TOPIC : DATA COMMUNICATION& NETWORKING

DATA COMMUNICATION

This refers to the electronic transfer of data, instructions, and information from one device to another via a transmission media.

ELEMENTS FOR DATA COMMUNICATION

Sender: The computer or device that generates and sends data is called the sender, source or transmitter. It can be a computer, workstation (node), telephone handset, video camera. Etc
Message: This is the information or data to be communicated. It consists of text, numbers, pictures, sound or video.
Transmission Medium: is the physical pathway by which a message travels from sender to receiver.
Receiver: The device or computer that receives the message is called receiver. The receiver can be a computer, printer, a fax machine, etc.
Protocol: This is a set of rules that allow devices to exchange information
A protocol defines the format for communication between systems. For example the Hyper Text Transfer Protocol (HTTP) defines the format for communication between Web browsers and Web servers on the internet
Other examples of communication protocols include: Internet Protocol (IP) Transmission Control Protocol (TCP), Trivial File Transfer Protocol (TFTP), Wireless Application Protocol (WAP), and Simple Mail Transfer Protocol (SMTP) for emails

Data communication tools

Data communication tools are devices that enable the users to send and receive messages. Etc. Data communication tools can be categorized into two: electronic and manual data communication tools.
Electronic data communication tools use electric power. Examples include Computers, Mobile phones and internet.
Manual data communication tools don't use electricity. Examples include drums, bells and messengers.

d) Types of electronic data communication tools

As technology progresses, new communications are born and old fade away. When you're trying to connect with employees, colleagues, bosses,

clients, customers or suppliers electronic media are critical to getting business done efficiently and cost- effectively.

Examples of data communications tools include

Computers, **Fax machines, Radio and Television, Mobile Devices like** phones and PDAs, internet services (Email, Websites, Social networking, chartrooms Forums, etc)

Data transmission media

The term transmission media refers to any physical or non-physical link / pathway between two or more devices and in which a signal can be made to flow from source to destination. A data signal cannot be sent from one place to another without a medium of communication.

Data communication media can be divided into two:

1. Physical /Wired / Bounded/ Guided transmission media
2. Wireless / Unbounded / Unguided transmission media

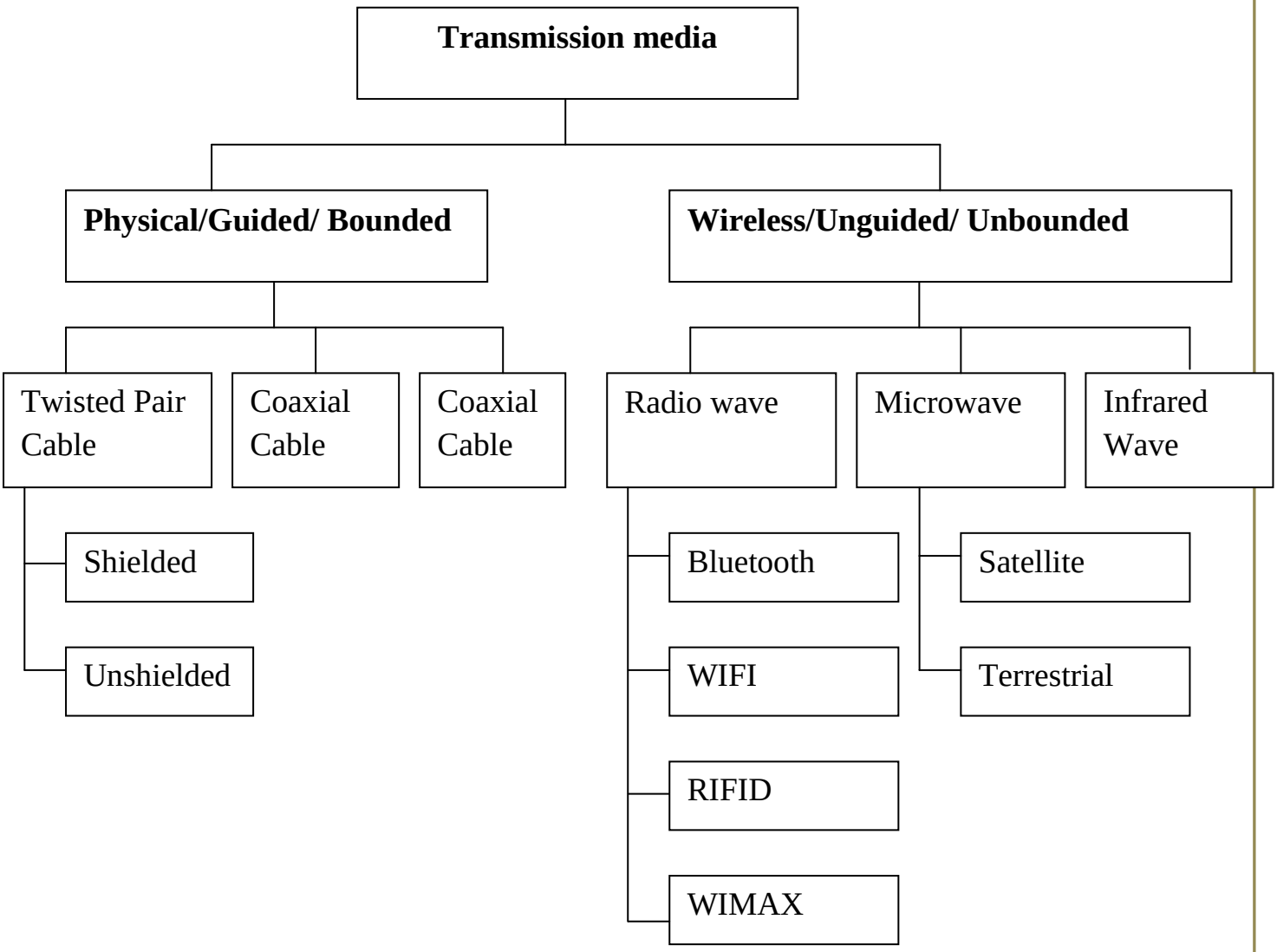
Physical /Wired / Bounded/ Guided transmission media

Physical transmission media use wire, cable, and other physical materials to send communications signals. Physical media transmits data signals from the source to the destination through a restricted pathway such as a cable.

Examples of physical transmission media

- Unshielded Twisted Pair **(UTP)** Cable
- Shielded Twisted Pair **(STP)** Cable
- Coaxial Cable
- Fiber Optic Cable

AN ILLUSTRATION DATA TRANSMISSION MEDIA



Twisted pair cable: Twisted pair cable is made up of solid copper wire strands wound in pairs within a single media. The winding of the wires is meant to avoid the development of an electromagnetic field around the two wires as they transmit data. TP is commonly used to interconnect devices on a Local Area Network

There are two common types of twisted pair cabling, STP and UTP. The S stands for Shielded, the U stands for Unshielded.
The extra covering in shielded twisted pair wiring protects the transmission line from electromagnetic interference leaking into or out of the cable, but makes it more expensive.

Coaxial cables
The Coaxial cable has a single copper conductor at its center. A plastic layer

provides insulation between the center conductor and a braided metal shield . The metal shield helps to block any outside magnetic interference from fluorescent lights, motors, and other
Coaxial cables have bandwidths in Gigabits per second. Hence, they are installed in a network to form the network backbone.

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Fiber Optic Cable
The fiber optic cable consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference.
This makes it ideal for certain environments that contain a large amount of electrical interference.
It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fibre optic cable utilizes light to transmit data from one point to another on the network. The electrical signal from the source are converted to light signals, and then propagated along the fiber optic cable.

Advantages of physical transmission media

- It is fast and supports high bandwidth
- Can be used in hazardous places (high flammable) because they do not generate electrical signal
- They can carry voice, data and video signal simultaneously.
- They are more resistant to radio and electromagnetic interference.
- Installation equipment are cheap and readily available.

Disadvantages of physical transmission media

- Connectivity devices and media are expensive.
- Installation is difficult because the cable must be carefully handled.
- It is relatively complex to configure

- It covers short distance since they use the physical wires
- Inconvenience due to inflexibility of restrictive cables.

Wireless / Unbounded / Unguided transmission media

Wireless or unbounded media is that is where data signals flow through the **air** In this case transmitting antenna and receivers aerial facilitates the communication
Example of wireless transmission media include:

The major wireless transmission media include radio waves, microwaves, and infrared which is part of the **electromagnetic spectrum**, which is the range of all possible frequencies of electromagnetic radiation.
Wireless media send communications signals through the air or space using radio, microwave, and infrared signals (electromagnetic waves).

Examples of wireless transmission media

- Microwaves
- Radio waves
- Infrared

MICROWAVES: Microwaves are high-frequency electromagnetic radiations that are sent through space to deliver telecommunications services. Microwaves are dependent on line of sight. Microwave communication systems are mainly classified into satellite and terrestrial.

Terrestrial microwave signals are sent from one ground-based antenna to another.
Satellite microwave signals travel from Earth to a satellite in space and then back to a station on the earth.

RADIO WAVES: Radio waves frequencies are easy to generate and are widely used for communication, both indoors and outdoors. Examples of communication technologies using radio waves include Bluetooth, Wireless Fidelity (Wifi)

Bluetooth is a short range wireless based information transmission system which works on the basis of microchips embedded in the digital devices like mobile phones, speakers and laptops.

Wireless Fidelity (WiFi) is used to create a hotspots from where information signals can be easily accessed by Wi-Fi enabled devices, forming a wireless

local area network **(**WLAN).

HOTSPOT
A hotspot is a specific location that provides Internet access via a wireless local area network (WLAN). The term is generally synonymous with a Wi-Fi connection. A network that creates a hotspot primarily includes a modem and wireless router. The radio frequency (RF) waves sent by the wireless network extend in different directions from its centralized location. These signals become weaker as they travel, either further from the central location or due to interference.

Wimax stands for Worldwide Interoperability for Microwave Access. It is a telecommunication technology providing wireless data over long distances in a variety of ways from point to point links to full mobile cellular type access.

Radio-frequency identification (*RFID*) uses radio waves to automatically identify and track tags attached to objects. The RFID tag can be affixed to an object and used to track and manage inventory, assets, people, etc. For example, it can be affixed to cars, computer equipment, books etc.

INFRARED uses electromagnetic waves with a **smaller wavelength** than **radio**.
A **TV remote control** is an example of an Infrared application.
IrDA (Infrared Data Association) ports transmit data via infrared light waves. As long as the devices are within a few feet and nothing obstructs the path of the infrared light wave, data can be transferred without the use of cables

Asynchronous and Synchronous transmissions

With **asynchronous transmission**, transmission occurs at irregular intervals in small bits (i.e., not synchronized).
Asynchronous transmission is relatively slow.
With synchronous transmission, large blocks of bytes are transmitted at regular intervals without any start/stop signals.
Synchronous transmission requires that both the sending and receiving devices be synchronized before any bytes are transmitted.
Synchronous transmission requires more expensive equipment but provides greater speed and accuracy than asynchronous transmission.
Characteristics of Asynchronous Transfer Mode

- It is scalable and flexible. It can support megabit-to-gigabit transfer speeds and is not tied to a specific physical medium.
- It efficiently transmits video, audio, and data through the implementation of several adaptation layers.

- Bandwidth can be allocated as needed, lessening the impact on and by high-bandwidth users.
- It transmits data in fixed-length packets, called cells, each of which is 53 bytes long, containing 48 bytes of payload and 5 bytes of header.
- It is asynchronous in the sense that although cells are relayed synchronously, particular users need not send data at regular intervals.
- It is connection oriented, using a virtual circuit to transmit cells that share the same source and destination over the same route.

Transmission Direction

The direction in which data flows along transmission media is characterized as simple, half-duplex, full-duplex or multiplex

Simplex transmission

Simplex transmission sends data in one direction only. Simplex transmission is used only when the sending device does not require a response from the receiving device. Examples of simplex transmission is television broadcasting and radio broad casting

Half-duplex transmission

Half-duplex transmission allows data transmission in either direction, but only one way at a time. Many fax machines, police radio calls, credit card verification systems and automatic teller machines use half-duplex transmission

Full-duplex transmission

In full-duplex transmission, data can flow in both directions at the same time. A regular telephone line, for example, supports full-duplex transmission, allowing both parties to talk at same time.

Multiplex transmission

In multiplex transmission, several different types of signals can be carried at once through the same line. E.g. During Video calls where Images

PACKET SWITCHING

When a computer sends data over the Internet, the data is divided into small pieces called packets. Each packet contains the data, as well as the recipient (destination), the origin (sender), and the sequence information used to reassemble the data at the destination.
Each packet travels along the fastest individual available path to the recipient's computer via communications devices called routers.
This technique of breaking a message into individual packets, sending the packets along the best route available, and then reassembling the data is called packet switching.

Services offered by data communication tools

Data communication tools offer services like Telephone, SMS, E-mail, Skype, Newsgroups and instant messaging.

Telephone voice calls help keep people talking even when they are distant and mobile.
Short Messaging Services SMS facilitate sending and receiving of brief text messages.
Electronic mail and fax : An electronic mail is the message transmitted electronically over the internet, from one user to another. A fax machine is a device that transmits and receives typed or hand written documents over telephone lines.
Skype supports voice and video calls, text, instant messaging and sharing conversation with (someone) over the Internet using the software application Skype, frequently also viewing by webcam.
Newsgroups are organized group of internet users who wish to share ideas and interests through discussion forums and debates.
Instant messaging: This is a more enhanced messaging service that allows two or more people to chat directly in real time.
Social networking e.g. Facebook and Twitter create digital societies through linking people of common interests.

Implications of using data communication services

Positive Implications

- Have led to faster, simpler communications between people e.g.through electronic-mail, mobile phones, social networks etc
- Communications costs have become lower e.g. Making cheap internet calls, for example via Google talk and Skype
- Community mobilization now easier - its now very simple to send a message to many people in one go e.g using Mailing lists and group chats.
- Data communication tools like the internet have facilitated emergence of

the worldwide-web where there is a wealth of information, such as news, weather reports, and airline schedules.

- Data communication tools like telephones and SMS Have revolutionized the way people transact businesses e.g access to mobile money services using phones.

Negative Implications

- ***Security and privacy***: data communication services have made it easy access private information e.g. on social networks, hence posing security concern.
- Spamming is high especially by advertisers who send unwanted e-mails in bulk, such as email adverts.
- There has been emergency of new kinds of crimes facilitated by data communication services, such as cyber-bullying.
- Inaccurate information on the internet can be misleading and lead to dire consequences to the users.
- Data communication services have facilitated the digital divide in society, hence disadvantaging the computer illiterate people when it comes to opportunities like jobs and government services

INTRODUCTION TO COMPUTER NETWORKS

Definition of a computer Network

A computer network is defined as a collection of computers linked together using transmission media for the purpose of communication and resource sharing.

Some of the shared resources include internet connectivity, printers, fax machines, modems, storage devices, networked software programs etc.

Basic requirements for setting up a computer network

NETWORKING HARDWARE includes all computers, peripherals and Communications devices that enable two or more computers to exchange items such as data, instructions, and information with each other.

Examples include: a network interface card, modem, Hub/Switch, Router, repeater, network Bridge, Firewall etc.

A network interface card (NIC), is a device that enables the computer or device that does not have built-in networking capability to access a network. Examples include adapter card, PC Card, USB network adapter, flash card e.t.c

A modem is a device which Modulates a digital signal from computers into an analog one to send data out over the phone line. Then for an incoming signal it Demodulates, the analog signal into a digital one.

A **hub**, (also called a multi-station access unit (MAU)) is a device that provides a central point for cables in a network. Unlike the hubs, a **switch** does not broadcast the data to all the computers, it sends the data packets only to the destined computer.

A **Router** connects multiple networks and routs communications traffic to the appropriate network using the fastest available path. A router allows multiple computers to share a single high-speed Internet connection such as through a cable modem

A **repeater** is a device that accepts a signal from a transmission medium, amplifies it, and retransmits it over the medium. As a signal travels over a long distance, it undergoes a reduction in strength, an occurrence called **attenuation**.

A **network bridge** is device that connects two networks making each accessible to the other. A bridge knows all of the addresses on each side of the bridge and sends information accordingly

A **firewall** is a networking device that is installed at the entrance to a LAN, particularly when connecting a private network to a public network, such as the internet. The firewall uses rules to filter inbound traffic into the private network, to protect the private network users and data from malevolent hackers. Unauthorized traffic is rejected, and authorized traffic passes as illustrated below.

A multiplexer is a device that combines two or more input signals from various devices into a single stream of data and then transmits it over a single transmission medium. By combining the separate data streams into one, a multiplexer increases the efficiency of communications and reduces the need for using multiple separate transmission media.

Networking / communications software

This consists of programs and applications that aid the setup and use of a network. It includes network operating.

A network operating system (NOS) is the system software that organizes and coordinates the activities on a network.

NOS software consists of programs that help users establish a connection to another computer or network, such as network drivers, and manage the transmission of data, instructions, and information.

Examples of NOSs include: Novell NetWare, Microsoft Windows server

2008, 2012, 2016, Sun Solaris, etc.

Network application software: These are programs that provide an interface for users to communicate over computer networks. A variety of examples of application software for communications include:

- E-mail client applications,
- FTP programs,
- Web browsers like Internet Explorer,
- Newsgroup/ message boards
- Chat apps,
- Instant messaging,
- Video conferencing applications e.g. Skype, and VoIP.

TYPES OF NETWORKS

Personal Area Network

A personal area network (PAN) is the interconnection of computer devices within the range of an individual person, typically within a range of 10 meters.

Local Area Network

A local area network (LAN) is a network that connects computers in a small geographic area such as a building like a computer laboratory, or an office. The nodes are connected to the LAN via cables. A wireless LAN (WLAN) is a LAN that does not use physical wires, but uses wireless media such as radio waves

Types of Local Area Networks

- Peer-to-peer Network.
- Client-Server Network

1. **Peer-to Peer Network**

This is a type of network where each computer can share the hardware, data, or information located on any other computer on the network. Each computer stores files on its own storage devices. Each computer on the network contains both the network operating system and application software.

Advantages of Peer-to Peer Network

- A peer-to-peer network is simple to setup i.e. does not require too much configuring
- It is not expensive to set up
- It does not require a dedicated server to control the network

- It is perfect for home and small business users.

Disadvantages of a Peer to Peer Network

- The system is not centralized, making administration difficult .
- Lack of security i.e. files can be accessed by any one on the network.

2. Client-Server Network

A client/server network has one or more computers acting as a server while the other computers (i.e., clients) on the network can request services from the server.

A client computer is a computer that can access the resources on a network.
While
A server is a computer that provides a centralized storage area for programs, data, and information.
A dedicated server is a server that performs a specific task. Examples of dedicated Servers include: file server, print server, database server, and a network server

Roles of Dedicated Servers

- A file server stores and manages files on a network
- A print server manages printers and print jobs.
- A database server stores and provides access to a database
- A network server (e.g., a DNS) manages network traffic.

Requirements of a server computer

- It needs a computer with very high processing speed
- It needs large amounts of RAM
- It needs a very big storage capacity
- It needs a very fast Network interface card
- It needs network operating system such as Novell Netware, Windows NT Server or Apple Share

Advantages of Client-Server Network

- All Resources are centralized and easier to access.
- Easy management and administration of the network.
- More data security since all network access is controlled through the server.
- The network is flexible, because changes and new technology can be easily included into system.

- Client /Server network is faster than P2P since data and resources are handled by a dedicated machine
- It is to Backup all data stored centrally on the server.
- Client Server network can support many computers as compared to a P2P network

Disadvantages of a Client /Server Network

- It is expensive to set up as compared to a P2P network.
- It requires an extra computer to serve as a dedicated server.
- Maintenance – large networks will require an administrator staff to ensure efficient operation
- Dependence – When the server goes down, operations will cease across the network
- Server can get overloaded since all the processing is controlled at one point.

A Campus Area Network (CAN) is a network that connects two or more LANs but is limited to a specific and contiguous geographical area such as a college campus, industrial complex, or a military base. It spans multiple LANs but smaller than a MAN

A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus. A MAN usually interconnects two or more LANs using a high-capacity backbone technology, such as fiber-optical links or other digital media. A MAN covers a smaller geographic area than a WAN.

A wide Area Network (WAN) is a network that covers a large geographic area. An example of a WAN is a network that connects the district office computers of a company across the country or across several counties in the world. Computers are often connected to a WAN via public networks such as the telephone system or by dedicated lines or satellites.

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 across the VPN may therefore benefit from the functionality, security, and management of the private network.

VPNs may allow employees to securely access a corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network.

Advantages of wireless networks:

Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc.

Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -in some cases, you will connect automatically to networks within range.

Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.

Expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. If you are also moving large amounts of data around a private network, a cabled connection will enable that work to proceed much faster.

Disadvantages of wireless networks:

Security - Be careful. Be vigilant. Protect your sensitive data with backups, isolate private networks, provide strong encryption and passwords, and monitor network access traffic to and from your wireless network.

Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.

Inconsistent connections - Wireless connections are not nearly as stable as those through a dedicated cable.

Network Protocol

This refers to a set of rules and procedures governing transmission between components in a computer network.

The role played by networking protocols as used in Networking

- Identifying each device in the communication path;
- Securing the attention of the other device;
- Verifying correct receipt of the transmitted message;

- Determining that a message requires retransmission if it is incomplete or has errors;
- Performing recovery when errors occur.

Common protocols as used as in networking

Simple Mail Transfer Protocol (SMTP) - an internet protocol for transferring of e-mails.
File Transfer Protocol (FTP): It allows files containing text, programs, graphics, numerical data, and so on to be downloaded off or uploaded onto a network.
Internet Protocol (IP) - does the packet forwarding and routing.
Transmission Control Protocol/Internet Protocol (TCP/IP) is a network standard that defines how messages (data) are routed from one end of a network to the other, ensuring the data arrives correctly.
Transmission Control Protocol (TCP) :responsible for delivery of data over the network.
Hypertext Transfer Protocol (HTTP): It allows Web browsers and servers to send and receive Web pages.
Simple Network Management Protocol (SNMP): It allows the management of networked nodes to be managed from a single point.

Telnet Protocol: It provides terminal emulation that allows a personal computer or workstation to act as a terminal, or access device, for a server.
Sequential Packet Exchange (IPX/SPX):works with the Novell's internet work' packet / sequential exchange; responsible for delivery of sequential data over the network

INTRANET, EXTRANET & INTERNET
Intranet refers to a connection of private computer networks within an organization**.**
Intranet refers to a connection of private computer networks within an organization.
An intranet has tools to facilitate communication between organization's employees or workgroups to improve the knowledge and data sharing capability.
Many schools and non-profit groups have deployed intranets. A simple intranet consists of an internal email system.
More complicated intranets include Web sites and databases containing company news, forms, and personnel information.

Advantages of Installing an Intranet

Sharing resources such as laser printers, fax machines, modems, scanners, etc. is simplified

Electronic Mail: Electronic mail on a LAN can enable students to communicate with teachers and peers at their own school.

Flexible Access: School networks allow students to access their files from computers throughout the school. Students can also work cooperatively through the network.

Disadvantages of Installing a School Network

- Expensive to Install. Although a network will generally save money over time, the initial costs of installation can be prohibitive.
- Requires Administrative Time. Proper maintenance of a network requires considerable time and expertise.
- Must Monitor Security Issues. Wireless networks are becoming increasingly common; however, security can be an issue with wireless networks

Extranet is a computer network that allows controlled access from the outside for specific business or educational purposes. Extranets are extensions to, or segments of, private intranet networks that have been built in many corporations for information sharing.

An extranet is a computer network that allows controlled access from the outside for specific business or educational purposes.

Extranets are extensions to, or segments of, private intranet networks that have been built in many corporations for information sharing.

Most extranets use the internet as the entry point for outsiders, a firewall configuration to limit access and a secure protocol for authenticating users

Advantages of extranet

- Exchange large volumes of data using Electronic Data Interchange (EDI)
- Share product catalogs exclusively with trade partners
- Collaborate with other companies on joint development efforts
- Jointly develop and use training programs with other companies
- Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks.
- Share news of common interest exclusively

Disadvantages of extranet

- Extranets can be expensive to implement and maintain within an organization (e.g., hardware, software, employee training costs)
- Security of extranets can be a concern when hosting valuable or proprietary information.

The internet is a global connection of computer networks. The internet links together millions of computers, to exchange and share information all over the world.

Benefits of installing an intranet in a school

- Facilitates internal emails
- Provides access to company contacts information, procedure manual and other frequently updated documents
- Used for posting and updating employee forms
- Posting internal job listings
- Provides electronic catalogs for ordering supplies
- Facilitates collaborative computing
- Scheduling meeting and appointments.
- Posting financial statements and other types of corporate information
- Maintains shared calendars, projects timelines and other project documents
- Provides access to company databases and other systems
- For monitoring internal security.

TOPIC: THE INTERNET AND THE WORLD WIDE WEB

THE INTERNET

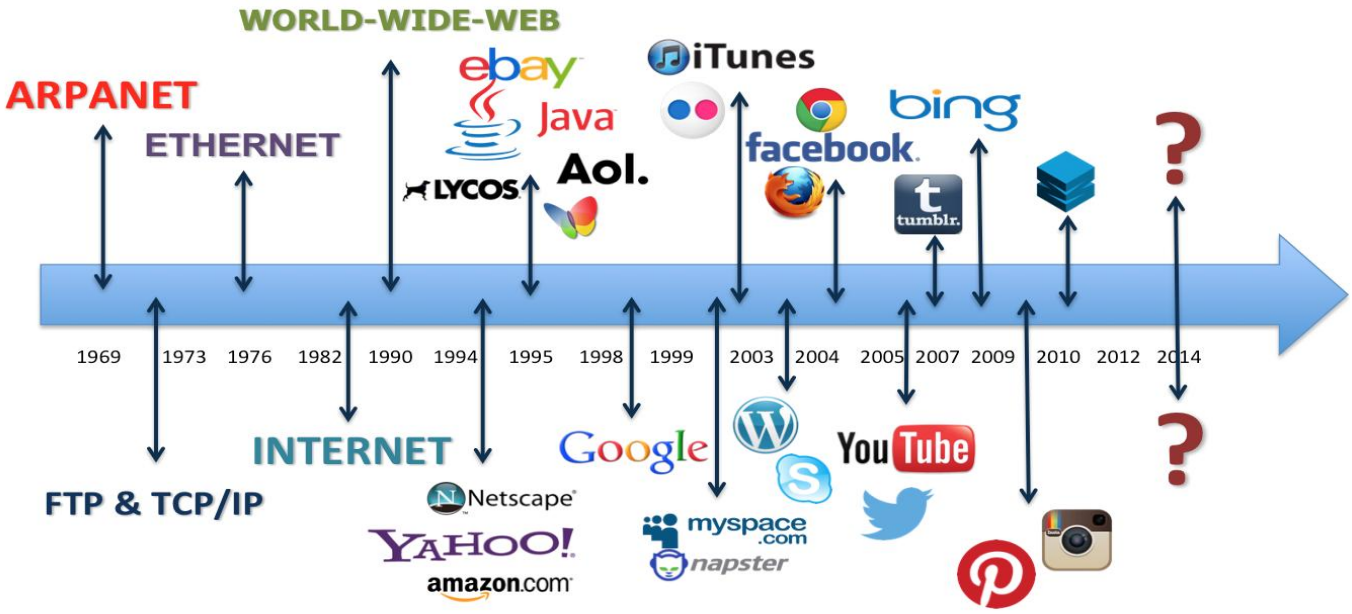
The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). The Internet is a worldwide collection of networks linked together.

HISTORY OF THE INTERNET

History of the Internet: In 1969 the U.S. Department of Defence commissioned the Advanced Research Projects Agency Network (ARPANET). The purpose was to provide communication links between supercomputers located at various regional sites (Universities and defence bases) within the United States.

It is this ARPANET that evolved into the Internet after computer networks were connected to it in different parts of the world. By1992, more than 1 million hosts existed on the Internet

THE DEVELOPMENT OF THE INTERNET



Requirements for Connecting to the Internet:

These include:

(a) **Computer / Device with a Network Interface Card.** The NIC may be based on Ethernet or wireless technologies.

(b) **An Internet Service Provider (ISP):** the company that takes care of the technical aspects of connecting to the internet. ISPs available in Uganda include Mobile telephone companies like Orange, MTN, Airtel, UTL, Smile etc

(c) **Modem:** This is a device that converts analogue telephone signals into digital computer information and vice-versa. Some computers have internal / inbuilt modems.

(d) **Required Software:** programs necessary to use the internet services such as web browsers and Email Clients, FTP software, etc.

Methods/ Ways of connecting to the internet

As technologies develop, bigger, better and faster Internet connections methods evolve. ISPs provide internet connectivity through the following

(a) Dial Up/ Analogue access / Phone Line Connection,

(b) Broadband (cable or Digital Subscriber Line (DSL))/ Fibre

(c) Satellite Connection

(d) Wireless broadcasts e.g Wi-Fi hotspots and Wi-Max.

FACTORS TO CONSIDER WHEN CHOOSING ISPs:

- **Availability:** Not all ISPs offer services in on all areas.
- **Speed/ Network Performance**
- **Price.** Prices vary by package
- **Support Services / Customer care**
- **Restrictions of use**
- **Reliability :** How long the ISP has been in business
- **Compatibility:** That the speed of their modems and their software should match
  the speed of yours
- **Email addresses:** Check whether the ISP has email and WWW services. Some ISPs can set up a custom email address when you activate your account. This would appear something like name@isp.com.

FACTORS AFFECTING THE SPEED OF AN INTERNET CONNECTION:

- Computer Processor speed
- Distance the data travels
- Traffic / number of users on the network
- Malware, Spyware and Viruses.
- Modem speed.
- Natural Conditions
- Positioning of wireless access points
- Memory available.
- Computer internet settings
- Technological Circumstances such as loose connections of cables or maintenance works being
  done by the ISP.
- Cookies: Over time, cookie files saved by websites in browser can compromise the speed .

Implications of the Internet (advantages/Disadvantages)

- **Interactive communication**; internet offers several communication tools such as emails, chatting, instant messaging, audio and video conferencing, online telephone calls etc.
- **Resource sharing**; data, information, software programs can be shared over the internet.
- **Research**; internet helps in conducting research using books online, encyclopaedia, audio and video tutorial to answer research questions.
- **Entertainment tools for leisure**; through on-line games, online chats, multimedia (audio, video) etc
- **Interactive communication**; internet offers several communication tools such as emails, chatting, instant messaging, audio and video conferencing, online telephone calls etc.
- **Resource sharing**; data, information, software programs can be shared over the internet.
- **Research**; internet helps in conducting research using books online, encyclopaedia, audio and video tutorial to answer research questions.
- **Entertainment tools for leisure**; through on-line games, online chats, multimedia (audio, video) etc.

Disadvantages of using the Internet

- Computer viruses can be spread over the internet.
- Internet provides access to unsuitable material such as Pornography, the biggest threat to healthy mental life.
- Theft of Personal information: If you use the Internet, you may be facing grave danger as your personal information such as name, address, credit card number etc. can be accessed by hackers or thieves.
- Spamming: Spamming refers to sending unwanted e-mails in bulk, which provide no purpose and needlessly obstruct the entire system.
- Some people get addicted to the internet, causing problems with their social interactions of friends and loved ones.
- The initial cost of connecting to the internet is high. e.g. buying computers.

- Many people are computer illiterate and so can not use internet, hence miss.
- There is a lot of wrong information on the internet. Anyone can post anything, and much of it is garbage/ inaccurate.

SERVICES OFFERED BY THE INTERNET

a. **Telnet** – enables users to use the resources of a computer in another part of the world. This is done by remotely logging to the distant computer which iscalled the host.

b. **Email** – It allows the transfer of messages, documents, and pictures among others, across the Internet.

c. **Mailing list** – This is based on the email protocol. As an electronic mailing list
it is very convenient when somebody wants to send a message or newsletter, for example, to many people in one go.

d. **Internet Relay Chat (IRC)** – A live interactive discussion in which parties on the network exchange ideas and observation electronically. Chats are usually organized in what we call chat rooms.

e. **File Transfer Protocol** – The standard method for transferring files, whether downloading or uploading, to and from your computer with another computer on the Internet.

f. **Newsgroups** – Worldwide discussion areas where notices can be posted for anyone to view. They are equivalent to a discussion group or an electronic bulletin board. There are newsgroups for every conceivable topic and more, e.g. educational technology.

g. **World Wide Web** – This refers to the global collection of websites consisting of linked electronic documents called Webpages stored on internet servers all over the world.
The www is the most exciting service that has revolutionized the Internet, people use this service to browse for information.

h. **Instant Messaging:** A combination of real-time chat and e-mail by which short text messages are rapidly exchanged over the Internet, with

messages appearing on recipient's display screen immediately upon arrival.

i. **Usenet**: A system of worldwide discussion groups

j. **Internet Telephony or Voice over IP**: Real-time voice conversations transmitted between computers on the Internet.

k. **Web Directory**: A listing of Web sites and their URLs, categorized by topic.

l. **Electronic Commerce/e-commerce:** Conducting commercial activities on the Internet.

m. **Social Networking.** A type of service where users can seek others who share their interests, find out what's going on in their areas of concern, and share information with one another (e.g. Facebook, Twitter).

n. **Cloud Computing:** A service in which computer software, hardware and data are used remotely over the Internet, instead of acquiring and using them on a local computer.

o. **Search Engines:** Software programs that look through the Web to locate sites matching a keyword entered by the user. Keyword: A string of letters or words that indicates the subject to be searched.

ELECTRONIC MAIL COMMUNICATIONS

Email communications refers to the transmission of messages via computer networks such as; a local area network, WANs, or internet.

The email can be simple text, or include an attachment such as a word processing document, PDF or graphic. Email software (Commonly known as email client) is a computer program used to access and manage a user's email account. It may be web based or not. Popular locally installed email clients include Microsoft Outlook, Pegasus Mail, KMail, Evolution and Apple Mail. Popular web-based email clients / webmail include: GMail, Yahoo!, Lycos mail, and Hotmail.

Advantages of using e-mail as a means of communication

1. Easy to use. Emails applications have user friendly tools that help during composing messages.
2. Email supports sending of attachments like documents, zipped files, e.t.c

3. It is very fast in terms of speed: The e-mail is delivered instantly, anywhere across the globe.
4. Easy to prioritize: Since the mails have subject lines, it is easy to prioritize them and ignore unwanted mails.
5. Email messages can be sent to many recipients at the same time
6. Emails can also carry hyperlinks that lead to other webpages with just a click
7. One can subscribe to news and other online services through email
8. Email software have management features that help users to organize their messages in folders like inbox, sent, draft, etc.
9. Easier for reference: When one needs to reply to a mail, there is a provision in the mailing system to attach the previous mails as references. This refreshes the recipient's knowledge, on what he is reading.
10. Environment friendly: Compared to postal mails which use paper and fuel to transport letters. Electronic mail saves a lot of trees from being axed. It also saves fuel needed in transportation.
11. Email software have address book features that may be sorted in alphabetical order.
12. Email software has a good degree of security features such as username and password before sign in
13. Email applications have inbuilt English dictionary which safeguards the sender from incorrect spelling and grammar.
14. Email is a relatively cheap means of communication since there are no printing or postage expenses involved.
15. 24/7 any time access. At any time of the day or night, one can communicate with friends, relatives, professors and business associates.
16. Messages remain permanent for future access from anywhere.
17. Use of graphics such as colorful greeting cards and interesting pictures can be sent through e-mails.
18. Advertising tool: many individuals and companies are using e-mails to advertise their products, services, etc.

Limitations of using Email as means of communication.

1. **Emails can spread Viruses:** The recipient needs to scan the mails, as viruses are transmitted through them and have the potential to harm computer systems.
2. **Spam and Junk:** E-mails when used to send unsolicited messages and unwanted advertisements create nuisance called Spam. Checking and deleting these unwanted mails can unnecessarily consume a lot of time, and it has become necessary to block or filter the unwanted e-mails by means of spam filters.
3. **E-mail spoofing** is another common practice. Spoofing involves disguising as different sender by altering the e-mail headers or the addresses from which the mail is sent.
4. **Hacking and email interception:** The act of unauthorized attempts to bypass the security mechanisms of an information system or network is termed as hacking. After the e-mail is sent and before it is received by the desired recipient, it "bounces" between servers located in different parts of the world. Hence, the e-mail can be intercepted by a professional hacker.
5. **Misinterpretation:** One has to be careful while posting any kind of content through an e-mail. If typed in a hurry, the matter could be misinterpreted. Since the content posted via e-mails is considered informal, there is a chance of business documents going unnoticed. Thus, vital communications and especially those requiring signatures are not managed through e-mails
6. **Crowded inbox:** Over a period of time, the e-mail inbox may get crowded with mails. It becomes difficult for the user to manage such a huge chunk of mails.
7. **Need to check the inbox regularly:** In order to be updated, one has to check his e-mail account regularly, which may be expensive in the long run.
8. Email cannot be used without computers especially in remote areas without electricity.
9. In case **one forgets his/her** password, signing in is not possible and this can lead to loss of information.
10. Email may violate privacy in case someone else gets to know your user password since the other may check your mails.

COMPONENTS/ STRUCTURE OF AN E-MAIL

1. **Headers** : The message headers contain information concerning the sender and recipients. The exact content of mail headers can vary depending on the email system that generated the message. Generally, headers contain the following information:

- **Subject**. The theme of the email message
- **Sender (From).** This is the senders Internet email address.
- **Date and time received (On).** The time the message was received.
- **Recipient (To :).** First/last name of email recipient, as configured by the sender.
- **CC: "Carbon copy"** enables copies of the email message to be sent to third party while acknowledging other recipients
- **Bcc:** Enables copies of the mail message to be sent to the third party without acknowledging nay other recipients.
- **Reply-to.** This is the Internet email address that will become the recipient of your reply if you click the Reply button.

2. **Body**:
   - The body of a message contains text that is the actual content.
   - The message body also may include signatures or automatically generated text that is inserted by the sender's email system.
3. **Attachments**
   - Attachments are optional and include any separate files that may be part of the message.

NETIQUETTE

Netiquette: rules of Behavior when using the Internet "Netiquette" refers to Internet etiquette. This simply means the use of good manners in online communication such as e-mail, forums, blogs, and social networking sites.

It is important to use netiquette and communicate to people online in the same manner you would communicate physically.

Netiquette guidelines:

- **Be clear:** Make sure the subject line (e-mail) or title (web page) reflects your content
- **Use appropriate language:** Avoid sending Abusive and Emotional messages.
- Don't use ALL CAPITAL LETTERS--it's equal to shouting or screaming
- **Be brief:** If your message is short, people will be more likely to read it
- **Make a good impression:** Your words and content represent you; review/edit your words and images before sending.
- **Don’t Forward e-mail messages you receive** *without permission of the original sender.*
- **Obey copyright laws:** Don't use others' images, content or use web site content without permission.
- **Do not send SPAM:** Spamming is posting or e-mailing unsolicited e-mail, often advertising messages, to a wide audience (another way of thinking of it is electronic junk mail).
- **Don't respond to "flames" or personal attacks**
- Always keep messages brief and use proper grammar and spellings.
- Never read someone’s private mail.
- Don’t Click on hyperlinks to unknown sites, especially on adverts and popups.
- Don’t download attachments from unknown sources.
- Avoid impersonation.
- Adhere to the same standards of behaviour online that you follow in real life.

- Respect other people's time and bandwidth.
- Make yourself look good online.
- Respect other people's privacy.
- Logout or log off your account after use.
- Post only acceptable information that has no harm to the public.
- Remember you are not anonymous. What you write in an e-mail and web site can be traced back to you.
- Know where you are in cyber space.

THE WORLD WIDE WEB

The World Wide Web (WWW), also called the Web, consists of a worldwide collection of electronic documents that can be access over the internet. Each of these documents on the Web is called a Web page

Web browsers

This is the type of software that is used for displaying Webpages from the internet or html documents on computers. It enables people to browse the World Wide Web.

Examples of web browsers

- ❖ Chrome
- ❖ Mozilla Firefox
- ❖ Internet Explorer
- ❖ Opera Mini
- ❖ Apple Safari
- ❖ Netscape

Search engines

The world wide web is a big place. If you know the web address, or URL, of a site you can find it by typing it into the address bar along the top of your browser. But what if you don't know the URL? You can find pages easily search by using a search engine.

A web search engine is a system that takes in user keywords, looks for information on the World Wide Web and return a line of results (hits), usually in form of a mix of links to matching web pages.

How search Engines Work

Web search engines work by storing information about many web pages, which they retrieve by a spider (an automated Web crawler) which follows every link on the web pages.

The search engine analyzes the contents of web pages and determines words to store in an **index database**.

Index words can be extracted from the

- titles,
- page content,
- headings (eg <H1>, <H2>), etc or
- Special fields called meta tags.

Popular search engines on the world wide web include

- Google
- Yahoo Search
- Wikipedia
- Baidu
- Bing search
- Bing
- Ask. Com

Effective Internet Searching

The challenge is to ask your question the right way, so that you don't end up overwhelmed with too many search results, underwhelmed with too few, or simply unable to locate the material that you need.

Keywords: Search engines don't read sentences the way people do: instead, they look for the key words in your query in the websites they search. Common words are ignored (that, to, which, a, the, …)

- Use "quotation marks" to search as a phrase and keep the words linked together.
- + and – can be used to include or exclude a word
- Boolean Syntax: Enter words and connect with Boolean Operators: AND, OR, NOT
    - AND will include sites where both words are found. Uses: joining different topics eg (ie. "global warming" AND California).

- OR - requires at least one of the terms is found Uses: join similar or synonymous topics (ie. “global warming” OR “greenhouse effect”)
- NOT – searches for the first term and excludes sites that have the second term Uses: join similar or synonymous topics (ie. Washington NOT school)

Other Syntax:

- **The wildcard operator (*):** Google calls it the *fill in the blank* operator. For example, amusement *
- **Site search:** Many Web sites have their own site search feature, but you may use a search engine to get results from one website Example: site:www.newvision.co.ug ICT in schools.
- **Related sites:** For example, related:www.youtube.com can be used to find sites similar to YouTube.

WEBSITES

The **Web (World Wide Web)** consists of websites hosted on **servers** on the internet globally. Websites contain information organized into Web pages.

Web pages are electronic documents with text and graphic images, written in Hyper Text Markup Language (HTML).

It contains hypertext links, or highlighted keywords and images that lead to related information.

A collection of linked Web pages that has a common theme or focus is called a **Web site**.

The main page that all of the pages on a particular Web site are organized around and link back to is called the site’s **home page**.

Client/Server Structure of the Web

Web is a collection of files that reside on computers, called **Web servers**, that are located all over the world and are connected to each other through the Internet.

When you use your Internet connection to become part of the Web, your computer becomes a **Web client** in a worldwide client/server network.

A **Web browser** is the software that you run on your computer to make it work as a web client.

Hypertext Markup Language (HTML)

WebPages are written in HTML, which is interpreted by web browsers.

HTML uses codes, or tags, to tell the Web browser software how to display the text contained in the document.

For example, a Web browser reading the following line of text:

<B> A Review of the Book<I>Wind Instruments of the 18th Century</I></B>

recognizes the <B> and </B> tags as instructions to display the entire line of text in bold and the <I> and </I> tags as instructions to display the text enclosed by those tags in italics.

Website Addresses

Each computer on the internet does have a unique identification number, called an IP (Internet Protocol) address.

The IPv4 addressing system uses a four-part number. For example, 106.29.242.17

Most web browsers do not use the IP address to locate Web sites and individual pages.

They use domain name addressing.

- A **domain name** is a unique name associated with a specific IP address by a program that runs on an Internet host computer.
- This program, which coordinates the IP addresses and domain names for all computers attached to it, is called **DNS (Domain Name System) software**.

Uniform Resource Locators

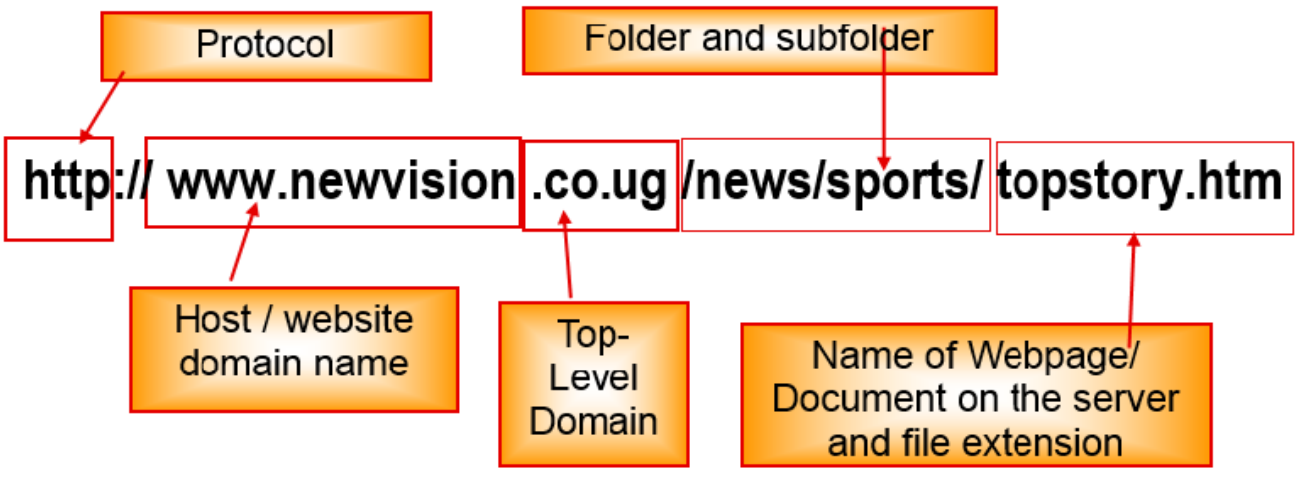
The IP address and the domain name each identify a particular computer on the Internet. However, they do not indicate where a Web page's HTML document resides on that computer.

To identify a Web pages exact location, Web browsers rely on a Uniform Resource Locator (URL).

URL is a four-part addressing scheme that tells the Web browser:

- What transfer protocol to use for transporting the file
- The domain name of the computer on which the file resides
- The pathname of the folder or directory on the computer on which the file resides
- The name of the file

STRUCTURE OF A UNIFORM RESOURCE LOCATOR



READING WEB ADDRESSES

Let's look at the parts of a typical URL:

- **http://www.sc.edu/beaufort/library/pages/bones/lesson1.html**

- Here's what it all means:
- **"http"** means hypertext transfer protocol and refers to the rules used to transfer and deal with information
- **"www"** stands for World Wide Web and is the general name for the host server that supports text, graphics, sound files, etc. (It is not an essential part of the address, and some sites choose not to use it)
- **"sc"** is the second-level domain name and usually designates the server's location, in this case, the University of South Carolina
- **"edu"** is the top-level domain name (see below)
- **"beaufort"** is the directory name
- **"library"** is the sub-directory name
- **"pages" and "bones"** are the folder and sub-folder names
- **"lesson1"** is the file name
- **"html"** is the file type extension and, in this case, stands for "hypertext mark-up language" (that's the language the computer reads).

TYPES OF WEBSITES

1. Web portal : An internet-based website that can perform many electronic functions and provide the user with quick access to a variety of information and services. EG. UNEB Results Portal

2. Content aggregator: Combines information such as news and entertainment, sports scores, weather forecasts, photographs and video from a variety of sources and makes the combined content available to its customers e.g Web-based feed readers like RSS Feeds, delicious.com, etc.

3. A wiki: A website that allows collaborative editing of its content and structure by its users. E.g. Wikipedia

4. A blog: A **blog** is a website in which journal entries are posted on a regular basis. A person who posts entries is called a **blogger**

Blog posts are typically displayed in reverse chronological order (the most recent post appears first).A majority are interactive, allowing visitors to leave comments.

Difference between a blog site and wiki site

Blog	**Wiki**
Blog usually has a single author	a Wiki usually has many authors
Blog is usually in reverse chronological structure	a Wiki has a structure determined by content and users
Blog is usually personal/someone's opinion	a Wiki is usually objective
The public can't edit someone's blog, can only add comments to a blog.	a Wiki can be edited by the public users.

5. Media sharing website

Media sharing sites allow you to upload your photos, videos and audio to a website that can be accessed from anywhere in the world. E.g youtube.com, dailymotion.com, blip.tv, slideshare.net, archive.org, podbean.com, and many, many others.

6. Social networking Website

An online service, platform, or site that focuses on building social relations among people who share interests by posting information, comments, messages, images, etc.

A type of website where users can seek others who share their interests, find out what's going on in their areas of concern, and share information with one another

Examples Social Networking sites include

- *Facebook*
- *Twitter*
- *Google Plus,*
- *Linkedn*

- *Whatsapp*
- *Instagram*
- *YouTube*
- *Pinterest*
- *Skype*

Advantages of Social Networking Websites

Staying Connected: The main purpose of social media is to be able to stay connected to friends and families The main purpose of social media is to be able to stay connected to friends and families

Finding People With Common Interests: Social networking is also a great way to meet peers.

Invaluable Promotional Tool: Companies, artists, etc use Social Media for advertising to the masses

Information Spreads Incredibly Fast
Breaking news and other important information can spread like wildfire on social media sites.

Helps To Catch And Convict Criminals: The Police uses social media to persecute criminals.

Disadvantages of Social Networking Websites

Perpetuates False And Unreliable Information: Anyone can post any unverified rumours which cause panic and severe misinformation in society.

Causing Major Relationship Problems: Online social interactions have cause many breakups.

Cyber Bullying: A new trend of cyber bullying is wreaking havoc all across the world. This is especially true with young kids publicly harassing one another, and posting mean or slanderous things which are broadcasted to the entire cyber world.

Used To Profile and Discriminate In The Job World: Employers are using social media to pre-screen their applicants.

The Addiction Is Real: One of the biggest problems with the social media craze is that people are becoming more and more addicted to using it. It is the number one time waster at work, in school, and at home.

Privacy Violation: Social Networks may violate privacy in case someone else gets to know your user password.

Misinterpretation: One has to be careful while posting any kind of information on social networks. If typed in a hurry, the matter could be misinterpreted

Evaluating the reliability of information found on a website

Check the last part of the URL. The top level domain can help to identify reliability (for example .gov, .ac, .ed, .sch are usually fairly reliable, while.org, .co, .com are less reliable).

See if responsible bodies have endorsed the site e.g. UNEB. If site is endorsed by reliable/reputable people/organizations it can be accepted as being reliable.

Checking the author's credentials. If the author's credentials are good it is likely to be reliable.

Can compare information from sites to see if it is reliable. If information is comparable to information from reliable/ authenticated/text books it is likely to be reliable.

Check the date of the last update. If the date of the last update was a long time ago it is likely to be unreliable.

Are any advertisements present? If site has excessive advertising it could be unreliable. If the advertising is related only to its own products it could be unreliable. If it has testimonials it is likely to be reliable.

CLOUD COMPUTING

Cloud computing is Internet-based computing, whereby shared resources e.g hardware, software and information are provided to other devices on-demand.

In simple terms, Cloud computing is using the internet to access someone else's software running on someone else's hardware in someone else's data center.

Cloud computing operates on a similar principle as web-based email clients, allowing users to access all of the features and files of the system without having to keep the bulk of that system on their own computers. In fact, most people already use a variety of cloud computing services without even realizing it such as Gmail, Google Drive, Google Docs, etc.

The online software services ‘on the cloud’ have long been referred to as Software as a Service (SaaS) and the hardware as Infrastructure as a service (IaaS).

Advantages of Cloud Computing

Lower computer costs:

- You do not need a high-powered and high-priced computer to run cloud computing's web-based applications.
- Since applications run in the cloud, not on the desktop PC, your desktop PC does not need the processing power or hard disk space demanded by traditional desktop software.

Improved performance: With few large programs hogging your computer's memory, you will see better performance from your PC.

Reduced software costs:

- Instead of purchasing expensive software applications, you can get most of what you need cheaply, e.g most cloud computing applications today, such as the Google Docs suite better than paying for similar commercial software.

Better Security: By using encryption, information on the cloud is less accessible by hackers or anyone not authorized to view the data. As an added security measure, with most cloud-based services, different security settings can be set based on the user.

Instant software updates:

- Another advantage to cloud computing is that you are no longer faced with choosing between obsolete software and high upgrade costs.
- When the application is web-based, updates happen automatically.

Improved document format compatibility

- You do not have to worry about the documents you create on your machine being compatible with other users' applications.

Unlimited storage capacity: Cloud computing offers virtually limitless storage on servers in powerful datacenters.

Increased data reliability/ safety: Unlike desktop computing, in which if a hard disk crashes and destroy all your valuable data, a computer crashing in the cloud should not affect the storage of your data.

Universal document access: That is not a problem with cloud computing, because you can access it whenever you have a computer and an Internet connection.

Easier group collaboration: multiple users can collaborate easily on documents and projects

Device independence: Even to a portable device, and your applications and documents are still available.

Disadvantages of Cloud Computing

Requires a constant Internet connection: Cloud computing is impossible if you cannot connect to the Internet. A dead Internet connection means no work.

Does not work well with low-speed connections: Web-based applications require a lot of bandwidth to download, as do large documents

Features might be limited: Many web-based applications simply are not as full-featured as their desktop-based applications. For example, you can do a lot more with Microsoft PowerPoint than with Google Presentation's web-based offering.

Disadvantages of Cloud Computing

Can be slow-Even with a fast connection, web-based applications can sometimes be slower than accessing a similar software program on your desktop PC. Everything about the program, from the interface to the current document, has to be sent back and forth from your computer to the computers in the cloud.

Stored data might not be secure: With cloud computing, all your data is stored on the cloud. Any unauthorized users gaining access to your password may access confidential data.

Migration issues: Each cloud system uses different protocols and different APIs, so your normal applications will have to be adapted to execute on these platforms.

TOPIC: SYSTEM SECURITY, ICT ETHICAL ISSUES & EMERGING TECHNOLOGIES

Sub Topic 1: **Computer System Security**
Sub Topic 2: **Privacy and ICT Ethical Issues**
Sub Topic 3: **Emerging Technologies**
Sub Topic 4: **ICT Industry**

Sub Topic 1: Computer System Security

Computer security
Refers to safe guarding computer resources, ensuring data integrity, limiting access to unauthorized users and maintaining data confidentiality.

Computer Integrity refers to methods and procedures of ensuring that data is real, accurate and safeguarded from unauthorized user modification in the computer.

Information security means protecting information and systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. - The purpose is to have digital equipment, information and services to be protected from unintended or unauthorized access, change or destruction. - It includes physical security to prevent theft of equipment and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security.

Cyber security is the process of applying security measures to ensure confidentiality, integrity, and availability of data. Cyber security assures protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. - The goal of cyber security is to protect data both in transit and at rest. Measures put in place to ensure cyber security include access control, awareness training, audit and accountability, risk assessment,

penetration testing, vulnerability management, and security assessment and authorization.

Physical Security refers to the measures put in place by protect computer systems from physical damage and mitigate physical security risks. Physical security includes:

- Locked doors
- Burglar proofs.
- Parameter fences.
- Security guards.
- Server room environmental protection, optimisation.
- Concrete walls.
- Lightening conductors.
- Fire extinguishers.
- Strategic server and storage placement

What is a computer security risk?

A computer security risk is an action that causes loss of or damage to computer system**.** Security threats to computers-based information systems, private or confidential data include:

- System failure
- information theft
- computer viruses, worms and Trojan horses
- unauthorized access and use
- hardware theft
- software theft
- unauthorized alteration
- malicious destruction of hardware software, data or network resources, as well as sabotage

ii. Security threats for (hardware and software)

Some of the causes of computerized information system failure include

- Hardware failure due to improper use.
- Unstable power supply as result of brownout or blackout and vandalism.
- Network breakdown.

- Natural disaster
- Program failure

What are hardware theft and hardware vandalism?

Hardware theft is act of stealing computer equipment and components. Cables sometimes used to lock equipment like some notebook computers use passwords, possessed objects, and biometrics as security methods. For PDAs, you can password-protect the device

Hardware vandalism is act of defacing or destroying computer equipment

Security threats for (hardware and software)

Software theft is the act of stealing or illegally copying software or intentionally erasing programs.

Software piracy is illegal duplication of copyrighted software. To guard against software theft and piracy, product activation is used.

Product activation allows user to input product identification number online or by phone and receive unique installation identification number

License agreement

A license agreement gives the right to use software. Single-user license agreement allows user to install software on one computer, make backup copy, and sell software after removing from computer.

Control measures against hardware failure

- Protect computers against brownout or blackout which may cause physical damages or data loss by using surge protectors and Uninterruptible power supply (UPS). For critical systems, most organizations have put into place fault tolerant systems.
- A fault tolerant system has redundant or duplicate storage, peripherals devices and software that provide a fail-over capability to backup components in the event of system failure.
- Disaster recovery plans Disaster recovery plan involves establishing offsite storage of an organization's databases so that in case of disaster or fire accidents, the company would have backup copies to reconstruct lost data

Computer Crimes

Computer crimes are criminal activities, which involve the use of information technology to gain an illegal or an unauthorized access to a computer system with intent of damaging, deleting or altering computer data. - Computer crimes also include the activities such as electronic frauds, misuse of devices, identity theft and data as well as system interference.

This is the criminal offence illegal or unauthorized use of computer technology to manipulate critical user data. It refers to any crime that involves a computer and a network.

Computer crimes may not necessarily involve damage to physical property. They rather include the manipulation of confidential data and critical information. - Computer crimes involve activities of software theft, wherein the privacy of the users is hampered. These criminal activities involve the breach of human and information privacy, as also the theft and illegal alteration of system critical information.

Types of computer crimes

Hacking: The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called hacking. It may involve hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source. - Phishing is carried out through emails or by luring the users to enter personal information through fake websites. - Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

Cyber stalking is the use of communication technology, mainly the Internet, to torture other individuals which include activities such as false accusations, transmission of threats and damage to data and equipment.

The physical theft of computer hardware and software is the most widespread related crime especially in developing countries. The most common issues now, we here cases of people breaking into an office or firm and stealing computers,

hard disks and other valuable computer accessories. In most cases such theft can be done by untrustworthy employees of firm or by outsiders. The reason behind an act may be commercial, destruction to sensitive information or sabotage

Control measures against theft

- Employ security agents to keep watch over information centers and restricted backup sites.
- Reinforce weak access points like windows, door and roofing with metallic grills and strong padlocks.
- Motivate workers so that they feel a sense of belonging in order to make them proud and trusted custodians of the company resources.
- Insure the hardware resources with a reputable insurance firm.
- Piracy is a form of intellectual property theft which means illegal copying of software, information or data. Software, information and data are protected by copyright and patent laws.

Control measures against piracy

There are several ways of reducing piracy

- Enforce laws that protect the owners of data and information against piracy.
- Make software cheap enough to increase affordability.
- Use licenses and certificates to identify original software.
- Set installation passwords that deter illegal installation of software.

Fraud is stealing by false pretense. Fraudsters can be either employees in a company, non-existent company that purports to offer internet services such as selling vehicles etc. other form of fraud may also involve computerized production and use of counterfeit documents. This is due to the dynamic growth of internet and mobile computing, sophisticated cybercrimes.

Sabotage refers to illegal destruction of data and information with the aim of crippling services delivery, or causing great loss to an organization. Sabotage is usually carried out by disgruntled employees or competitors with the intention of causing harm to an organization.

Surveillance refers to monitoring use of computer system and networks using background programs such as spyware and cookies. The information gathered may be used for one reason or the other e.g. spreading sabotage.

Identity theft-Act of pretending to be someone else by using another person's identity

Computer industrial espionage-Involves stealing of trade secrets or spying through tech means for bribery, blackmail, etc

Software piracy-The illegal act of duplicating copyrighted software.

Phreaking-The act of illegally breaking into a communication system to make calls without paying

Unauthorized use This is the use of a computer or its data for illegal/unapproved activities.

Spoofing Is a malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

Spamming=Sending of unwanted e-mails.

Knowingly selling-Is the act of distributing and selling child pornography.

A backdoor is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. - The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device. - A specific form of backdoor is a rootkit, which replaces system binaries and/or hooks into the function calls of an operating system to hide the presence of other programs, users, services and open ports. - It may also fake information about disk and memory usage.

Denial of Service attack-This is an attack designed to render the system unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. - These types of attacks are, in practice, difficult to prevent, because the behaviour of whole networks needs to be analyzed, not just the behavior of small pieces of code.

Eavesdropping is the act of secretly listening to a private conversation, typically between hosts on a network or telephone conversations. - For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers.

Cyber extortion is a form of cyber terrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks.

Information disclosure (privacy breach or data leak) describes a situation where information, thought to be secure, is released in an untrusted environment.

Others include

- **Cyber terrorism**
- **Cyber bullying**
- **Cyber harassment.**

Computer Viruses

A computer virus is a program designed specifically to damage, infect and affect other programs, data or cause irregular behavior to the computer. OR

A computer virus is a piece of software that can replicate itself and infect a computer, data and software without the knowledge of the user.

Computer Malware

Malware or short for malicious software is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. - Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. - Malwares include computer viruses, worms, Trojan horses, ransom ware, spyware, adware, scare ware, and other malicious programs. Malware is often disguised as, or embedded in, non-malicious files

Symptoms of a virus infected computer

- System slows down.
- System crushes and hangs up.
- Hard disk wont boot.
- Corrupted hard disk data.
- Program sizes keep changing.
- Computer programs take long to boot than normal.

- Files won’t open.

TYPES OF VIRUSES

A boot sector virus-This executes when a computer starts up because it resides in the boot sector of a floppy disk or the master boot record of a hard disk.

A file virus-This attaches itself to program files, and is loaded into memory when the infected program is run.

A macro virus -This uses the macro language of an application (e.g., word processor or spread sheet) to hide the virus code.

A logic bomb-This is a virus that activates when it detects a certain condition.

A time bomb-This is a kind of logic bomb that activates on a particular date.

A worm -This copies itself repeatedly in memory or on a disk drive until no memory or disk space remains, which makes the computer stops working.

A Trojan horse -This is a program that hides within or looks like a legitimate program, but executes when a certain condition or action is triggered.

A polymorphic virus -This modifies its program code each time it attaches itself to another program or file, so that even an antivirus utility has difficulty in detecting it

Scare-ware is a type of malware designed to trick victims into purchasing and downloading useless and potentially dangerous software. – Scare-ware, which generates pop-ups that resemble Windows system messages, usually purports to be antivirus or antispyware software, a firewall application or a registry cleaner.

Adware-The term **adware** is frequently used to describe a form of malware (malicious software), usually that which presents unwanted advertisements to the user of a computer. The advertisements produced by adware are sometimes in the form of a pop-up.

Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another individual without the consumer's consent, or that claims control over a computer without the consumer's knowledge.

A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and other malicious codes into one single threat. - Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack.

Viruses are activated in three basic ways

- Opening an infected file
- Running an infected program
- Starting up the computer with an infected floppy disk, flash disk

How viruses are spread

- Through E-mail attachments.
- Rogue websites. E.g. some adult sites, gambling sites, e.t.c.
- Sharing infected disks.
- Through networks.
- Through infected software.
- Hackers.
- Through downloads from the internet.
- Through software updates

Precautions to prevent virus infection

- Ensure that the e-mail is from a trusted source before opening or executing any e-mail attachment.
- Install an antivirus utility and update its virus definitions frequently for detecting and removing viruses.
- Never start up a computer with a floppy disk in the floppy drive.
- Scan all floppy disks and files for possible virus infection before opening them.
- Set the security level for macros in an application so that the user can choose whether or not to run potentially unsafe macros.
- Write-protect the recovery disk before using it.
- Back up important files regularly.
- Ensure that there is a policy of how computers are used and protected.

How to protect data from viruses in a computer system

- Make a back-up of all important files.
- Always update your software.
- Perform regular maintenance.
- Scan all disks from other computers.
- Protect your password and change it after some time.
- Use anti-virus software.

Anti-Virus Software

Anti-Virus Software Antivirus software is a set of utility programs that looks for and eradicates a wide range of problems, such as viruses, Trojan horses, and worms.

Examples of Anti-Virus Software

- AVG Anti-Virus
- Avira Anti-Virus
- Norton Anti-Virus Software
- Kaspersky Anti-Virus
- Avast Anti-virus
- Smadav USBAnti-Virus

How to protect Computer Systems

Installing Antivirus Program:- Computer programs that attempt to identify, prevent and eliminate computer viruses and other malicious software (malware).

Installing Firewall:- This serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks.

Data Encryption:- This method is used to alter the information in a form that it cannot be understood or followed by other people during transmission.

Data Backup:- Users should frequently duplicate (copy) the information to different storage devices such as DVDs, external hard disk to be able to recover their information in case of a disaster.

User ID and Passwords:- This is to restrict access to the computer systems, only allowing authorized users. A password is a secret code that combines characters and numbers that allow a user to access a computer or a network.

Access rights:- Access rights help to protect the IT system and the data stored on the system by restricting who can do what. Most company networks will be set up so that different users have appropriate levels of access rights. For example a manager of the company will have higher level access right than his subordinate staffs.

Audit Logs:- Network managers should ensure that their system is able to create an audit log. An audit log will record every important event in an 'audit file such as who logged on to the system at what time and onto which computer, which files were opened, altered, saved or deleted or log events such as attempts to access proxy servers

Rules for creating Secure Passwords

- Do not use your name or names of your close friends.
- Pick a mix of alphabetic and numeric characters. Never use an all-numeric password (especially your phone number or social security number).
- Pick long passwords. If your password is only a few letters long, an attacker will find it easy to try all combinations.
- Pick different passwords for the different machines or network nodes you access.

Intellectual property (IP)

Is a legal term that refers to creations of the mind that may include software, music, literature, discoveries and inventions.

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time. - Intellectual property rights include patents, copyright, industrial design rights, trademarks, trade dress, and trade secrets.

A patent grants an inventor the right to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention. - An invention is a solution to a specific technological problem, which may be a product or a process.

A copyright is the exclusive legal right that prohibits copying of intellectual property without permission of the copyright holder. - A copyright gives the

creator of original work exclusive rights to it, usually for a limited time. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or "works". Copyright does not cover ideas and information themselves, only the form or manner in which they are expressed.

A trademark is a recognizable sign, design or expression which distinguishes products or services of a particular trader from the similar products or services of other traders.

Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. - It is the process of scrambling plaintext (ordinary text, sometimes referred to as clear-text) into an unreadable format (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as

Cryptographers. - It is a technique used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified. - The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. - Only those who possess a secret key can decipher (or decrypt) the message into plain text.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. - Cryptography is used to protect e-mail messages, credit card information, and corporate data. - Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and asymmetric-key systems (public-key systems) that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Secret Vs. Public Key

Secret Keys (Symmetric Systems):- Both sender and receiver use the key to encrypt and decrypt. This is the fastest computation method, but getting the secret key to the recipient in the first place is a problem. ii)

Public Keys

Asymmetric Systems):- Each recipient has a private key that is kept secret and a public key that is published for everyone. - The sender is sent the recipient's public key and uses it to encrypt the message.

The recipient uses the private key to decrypt the message and never publishes or transmits the private key to anyone. - Thus, the private key is never in transit and remains invulnerable.

Use of Biometrics

Biometrics is the identification of a person by the measurement of their biological features. - For example, users identifying themselves to a computer or building by their finger print or voice is considered a biometric identification. - When compared to a password, this type of system is much more difficult to fake since it is unique to the person. Below is a listing of all known biometric devices.

Types of biometric devices

- A **fingerprint scanner**, which captures curves and indentations of a fingerprint
- A **hand geometry system**, which can measure the shape and size of a person's hand
- **A face recognition system**, which captures a live face image and compares it with a stored image
- A **voice recognition system**, which compares a person's live speech with their stored voice pattern
- **A signature verification system**, which recognizes the shape of handwritten signature of a person
- **An iris recognition system**, which reads patterns in the tiny blood vessels in the back of the eye, which are as unique as a fingerprint.

Computer Ethics

These refer to a set of moral principles that regulate the use of computers. The human values and moral conduct relating to right and wrong decision made when using computers. Moral guidelines that govern use of computers and information systems

A code of conduct is a written guideline that helps determine whether a specific action is ethical or unethical.

Three useful ethical principles

- An act is ethical if society benefits from the act.

- An act is ethical if people are treated as an end and not as a means to an end.
- An act is ethical if it is fair to all parties involved.

Computer ethics involves use of computers & software in morally acceptable way. Standards or guidelines are important in this industry, because technology changes are outstripping the legal system's ability to keep up

Computer Ethics for Computer Professionals

- According to the Association for Computing Machinery (ACM) code, a computing professional:
- Contributes to society and human well-being.
- Always avoids harm to others.
- Should be honest and trustworthy.
- Should exercise fairness and takes action not to discriminate.
- Honors property rights, including copyrights and patents
- Gives proper credit when using the intellectual property of others.
- Respects other individuals' rights to privacy.
- Honors confidentiality.

Information privacy

Right of individuals and companies to restrict collection and use of information about them.

Private data or information is the collection and use of personal information. This information should not be accessed or disclosed to any other person unless permitted by the owner.

Data held by an organization or government that should be disclosed to authorized people only is said to be confidential.

Concerns related to collection and use of private data

- Data should not be disclosed to other people without the owner's permission.
- Data and information should be kept secured against loss or exposure
- Data and information should be kept longer than necessary
- Data and information should be accurate and up to date.

- Data and information should be collected, used and kept for specified lawful purposes.

What are some ways to safeguard personal information?

- Limit the amount of information you provide to Web sites; fill in only required information
- Inform merchants that you do not want them to distribute your personal information
- Set up a free e-mail account; use this e-mail address for merchant forms
- Sign up for e-mail filtering through your Internet service provider or use an anti-spam program
- Do not reply to spam for any reason
- Install a personal firewall
- Turn off file and print sharing on your Internet connection
- Surf the Web anonymously with a program such as Freedom Web Secure or through an anonymous Web site such as Anonymizer.com
- Install a cookie manager to filter cookies
- Clear your history file when you are finished browsing.

Unethical computer codes of conduct

- Modifying certain information on the internet
- Selling information to others without the owner's permission
- Using information without authorization
- Invasion of privacy
- Involving in the stealing of software.

Computer ethics to be put in place

- Respect the privacy of others.
- Always identify the user accurately
- Respect copyrights and licenses
- Respect the intellectual property.
- Respect the integrity of the computer system.
- Exhibit responsible and sensible use of hardware and software

Emerging Technologies

This involves innovations and advancements in the use of new technological tools that make technology more amazing.

Concepts of emerging technologies covers the rapid evolution of computers and information technology with the future trends in computer and information and communication technology which is characterized by artificial intelligence and digital forensics.

Application areas of specific emerging technologies

Affective computing - Is the study and development of systems and devices that can recognize, interpret, process, and simulate human affects. It is an interdisciplinary field spanning computer science, psychology, and cognitive science.

Affect is the experience of feeling or emotion. Affect is a key part of the process of an organism's interaction with stimuli. The word also refers sometimes to affect display, which is "a facial, vocal, or gestural behavior that serves as an indicator of affect"

Ambient Intelligence (AmI)

In computing, ambient intelligence refers to electronic environments that are sensitive and responsive to the presence of people. - Ambient intelligence is a vision on the future of consumer electronics, telecommunications and computing that was originally developed in the late 1990s for the time frame 2010–2020.

Artificial Intelligence (AI)

Artificial intelligence refers to a branch of computer science that is concerned with the development of machines that emulate human-like qualities such as learning, reasoning, communication seeing and hearing. Also artificial intelligence refers to the ability of a machine to perform tasks that normally require human intelligence.

Computer scientist and engineers are still working hard to come up with computer reality in near future which can think and learn instead of relying on static programmed instructions

This is the intelligence exhibited by machines or software. It is an academic field of study which studies the goal of creating intelligence.

Major AI researchers and textbooks define this field as "the study and design of intelligent agents", where an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success.

There are four main application areas of artificial intelligence namely:

- Expert systems. Software that operate at the level of human expert in specific application.
- Natural language processing.
- Artificial neural networks.
- Robotics/perception systems.

Bioelectronics

This is a recently coined term for a field of research that works to establish a synergy between electronics and biology. The emerging field of Bioelectronics seeks to exploit biology in conjunction with electronics in a wider context encompassing, for example, biological fuel cells, bionics and biomaterials for information processing, information storage, electronic components and actuators.

A key aspect is the interface between biological materials and micro- and nano-electronics.

Digital forensics

Digital forensic refers to the science encompassing the recovery and investigation of material found in digital devices often in relation to computer crime.

Main application areas of digital forensic namely

- Legal consideration-use of digital evidence in court
- Branches-perception of the computer forensic, mobile device forensic, network forensic
- Application of digital forensic such as electronic discovery, intrusion etc
- Forensic process-analysis and reporting

Cloud computing

Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer

services or resources. Clouds can be classified as public, private or hybrid. – This is a recently evolved computing terminology or metaphor based on utility and consumption of computing resources.

Future Internet

As wireless and mobile technology advance, users can not only surf the online world - but can also do it on the move, through a plethora of portable devices, including laptops, smart phones and tablets; with an increasing need for high-bandwidth, high-speed broadband that can cope with rich multimedia content.

Other Emerging technologies

Virtual reality/artificial reality-Simulates physical presence in places of a real world as well as an imaginary world

Computer vision-Includes methods of acquiring, processing, analyzing, understanding images so as to produce symbolic information.

Implications of emerging technologies

- Technophobia/techno stress
- Loss of jobs say for massagers in case of networking
- Health issues for eye defects, back pain.
- Fear of cost of retaining or learning new skills
- Fear of increased electricity and subscriptions costs
- Fear of computer related crimes like forging of documents
- Fear of loss of man-hours through computer games and video during working hours
- Data loss by virus and system crashing
- Computer related errors and accident
- Unemployment//redundancy//financial/family problems.
- Local businesses/economy affected
- Possible increase in crime (Idle youth)
- People leaving community (to find other work)
- Opportunities for high skilled/programming jobs

Computer Professionals

A computer professional might be: - A person working in the field of information technology. A person who has undergone training in a computer-related field colleges, universities and computer institutes. A person who has an extensive knowledge in the area of computing.

Careers in ICT field

a) Computer operator

- Some of the responsibilities of a computer operator include;
- Entering data into the computer for processing.
- Keeping up-to-date records (log files) of all information processing activities.

b) Computer technician

- Troubleshooting computer hardware and software related problems.
- Assembling and upgrading computers and their components.
- Ensuring that all computer related accessories such as printers modems, storage media devices are in good working condition.

c) Computer engineer

- Computer and electronic engineers are coming up with new and more efficient technologies in information and communication technology almost daily. Since computers are electronic devices, hardware designers must be good in electronic engineering in order to be able to:
- Design and develop computer components such as storage devices, motherboards and other electronic components.
- Determine the electrical power requirement of each component.
- Re-engineer computer components to enhance its functionality and efficiency.
- Design and develop engineering and manufacturing computer controlled devices such as robots.

d) Computer programmer

- Large organizations such as insurance companies, banks, manufacturing firms and government agents hire programmers to work together with system analysts in order to:
- Develop in house application programs or system programs.
- Customize commercial application packages to suite the organization needs.
- Install, test, debug, and maintain programs developed or customized for the organization.

e) Web administrator/webmaster

- Developing and testing websites.
- Maintaining, updating and modifying information on the website to meet new demands by the users.

f) Software engineers

Most Software engineers analyses user needs and create application software. Software engineers usually have experience in programming, but focus on the design and development of programs using the principles of mathematics and engineering.

g) Computer Trainers

Computer trainers typically teach new users how to use the computer software and hardware.

h) Network administrator

- A network administrator is a specialist whose responsibilities are to:
- Set-up a computer network.
- Maintain and enforce security measures on the network.
- Monitor the use of network resources.
- Maintain and troubleshoot network related problems.

i) Database Administrator (DBA)

Database Administrator (DBA) is an IT professional responsible for installation, configuration, upgrade, administration, monitoring, maintenance, and securing of databases in an organization.

j) Graphic designer

A graphic designer is a professional within the graphic design and graphic arts industry who assembles together images, typography, or motion graphics to create a piece of design.

k) System Administrators

A system administrator, or system admin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers

A system administrator may acquire, install, or upgrade computer components and software; provide routine automation; maintain security policies; troubleshoot; train or supervise staff; or offer technical support for projects.