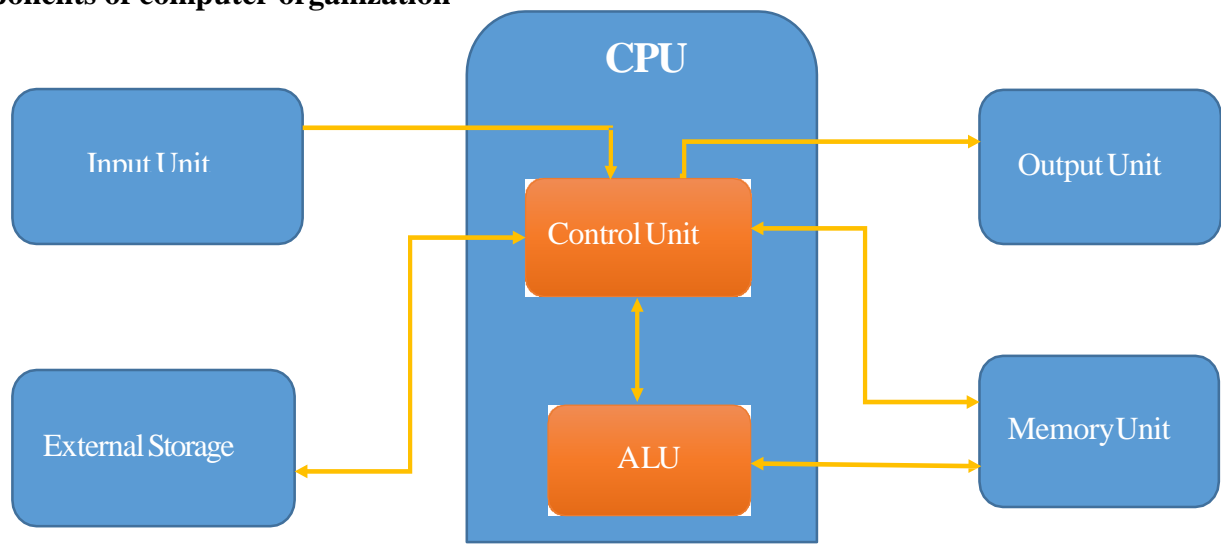## MODULE-2

## COMPUTER ORGANIZATION & SECURITY

**Computer Organization:**

- Computer system is made up of integrated parts like input, output, CPU, and storage unit wherein all the parts work together to process data.

**Components of computer organization**



**Central Processing Unit:**

- CPU is the major component of a computer
- CPU is also known as Processor
- CPU is referred to as the 'brain' of the computer system
- CPU interprets instructions and carries out logical and arithmetic operations
- CPU controls all internal and external devices
  - o **Components of Central Processing Unit:**
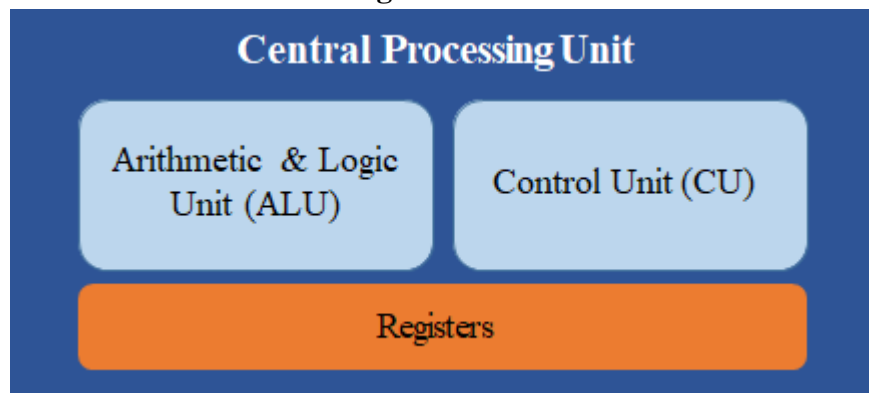


**Arithmetic Logic Unit (ALU):**
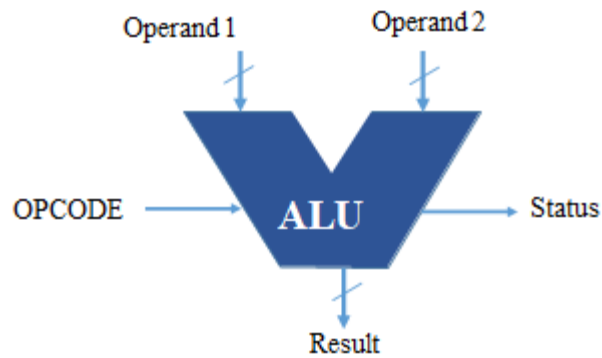
- o ALU is referred to as computer's calculator
- o Arithmetic unit performs arithmetic operations
- o Logic unit performs logical operations
- o ALU consists of numerous accumulators

**Control Unit (CU):**
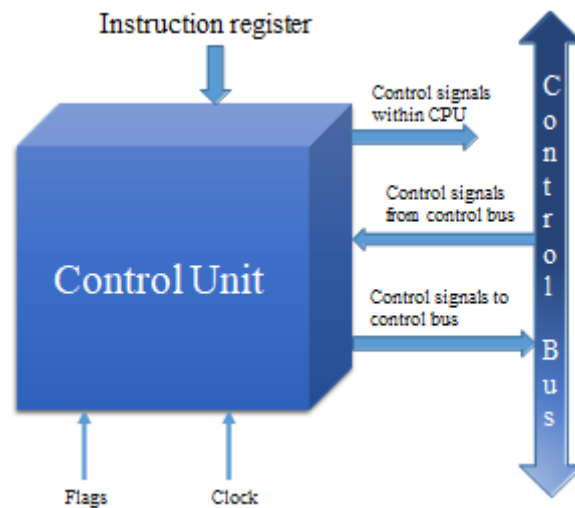


- o CU directs operation within processor
- o CU handles all the control signals in a CPU
- o CU controls the execution of an instruction in a sequence
- o CU controls the exchange of information between peripherals

**Registers:**
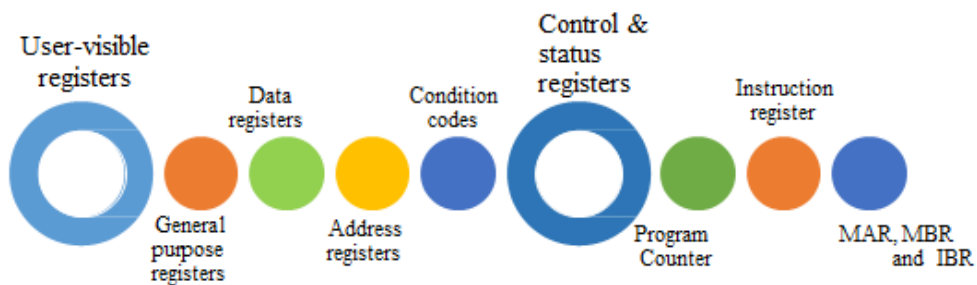


- o Registers are the fast memory locations within CPU that are used to create and store the results of CPU operations and other calculations.

### User-Visible Registers

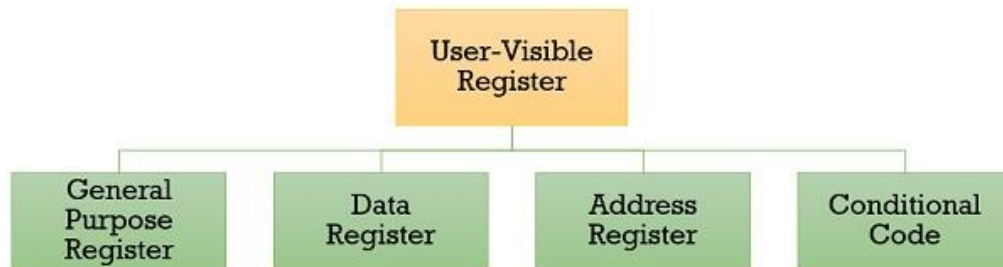These registers are visible to the assembly or machine language programmers and they use them effectively to minimize the memory references in the instructions. Well, these registers can only be referenced using the machine or assembly language.



The registers that fall in this category are discussed below:

1. General Purpose Register: The general-purpose registers detain both the addresses or the data. Although we have separate data registers and address registers. The general purpose register also accepts the intermediate results in the course of program execution.

2. Data Register: The term itself describes that these registers are employed to hold the data. But the programmers can't use these registers for calculating operand address.

3. Address Register: Now, the address registers contain the address of an operand or it can also act as a general-purpose register. An address register may be dedicated to a certain addressing mode.

4. Condition Code: Condition codes are the flag bits which are the part of the control register. The condition codes are set by the processor as a result of an operation and they are implicitly read through the machine instruction. The programmers are not allowed to alter the conditional codes. Generally, the condition codes are tested during conditional branch operation.

### Control and Status Registers

The control and status register holds the address or data that is important to control the processor's operation. The most important thing is that these registers are not visible to the users. Below we will discuss all the control and status registers are essential for the execution of an instruction.
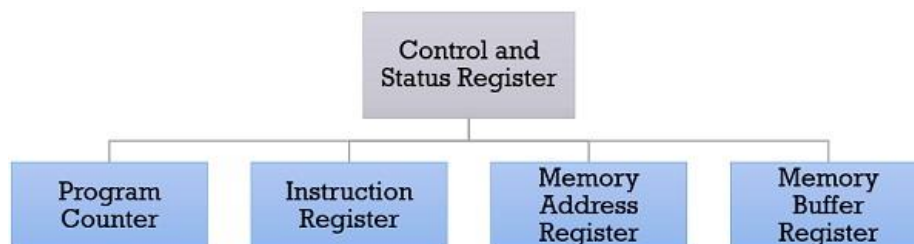
1. Program Counter: The program counter is a processor register that holds the address of the instruction that has to be executed next. It is a processor which updates the program counter with the address of the next instruction to be fetched for execution.

2. Instruction Register: Instruction register has the instruction that is currently fetched. It helps in analyzing the opcode and operand present in the instruction.

3. Memory Address Register (MAR): Memory address register holds the address of a memory location.

4. Memory Buffer Register (MBR): The memory buffer register holds the data that has to be written to a memory location or it holds the data that is recently been read.

The memory address registers (MAR) and memory buffer registers (MBR) are used to move the data between processor and memory.

## INSTRUCTION FORMAT:

- **Instruction format** describes the internal structures (layout design) of the bits of an instruction, in terms of its constituent parts.
- An **Instruction format** must include an **opcode**, and **address** is dependent on an availability of particular operands.
- The format can be **implicit or explicit** which will indicate the addressing mode for each operand.
  Designing of an **Instruction format** is very complex. As we know a computer uses a variety of instructional. There are many designing issues which affect the instructional design, some of them are given are below:
  **Instruction length:** It is a most basic issue of the format design. A longer will be the instruction it means more time is needed to fetch the instruction.
  **Memory size:** If larger memory range is to be addressed then more bits will be required in the address field.
  **Memory organization:** If the system supports the virtual memory then memory range which needs to be addressed by the instruction, is larger than the physical memory.
  **Memory transfer length:** Instruction length should be equal to the data bus length or it should be multiple of it.
  **Instruction formats** are classified into 5 types based on the type of the CPU organization. CPU organization is divided into three types based on the availability of the ALU operands, which are as follows here:
  1) STACK CPU: In this organization, ALU operands are performed only on a stack data. This means that both of the ALU operations are always required in the stack. The computable instruction format of STACK CPU is Zero Address Instruction Format.

```
┌──────────┐
│ OPCODE   │
└──────────┘
```

2) Accumulator CPU: In this organization, one of the ALU operands is always present in the accumulator. The computable instruction format of Accumulator CPU is One Address Instruction Format.

```
┌──────────┬──────────┐
│ OPCODE   │ ADDRESS  │
└──────────┴──────────┘
```

3) General Register CPU:  Based on the number of the registers possible in the processors, the architecture is divided into two types:

   i.   Register-Memory references CPU
   ii.  Register-Register references CPU

   i)  Register-Memory Reference CPU:  In this architecture, processors support less number of registers. Therefore register file size is small. In this organization, the first ALU operand is always required in the register. The computable instruction format of the register to memory reference CPU is Two Address Instruction Format.

```
┌──────────┬───────────┬───────────┐
│ OPCODE   │ ADDRESS 1 │ ADDRESS 2 │
└──────────┴───────────┴───────────┘
```

   ii) Register-Register Reference CPU: In this architecture, processors support number of registers, therefore, register file size is large. In this organization, ALU operands are performed only on a registers data that means both of the ALU operands are required in the register. The computable instruction format of Register-Register Reference CPU is Three Address Instruction Format.

```
┌──────────┬───────────┬───────────┬──────────┐
│ OPCODE   │ ADDRESS 1 │ ADDRESS 2 │ ADDRESS  │
│          │           │           │    3     │
└──────────┴───────────┴───────────┴──────────┘
```
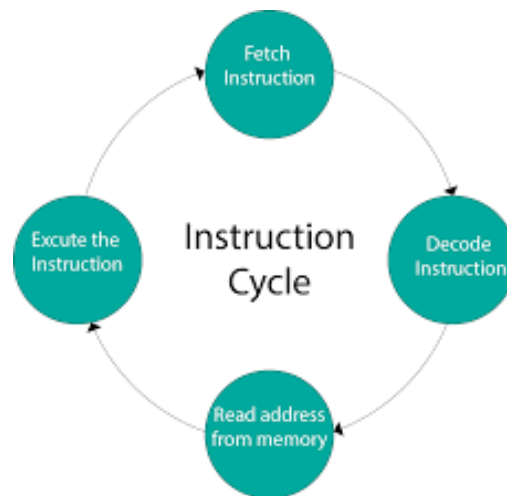
**INSTRUCTION SET:**
- An instruction set (used in what is called ISA or Instruction Set Architecture) is code that the computer processor (CPU) can understand. The language is 1s and 0s, or machine language. It contains instructions or tasks that control the movement of bits and bytes within the processor.
- The instruction set consists of a limited set of unique codes that let the processor know what to do next, along with some basic rules of how to express them.
  - ✓ Instruction length (this can vary)
  - ✓ Opcodes  (the command to be carried out)
  - ✓ Operands (what the command will operate on)
  - ✓ Registers (internal locations - limited in number and ability, but quick to access)

✓ Memory (external storage - a larger and more versatile number of locations, but slower to access)

## INSTRUCTION CYCLE:

- A program residing in the memory unit of a computer consists of a sequence of instructions. These instructions are executed by the processor by going through a cycle for each instruction.



- In a basic computer, each instruction cycle consists of the following phases:
  - Fetch instruction from memory.
  - Decode the instruction.
  - Read the effective address from memory.
  - Execute the instruction.

## MEMORY UNIT:

- Memory is a unit in computer that is capable of storing programs or data on a temporary or a permanent basis.
  Memory unit has two basic operations:
  read and write.
- Read operation reads the previously stored data
- Write operation stores new data in the memory
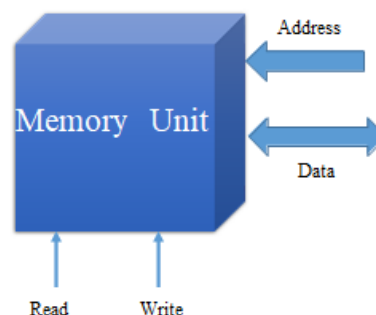
**SECONDARY MEMORY:**
- Secondary memory is also referred to as auxiliary memory
- It is a non-volatile memory that extends the storage capacity of the computer
- It is slow, but are cheaper compared to that of the primary memory and have a greater capacity
- Information are retained even when the power is turned off.
- It is classified into magnetic storage devices, optical storage devices, and flash memory devices
- Floppy disk drive, hard disk drive, USB flash disk, etc., are some the examples of secondary memory

**Solid-state drive (SSD):**

A solid-state drive (SSD) is a solid-state storage device that uses integrated circuit assemblies as memory to store data persistently. It is also sometimes called a solid-state device or a solid-state disk

SSDs lack the physical spinning disks and movable read-write heads used by conventional electromechanical storage such as hard drives ("HDD") or floppy disks. Because of this, it is more portable, and produces less heat compared to traditional magnetic storage devices. Less heat means that components last longer.

Solid state storage is also faster than traditional hard disk drives because the data is stored electrically in silicon chips called cells.

Within the cells, the binary data is stored by holding an electrical current in a transistor with an on / off mode.

**Magnetic devices:**

Magnetic devices such as hard disk drives use magnetic fields to magnetise tiny individual sections of a metal spinning disk. Each tiny section represents one bit. A magnetised section represents a binary '1' and a demagnetised section represents a binary '0'. These sections are so tiny that disks can contain terabytes (TB) of data.

As the disk is spinning, a read/write head moves across its surface. To write data, the head magnetises or demagnetises a section of the disk that is spinning under it. To read data, the head makes a note of whether the section is magnetised or not.

Magnetic devices are fairly cheap, high in capacity and durable. However, they are susceptible to damage if dropped. They are also vulnerable to magnetic fields - a strong magnet might possibly erase the data the device holds.

**Optical devices:**

Optical devices use a laser to scan the surface of a spinning disc made from metal and plastic. The disc surface is divided into tracks, with each track containing many flat areas and hollows. The flat areas are known as lands and the hollows as pits.

When the laser shines on the disc surface, lands reflect the light back, whereas pits scatter the laser beam. A sensor looks for the reflected light. Reflected light - land - represents a binary '1', and no reflection - pits - represents a binary '0'.

Examples:

1. A *compact disc*, or CD, is a thin circular piece of equipment that can be used to store data, including graphics and music. It was developed in the late 1970s and was the first mainstream way to digitally store music. Standard CDs are 12 centimeters, or about 4.7 inches, in diameter.

    a. CD-ROM drives could read CDs but not write them.

    b. *CD-RW*, for CD-rewritable. These discs can be written more than once, so if one has data on it, it can be rewritten with a new set of files or music.

2. Digital versatile discs, or DVD_s: They could also be used to store files and held up to about 8.5 gigabytes worth of data, a dramatic increase from CDs.

3. Blu-ray was first introduced at the CES on January 4, 2006, and can store up to 25 GB single-layer disc and 50 GB on a dual-layer disc, each disc being the same size as a standard CD. Blu-ray technology gets its name from the blue-violet laser that is used to read Blu-ray disks. a blue laser permits more information to be stored at a greater density.

**INPUT AND OUTPUT DEVICES:**

**1. OMR**

Definition:

Optical mark recognition (also called optical mark reading and OMR) is the process of capturing human-marked data from document forms such as surveys and tests. They are used to read questionnaires, multiple choice examination papers in the form of lines or shaded areas.

Working:

The OMR device uses a dedicated scanner that focuses a beam of light onto the concerned area. Since black spots reflect lesser light than white areas, the scanner detects them. Then, a digital blue print of the paper is prepared by different computing algorithms.

Nowadays, we also use Digital Image Processing techniques for OMR. In that case an image of the page is taken, algorithms (mainly differential techniques) are run to extract the required contrasts (for e.g. black bubbles or horizontal lines) and finally computed further.

Applications

There are many other applications for OMR, for examples:

- In the process of institutional research
- Community surveys

- Consumer surveys
- Tests and assessments
- Evaluations and feedback
- Data compilation
- Product evaluation

Advantages:
OMR scanning is cost effective
Easy to implement and support

Disadvantages:
Collecting large amount of text OMR complicates the data collection.
Document for mark reader are complicated to design

## 2. OCR

Definition:

OCR involves examining the text of a document and translating the characters into code that can be used for data processing. OCR is sometimes also referred to as text recognition.

OCR systems are made up of a combination of hardware and software that is used to convert physical documents into machine-readable text.

Working:

The first step of OCR is using a scanner to process the physical form of a document. Once all pages are copied, OCR software converts the document into a two-color, or black and white, version. The scanned-in image or bitmap is analyzed for light and dark areas, where the dark areas are identified as characters that need to be recognized and light areas are identified as background.

The dark areas are then processed further to find alphabetic letters or numeric digits. OCR programs can vary in their techniques, but typically involve targeting one character, word or block of text at a time. Characters are then identified using one of two algorithms:

1. Pattern recognition- OCR programs are fed examples of text in various fonts and formats which are then used to compare, and recognize, characters in the scanned document.

2. Feature detection- OCR programs apply rules regarding the features of a specific letter or number to recognize characters in the scanned document. Features could include the number of angled lines, crossed lines or curves in a character for comparison. For example, the capital letter "A" may be stored as two diagonal lines that meet with a horizontal line across the middle.

When a character is identified, it is converted into an ASCII code that can be used by computer systems to handle further manipulations.

Applications:

- Scanning printed documents into versions that can be edited with word processors, like Microsoft Word or Google Docs.

- Automating data entry, extraction and processing.

- Recognizing text, such as license plates, with a camera or software.

Advantages:
- Being able to edit and search documents.
- Saved time, decreased errors and minimized effort.

Disadvantages:
- OCR systems are expensive.
- Images produced by scanner consume lot of memory space.

3. **MICR**

Definition:

MICR (magnetic ink character recognition) is a technology used to verify the legitimacy or originality of paper documents, especially checks. Special ink, which is sensitive to magnetic fields, is used in the printing of certain characters on the original documents. Information can be encoded                in                the                magnetic                characters. The use of MICR can enhance security and minimize the losses caused by some types of crime.

Working:

Each check is printed with a series of characters on the bottom of the document. These characters are printed with a special type of ink that has iron oxide.

As the check enters the scan path, the magnetic ink passes over a magnet in the scanner to "charge" the ink before it passes over the MICR read head. The MICR read head is a device built into the scanner designed to read the magnetic signal emitted by the MICR ink characters on the check.

Each character produces a unique waveform which is read and translated by the MICR read head.

Two major fonts E-13B and CMC-7

Applications:

- Widely used in Banking industry

Advantages:
- Readability and Security
- Few Errors

Disadvantages:
- Expensive Equipment
- High Standards

4. **Scanner:**

Definition:

A scanner is an electronic device which can capture images from physical items and convert them into digital formats, which in turn can be stored in a computer, and viewed or modified using software applications.

Different types of scanners are available with different resolutions.

Working:

The basic principle of a scanner is to analyze an image and process it in some way. Image and text capture (optical character recognition or OCR) allow you to save information to a file on your computer. You can then alter or enhance the image, print it out

Applications:

- Copying
- Archiving

Advantages:

- Old materials into digital one.
- retouch and repair old photographs digitally

Disadvantages:

- Scanned Output Quality Can Vary
- Scanner Maintenance Can Be Expensive

5. **Mouse:**

Definition:

is a hand-held pointing device that detects two-dimensional motion relative to a surface. This motion is typically translated into the motion of a pointer on a display, which allows a smooth control of the graphical user interface.

Working:

The ball rolls under its own weight and pushes against two plastic rollers linked to thin wheels. One of the wheels detects movements in an up-and-down direction (like the y-axis on graph/chart paper); the other detects side-to-side movements (like the x-axis on graph paper).

An optical mouse shines a bright light down onto the desk from an LED (light-emitting diode) mounted on the bottom of the mouse. The light bounces straight back up off the desk into a photocell(photoelectric cell), also mounted under the mouse, a short distance from the LED. The photocell has a lens in front of it that magnifies the reflected light, so the mouse can respond more precisely to your hand movements. As you push the mouse around your desk, the pattern of

reflected light changes, and the chip inside the mouse uses this to figure out how you're moving your hand.

Applications:

- A computer mouse enables its user to move a cursor smoothly
- Provides an easy drag and drop control

Advantages:

- Movement Flexibility
- Variety

Disadvantages:

- Wear and tear
- Excessive use can lead to health problems

6. **Modem**

Definition:

A modem is a network device that both modulates and demodulates analog carrier signals for encoding and decoding digital information for processing. Modems accomplish both of these tasks simultaneously and, for this reason, the term modem is a combination of "modulate" and "demodulate."

Working:

The computer at one end needs a modem to modulate its digital signals (add them on top of an analog telephone signal) so they can travel down the phone line just like the sound of one's voice. Once the signals have reached the other end, they have to pass through a second modem, which demodulates them (separates them out from the telephone signal and turns them back into digital form) so the ISP computer can understand them. When the ISP computer replies, it sends its signals through a modulator back down the line to the user. Then a demodulator turns the signals back into digital form which computer can understand.

Applications:

- Connecting users to the Internet
- Data Transfers

Advantages:

- Makes use of telephone lines
- Cost efficient

Disadvantages:

- Risks With Modems - vulnerable to malwares
- Choosing a Modem

**COMPUTER HARDWARE AND SOFTWARE:**

Computer Hardware:
- It includes physical components of computer system.
- It consists of electronic components like ICs, diodes, registers, crystals, boards, insulators, etc.
- Hardware design is based on architectural decisions to make it work over a range of environmental conditions and time.
- It is mostly constructed for all types of computer systems.
- The hardware can understand only low-level language or machine language.
- The hardware works only on binary codes 1's and 0's.
- The hardware consists of input devices, output devices, memory, etc.

Computer Software:
- It is a collection of programs to bring computer hardware system into operation.
- It includes numbers, alphabets, alphanumeric symbols, identifiers, keywords, etc.
- Software products evolve by adding new features to existing programs to support hardware.
- It will vary as per computer and its built-in functions and programming language.
- It is designed and developed by experienced programmers in high-level language.
- It is represented in any high-level language such as BASIC, COBOL, C, C++, JAVA, etc.
- The software is categorized as operating system, utilities, language processor, application software, etc.

**MACHINE LANGUAGE AND HIGH LEVEL LANGUAGE**

High Level Language:
- It is programmer friendly language.
- High level language is less memory efficient.
- It is easy to understand.
- It is simple to debug.
- It is simple to maintain.
- It is portable.
- It can run on any platform.
- It needs compiler or interpreter for translation.
- It is used widely for programming.

Machine Language:
- It is a machine friendly language.
- Low level language is high memory efficient.
- It is tough to understand.
- It is complex to debug comparatively.
- It is complex to maintain comparatively.

- It is non-portable.
- It is machine-dependent.
- It needs assembler for translation.
- It is not commonly used now-a-days in programming.

## APPLICATION SOFTWARE

- Application software is commonly defined as any program or number of programs designed for end-users. That's it, in a nutshell.
- Examples of application software include items like Microsoft Word, Microsoft Excel, or any of the web browsers used navigate the Internet.

Types of Application Software
  - o Utility software: This could include firewall utilities and antivirus applications.
  - o Integrated software: Software that does more than one thing, or includes different bundled applications.
  - o Specific application software: This would be a single application developed for one defined purpose that is not a utility.

## COMPUTER PROGRAM

- A computer program is a list of instructions that tell a computer what to do.
- A computer program is written in a programming language.
- A computer program is stored as a file on the computer's hard drive. When the user runs the program, the file is read by the computer, and the processor reads the data in the file as a list of instructions. Then the computer does what the program tells it to do.
- A program is prepared by first formulating a task and then expressing it in an appropriate computer language

## OPERATING SYSTEM

- An Operating system (OS) is a software which acts as an interface between the end user and computer hardware. Every computer must have at least one OS to run other programs.
- The OS helps you to communicate with the computer without knowing how to speak the computer's language.

### Features of Operating System

- Protected and supervisor mode
- Allows disk access and file systems Device drivers Networking Security
- Program Execution
- Memory management Virtual Memory Multitasking
- Handling I/O operations
- Manipulation of the file system
- Error Detection and handling
- Resource allocation
- Information and Resource Protection

**Functions of an Operating System**
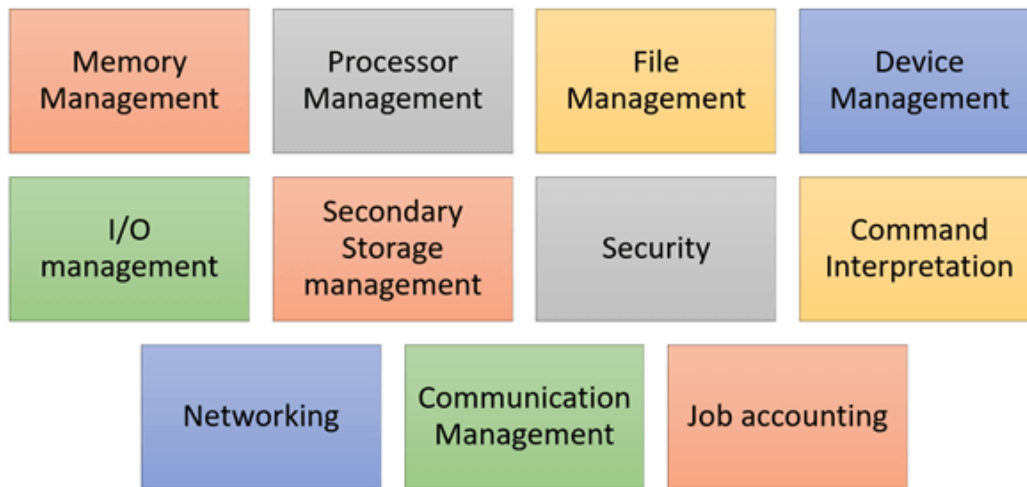


- o **Process management**:- Process management helps OS to create and delete processes. It also provides mechanisms for synchronization and communication among processes.
- o **Memory management:-** Memory management module performs the task of allocation and de-allocation of memory space to programs in need of this resources.
- o **File management**:- It manages all the file-related activities such as organization storage, retrieval, naming, sharing, and protection of files.
- o **Device Management**: Device management keeps tracks of all devices. This module also responsible for this task is known as the I/O controller. It also performs the task of allocation and de-allocation of the devices.
- o **I/O System Management:** One of the main objects of any OS is to hide the peculiarities of that hardware devices from the user.
- o **Secondary-Storage Management**: Systems have several levels of storage which includes primary storage, secondary storage, and cache storage. Instructions and data must be stored in primary storage or cache so that a running program can reference it.
- o **Security**: Security module protects the data and information of a computer system against malware threat and authorized access.
- o **Command interpretation**: This module is interpreting commands given by the and acting system resources to process that commands.
- o **Networking:** A distributed system is a group of processors which do not share memory, hardware devices, or a clock. The processors communicate with one another through the network.
- o **Job accounting**: Keeping track of time & resource used by various job and users.
- o **Communication management**: Coordination and assignment of compilers, interpreters, and another software resource of the various users of the computer systems.

**Types of Operating System**
- • Batch Operating System
- • Multitasking/Time Sharing OS

- Multiprocessing OS
- Real Time OS
- Distributed OS
- Network OS
- Mobile OS

o **Batch Operating System**
- Some computer processes are very lengthy and time-consuming. To speed the same process, a job with a similar type of needs are batched together and run as a group.
- The user of a batch operating system never directly interacts with the computer. In this type of OS, every user prepares his or her job on an offline device like a punch card and submit it to the computer operator.

o **Multi-Tasking/Time-sharing Operating systems**
- Time-sharing operating system enables people located at a different terminal(shell) to use a single computer system at the same time. The processor time (CPU) which is shared among multiple users is termed as time sharing.

o **Real time OS**
- A real time operating system time interval to process and respond to inputs is very small. Examples: Military Software Systems, Space Software Systems.

o **Distributed Operating System**
- Distributed systems use many processors located in different machines to provide very fast computation to its users.

o **Network Operating System**
- Network Operating System runs on a server. It provides the capability to serve to manage data, user, groups, security, application, and other networking functions.

o **Mobile OS**
- Mobile operating systems are those OS which is especially that are designed to power smartphones, tablets, and wearables devices.
- Some most famous mobile operating systems are Android and iOS, but others include BlackBerry, Web, and watchOS.

## COMPUTER VIRUS, ANTIVIRUS AND COMPUTER SECURITY

Computer Virus:
- A computer virus is "malware attached to another program (such as a document), which can replicate and spread after an initial execution on a target system where human interaction is required. Many viruses are harmful and can destroy data, slow down system resources, and log keystrokes."

1. Resident Virus: Resident viruses set up shop in your RAM and meddle with your system operations. They're so sneaky that they can even attach themselves to your anti-virus software files.

2. Multipartite Virus: This virus infects the entire system. Multipartite viruses spread by performing unauthorized actions on your operating system, folders, and programs.

3. Direct Action: This virus targets a specific file type, most commonly executable files (.exe), by replicating and infecting files. Due to its targeted nature, this virus type is one of the easier ones to detect and remove.

4. Browser Hijacker: Easily detected, this virus type infects your browser and redirects you to malicious websites.

5. Overwrite Virus: Like the name implies, overwrite viruses overwrite file content to infect entire folders, files, and programs.

6. Web Scripting Virus: This sneaky virus disguises itself in the coding of links, ads, images, videos, and site code. It can infect systems when users download malicious files or visit malicious websites.

7. File Infector: By targeting executable files (.exe), file infector viruses slow down programs and damage system files when a user runs them.

8. Network Virus: Network viruses travel through network connections and replicate themselves through shared resources.

9. Boot Sector Virus: One of the easier viruses to avoid, this virus hides out in a file on a USB drive or email attachment. When activated, it can infect the system's master boot record to damage the system.

Computer Antivirus:
- Antivirus software helps protect your computer against malware and cybercriminals. Antivirus software looks at data — web pages, files, software, applications — traveling over the network to your devices.
- It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior.
- Examples: Kaspersky, McAfee, Norton. AVG and Panda

Computer Security:
- Computer security, also known as cyber security or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.
- It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

**INTRODUCTION TO MICROPROCESSORS – RISC AND CISC**
**CISC:**
  o   A large number of instructions are present in the architecture.

- o Some instructions with long execution times.
- o Variable-length encodings of the instructions.
- o Example: IA32 instruction size can range from 1 to 15 bytes.
- o Multiple formats are supported for specifying operands.
- o CISC supports array.
- o Arithmetic and logical operations can be applied to both memory and register operands.
- o Implementation programs are hidden from machine level programs. The ISA provides a clean abstraction between programs and how they get executed.
- o Condition codes are used.

## RISC:
- o Very fewer instructions are present. The number of instructions are generally less than 100.
- o No instruction with a long execution time due to very simple instruction set.
- o Fixed-length encodings of the instructions are used.
- o Example: In IA32, generally all instructions are encoded as 4 bytes.
- o Simple addressing formats are supported.
- o RISC does not supports array.
- o Arithmetic and logical operations only use register operands. Memory referencing is only allowed by load and store instructions, i.e. reading from memory into a register and writing from a register to memory respectively.
- o Implementation programs exposed to machine level programs. Few RISC machines do not allow specific instruction sequences.
- o No condition codes are used.

***