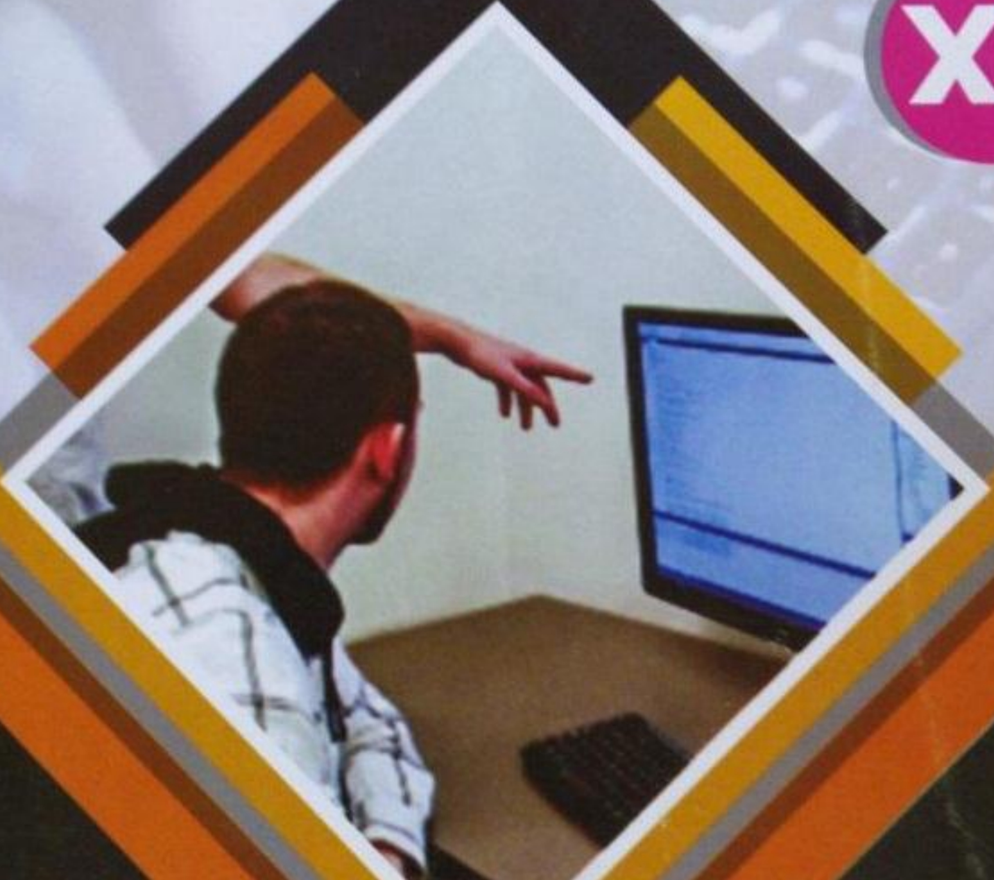
हिमाचल प्रदेश

1228

COMPUTER SCIENCE

XII



HIMACHAL PRADESH BOARD OF SCHOOL EDUCATION,

DHARAMSHALA

CHAPTER - 1

NETWORK OPERATING SYSTEM

1.1 Networking :

In the world of computers, ***networking is a practice of linking two or more computing devices together in order to share resources, exchange of files or allow electronic communication.*** Networking involves designing, implementing, upgrading, managing the computer networks.

1.2 Computer Networks :

Computer has become the integral part of every organization. These computers may be located at different locations within a building/ campus/organization. Each computer may perform different set of task and may work in a different environment without interacting with each other. This may result in overlapping of same task/work of computations. If computers are connected by a network, many of the overlapping tasks will be minimized and we will be able to extract information from each computer and share the existing information.

Computer network is a collection of interconnected independent computers and peripherals connected by communication facilities for exchanging information and sharing resources. A computer network can be anything ranging from two interconnected computers to thousands of interconnected computers.

In other words, A ***computer network is interconnection of geographically distributed multiple computers so that a meaningful transmission and exchange of information may take place among them.***

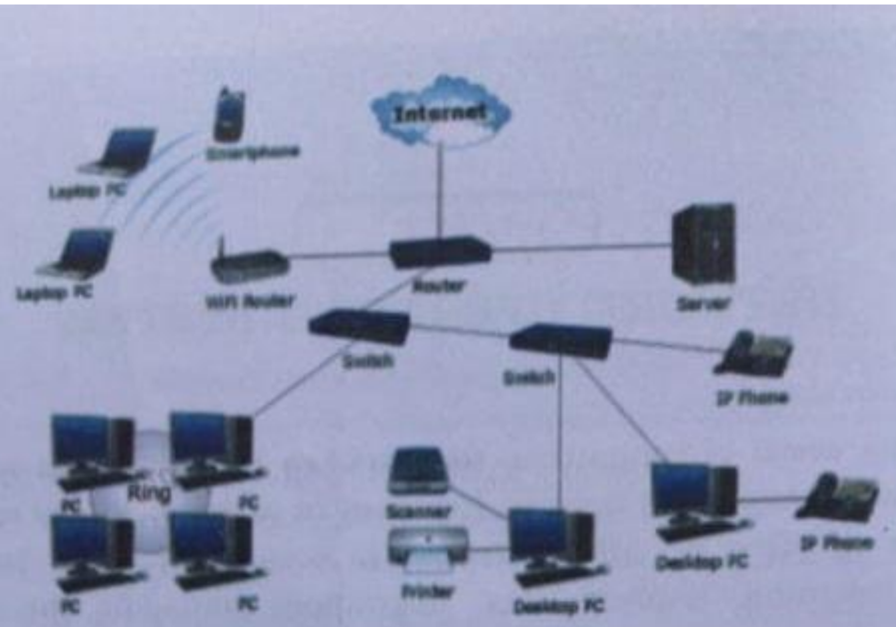


Figure 1.1 Computer Network

1.2.1 Need of Computer Network :

A computer in itself is useful but several computers connected with each other can be even more useful. Some benefits causing the need of computer networks are:

i) *Sharing of resources* : Computer network not only provide the ability to share information but also the resources. Resources can either be hardware resources (like printer, scanner, CD ROM, Fax machine) or software resources (like application program) for example: using a computer network, an expensive laser printer can be shared among various employees in a department of a company instead of giving each employee a separate laser printer.

ii) *Connecting and communication* : Networks connect computers and users of those computers. Once they are connected it is possible for the user to communicate with each other. Since the modern organizations are widely dispersed with offices geographically apart, networking provides communication among them.

iii) **Improved performance** : Network's performance can be increased for some applications by distributing the computational task on various computers.

iv) **Cost factor** : Rather than having one microcomputer per user, on organization can use a network of terminals with data stored on one shared file server machine. This gives better price/ performance ratio.

v) **Reliability** : A file can have copies on two or three different machine, so if one of them is unavailable due to hardware crash, the other copies could be used.

vi) **Flexible working environment** : The use of networking allows a very flexible working environment. Employee can work at home by using terminals attached through networking into the computer at office.

1.2.2 Disadvantages of networking :

Of course today everyone thinks that networking is worthwhile but along with various benefits, networking has few drawbacks. Some of these are:

i) **Data security concerns** : A poorly secured network puts critical data at risk. For example when files are shared among user then there is always a threat that unauthorized user can alter or use the sensitive data.

ii) **Network hardware, software cost** : To set up a network requires investment in hardware and software.

iii) **Threat of virus** : The effect of viruses on the network is more as compared with standalone systems because viruses can easily spread from one computer to another over network.

iv) **Illegal use** : network brings certain problem like illegal or illicit material, software piracy and illegal use of computer resources.

1.3 Components of Networking :

A computer network is build up from several components. These components together make it possible to transfer data from one device to another and make smooth communication between two different devices. Basic components of a computer network are:

a) **Servers** : Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.

b) **Clients** : Clients are computers that request and receive service from the servers to access and use the network resources.

c) **Transmission Media** : All computers in a computer network are connected with each other through a transmission media such as wires, optical fibre cables, coaxial cables etc.

d) **Network Interface card** : Each system or computer in a computer network must have a card called network interface card (NIC). The main purpose of NIC is to format the data, send the data and receive the data at the receiving node. NIC is a hardware component used to connect a computer with another computer onto a network. It can support a transfer rate of 10,100 to 1000 Mb/s.

e) **Hub** : A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped. The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

f) **Switch** : A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

g) **Router** : A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network. Router joins multiple computer networks to each other. For example let's say a company runs 100 computers over a local area network (LAN) and another company runs another LAN of 150 computers. These both LANs can be connected with each other through a internet connection which is provided by the router.

h) **LAN cable** : A wire that is used to connect more than one computer or other devices such as printers and scanner to each other.

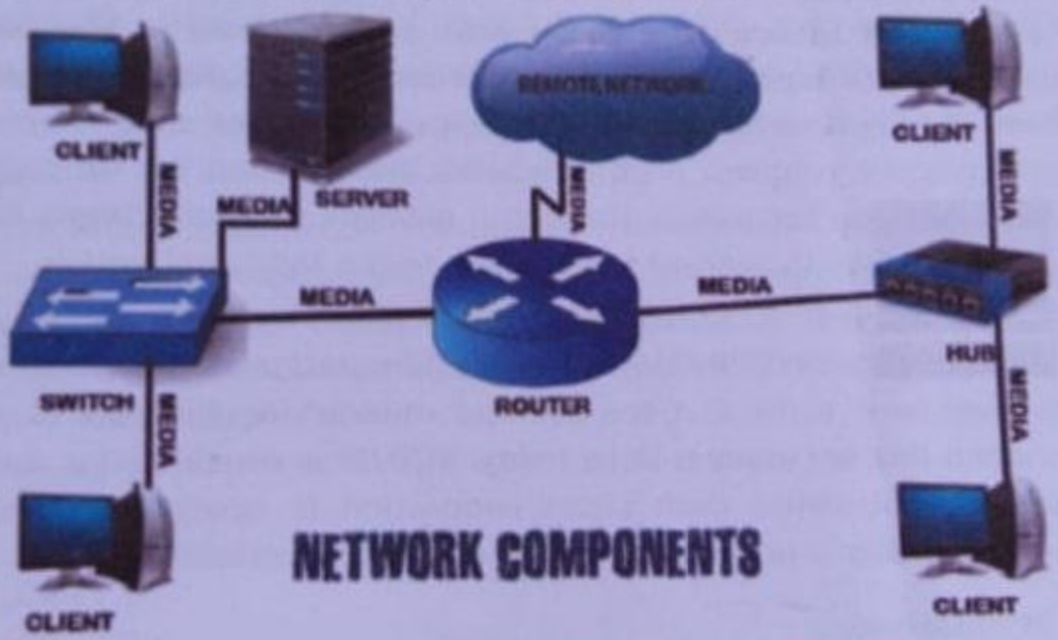


Figure 1.2 Components of Computer Network

1.4 Transmission Control Protocol / Internet Protocol (TCP/IP) :

Transmission Control Protocol (TCP) and Internet Protocol (IP) are two distinct computer network protocols. ***The Internet works by using a***

protocol called TCP/IP, or Transmission Control Protocol/Internet Protocol. TCP/IP is the underlying communication language of the Internet. In base terms, ***TCP/IP allows one computer to talk to another computer via the Internet through compiling packets of data and sending them to right location.***

A packet, sometimes more formally referred to as a network packet, is a unit of data transmitted from one location to another. A packet is the smallest unit of transmitted information over the Internet.

TCP : As with any form of communication, two things are needed: a message to transmit and the means to reliably transmit the message. **The TCP layer handles the message part. The message is broken down into smaller units, called packets, which are then transmitted over the network.** The packets are received by the corresponding TCP layer in the receiver and reassembled into the original message.

IP : The bottom layer, **IP, is the locational aspect of the pair allowing the packets of information to be sent and received to the correct location. The IP layer is primarily concerned with the transmission portion.** This is done by means of a unique IP address assigned to each and every active recipient on the network. Much like a car driving on a highway, each packet passes through a gateway computer (signs on the road), which serve to forward the packets to the right destination.

TCP/IP is needed to ensure that information reaches its intended destination. Without TCP/IP, packets of information would never arrive where they need to be and the Internet wouldn't be the pool of useful information that we know it to be today. TCP/IP is considered a stateless protocol suite because each client connection is newly made without regard to whether a previous connection had been established.

1.5 IP Addressing :

An Internet Protocol (IP) address is a numerical label assigned to each device connected to a computer network that uses the internet protocol for communication. Every machine working over the internet has a unique number assigned to it, which means no other machine can have same IP address over the network. Without IP address your machine would not be able to communicate over the internet.

An IP address is a 32 bit number that identifies a computer on the internet. These bits are divided into four sections referred to as octets, each contains 8 bits.

Internet Protocol Version4 (IPV4) use 32 bit IP address mechanism, which means that it can have 2^{32} i.e. 4,294,967,296 address. These addresses are in the form:

- Dotted decimal as **192.68.10.2**
- Binary as **10101101.00011000.01010011.00110010**

1.6 Classes of IP address :

IPV4 address is divided into two parts :

- Network ID
- Host ID

Network ID : The network id identifies the network to which IP address belongs. It is assigned by the internet network information center.

Host ID : The host id identifies host on the specified network. It is assigned by the local network administrator.

Internet Protocol hierarchy contains several classes of IP addresses to be used efficiently in various situations as per the requirements of hosts per network broadly, the IPV4 addressing system is divided into five classes of IP addresses. All the five classes are identified by the first octet of IP address. These classes are:

- **Class A**
- **Class B**
- **Class C**
- **Class D**
- **Class E**

a) Class A address : Class A addresses are designed for large organizations with a large number of host or routers. IP address is 32 bit long. In class A address, 7 bits are used for network address and 24 bits are used for host address. ***The first bit is always zero (0) for class A***. To find the range of class A the minimum value will be 00000000 (when all are 0) i.e. 0 and highest value will be 01111111 i.e. 127. So the range of class A is

0.0.0.0 to 127.255.255.255

b) **Class B address :** Class B addresses are designed for medium sized organizations. ***The first two bits are always 1, 0.*** The 14 bits are used to identify the network and 16 bits are used to identify the host. The range of class B begin with 10000000 i.e. 128 to 10111111 i.e. 191. So the range of class B is

128.0.0.0 to 191.255.255.255

c) **Class C address :** The class C addresses are designed for small organizations. ***In class C, the first three bits are always 1, 1, 0.*** The 21 bits are used for network identification and only 8 bits are used for host identification. The starting address of class C is 11000000 i.e. 192 and final address is 11011111 i.e. 223. So the range of class C is

192.0.0.0 to 223.255.255.255

d) **Class D address :** The class D addresses are used for multicast groups. Multicast means a datagram is directed to multiple hosts. ***In class D address, first four bits are 1, 1, 1, 0*** and number of network and host address bit are not fixed. The starting address of class D will be 11100000 i.e. 224 to 11101111 i.e. 239. So the range of class D is

224.0.0.0 to 239.255.255.255

e) **Class E address :** Class E addresses are reserved for future use. Some researcher use class E address for experimental purposes. ***The first four bits are always set to 1,1,1,1 for class E address.*** The number of network and host address bit are not specified. The starting address of class E will be 11110000 i.e. 240 to 11111111 i.e. 255. The range of class E is

240.0.0.0 to 255.255.255.255

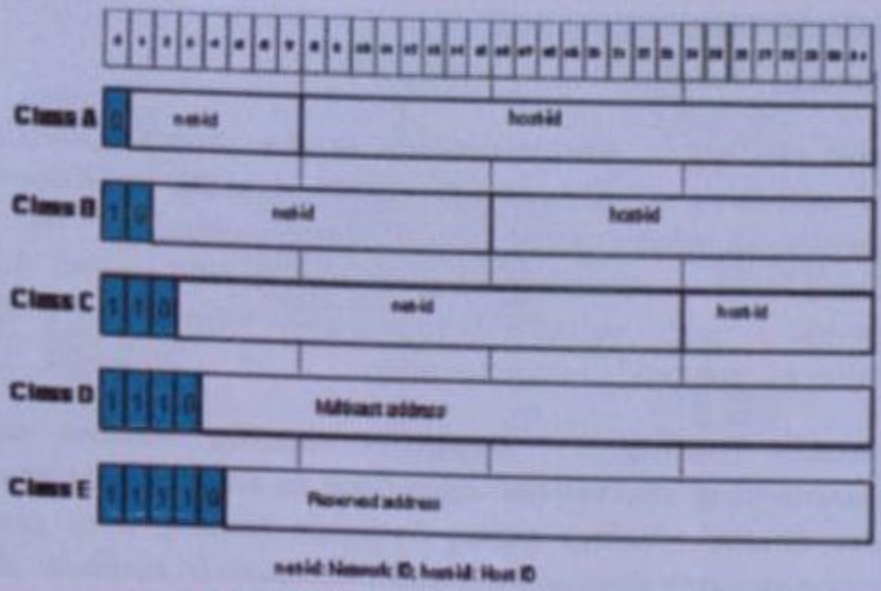


Fig. 1.3 Network ID & Host ID

IP Class	Network ID	Host ID	Reserved Bit	Range
Class A	8 bit	24 bit	0	0 to 127
Class B	16 bit	16 bit	10	128 to191
Class C	24 bit	8 bit	110	192 to 223
Class D	Multicasting		1110	224 to 239
Class E	Future Use		1111	240 to 255

Table 1.1 IP Address Classes

1.7 IP Routing :

Routing is the process of selecting path for traffic in a network or across multiple networks. ***IP routing is the process of transporting data from source to destination on a determined path across two or more networks. IP routing provides the path for reaching the destination devices.*** IP routing enables two or more devices on different TCP / IP networks to connect with each other. It is implemented, operated and managed by the router. It is of two types :

- **Static routing**
- **Dynamic routing.**

a) **Static routing :** ***Static routing is the manual configuration and selection of a network route, usually managed by the network administrator.*** Using ***route*** command, the system's routing table is manipulated. It is simple and useful for smaller network. It adds security because only administrator can allow routing to particular networks only.

b) **Dynamic routing :** ***Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table.*** Dynamic routing uses protocols to discover network destinations and the routes to reach it. Automatic adjustment will be made to reach the network destination if one route goes down. ***Router Information Protocol (RIP)*** is the example of dynamic routing. It is easy to configure and it is more effective at selecting the best route to a destination remote network. It is less secure than static routing. It consumes more bandwidth for communicating with other neighbours.

1.8 Network Operating System :

An operating system that provides the connectivity among a number of autonomous computers is called a network operating system. Network Operating System (NOS) includes special functions for connecting computers and devices into a local area network (LAN) or inter-network.

A typical configuration for a NOS is a collection of personal computers along with a common printer, server and file server for archival storage, all tied together by a local network. Some popular network operating systems are Novell Netware, Window NT/2000, Linux, Sun Solaris, Unix. The network operating system which was first developed is Novell Netware. It was developed in 1983.

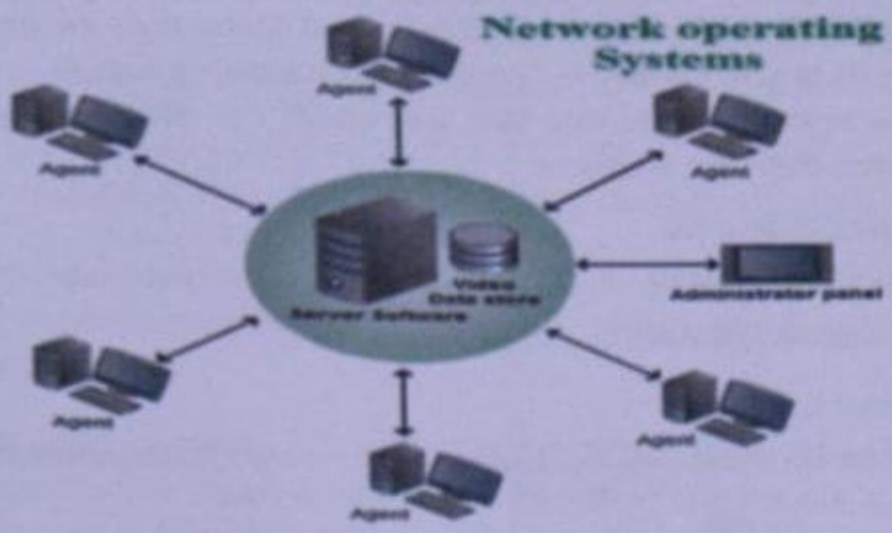


Fig. 1.4 NOS

Some features of Network Operating System are :

a) It allows multiple computers to connect so that they can share data, files and hardware devices.

b) It provides security features such as authentication, logon restrictions and access control.

c) It provides remote access to the devices.

d) It provides file, print, web services and back up services.

e) It supports internet working such as routing and WAN ports.

f) It detects the new hardware whenever it is added to the system.

1.9 Linux Operating System :

The Linux OS, is a freely distributable operating system based on Unix that can be installed on PCs, laptops, netbooks, mobile, video game consoles, servers, super computers and more. The Linux OS is frequently packaged as a Linux distribution for both desktop and server use and includes the Linux kernel as well as supporting tools and libraries. Some popular Linux OS distributions include Debian, Ubuntu, Fedora, Red Hat etc.

Linux performs many of the same functions as Unix, Macintosh, Windows and Window NT does. It was developed by Linus Torvalds in 1991. The name Linux is a combination of Linus and Unix. It is an open source software. It is also known as "product of internet". Linux is a multi user operating system and is very fast and stable OS. We can download it's distribution from the websites:

https://redhat.com

https://ubuntu.com

https://getfedora.com

1.10 Linux Structure :

Linux structure comprises of three major components, namely these are :

- Kernel
- Shell
- Application

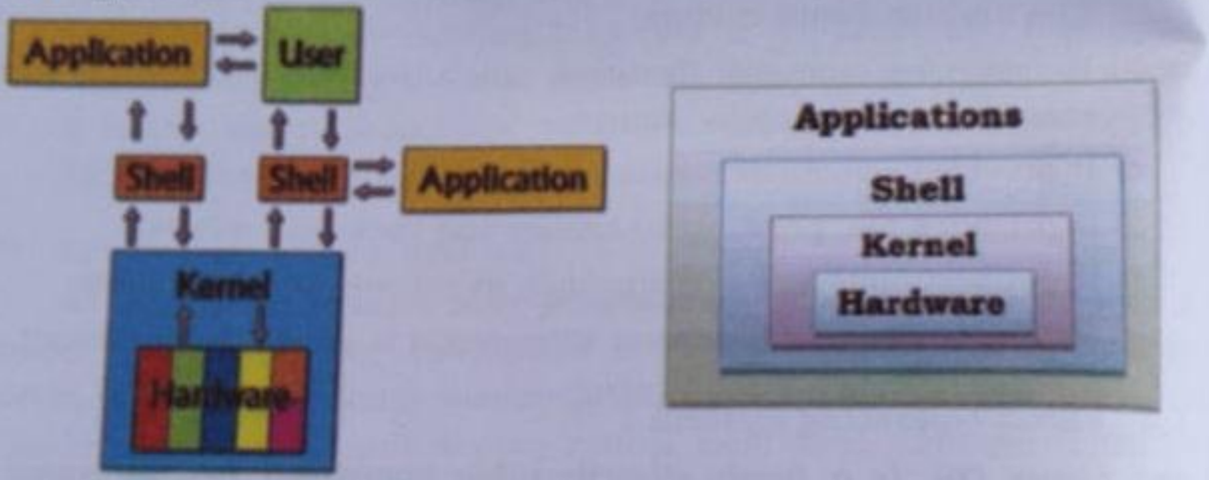


Fig. 1.5 Linux Structure

1.10.1 Kernel :

The Linux kernel is the main component of a Linux operating system. Kernel is the core interface between a computer's hardware and its processes. It communicates between the two and managing resources as efficiently as possible.

The kernel is the program that is responsible for allocating the computer's resources and scheduling the user jobs in a fair manner.

The kernel is the *'lowest'* level of the operating system. It is also called the heart of the Linux. The kernel is so named because – *like a seed inside a hard shell* – it exists with in the OS and controls all the major functions of the hardware.

The various functions performed by Linux kernels are :

a) **Memory management** : Kernel keeps track of how much memory is used to store. It allows the processes to safely access this memory as they require it.

b) **Process management** : It determines which process can use the CPU, and for how much long interval. Kernel allows the execution of applications and supports them with providing required resources.

c) **Device management** : Kernel acts as a mediator or interpreter between the hardware and processes. It maintains a list of available devices and provides the I/O to allow drivers to physically access their devices through some port.

d) **System Call** : A system call is a mechanism used by the application program to request a service from the OS. Kernel provides an API to invoke a system call.

e) **Security** : Kernel also provides protection from faults and from malicious behaviour.

The kernel is invisible to the user. It works with in its own little world called 'Kernel Space", where it allocates memory and keeps track of where everything is stored.

Where as, what the user sees like web browser, files etc. – are known as the "User Space". These applications interact with the kernel via a system call interface (SCI).

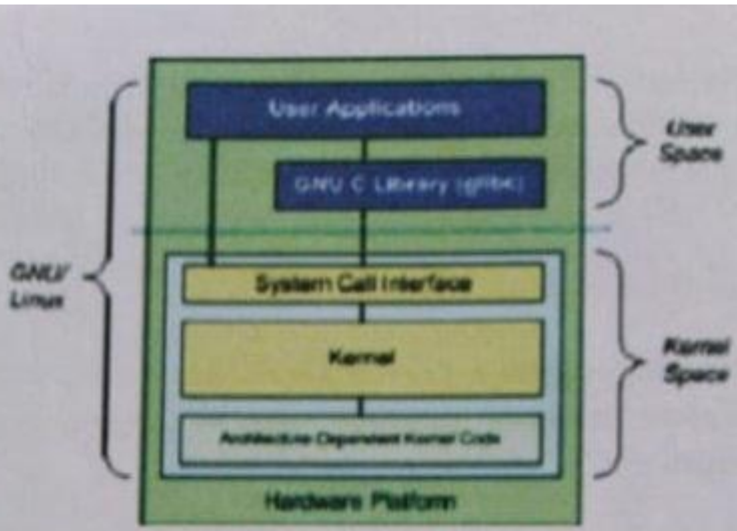


Fig. 1.6 Linux Kernel

1.10.2 Shell :

A shell provides you with an interface to the Linux system. It gathers input from you and executes programs based on that input. When a program finishes, it displays output of that program.

In short, shell is an environment in which we can run our commands, programs and shell scripts. The shell is classified into two types :

- Command line shells
- Graphical shells

The command line shell provides a command line interface, while graphical shell provide a graphical user interface.

1.10.3 Applications :

Linux has a variety of high quality softwares which can be easily downloaded and installed similarly like Windows, Mac. The languages like C, C++ are used to develop the applications.

1.11 Advantages of Linux :

a) **Open source :** One of the main advantages of Linux is that it is an open source operating system i.e. its source code is easily available for every one. Any one capable of coding can contribute, modify, enhance and distribute the code to anyone and for any purpose.

b) **Security :** Linux is more secure in comparison to other OS such as Windows. Every program in Linux whether an application or a viruse need authorization from the administrator in the form of a password. Unless the password is typed viruse won't execute.

c) **Software Updates :** In Linux you encounter a large number of software updates. These software updates are much faster than updates in any other OS.

d) **Free to Use (Low Cost) :** Linux is freely available on the web to download and use. You do not need to buy the license for it as Linux and many of its software comes with GNU (General Public License).

e) **Stability (Reliability) :** Linux provides high stability. Linux system rarely slows down or freezes. It does not require rebooting after installation or uninstallation of software like as in Windows.

f) **Fast and Easy Installation :** Linux can be easily installed from the web and does not require any pre requirements as it can run on any hardware, even on your oldest system.

g) **Customization :** You can customize any feature, add or delete any feature according to your need as it is an open source OS.

h) **Various Distributions :** There are many distributions of Linux are available like Fedora, Ubuntu, Debian, Red Hat and many more. It provides various choices or flavours to the user.

i) **Large Community Support :** Some forums are made on web by the users to help and solve the problem any other user is facing. There are a lot of dedicated programmers to help you out when ever possible.

j) **Performance :** Linux provides high performance on various networks and workstations. It allows large number of user to work simultaneously and handles them efficiently.

k) **Privacy :** Linux ensure the privacy of user's data as it never collects much data from the user while using its distribution or software.

1.12 Linux Desktop :

The desktop of Ubuntu is GNOME. GNOME is a desktop environment for free and open source system. Desktop is the place where icons, menus, panels, backgrounds are arranged and displayed.

To login to Linux OS enter password and press enter button. The Linux desktop will appear on the screen.

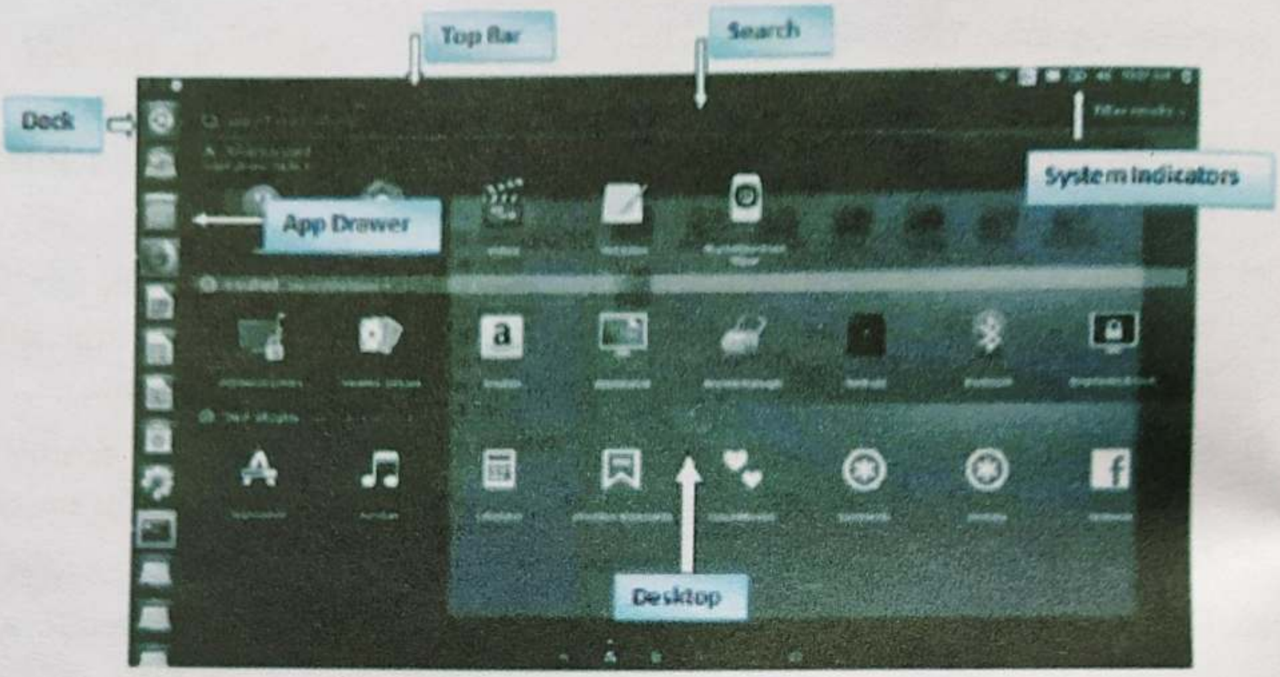


Fig. 1.7 Linux Desktop

The various compo:nents of Linux desktop are :

i) **Top Bar :** The bar across the top of screen provides access to the :

- Date and time
- System indicators
- Currently open applications

ii) **Desktop :** It is the area where you can open, run, rearrange multiple program and application.

iii) **Dock :** The dock occupies the left side of the screen. It shows currently open apps and shortcut of your favourite.

iv) **App Drawer :** It is at the bottom of the dock. When clicked, it lists all of the apps installed on your computer in a grid of icons.

v) **Search** : It appears at the top of the activities overview. Click activities option to open search bar.

vi) **System Indicator** : These are individual icons showing battery life, network connectivity, sound, Bluetooth and many more.

1.13 Shell :

In Linux ***shell refers to the program that is used to interpret the typed commands the user sends to the operating system.*** The shell is used for programming because we can program the shell quickly and simply. Shell has similarities to the Windows command prompt but it is more powerful and capable of running reasonably complex programs. The shell executes shell programs, often called Scripts, which are interpreted at runtime. Linux has following types of shells :

- Bourne Shell
- C Shell
- TC Shell
- Korn Shell
- Bash Shell

a) **Bourne Shell** : The original Bourne shell is named after its developer "Steve Bourne". It was the first shell used for the Unix operating system. It provides features which are sufficient for most programming needs.

b) **C Shell** : It was designed to allow user to write shell scripts programs using a syntax similar to C programming language. It is known as 'csh'.

c) **TC Shell** :-TC shell is an expansion of C shell. It has all the same feature, but add the ability to use keystrokes from the Emacs word processor to edit text on the command line. It is also known as 'tcsh'.

d) **Korn Shell** : It was written by 'David Korn'. It attempts to merge the feature of the C shell, TC shell and Bourne shell under one package. It also includes the ability for developers to create new shell commands.

e) **Bash Shell :** It is the updated version of the original Bourne shell that was created by the free software foundation for its Open Source GNU project. Its syntax is similar to the Bourne shell. It incorporates some advanced feature found in C, TC and Korn shell.

1.14 Shell Commands :

Shell commands run on command line interface. To invoke a command line interface, ***go to search option and enter the command keyword in the search box***. You can also invoke command window by ***clicking on App Drawer option from the left bottom of the desktop***.

Shell prompt: The prompt **$**, which is called the command prompt, is issued by the shell. You can type a command over here. Shell reads your input after you press Enter.

Some useful shell related commands are :

a) User related commands :

i) **who :** who command lists all users currently on system. The syntax is

```
$ who
```

ii) **who am i :** who am i command reports the user name of the command user. The syntax is

```
$ who am i
```

b) File and Directory related command :

i) **mkdir :** mkdir command is used for creating a new directory in Linux. The syntax is

```
$ mkdir DirectoryName
```

e.g. **$ mkdir Folder1**

It will create the directory named as Folder1.

ii) **cd :** cd command is used for changing the directory. The syntax is

```
$ cd DirectoryName
```

e.g. **cd Folder1**

Using this command user will move in the Folder1 directory.

e.g. **$ cd**

Using this command user will go to home directory.

iii) **rmdir :** rmdir command is used for removing a directory. The syntax is

```
$ rmdir DirectoryName
```

e.g. $ rmdir Folder1

This command removes the directory named as Folder1.

iv) **ls :** ls command is used to display a list of files and directories in the current working directory. The syntax is

```
$ ls
```

This command can be used along with various switches to enhance its working.

e.g. $ ls –l

This command display the detail of all files in the list form.

e.g. $ ls –a

This command show all the hidden files.

v) **pwd :** pwd command is used to find the directory in which user is currently working. pwd stands for print working directory. The syntax is

```
$ pwd
```

vi) **cp :** cp command is used to copy a file or directory. The syntax is

```
$ cp file1 file2
```

This command will copy file1 to file2 or copy one or more files to the same names under directory. If destination has an existing file, the file is overwritten.

c) Some common commands are :

i) **echo :** echo command is used to display a message on the terminal window. The syntax is

```
$ echo message
```

e.g. $ echo Hello, How are you?

This command will display the string "Hello, How are you?" on the screen.

ii) **grep :** grep command is used to search the content in the given file. It prints the matching lines. The syntax is

```
$ grep 'String' filename
e.g. $ grep 'why' ABC.txt
```

It will search the word **why** in the file ABC.txt

iii) **chmod :** chmod command is used to change the access mode of one or more files. Only the owner of the file or a privileged user may change the mode. The syntax is

```
$ chmod {option} mode files
```

This command uses various keywords like

u – user, g – group, o – other, a – all, + to add permission, - to remove permission, = to assign permission.

The various permissions are

r – read, w – write, x – execute

e.g. if you want to give permission read, write, execute to the user and read to the group on a file ABC.txt, the command will be:

```
$ chmod u = rwx, g=r ABC.txt
```

iv) **cat :** cat command, also known as concatenate, allow user to create single or multiple files, view content of file or concatenate files. It can be used in various ways, like

- To display the content of the file, the syntax will be

```
$ cat ABC.txt
```

- To create a new file, the syntax will be

```
$ cat > newfile
```

After typing the content press **Ctrl +D** to exit the entry mode.

- To append data in a file, the syntax will be

```
$ cat >> ABC.txt
```

- To combine two files, the syntax will be

```
$ cat File1 File2 > newfile
```

v) **find** : The find command is used to find the files in the hard drive. We can search a file by date or time.

```
e.g. $ find /user/bin – type f – name "*.txt"
```

vi) **date** : date command is used to display the current system date and time. The syntax is

```
$ date
```

vii) **cal** : cal command is used to print a 12 month calendar for a given year. The syntax is

```
$ cal 2019
```

viii) **cmp** : cmp command compare two files that they are identical. It shows 0 if they are identical otherwise it shows 1. The syntax is

```
$ cmp File1 File2
```

ix) **sort** : It print the lines of file in sorted order. The syntax is

```
$ sort FileName
```

x) **ps** : It is used to view the processes that user is running. The syntax is

```
$ ps [option]
```

e.g. $ ps –u UserName displays the processes of the specified user.

xi) **kill** : kill command is used for terminating the process. The syntax is

```
$ kill ProcessID
```

xii) **netstat** : netstat command displays the network status. It print information about active socket, routing table, interfaces etc. The syntax is

```
$ netstat
```

xiii) **logout** : logout command is used for logging out the Linux. The syntax is

```
$ logout
```

1.14.1 Wildcards :

Wildcards are a set of characters that allow you to create a pattern defining a set of files or directories. The basic types of wild cards are:

i) * represent zero or more character

ii) ? represents a single character

Suppose user's directory contains files as :

First.txt Second.txt File1.txt File2.txt Video.mpeg
Color.png Example.png

i) *** Wildcard character :**

**** is called asterisk symbol. It represent group of characters.*** It can be used in different ways. Some of its examples are:

- If user want to display files beginning with 'F'

  The command will be **$ ls F***

  The output will be **First.txt File1.txt File2.txt**

- If user want to display the files having extension '.txt'

  The command will be **$ ls *.txt**

  The result will be **First.txt File1.txt File2.txt Second.txt**

ii) **? Wildcard character :**

This wildcard replace one character. e.g. **$ ls F????.txt**

It will give result as **First.txt File1.txt File2.txt**

1.15 I/O redirection :

Redirection is a feature in Linux such that when executing a command, you can change the standard input / output devices. The basic workflow of any Linux command is that it takes an input and gives an output.

The standard input device is the keyboard.

The standard output device is the screen.

Output redirection : The output from a command normally intended for standard output, but it can be easily diverted to a file. This capability is known as output redirection. A greater than character (>) is used for output redirection.

```
e.g. $ who > users
```

Here no output appears at the terminal. This is because the output has been redirected from the default output device (the terminal) into the specified file. We can check the content of file users using

```
$ cat users
```

If a command has its output redirected to a file and file already contains some data, that data will be lost.

You can use **>>** operator to append the output in an existing file. We can use the following syntax:

```
$ echo Hello everyone >> users
```

This command will append the line **Hello everyone** in the file users.

Input redirection: Input of a command can be redirected from a file. The less – than character (<) is used to redirect the input of a command.

```
e.g. $ command [arguments] < filename
     $ mail ram < mail_contents
```

Here the text file mail_contents will be used as input for command mail ram.

1.16 Pipelines :

Pipes are used to redirect a stream from one program to another. We pipe the output of one program to the input of another. A pipe is nothing but a temporary storage place where the output of one command is stored and then passed as the input for second command. ***The Linux pipe is represented by a vertical bar (|).*** The syntax is

```
$ command1 | command2
e.g. $ ls | lpr
```

Here the list of filenames output by **ls** command is piped into the **lpr** command.

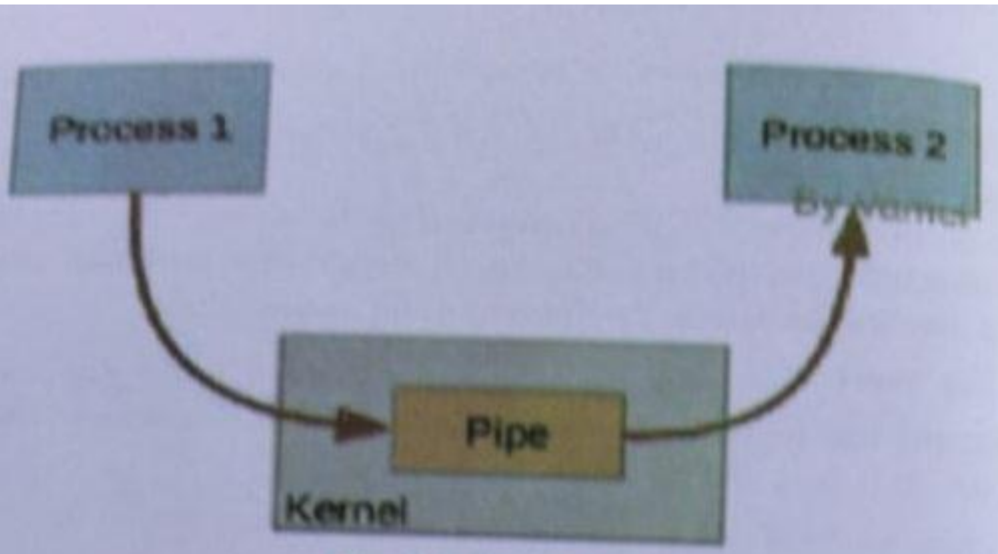


Fig. 1.8 Pipelining

1.17 Vi editor :

Vi editor stands for visual editor. Vi editor is a comprehensive screen editor provided by Linux OS. Vi editor provides three operating modes:

- Command mode
- Insert mode
- Replacement mode

Command mode : This is the default mode, in which we open a file. ***This mode allows typing commands.*** While in regular mode, you can move the cursor around with arrow key. Using ***h, i, k, j*** keywords you can move the cursor ***left, right, up, down***. You can use **x** key to delete the character under the cursor.

Insert mode : This mode makes it possible to insert character inside a document. To switch to insert mode, just press the **insert** key from the keyboard or just press **i** key.

Replacement mode : This mode allows to replace existing text by the text you capture. By pressing **r** key you can invoke replacement mode. To return back to **regular / command** mode you just press **Esc** key.

To save and exit from vi editor, first you have to be in command mode. Now type '**wq**' and press enter to write the file to disk and quit vi editor.

Some useful commands of vi editor are :

For Navigation :	
h	Move one character left
j	Move one character down
k	Move one character up
l	Move one character right
For Deletion :	
x	Deletes the character at current cursor position
X	Deletes the character just behind the cursor
dw	Deletes the current word
dd	Deletes the current line
For Undo :	
u	Undo the last edit
U	Undo all the previous edits on the current line
Saving and Exiting :	
W	Saves the file
zz	Saves the file and quits
Q	Quits the file if there are no unsaved changes

1.18 File System of Linux :

Everything in Linux is considered a file, even a hard disk or a CD-ROM device. All files and directories appear under the **root directory** (represented with a single slash – /). You can refer to any file or directory using either a full path (for example, **/home/gn/file.txt**) or a relative path (for example, if your current directory is **/home/gn/**, you can refer to the file simply by typing **file.txt**). Such a storage structure is known as **hierarchical or tree based file system**.

A directory is similar to a folder in Windows, and it can contain files and other directories. Hardware devices are represented by a special file stored in the **/dev** directory (for example, **/dev/sda** usually represents the first hard disk on the system). All files and directories appear under the **root directory** (/). A user can create his own directories for his own files, as well as easily move files from one directory to another. User can also set permission on directories and files, allowing others to access them or restricting access to yourself alone. Below that is a set of common directories in the Linux system (**bin**, **dev**, **home**, **lib**...):

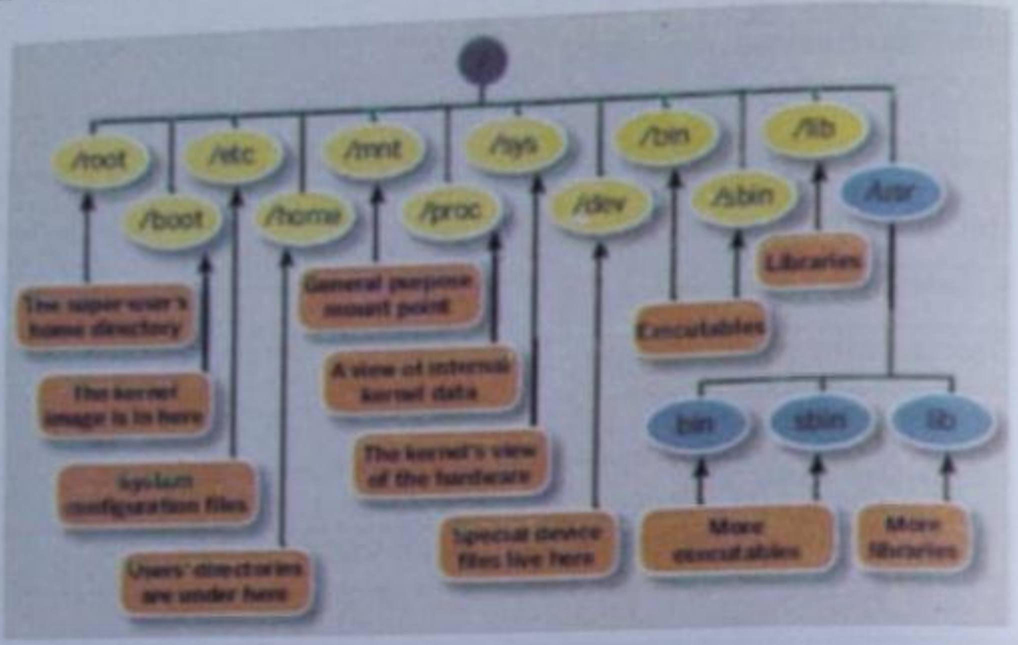

/
/root
/boot
/etc
/home
/mnt
/proc
/sys
/dev
/bin
/sbin
/lib
/usr
The super user's home directory
The kernel image is in here
System configuration files
Users' directories are under here
General purpose mount point
A view of internal kernel data
The kernel's view of the hardware
Special device files live here
Executables
Libraries
bin
sbin
lib
More executables
More libraries

Fig. 1.9 Linux File Structure

Most Linux distributions have almost identical directory structures because of the **File system Hierarchy Standard (FHS)**. FHS defines the directory structure and content in UNIX-like operating systems. It is based on the older standard **FSSTND (File system Standard)**.

Linux distributions usually closely follow the FHS. For example, configuration files are located in the same location regardless of Linux distribution (usually in the **/etc** directory). This makes developing software for Linux much easier, since software developers don't have to write different versions of applications for each distribution. In the FHS all files and directories appear under the **root directory** (/). here is a list of the most important directories:

/boot – contains files related to the initial booting of the computer.

/bin – contains certain critical executable files, such as ls, cp, and mount.

/dev – contains device files like hard disks or CD-ROMs.

/sbin – similar to /bin, but it contains programs that are normally run only by the system administrator.

/etc – contains configuration files.

/home – user's home directory.

/lib – contains program libraries.

/media – mount point for removable media.

/usr – contains the majority of user utilities and applications.

/var – variable files such as logs.

/tmp – contains temporary files.

1.19 Safety and Security :

Linux is a multi-user OS. Linux OS can provide services for more than one user at any time. Every user has their own profile with custom settings that can be set by the user. Linux is considered a safer OS as it follows a safety model at various tiers. Certain rules followed to ensure its safety model are:

- The user Root (uid == 0) can do everything because it has all the access and permission on the system.
- Files have owner, group, access permission for user, group, and others, which is very effective as a safety measure.
- Only using administrative privileges user can change the privileges on a entity.
- The safety model is hardcoded into Linux kernel.

1.20 Cyber Crimes & Laws :

1.20.1 Cyber Crimes :

The crimes committed with the use of computers or relating to computer, using internet is called cyber-crime. One another definition of cyber-crime is, **An unlawful act where computer is either a tool or a target or both.**

Cyber-crime is different from other crimes because the cyber-crimes are committed over an electronic medium. Cybercrime involves the use of computer and network in attacking computers and networks as well. Cyber-crime is obviously a criminal offense and is penalized by the law. Cybercriminals devise various strategies and programs to attack computers and systems. These are the most common types of cybercrime acts:

Fraud

Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain.

Hacking

Hacking involves the partial or complete acquisition of certain functions within a system, network, or website. It also aims to access to important data and information, breaching privacy. Most "hackers" attack corporate and government accounts. There are different types of hacking methods and procedures.

Identity Theft

Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft.

Scamming

Scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users to shell out hundreds of money for cyber problems that do not even exist. Any illegal plans to make money falls to scamming.

Computer Viruses

Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

Ransomware

Ransomware is one of the most destructive malware-based attacks. It enters your computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransomware. In 2017, over $5 billion is lost due to global ransomware.

DDoS Attack

DDoS or the Distributed Denial of Service attack is one of the most popular methods of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DDoS attack, giving hackers the chance to hack the system.

Botnets

Botnets are controlled by remote attackers called "bot herders" in order to attack computers by sending spams or malware. They usually attack businesses and governments as botnets specifically attack the information technology infrastructure. There are botnet removal tools available on the web to detect and block botnets from entering your system.

Spamming

Spamming uses electronic messaging systems, most commonly emails in sending messages that host malware, fake links of websites, and other malicious programs. Email spamming is very popular. Unsolicited bulk messages from unfamiliar organizations, companies, and groups are sent to large numbers of users. It offers deals, promos, and other attractive components to deceive users.

Phishing

Phishers act like a legitimate company or organization. They use "email spoofing" to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

Social Engineering

Social engineering is a method in which cybercriminals make a direct contact with you through phone calls, emails, or even in person. Basically, they will also act like a legitimate company as well. They will befriend you to earn your trust until you will provide your important information and personal data.

Malvertising

Malvertising is the method of filling websites with advertisements carrying malicious codes. Users will click these advertisements, thinking they are legitimate. Once they click these ads, they will be redirected to fake websites or a file carrying viruses and malware will automatically be downloaded.

Cyberstalking

Cyberstalking involves following a person online anonymously. The stalker will virtually follow the victim, including his or her activities. Most of the victims of cyberstalking are women and children being followed by men and pedophiles.

Software Piracy

The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

Child Pornography

Porn content is very accessible now because of the internet. Most countries have laws that penalize child pornography. Basically, this cybercrime involves the exploitation of children in the porn industry.

Cyberbullying

Cyberbullying is one of the most rampant crimes committed in the virtual world. It is a form of bullying carried over to the internet. On the other hand, global leaders are aware of this crime and pass laws and acts that prohibit the proliferation of cyberbullying.

1.20.2 Cyber Laws :

Cyber law is a generic term which refers to all the legal and regulatory aspects of internet and World Wide Web. The growth of Electronic commerce has propelled the need for effective regulatory mechanism which would strengthen the legal infrastructure related to electronic commerce.

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The Act was later amended in December, 2008 through the IT (Amendment) Act, 2008. It provides additional focus on Information Security by adding some new sections on offences including Cyber Terrorism and Data Protection. Some amendments of ITAA 2008 include:

- **Digital Signature** : Authentication of electronic records by digital signature gets recognition.
- **e – governance :** e–documents get legal recognition. Documents required as per law by the government may be supplied in the electronic form.
- **Penalties :**the maximum penalty for any damage to computer or computer system is a fine up to Rs. 1Crore.