various kinds as a web of nodes in which the user can browse at will", and they publicly introduced the project in December.

Browser

A web browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An *information resource* is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video, or other piece of content. Hyperlinks present in resources enable users easily to navigate their browsers to related resources. A web browser can also be defined as an application software or program designed to enable users to access, retrieve and view documents and other resources on the Internet.

Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems. The major web browsers are Firefox, Google Chrome, Internet Explorer, Opera, and Safari.

URL

A Uniform Resource Locator (URL), colloquially termed a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL is a specific type of Uniform Resource Identifier (URI), although many people use the two terms interchangeably. URLs occur most commonly to reference web pages (http), but are also used for file transfer (ftp), email (mailto), database access (JDBC), and many other applications.

Most web browsers display the URL of a web page above the page in an address bar. A typical URL could have the form http://www.example.com/index.html, which indicates a protocol (http), a hostname (www.example.com), and a file name (index.html).

Web Site

A website or web site is a collection of related network web resources, such as web pages, multimedia content, which are typically identified with a common domain name, and published on at least one web server. Notable examples are wikipedia.org, google.com, and amazon.com.

Websites can be accessed via a public Internet Protocol (IP) network, such as the Internet, or a private local area network (LAN), by a uniform resource locator (URL) that identifies the site.

Websites can have many functions and can be used in various fashions; a website can be a personal website, a corporate website for a company, a government website, an organization website, etc. Websites are typically dedicated to a particular topic or purpose, ranging from entertainment and social networking to providing news and education. All publicly accessible websites collectively constitute the World Wide Web, while private websites, such as a company's website for its employees are typically part of an intranet.

Search Engines

A web search engine is designed to search for information on the World Wide Web. The search results are generally presented in a list of results often referred to as search engine results pages (SERPs). The information may consist of web pages, images, information and other types of files. Some search engines also mine data available in databases or open directories. Unlike web directories, which are maintained only by human editors, search engines also maintain real-time information by running an algorithm on a web crawler.

HTTP

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems.[1] HTTP is the foundation of data communication for the World Wide Web. Hypertext is a multi-linear set of objects, building a network by using logical links (the so called hyperlinks) between the nodes (e.g. text or words). HTTP is the protocol to exchange or transfer hypertext.

The standards development of HTTP was coordinated by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), culminating in the publication of a series of Requests for Comments (RFCs), most notably RFC 2616 (June 1999), which defines HTTP/1.1, the version of HTTP in common use.

Computer VIRUS

A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

One of the ideal methods by which viruses spread is through emails – opening the attachment in the email, visiting an infected website, clicking on an executable file, or viewing an infected advertisement can cause the virus to spread to your system. Besides that, infections also spread while connecting with already infected removable storage devices, such as USB drives.

A computer virus operates in two ways. The first kind, as soon as it lands on a new computer, begins to replicate. The second type plays dead until the trigger kick starts the malicious code. In other words, the infected program needs to run to be executed. Therefore, it is highly significant to stay shielded by installing a robust antivirus program.

Types of Computer Viruses

A computer virus is one type of malware that inserts its virus code to multiply itself by altering the programs and applications. The computer gets infected through the replication of malicious code. Computer viruses come in different forms to infect the system in different ways. Some of the most common viruses are:

1. **Boot Sector Virus –** This type of virus infects the master boot record and it is challenging and a complex task to remove this virus and often requires the system to be formatted. Mostly it spreads through removable media.
2. **Direct Action Virus –** This is also called non-resident virus, it gets installed or stays hidden in the computer memory. It stays attached to the specific type of files that it infect. It does not affect the user experience and system's performance.
3. **Resident Virus –** Unlike direct action viruses, resident viruses get installed on the computer. It is difficult to identify the virus and it is even difficult to remove a resident virus.
4. **Multipartite Virus –** This type of virus spreads through multiple ways. It infects both the boot sector and executable files at the same time.
5. **Polymorphic Virus –** These types of viruses are difficult to identify with a traditional anti-virus program. This is because the polymorphic viruses alter its signature pattern whenever it replicates.
6. **Overwrite Virus –** This type of virus deletes all the files that it infects. The only possible mechanism to remove is to delete the infected files and the end-user has to lose all the contents in it. Identifying the overwrite virus is difficult as it spreads through emails.

7. **Spacefiller Virus –** This is also called “Cavity Viruses”. This is called so as they fill up the empty spaces between the codes and hence does not cause any damage to the file.

Antivirus:

Antivirus software, or anti-virus software (abbreviated to AV software), also known as anti-malware, is a computer program used to prevent, detect, and remove malware.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect users from: malicious browser helper objects (BHOs), adware and spyware.

Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

Cloud Computing

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server.

Clouds may be limited to a single organization (enterprise clouds), or be available to many organizations (public cloud).

Cloud computing relies on sharing of resources to achieve coherence and economies of scale.

Advocates of public and hybrid clouds note that cloud computing allow companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand. Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.

Types of cloud deployments

There are three types of cloud deployments categorized based on an organization’s ability to manage and secure assets as well as business needs.

Public cloud:

Public cloud, in general, is Software as a Service (SaaS) services offered to users over the internet. It is the most economical option for users in which the service provider bears the expenses of bandwidth and infrastructure. It has limited configurations, and the cost is determined by usage capacity. That said, the limitations of the public cloud are its lack of SLA specifications. Despite high reliability, lower costs, zero maintenance and on-demand scalability, the public cloud is not suitable for organizations operating with sensitive information as they have to comply with stringent security regulations.

Private cloud:

As the name suggests, the private cloud is used by large organizations to build and manage their own data centres for specific business and IT needs/ operations. The private cloud provides more control over customizability, scalability and flexibility, while improving security of assets and business operations. This sort of infrastructure can be built on premises or outsourced to a third party service provider – either way, it has the ability to maintain the hardware and software environment over a private network solely for the owner. Large- and medium-scale financial enterprises and government agencies typically opt for private clouds.

Hybrid cloud:

Hybrid cloud is the combination of a private and public cloud, providing for more flexibility to businesses while having control over critical operations and assets, coupled with improved flexibility and cost efficiency. The hybrid cloud architecture enables companies to take advantage of the public cloud as and when necessary due to their easy workload migration. For instance, businesses can use the public cloud for running high-volume applications like emails, and utilize private clouds for sensitive assets like financials, data recovery, and during scheduled maintenance and rise in demand.

Advantages:

1. **Easy implementation:** Cloud hosting allows business to retain the same applications and business processes without having to deal with the backend technicalities. Readily manageable by the Internet, a cloud infrastructure can be accessed by enterprises easily and quickly.
2. **Accessibility:** Access your data anywhere, anytime. An Internet cloud infrastructure maximizes enterprise productivity and efficiency by ensuring your application is always accessible. This allows for easy collaboration and sharing among users in multiple locations.
3. **No hardware required:** Since everything will be hosted in the cloud, a physical storage center is no longer needed. However, a backup could be worth looking into in the event of a disaster that could leave your company's productivity stagnant.
4. **Cost per head:** Overhead technology costs are kept at a minimum with cloud hosting services, enabling businesses to use the extra time and resources for improving the company infrastructure.
5. **Flexibility for growth:** The cloud is easily scalable so companies can add or subtract resources based on their needs. As companies grow, their system will grow with them.
6. **Efficient recovery:** Cloud computing delivers faster and more accurate retrievals of applications and data. With less downtime, it is the most efficient recovery plan.

Disadvantages:

1. **No longer in control:** When moving services to the cloud, you are handing over your data and information. For companies who have an in-house IT staff, they will be unable to handle issues on their own. However, Stratosphere Networks has a 24/7 live help desk that can rectify any problems immediately.
2. **May not get all the features:** Not all cloud services are the same. Some cloud providers tend to offer limited versions and enable the most popular features only, so you may not receive every feature or customization you want. Before signing up, make sure you know what your cloud service provider offers.
3. **Doesn't mean you should do away with servers:** You may have fewer servers to handle which means less for your IT staff to handle, but that doesn't mean you can let go of all your servers and staff. While it may seem costly to have data centers and a cloud infrastructure, redundancy is key for backup and recovery.
4. **No Redundancy:** A cloud server is not redundant nor is it backed up. As technology may fail here and there, avoid getting burned by purchasing a redundancy plan. Although it is an extra cost, in most cases it will be well worth it.
5. **Bandwidth issues:** For ideal performance, clients have to plan accordingly and not pack large amounts of servers and storage devices into a small set of data centers.

क्लाउड कम्प्यूटिंग (Cloud Computing) या **मेघ संगणना** वास्तव में इंटरनेट-आधारित प्रक्रिया और कंप्यूटर ऐप्लीकेशन का इस्तेमाल है। गूगल एप्स क्लाउड कंप्यूटिंग का एक उदाहरण है जो बिजनेस ऐप्लीकेशन ऑनलाइन मुहैया कराता है और वेब ब्राउजर का इस्तेमाल कर इस तक पहुंचा जा सकता है।

इंटरनेट पर सर्वरों में जानकारियाँ (अनुप्रयोग, वेब पेजेस, प्रोग्राम इत्यादि सभी) सदा सर्वदा के लिए भंडारित रहती हैं और ये उपयोक्ता के डेस्कटॉप, नोटबुक, गेमिंग कंसोल इत्यादि पर आवश्यकतानुसार अस्थाई रूप से संग्रहित रहती हैं। इसे थोड़ा विस्तारित और सरल रूप में कहें तो सीधी सी बात है कि अब तक जो सॉफ्टवेयर प्रोग्राम आप स्थानीय रूप से अपने कम्प्यूटर और लैपटॉप-नोटबुक पर संस्थापित करते रहे थे, अब इनकी कतई आवश्यकता नहीं होगी क्योंकि ये सब सॉफ्टवेयर अब आपको वेब सेवाओं के जरिए मिला करेंगी। वेब होस्टिंग के क्षेत्र में भी क्लाउड का उपयोग कर नवीनतम प्रकार की वेब होस्टिंग सेवा क्लाउड होस्टिंग प्रस्तुत की गई है। यही नहीं, गूगल गियर जैसे अनुक्रमों के जरिए आपको इस तरह की बहुत सारी सुविधाएं ऑफ़लाइन भी मिला करेंगीं।

क्लाउड कंप्यूटिंग कंप्यूटिंग की एक शैली है जिसमें गतिक रूप से परिमाप्य और अक्सर आभासी संसाधनों को इंटरनेट पर एक सेवा के रूप में उपलब्ध कराया जाता है।

उपयोगकर्ताओं को उनकी मदद करने वाले "क्लाउड" के तकनीकी ढांचे के ज्ञान, उसमें विशेषज्ञता या उस पर नियंत्रण की कोई आवश्यकता नहीं होती है।