A computer is a programmable electronic device that accepts raw data as input and processes it with a set of instructions (a program) to produce the result as output. It renders output just after performing mathematical and logical operations and can save the output for future use. It can process numerical as well as non-numerical calculations. A computer is designed to execute applications and provides a variety of solutions through integrated hardware and software components. It works with the help of programs and represents the decimal numbers through a string of binary digits. It also has a memory that stores the data, programs, and result of processing.

Dr.R. Jayaprakash has done his Ph.D in Computer Science from Bharathiar University in 2021. He did his M.Phil in 2017 and MCA from Anna University. He is currently working as an Assistant Professor in Nallamuthu Gounder Mahalingam College, Pollachi.

9 7 8 6 2 0 4 7 4 3 9 6 7

Dr. R. Jayaprakash

Fundamentals of Computer

Basic Level

LAP LAMBERT Academic Publishing

Dr. R. Jayaprakash

Fundamentals of Computer

Dr. R. Jayaprakash

Fundamentals of Computer

Basic Level

LAP LAMBERT Academic Publishing

Imprint

Cover image: www.ingimage.com

Publisher:
LAP LAMBERT Academic Publishing
is a trademark of
Dodo Books Indian Ocean Ltd., member of the OmniScriptum S.R.L Publishing group
str. A.Russo 15, of. 61, Chisinau-2068, Republic of Moldova Europe
Printed at: see last page
ISBN: 978-620-4-74396-7

FUNDAMENTALS OF COMPUTER

CHAPTER – I

Basic Things of Computer

What is Computer?

Computer is an *electronic device* i.e. used *to work with information or compute*. It is derived from the Latin word "computare" which means to calculate.

A computer is a programmable electronic device that accepts raw data as input and processes it with a set of instructions (a program) to produce the result as output. It renders output just after performing mathematical and logical operations and can save the output for future use. It can process numerical as well as non-numerical calculations.

A computer is designed to execute applications and provides a variety of solutions through integrated hardware and software components. It works with the help of programs and represents the decimal numbers through a string of binary digits. It also has a memory that stores the data, programs, and result of processing. The components of a computer such as machinery that includes wires, transistors, circuits, hard disk are called hardware. Whereas, the programs and data are called software.

It is believed that the Analytical Engine was the first computer which was invented by Charles Babbage in 1837. It used punch cards as read-only memory. Charles Babbage is also known as the father of the computer.

Parts of Computer

- **Processor:** It executes instructions from software and hardware.
- **Memory:** It is the primary memory for data transfer between the CPU and storage.
- **Motherboard:** It is the part that connects all other parts or components of a computer.
- **Storage Device:** It permanently stores the data, e.g., hard drive.

- **Input Device:** It allows you to communicate with the computer or to input data, e.g., a keyboard.
- **Output Device:** It enables you to see the output, e.g., monitor.

Types of Computer

1. Micro Computer
2. Mini Computer
3. Mainframe Computer
4. Super Computer
5. Workstations

1. Micro Computer

It is a single-user computer which has less speed and storage capacity than the other types. It uses a microprocessor as a CPU. The first microcomputer was built with 8-bit microprocessor chips. The common examples of microcomputers include laptops, desktop computers, personal digital assistant (PDA), tablets, and smartphones. Microcomputers are generally designed and developed for general usage like browsing, searching for information, internet, MS Office, social media, etc.

2. Mini Computer

Mini-computers are also known as "Midrange Computers." They are not designed for a single. They are multi-user computers designed to support multiple users simultaneously. So, they are generally used by small businesses and firms. Individual departments of a company use these computers for specific purposes. For example, the admission department of a University can use a Mini-computer for monitoring the admission process.

3. Mainframe Computer

It is also a multi-user computer capable of supporting thousands of users simultaneously. They are used by large firms and government organizations to run their business operations as they can

store and process large amounts of data. For example, Banks, universities, and insurance companies use mainframe computers to store the data of their customers, students, and policyholders, respectively.

4. Super Computer

Super-computers are the fastest and most expensive computers among all types of computers. They have huge storage capacities and computing speeds and thus can perform millions of instructions per second. The super-computers are task-specific and thus used for specialized applications such as large-scale numerical problems in scientific and engineering disciplines including applications in electronics, petroleum engineering, weather forecasting, medicine, space research and more. For example, NASA uses supercomputers for launching space satellites and monitoring and controlling them for space exploration.

5. Work stations

It is a single-user computer. Although it is like a personal computer, it has a more powerful microprocessor and a higher-quality monitor than a microcomputer. In terms of storage capacity and speed, it comes between a personal computer and minicomputer. Work stations are generally used for specialized applications such as desktop publishing, software development, and engineering designs.

Benefits of Using a Computer:

- **Increases your productivity:** A computer increases your productivity. For example, after having a basic understanding of a word processor, you can create, edit, store, and print the documents easily and quickly.
- **Connects to the Internet:** It connects you to the internet that allows you to send emails, browse content, gain information, use social media platforms, and more. By connecting to the internet, you can also connect to your long-distance friends and family members.
- **Storage:** A computer allows you to store a large amount of information, e.g., you can store your projects, ebooks, documents, movies, pictures, songs, and more.

- **Organized Data and Information:** It not only allows you to store data but also enables you to organize your data. For example, you can create different folders to store different data and information and thus can search for information easily and quickly.
- **Improves your abilities:** It helps write good English if you are not good at spelling and grammar. Similarly, if you are not good at math, and don't have a great memory, you can use a computer to perform calculations and store the results.
- **Assist the physically challenged:** It can be used to help the physically challenged, e.g., Stephen Hawking, who was not able to speak used computer to speak. It also can be used to help blind people by installing special software to read what is on the screen.
- **Keeps you entertained:** You can use the computer to listen to songs, watch movies, play games and more.

The computer has become a part of our life. There are plenty of things that we do in a day are dependent on a computer. Some of the common examples are as follows:

1. **ATM:** While withdrawing cash from an ATM, you are using a computer that enables the ATM to take instructions and dispense cash accordingly.
2. **Digital currency:** A computer keeps a record of your transactions and balance in your account and the money deposited in your account in a bank is stored as a digital record or digital currency.
3. **Trading:** Stock markets use computers for day to day trading. There are many advanced algorithms based on computers that handle trading without involving humans.
4. **Smartphone:** The smartphone that we use throughout the day for calling, texting, browsing is itself a computer.
5. **VoIP:** All voice over IP communication (VoIP) is handled and done by computers.

Generations of Computers

A generation of computers refers to the specific improvements in computer technology with time. In 1946, electronic pathways called circuits were developed to perform the counting. It replaced the gears and other mechanical parts used for counting in previous computing machines.

In each new generation, the circuits became smaller and more advanced than the previous generation circuits. The miniaturization helped increase the speed, memory and power of computers. There are five generations of computers which are described below;

First Generation Computers

The first generation (1946-1959) computers were slow, huge and expensive. In these computers, vacuum tubes were used as the basic components of CPU and memory. These computers were mainly depended on batch operating system and punch cards. Magnetic tape and paper tape were used as output and input devices in this generation;

Some of the popular first generation computers are;

- **ENIAC** (Electronic Numerical Integrator and Computer)
- **EDVAC** (Electronic Discrete Variable Automatic Computer)
- **UNIVACI**(Universal Automatic Computer)
- **IBM-701**
- **IBM-650**

Second Generation Computers

The second generation (1959-1965) was the era of the transistor computers. These computers used transistors which were cheap, compact and consuming less power; it made transistor computers faster than the first generation computers.

In this generation, magnetic cores were used as the primary memory and magnetic disc and tapes were used as the secondary storage. Assembly language and programming languages like COBOL and FORTRAN, and Batch processing and multiprogramming operating systems were used in these computers.

Some of the popular second generation computers are;

- **IBM 1620**

- **IBM 7094**
- **CDC 1604**
- **CDC 3600**
- **UNIVAC 1108**

Third Generation Computers

The third generation computers used integrated circuits (ICs) instead of transistors. A single IC can pack huge number of transistors which increased the power of a computer and reduced the cost. The computers also became more reliable, efficient and smaller in size. These generation computers used remote processing, time-sharing, multi programming as operating system. Also, the high-level programming languages like FORTRON-II TO IV, COBOL, PASCAL PL/1, ALGOL-68 were used in this generation.

Some of the popular third generation computers are;

- **IBM-360 series**
- **Honeywell-6000 series**
- **PDP(Personal Data Processor)**
- **IBM-370/168**
- **TDC-316**

Fourth Generation Computers

The fourth generation (1971-1980) computers used very large scale integrated (VLSI) circuits; a chip containing millions of transistors and other circuit elements. These chips made this generation computers more compact, powerful, fast and affordable. These generation computers used real time, time sharing and distributed operating system. The programming languages like C, C++, DBASE were also used in this generation.

Some of the popular fourth generation computers are;

- **DEC 10**

- **STAR 1000**
- **PDP 11**
- **CRAY-1(Super Computer)**
- **CRAY-X-MP(Super Computer)**

Fifth Generation Computers

In fifth generation (1980-till date) computers, the VLSI technology was replaced with ULSI (Ultra Large Scale Integration). It made possible the production of microprocessor chips with ten million electronic components. This generation computers used parallel processing hardware and AI (Artificial Intelligence) software. The programming languages used in this generation were C, C++, Java, .Net, etc.

Some of the popular fifth generation computers are;

- **Desktop**
- **Laptop**
- **Note Book**
- **Ultra Book**
- **Chrome Book**

On the basis of data handling capabilities, the computer is of *three* types:

- Analogue Computer
- Digital Computer
- Hybrid Computer

1) Analogue Computer

Analogue computers are designed to process analogue data. Analogue data is continuous data that changes continuously and cannot have discrete values. We can say that analogue computers are used where we don't need exact values always such as speed, temperature, pressure and current.

Analogue computers directly accept the data from the measuring device without first converting it into numbers and codes. They measure the continuous changes in physical quantity and generally render output as a reading on a dial or scale. Speedometer and mercury thermometer are examples of analogue computers.

2) Digital Computer

Digital computer is designed to perform calculations and logical operations at high speed. It accepts the raw data as input in the form of digits or binary numbers (0 and 1) and processes it with programs stored in its memory to produce the output. All modern computers like laptops, desktops including smartphones that we use at home or office are digital computers.

3) Hybrid Computer

Hybrid computer has features of both analogue and digital computer. It is *fast like an analogue* computer and has memory and *accuracy like digital computers*. It can process both continuous and discrete data. It accepts analogue signals and converts them into digital form before processing. So, it is widely used in specialized applications where both analogue and digital data is processed.

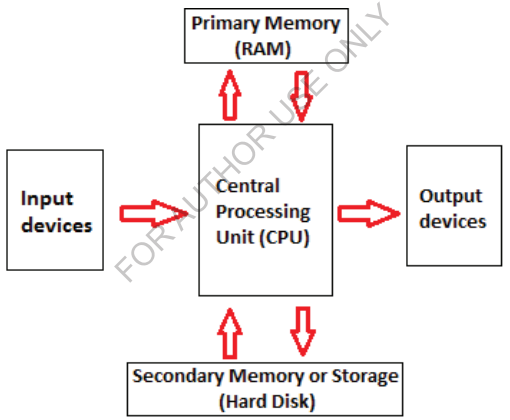
CHAPTER - II

Computer Components

Computer Components

There are 5 main computer components that are given below:

- Input Devices
- CPU
- Output Devices
- Primary Memory
- Secondary Memory



The operations of computer components are given below:

1) Inputting: It is the process of entering raw data, instructions and information into the computer. It is performed with the help of input devices.

2) Storing: The computer has primary memory and secondary storage to store data and instructions. It stores the data before sending it to CPU for processing and also stores the processed data before displaying it as output.

3) Processing: It is the process of converting the raw data into useful information. This process is performed by the CPU of the computer. It takes the raw data from storage, processes it and then sends back the processed data to storage.

4) Outputting: It is the process of presenting the processed data through output devices like monitor, printer and speakers.

5) Controlling: This operation is performed by the control unit that is part of CPU. The control unit ensures that all basic operations are executed in a right manner and sequence.

Input Devices

Input device enables the user to send data, information, or control signals to a computer. The Central Processing Unit (CPU) of a computer receives the input and processes it to produce the output.

Some of the popular input devices are:

1. Keyboard
2. Mouse
3. Scanner

Keyboard

The keyboard is a basic input device that is used to enter data into a computer or any other electronic device by pressing keys. It has different sets of keys for letters, numbers, characters, and functions. Keyboards are connected to a computer through USB or a Bluetooth device for wireless communication.

Mouse

The mouse is a hand-held input device which is used to move cursor or pointer across the screen. It is designed to be used on a flat surface and generally has left and right button and a scroll wheel between them. Laptop computers come with a touchpad that works as a mouse. It lets you

control the movement of cursor or pointer by moving your finger over the touchpad. Some mouse comes with integrated features such as extra buttons to perform different buttons.

Scanner

The scanner uses the pictures and pages of text as input. It scans the picture or a document. The scanned picture or document then converted into a digital format or file and is displayed on the screen as an output. It uses optical character recognition techniques to convert images into digital ones.

A joystick is also a pointing input device like a mouse. It is made up of a stick with a spherical base. The base is fitted in a socket that allows free movement of the stick. The movement of stick controls the cursor or pointer on the screen.

The first joystick was invented by C. B. Mirick at the U.S. Naval Research Laboratory. A joystick can be of different types such as displacement joysticks, finger-operated joysticks, hand operated, isometric joystick, and more. In joystick, the cursor keeps moving in the direction of the joystick unless it is upright, whereas, in mouse, the cursor moves only when the mouse moves.

Output device

The output device displays the result of the processing of raw data that is entered in the computer through an input device. There are a number of output devices that display output in different ways such as text, images, hard copies, and audio or video.

Monitor

The monitor is the display unit or screen of the computer. It is the main output device that displays the processed data or information as text, images, audio or video.

Printer

A printer produces hard copies of the processed data. It enables the user, to print images, text or any other information onto the paper.

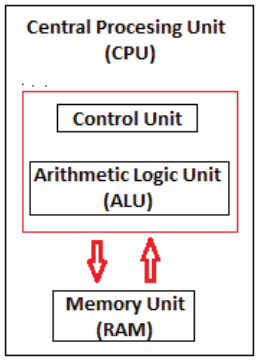
Central Processing Unit (CPU)

A Central Processing Unit is also called a processor, central processor, or microprocessor. It carries out all the important functions of a computer. It receives instructions from both the hardware and active software and produces output accordingly. It stores all important programs like operating systems and application software. CPU also helps Input and output devices to communicate with each other. Owing to these features of CPU, it is often referred to as the brain of the computer.

CPU is installed or inserted into a CPU socket located on the motherboard. Furthermore, it is provided with a heat sink to absorb and dissipate heat to keep the CPU cool and functioning smoothly.

Generally, a CPU has three components:

- ALU (Arithmetic Logic Unit)
- Control Unit
- Memory or Storage Unit



Control Unit: It is the circuitry in the control unit, which makes use of electrical signals to instruct the computer system for executing already stored instructions. It takes instructions from memory and then decodes and executes these instructions. So, it controls and coordinates the functioning of all parts of the computer. The Control Unit's main task is to maintain and regulate the flow of information across the processor. It does not take part in processing and storing data.

ALU: It is the arithmetic logic unit, which performs arithmetic and logical functions. Arithmetic functions include addition, subtraction, multiplication division, and comparisons. Logical functions mainly include selecting, comparing, and merging the data. A CPU may contain more than one ALU. Furthermore, ALUs can be used for maintaining timers that help run the computer.

Memory or Storage Unit/ Registers: It is called Random access memory (RAM). It temporarily stores data, programs, and intermediate and final results of processing. So, it acts as a temporary storage area that holds the data temporarily, which is used to run the computer.

Hardware

Hardware, which is abbreviated as HW, refers to all physical components of a computer system, including the devices connected to it. You cannot create a computer or use software without using hardware. The screen on which you are reading this information is also a hardware.

Software

Software, which is abbreviated as SW or S/W, is a set of programs that enables the hardware to perform a specific task. All the programs that run the computer are software. The software can be of three types: system software, application software, and programming software.

Operating System

As the name suggests, an operating system is a type of software without which you cannot operate or run a computer. It acts as an intermediary or translation system between computer hardware and application programs installed on the computer. In other words, you cannot directly use computer programs with computer hardware without having a medium to establish a connection between them.

Besides this, it is also an intermediary between the computer user and the computer hardware as it provides a standard user interface that you see on your computer screen after you switch on your computer. For example, the Windows and the Mac OS are also operating systems that provide a graphical interface with icons and pictures to enable users to access multiple files and applications simultaneously.

So, although the operating system is itself a program or software, it allows users to run other programs or applications on the system. We can say that is works behind the scenes to run your computer.

Major Functions of Operating System:

- **Memory management**: It manages both the primary and secondary memory such as RAM, ROM, hard disk, pen drive, etc. It checks and decides the allocations and deallocation of memory space to different processes. When a user interacts with a system, the CPU is supposed to read or write operations, in this case, OS decides the amount of memory to be allocated for loading the program instructions and data into RAM. After this program is terminated, the memory area is again free and is ready to be allocated to other programs by the OS.
- **Processor Management**: It facilitates processor management, where it decides the order for the processes to access the processor as well as decides the processing time to be allocated for each process. Besides this, it monitors the status of processes, frees the processor when a process is executed then allocates it to a new process.
- **Device/ hardware management**: The operating system also contains drivers to manage devices. A driver is a type of translation software that allows the operating system to communicate with devices, and there are different drivers for different devices as each device speaks a different language.
- **Run software applications**: It offers the environment to run or use software applications developed to perform specific tasks, for example, Ms Word, Ms Excel, Photoshop, etc.
- **Data management**: It helps in data management by offering and displaying directories for data management. You can view and manipulate files, folders, e.g., you can move, copy, name, or rename, delete a file or a folder.
- **Evaluates the system's health**: It gives us an idea about the performance of the hardware of the system. For example, you can see how busy the CPU is, how fast the data is retrieved from the hard disk, etc.
- **Provides user interface**: It acts as an interface between the user and the hardware. It can be a GUI where you can see and click elements on the screen to perform various tasks. It enables you to communicate with the computer even without knowing the computer's language.
- **I/O management**: It manages the input output devices and makes the I/O process smooth and effective. For example, it receives the input provided by the user through an input

device and stores it in the main memory. Then it directs the CPU to process this input and accordingly provides the output through an output device such as a monitor.

- **Security**: It has a security module to protect the data or information stored in the memories of the computer against malware and unauthorized access. Thus, it not only manages your data but also helps to protect it.
- **Time Management**: It helps CPU in time management. The Kernel OS keeps checking the frequency of processes that requests CPU time. When two or more processes that are equally important compete for the CPU time, then the CPU time is sliced into segments and allocated to these processes in a round-robin fashion to prevent a single process from monopolizing the CPU.
- **Deadlock Prevention**: Sometimes a resource that is supposed to be shared by two or more processes is held by one process due to which the resource cannot continue. This situation is known as deadlock. The OS does not let this situation arise by carefully distributing the resources among the different processes.

Computer Memory

The computer memory holds the data and instructions needed to process raw data and produce output. The computer memory is divided into large number of small parts known as cells. Each cell has a unique address which varies from 0 to memory size minus one.

Computer memory is of two types: Volatile (RAM) and Non-volatile (ROM). The secondary memory (hard disk) is referred as storage not memory.

But, if we categorize memory on behalf of space or location, it is of four types:

- Register memory
- Cache memory
- Primary memory
- Secondary memory

Computer Network

A network set up by connecting two or more computers and other supporting hardware devices through communication channels is called a computer network. It enables computers to communicate with each other and to share commands, data, etc., including the hardware and software resources.

Uses of Computer Network:

- It allows you to share resources such as printers, scanners, etc.
- You can share expensive software and database among network users.
- It facilitates communications from one computer to another computer.
- It allows the exchange of data and information among users through a network.

Popular Computer Networks:

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

Computer Virus

Computer viruses are unwanted software programs or pieces of code that interfere with the functioning of the computer. They spread through contaminated files, data, and insecure networks. Once it enters your system, it can replicate to produce copies of itself to spread from one program to another program and from one infected computer to another computer. So, we can say that it is a self-replicating computer program that interferes with the functioning of the computer by infecting files, data, programs, etc.

There are many antiviruses, which are programs that can help you protect your machine from viruses. It scans your system and cleans the viruses detected during the scan. Some of the popular antiviruses include Avast, Quickheal, McAfee, Kaspersky, etc.

Internet

Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.

Intranet

The intranet is a private network that belongs to a particular organization. It is designed for the exclusive use of an organization and its associates, such as employees, customers, and other authorized people. It offers a secure platform to convey information and share data with authorized users. Confidential information, database, links, forms, and applications can be made available to the staff through the intranet. So, it is like a private internet or an internal website that is operating within an organization to provide its employees access to its information and records. Each computer in intranet is identified by a unique IP Address.

CHAPTER – III

Browser

What is a Browser?

A browser is a software program that is used to explore, retrieve, and display the information available on the World Wide Web. This information may be in the form of pictures, web pages, videos, and other files that all are connected via hyperlinks and categorized with the help of URLs (Uniform Resource Identifiers). For example, you are viewing this page by using a browser.

A browser is a client program as it runs on a user computer or mobile device and contacts the web server for the information requested by the user. The web server sends the data back to the browser that displays the results on internet supported devices. On behalf of the users, the browser sends requests to web servers all over the internet by using HTTP (Hypertext Transfer Protocol). A browser requires a Smartphone, computer, or tablet and internet to work.

Google Chrome

Google Chrome is an open-source and the most popular internet browser that is used for accessing the information available on the World Wide Web. It was developed by Google on 11 December 2008 for Windows, Linux, Mac OS X, Android, and iOS operating systems. It uses sandboxing-based approach to provide Web security. Furthermore, it also supports web standards like HTML5 and CSS (cascading style sheet).

Google Chrome was the first web browser that has a feature to combine the search box and address bar, that was adopted by most competitors. In 2010, Google introduced the Chrome Web Store, where users can buy and install Web-based applications.

Mozilla Firefox

Mozilla Firefox is an open-source web browser that is used to access the data available on the World Wide Web. As compared to Internet Explorer, the popular Web browser Firefox provides users a simple user interface and faster download speeds. It uses the Gecko layout engine to translate web pages, which executes current and predicted web standards.

Firefox was widely used as an alternative to Internet Explorer 6.0 as it provided user protection against spyware and malicious websites. In the year of 2017, it was the fourth-most widely used web browser after Google Chrome, Apple Safari, and UC Browser.

Internet Explorer

Internet Explorer is a free web browser, commonly called IE or MSIE, that allows users to view web pages on the internet. It is also used to access online banking, online marketing over the internet, listen to and watch streaming videos, and many more. It was introduced by Microsoft in 1995. It was produced in response to the first geographical browser, Netscape Navigator.

Microsoft Internet Explorer was a more popular web browser for many years from 1999 to 2012 as it surpassed the Netscape Navigator during this time. It includes network file sharing, several internet connections, active Scripting, and security settings. It also provides other features such as:

- **Remote administration**
- **Proxy server configuration**
- **VPN and FTP client capabilities**

What is a server?

A server commonly refers to a computer program that receives and responds to requests made over a network. It receives the request for a web document from the client and sends the requested information to the client computer on the Internet. A device can be both a client and a server at the same time, as an individual system has the ability to provide resources and use them from another system in one go. There are different types of servers, including mail servers, virtual servers, and web servers.

There are many types of servers, which are as follows:

- Webserver
- Application server

- Blade server
- Cloud server
- Database server
- Dedicated server
- Print server
- Proxy server
- File server
- Mail server
- Standalone server
- Domain name service

How do servers work?

Servers work in several ways to connect users to different data functions. They house large amounts of data for organizations and make it accessible to users through internal networks or via the internet. They respond to user requests to retrieve appropriate files from stored or interconnected data sources. They also work in tandem with an operating system to better listen to and respond to user requests.

IT professionals can increase the functionality of a server by installing software that creates additional roles such a responding to website requests from an internet browser. Servers can also act as safeguards to verify the identity of users before allowing access to a network.

Server components

Physical servers are made up of the following parts:

- **Motherboard:** A motherboard connects all parts of a server. A motherboard's size dictates the amount of storage and the number of hard drives that can connect to a server.
- **Central Processing Unit (CPU):** The CPU controls the overall functions of a server. It's the center for all processing within a server device. CPUs are measured by processing speed.

- **Memory:** This part of a server dictates the amount of storage available. Memory needs to be compatible with the motherboard.
- **Hard drives:** A hard drive stores both user and software data for a computer. It uses a controller card for optimum processing functions. A server housing large amounts of data may need multiple hard drives.
- **Network connection:** A server needs to connect to a network in order to function. A good network connection will ensure a server is able to receive and respond to user requests. Many motherboards already contain a network adapter however, if they don't, the server will need an external network connection installed.
- **Power supply:** Servers that provide data to large numbers of clients need a bigger power supply than a typical personal computer. Most servers need a power supply of at least 300 watts.

What is server architecture?

Server architecture is the design of how a server functions. Server architecture refers to the layout of a server in its operational capacity.

A server's architecture can be defined by:

- How it communicates with other devices
- The types of operating systems it uses
- Hardware and software components

CHAPTER – IV

Middleware

Middleware

Middleware is software which lies between an operating system and the applications running on it. Essentially functioning as hidden translation layer, middleware enables communication and data management for distributed applications.

Examples of middleware:

Common middleware examples include database middleware, application server middleware, message-oriented middleware, web middleware, and transaction-processing monitors.
Middleware technologies:

Middleware is the software that connects network-based requests generated by a client to the back-end data the client is requesting. It is a general term for software that serves to "glue together" separate, often complex and already existing programs

Types of middleware:

Middleware functions can be divided into three main categories: application-specific, information-exchange and management and support middleware.

API and middleware:

These two words are quite different in meaning. API refers to callable services, while middleware refers to the product that does the integration work in the integration ecosystem.

Storage Unit

Storage Unit: A storage unit is that part of the computer system which is used to store the data and instructions to be processed. There are two types of storage:

Primary storage

Secondary storage.

Primary memory is also known as internal memory. This is a section of the CPU which holds program instructions, input data and intermediate results. Primary memory is also known as main memory.

Secondary storage is a memory that is stored external to the computer. It is used mainly for permanent and long term storage of programs and data.

Characteristics of Storage units:

The storage units have special characteristics which decide the

- Speed of operation of the computer,
- Its efficiency,
- Cost and
- The amount of data which the computer can store.

The storage unit of the computer is graded according to the following characteristics (whether primary or secondary):

Access time:

This is the time required to locate and retrieve a particular data from the storage unit. A fast access to data and programs always yields higher efficiency.

Storage Capacity:

Storage capacity is the amount of data that can be stored by a storage unit. Large capacity of data storage is always desirable.

As seen earlier, the smallest unit of data which the computer understands is the bit. A group of 8 bits forms a byte. The storage capacity of a computer system is defined in terms of bytes or words. One kilobyte (1 KB) is 2^ or 1024 bytes, eg. 4 KB memory implies that it can store 4 x

1024 bytes or characters. Storage capacities of primary and secondary units are measured in Kilobytes, megabytes, gigabytes.

Cost:

Low cost storage media are always desirable. Thus, storage units with faster access time, higher storage capacity and low costs are the ones which are considered to be of a superior nature.

PRIMARY STORAGE

Primary storage is characterized by faster access time, less storage capacity and higher costs as compared to secondary storage units. Primary storage or main memory is that part of the computer system which stores the programs, data and intermediate results during the program execution.

A primary storage comes as an integral part of all computer systems. It comprises of a number of small locations. Each location has a unique number assigned to it. This is called as the address of the location and it is used to identify the location. Each location has a capacity to store a fixed number of bits. The number of bits that a location can store is called as word length. Each location contains the same number of bits.

Normally, primary memory size ranges from a few kilobytes on small computers to several thousand kilo bytes and megabytes on larger machines.

The primary storage is volatile. Whenever the power is turned off the data is lost. Primary storage is also called Random Access Memory (RAM). RAM means it is possible to randomly select and use any storage location for storage and retrieval of data. RAM is also called a read/write memory because data can both be read from and written onto these units. When the power is switched off the data stored in the RAM is lost.

ROM: ROM is Read Only Memory. In this type of memory the data is permanently stored. The information can only be read and new data cannot be written onto this memory. However the contents of the ROM are not lost even when the power is turned off i.e. this memory is non-volatile. Such memories are also called as field stores or permanent stores.

There are a number of high level functions which are required to be performed by the computer system. Such functions are performed by writing special programs called micro programs. Micro programs generally execute the low level machine functions. These programs are mainly used as a substitute for hardware. Such programs can be stored on ROMs and be used again and again. This results in reducing the hardware of the system. ROM helps to increase the

Efficiency of the CPU as it can perform specialized tasks. ROM comes in the form of a chip. Once information is stored on a ROM chip it cannot be changed or altered.

PROM: PROM is Programmable Read Only Memory. These are ROMs which can be programmed. A special PROM programmer is used to enter the program on the PROM.

Once the chip has been programmed, information on the PROM cannot be altered. PROM is non volatile ie. Data is not lost when power is switched off.

EPROM: Another type of memory is the Erasable Programmable Read Only Memory.

It is possible to erase the data which has been previously stored on an EPROM and write new data onto the chip.

Cache Memory: This is a very special type of high speed memory. This memory cannot be accessed by the user. The main function of this cache memory is to make the programs and data available to the CPU very fast.

Access time of memory is generally very high as compared to the execution time of the GPU. Therefore a cache, which is a very small but fast memory, is used between the CPU and the main memory. This memory also called a high speed buffer. A cache stores those segments of programs and data which are frequently needed. It makes available this data to the CPU at a very fast rate thus increasing the efficiency.

Registers:

Registers are used to retain information temporarily. These are special memory units which are not actual parts of the main memory, but allow efficient mov ement of information between the

various units of the computer system. The registers receive information, hold it temporarily and make it available as and when required.

A computer uses a number of registers, where each register performs a specific function. Some of the common registers are

Memory Address Register (MAR): The function of this register is to hold the address of the current or active memory location.

Memory Buffer Register (MBR): This register holds the contents of the address from which data is read or to which data has been written.

Program Control Register: It holds the address of the next instruction to be executed.

Accumulator Register: It holds the initial data, the intermediate results and the final data of the program under execution.

Instruction Register: This register holds the current instruction being executed. Input/output Register: The function of this register is to communicate with the Input/output devices.

The storage capacity of primary storage is limited. It is normally not sufficient to accommodate all the data. Therefore secondary storage medium is used to store large volumes of data. The cost of secondary memory is much less as compared to primary memory, however access time of primary memory is very fast. The data stored on secondary storage is transferred to the primary storage as and when required. Secondary storage is also called auxiliary memory. Secondary storage is used for storing copies of data and programs. This is a non volatile memory and is stored external to the computer.

Information stored on secondary storage devices can be accessed in two ways:

- Sequential Access and
- Direct Access

In sequential access data can be accessed only in the sequence in which it has been stored. Typical sequential access storage device is the magnetic tape. These types of devices are useful in applications like pay slip printing where the data is to be accessed one after the other.

Types of Access Devices:

a) Punch Paper Tape:

Punched paper tapes were the early devices of data storage. Data is coded onto a paper tape as a combination of punched holes across the width of the tape. Each row on the tape represents one character. The data has to be coded on the tapes using special coding systems. The punched paper tapes are a low cost storage medium and their storage capacity is unlimited. However, the paper is susceptible to wear and tear and mishandling. Nowadays, punched paper tapes are rarely being used wear and tear and mishandling. Nowadays, punched paper tapes are rarely being used.

b) Magnetic Tape:

A magnetic tape is a ribbon of Mylar which is coated with a thin layer of iron oxide material on one side. This tape is stored on a cassette or cartridge, or reel .The iron oxide material can be magnetized and the data is recorded on the tape in the form of magnetized and non-magnetized spots. A magnetic tape drive is used to read data from the tape or write information to the tape. The tape drive has a read/write head to access or store information respectively.

Magnetic tape is a read write device where the data can be written as well as erased and new data recorded on the same area. The tape is divided into vertical columns and horizontal rows. The columns are called frames and the rows are called tracks. Special computer codes are used for recording data on the tape. One character is recorded on each frame. Most modern tapes have 9 tracks, and use the EBCDIC code for data representation. The actual number of characters that can be stored on an inch of a tape is known as the density of the tape.

The storage capacity of magnetic tapes is very large. This capacity is measured in terms of bytes per inch. Most common tape densities are 800 bpi, 1600 bpi. Nowadays tapes with much higher densities of the order of 6000 bpi are also available.

The records in a tape can be of any size. Also all the records in a given file need not be same in length. Thus the tapes can store fixed length and v variable length records. In between two consecutive records the computer automatically keeps a fraction of the tape blank. This blank space is called the Interlock gap, While reading from the tape, the drive takes a finite amount of time to physically stop when the end of the record is reached. Therefore this interlock gap is created to avoid loss of any data of the subsequent record that may have been store while the drive mechanism comes to a halt.

Advantages of Magnetic Tapes:

- High data density and virtually unlimited storage
- Low in cost
- Easy to handle and portable from one computer to another.

Limitations are:

- Support only Sequential access

- Tapes are sensitive to dust; humidity and temperature, hence require proper storage facilities.

Direct Access Storage Devices Random or direct access

In random access the data at any location on the storage unit can be accessed directly without having to follow the sequence in which it has been stored. Typical devices that support direct access are the magnetic disk and magnetic drum.

Magnetic Disk: A magnetic disk is a thin metallic/Mylar platter circular in shape. It is coated on both sides with magnetic material. A number of these disks are mounted on a disk pack, on a central shaft. Thus all the disks in the disk pack move at the same speed, simultaneously in the

same direction. These disks are also called as hard disks or fixed disks. Hard disk can be permanently installed in the drive or can also be in the form of a removable cartridge. The data are recorded as magnetic spots on the coating of the disk. The presence of a magnetic spot represents1 and the absence represents a 0. The standard binary code, 8 -bit EBCDIC is used for recording data on the disk. Information is stored on both the surfaces of the disk. Each disk is divided into a number of concentric circles called tracks. All the corresponding tracks in all the surfaces are together called a cylinder. Information is not stored on the outer surface of the upper plate and the lower surface of the bottom plate.

In some of the disks the outer tracks contain more data bits since the outer circumference is greater. However, in most of the disks each track stores the same number of characters. This means that the inner tracks, with a smaller circumference are more densely packed than the outer tracks.

Magnetic disk is a random or direct access storage device. The data is read from or written onto the disk surface with the use of read/write heads. These heads are of flying type. They do not come in actual contact with the surface of the disk.

There are two types of disk systems:

Moving head System:

This consists of one read/write head for each disk surface. This head is mounted on an access arm which moves in and out. Thus each head moves horizontally across the surface of the disk and can access each track individually.

Fixed head System:

In this system the access arm does not move. A large number of read/write heads one for each track are distributed over the surface of the disk. In this system the data access becomes very fast. However, extra space is needed to accommodate all the heads. The time required to access the data stored on the disk depends upon the following factors:

- The seek time - the time required for positioning the read/write head over the appropriate track

- The latency time - the time required to spin the required data under the head. This time is also called the search time.

Floppy Disks : Floppy disks are made up of flexible Mylar coated with iron oxide. This disk is enclosed in a square plastic jacket to protect the surface of the disk from dust. A floppy disk is to be inserted in the floppy disk drive of the computer system to read or write information. The read/write head of the drive makes a direct contact with the floppy disk.

While accessing or storing data, Floppy disks come in various sizes

- 8 inch floppy disks
- 51/4 inch floppy disks
- 31/2 inch floppy disks

A floppy disk can be single sided or double sided i.e data can be written on a Fig. 3.4 Floppy disks: 51/4 inch and 31/2 inch single side or on both the sides. A double sided disk drive is required to read data from

a double sided disk. This disk drive has two heads, one for each side. A single sided drive has only one head. Floppy disks can also be single side double density and double side double density depending upon their storage capacity.

Floppy disks are a very popular storage medium since they are small in size, relatively cheap and can store data on line. Floppy disks are also very portable. They can be carried form one place to another very easily.

Winchester Disk: In a Winchester, the disks are permanently enclosed in a sealed container. The disks are coated with a special lubricant to reduce friction with the read/write head. This

technology allows for an increase in the number of tracks on the disk, and higher storage density. Winchester disks are fast and highly reliable. They are used extensively in micro computers.

Magnetic Drum: This is a cylinder whose outer surface is coated with a thin layer of magnetic material. A motor rotates on the cylinder at a constant speed. Data is recorded on the tracks of the drum as magnetized spots. A set of stationary read/write heads are positioned slightly away from the surface of the drum. Data is read from and written onto this drum with the help of these heads. The drum rotates are relatively fast speeds of the order of a several thousand rotations per minute. Magnetic drums have faster data transfer rates as compared to disks. However their storage capacity is limited. Magnetic drums are rarely used today.

Optical Devices: Optical Disk: An optical disk is made up of a rotating disk which is coated with a thin reflective metal. To record data on the optical disk, a laser beam is focused on the surface of the spinning disk. The laser beam is turned on and off at varying rates! Due to this, tiny holes (pits) are burnt into the metal coating along the tracks. When data stored on the optical disk is to be read, a less powerful laser beam is focused on the disk surface. The storage capacity of these devices is tremendous. Optical disk access time is relatively fast. The biggest drawback of the optical disk is that it is a permanent storage device. data once written cannot be erased. Therefore it is a read only storage medium. A typical example of the optical disk is the CD-ROM.

Optical Card: The optical card has an optical laser encoded strip which can store approximately 2 megabytes of data. These cards are the size of a credit card. Optical cards find use only in specific areas like storing credit records or medical histories of people.

Optical Tape: Optical tapes are similar to magnetic tapes in appearance. However optical laser techniques are used to write data on the tapes. Like optical disks optical tapes too are read only storage devices.

Client and server communication: The client sends a request, and the server returns a response. This exchange of messages is an example of inter-process communication. To communicate, the computers must have a common language, and they must follow rules so that both the client and the server know what to expect.

Client/Server communication involves two components, namely a client and a server. They are usually multiple clients in communication with a single server. The clients send requests to the server and the server responds to the client requests. There are three main methods to client/server communication.

Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is a protocol implemented using TCP that governs communication for the World Wide Web (WWW). It assumes a client/server architecture between a web browser and a web server. HTTP specifies the format of messages exchanged between browsers and servers.

Relationship between clients and servers on the Internet

The client-server model is the relationship between two computers in which one, the client, makes a service request from another, the server. The key point about a client-server model is that the client is dependent on the server to provide and manage the information. For example, websites are stored on web servers.

Web browsers communicate with web servers using the Hyper Text Transfer Protocol (HTTP). When you click a link on a web page, submit a form, or run a search, the browser sends an HTTP Request to the server.

The main difference between client and server is that a client is a machine or a program that requests for services through the web while a server is a machine or a program that provides services to the clients according to the client's requests.

Which protocol is used for communication between server and client?

TCP/IP Protocol. Transmission Control Protocol/Internet Protocol (TCP/IP) is the standard communication protocol suite used for client/server communication over a network.

What type of communication we can use in client-server?

Sockets: Sockets facilitate communication between two processes on the same machine or different machines. They are used in a client/server framework and consist of the IP address and

port number. Many application protocols use sockets for data connection and data transfer between a client and a server.

There are four various types of client-server architecture.

- 1 Tier Architecture.
- 2 Tier Architecture.
- 3 Tier Architecture.
- N Tier Architecture.

The communication process is made up of four key components. Those components include encoding, medium of transmission, decoding, and feedback. There are also two other factors in the process, and those two factors are present in the form of the sender and the receiver.

Server itself might be a client. For example, the server could request something from a database server, which in this case, would make the server a client of the database server. Examples of computer applications that use the client–server model are E-mail, network printing, and the World Wide Web.

CHAPTER – V

Protection

Today we use our computers to do so many things, and as a result, our computers contain a wealth of personal information about us. Information that you want to protect, if your computer is not protected, identity thieves and other fraudsters may be able to get access and steal your personal information. By using safety measures and good practices to protect your computer, you can protectyour privacy.

The following tips are offered to help you lower your risk while you're online.

A firewall is a software program or piece of hardware that blocks hackers from entering and using your computer. A firewall can block all communications to and from sources you don't permit.

Anti-virus software protects your computer from viruses that can destroy your data, allow spammers to send email through your account. Anti-virus protection scans your computer and your incoming email for viruses, and then deletes them. You must keep your anti-virus software updated.

Hackers are constantly trying to find flaws or holes in operating systems and browsers. To protect your computer and the information on it, put the security settings in your system and browser at medium or higher. Check the "Tool" or "Options" menus for how to do this.

Protect your computer from intruders by choosing passwords that are hard to guess. Use strong passwords with at least eight characters, a combination of letters, numbers and special characters. Don't use a word that can easily be found in a dictionary. Some hackers use programs that can try every word in the dictionary. Try using a phrase to help you remember your password, using the first letter of each word in the phrase. For example, *HmWc@w2 - How much wood could a woodchuck chuck*. Protect your password the same way you would the key to your home. After all, it is a "key" to your personal information.

Many users enjoy sharing digital files, such as music, movies, photos, and software. File-sharing software that connects your computer to a network of computers is often available for free. File-

sharing can pose several risks. When connected to a file-sharing network, you may allow others to copy files you didn't intend to share. You might download a virus or bit of spyware that makes your computer vulnerable to hackers. You might also break the law by downloading material that is copyright protected

When shopping online, check out the Web site before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. (If there is no privacy policy posted, beware! Shop elsewhere.) Learn how to tell when a Web site is secure. Look for "https" in the addressbar or an unbroken padlock icon at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers as it moves across the Internet

CHAPTER- VI

Steps to Protect Your Data

The most valuable thing on the devices and networks you use is the data you create and store there. Applications and operating systems can always be reinstalled, but user-created data is unique. If it gets lost or viewed without authorization, the outcome can be devastating.

1. Apply Software Updates

Software companies often release updates that patch bugs and vulnerabilities when they are discovered. So, don't put off software updates, especially on operating systems. Software left outdated may still contain security flaws that can leave you susceptible to a data or privacy breach.

2. Protect Passwords

Creating strong passwords and never using the same password across sites or devices is one of the best things you can do to protect yourself from digital invasion. On your phone, lock it with a strong password and fingerprint or Touch ID. To keep track of all of your password combinations, use a password manager like 1Password or Last Pass to keep your passwords stored, strong and unique across all of your devices and accounts.

A company's network may contain documents with trade secrets, personal information about employees or clients, or the organization's financial records. Applications on your phone, computer or other personal devices may expose your social security number, credit cards, and bank account information. In either case, identity theft is a real possibility — one that's becoming all-too-frequent in our digital age. Although vital, protecting your privacy and security doesn't have to be a complex or daunting task.

3. Disable Lock-Screen Notifications

Turning off lock-screen app notifications on your smartphone is a simple way to hide personal information that can pop up on your phone's lock screen. Disable app notifications to keep text messages and social media notifications away from prying eyes.

4. Lock Your Apps

Once you've set a lock on your phone, go a step further and lock your actual apps. App lockers provide an extra level of security for your apps and work just like the lock-screen feature. If someone else uses your phone or if your device is stolen, the contents of your apps remain locked behind a passcode.

5. Keep Your Browsing to Yourself

If you use free WiFi hotspots in public places, use a Virtual Private Network (VPN) to obscure your personal information from others who may be using the same unsecured public network. Just make sure the VPN service is legitimate and one you trust to maintain your privacy. In addition to shielding your browsing information, the VPN will encrypt all of the data coming to or leaving your computer or phone, and hide your location.

6. Encrypt Your Data

Encryption is designed to scramble your data so no one can understand what it says without a key. It's not only useful for protecting information on your computer, but also for making sure text messages and emails on your phone aren't subject to prying eyes.

There are free apps available for iPhone and Android that are easy to use, including Signal and WhatsApp. On your computer, productivity applications such as Microsoft Office and Adobe Acrobat allow you to set passwords on individual documents and specify the type of encryption to be used. Encrypting File System (EFS) and disk encryption products allow you to encrypt files, folders, removable USB drives, flash drives, and more.

7. Back It Up

If something should happen to the data you create on your devices or network, or you lose it all, you can recover quickly without hassle if it's backed up. Backups help protect your photos, documents, and other data not only from a technical malfunction but from ransomware and other malicious hacking. Back up to an online service, external hard drive, or both, for the best data protection.

What Is Data Protection and Why Is It Important?

Data protection is a set of strategies and processes you can use to secure the privacy, availability, and integrity of your data. It is sometimes also called data security.

A data protection strategy is vital for any organization that collects, handles, or stores sensitive data. A successful strategy can help prevent data loss, theft, or corruption and can help minimize damage caused in the event of a breach or disaster.

What Are Data Protection Principles?

Data protection principles help protect data and make it available under any circumstances. It covers operational data backup and business continuity/disaster recovery (BCDR) and involves implementing aspects of data management and data availability.

Here are key data management aspects relevant to data protection:

- **Data availability**—ensuring users can access and use the data required to perform business even when this data is lost or damaged.
- **Data lifecycle management**—involves automating the transmission of critical data to offline and online storage.
- **Information lifecycle management**—involves the valuation, cataloging, and protection of information assets from various sources, including facility outages and disruptions, application and user errors, machine failure, and malware and virus attacks.

What Is Data Privacy and Why Is it Important?

Data privacy is a guideline for how data should be collected or handled, based on its sensitivity and importance. Data privacy is typically applied to personal health information (PHI) and personally identifiable information (PII). This includes financial information, medical records, social security or ID numbers, names, birthdates, and contact information.

Data privacy concerns apply to all sensitive information that organizations handle, including that of customers, shareholders, and employees. Often, this information plays a vital role in business operations, development, and finances.

Data privacy helps ensure that sensitive data is only accessible to approved parties. It prevents criminals from being able to maliciously use data and helps ensure that organizations meet regulatory requirements.

Data Protection

Data protection regulations govern how certain data types are collected, transmitted, and used. Personal data includes various types of information, including names, photos, email addresses, bank account details, IP addresses of personal computers, and biometric data.

Data protection and privacy regulations vary between countries, states, and industries. For example, China has created a data privacy law that went into effect on June 1, 2017, and the European Union's (EU) General Data Protection Regulation (GDPR) went into effect during 2018. Non-compliance may result in reputation damages and monetary fines, depending on the violation as instructed by each law and governing entity.

Compliance with one set of regulations does not guarantee compliance with all laws. Additionally, each law contains numerous clauses that may apply to one case but not another, and all regulations are subject to changes. This level of complexity makes it difficult to implement compliance consistently and appropriately.

Data Protection vs Data Privacy

Although both data protection and privacy are important and the two often come together, these terms do not represent the same thing.

One addresses policies, the other mechanisms

Data privacy is focused on defining who has access to data while data protection focuses on applying those restrictions. Data privacy defines the policies that data protection tools and processes employ.

Creating data privacy guidelines does not ensure that unauthorized users don't have access. Likewise, you can restrict access with data protections while still leaving sensitive data vulnerable. Both are needed to ensure that data remains secure.

Users control privacy, companies ensure protection

Another important distinction between privacy and protection is who is typically in control. For privacy, users can often control how much of their data is shared and with whom. For protection, it is up to the companies handling data to ensure that it remains private. Compliance regulations reflect this difference and are created to help ensure that users' privacy requests are enacted by companies.

12 Data Protection Technologies and Practices to Protect Your Data

When it comes to protecting your data, there are many storage and management options you can choose from. Solutions can help you restrict access, monitor activity, and respond to threats. Here are some of the most commonly used practices and technologies:

1. **Data discovery**—a first step in data protection, this involves discovering which data sets exist in the organization, which of them are business critical and which contains sensitive data that might be subject to compliance regulations.
2. **Data loss prevention (DLP)**—a set of strategies and tools that you can use to prevent data from being stolen, lost, or accidentally deleted. Data loss prevention solutions often include several tools to protect against and recover from data loss.
3. **Storage with built-in data protection**—modern storage equipment provides built-in disk clustering and redundancy. For example, Cloudian's Hyperstore provides up to 14 nines of durability, low cost enabling storage of large volumes of data, and fast access for minimal RTO/RPO.

4. **Backup**—creates copies of data and stores them separately, making it possible to restore the data later in case of loss or modification. Backups are a critical strategy for ensuring business continuity when original data is lost, destroyed, or damaged, either accidentally or maliciously. Learn more in our guide to data availability.
5. **Snapshots**—a snapshot is similar to a backup, but it is a complete image of a protected system, including data and system files. A snapshot can be used to restore an entire system to a specific point in time.
6. **Replication**—a technique for copying data on an ongoing basis from a protected system to another location. This provides a living, up-to-date copy of the data, allowing not only recovery but also immediate failover to the copy if the primary system goes down.
7. **Firewalls**—utilities that enable you to monitor and filter network traffic. You can use firewalls to ensure that only authorized users are allowed to access or transfer data.
8. **Authentication and authorization**—controls that help you verify credentials and assure that user privileges are applied correctly. These measures are typically used as part of an identity and access management (IAM) solution and in combination with role-based access controls (RBAC).
9. **Encryption**—alters data content according to an algorithm that can only be reversed with the right encryption key. Encryption protects your data from unauthorized access even if data is stolen by making it unreadable.
10. **Endpoint protection**—protects gateways to your network, including ports, routers, and connected devices. Endpoint protection software typically enables you to monitor your network perimeter and to filter traffic as needed.
11. **Data erasure**—limits liability by deleting data that is no longer needed. This can be done after data is processed and analyzed or periodically when data is no longer relevant. Erasing unnecessary data is a requirement of many compliance regulations, such as GDPR. For more information about GDPR, check out our guide: GDPR Data Protection.
12. **Disaster recovery**—a set of practices and technologies that determine how an organization deals with a disaster, such as a cyber attack, natural disaster, or large-scale equipment failure. The disaster recovery process typically involves setting up a remote disaster recovery site with copies of protected systems, and switching operations to those systems in case of disaster.

Keep awake

1: Back up early and often

The single most important step in protecting your data from loss is to back it up regularly. How often should you back up? That depends–how much data can you afford to lose if your system crashes completely? A week's work? A day's work? An hour's work?

You can use the backup utility built into Windows (ntbackup.exe) to perform basic backups. You can use Wizard Mode to simplify the process of creating and restoring backups or you can configure the backup settings manually and you can schedule backup jobs to be performed automatically.

There are also numerous third-party backup programs that can offer more sophisticated options. Whatever program you use, it's important to store a copy of your backup offsite in case of fire, tornado, or other natural disaster that can destroy your backup tapes or discs along with the original data.

2: Use file-level and share-level security

To keep others out of your data, the first step is to set permissions on the data files and folders. If you have data in network shares, you can set share permissions to control what user accounts can and cannot access the files across the network. With Windows 2000/XP, this is done by clicking the Permissions button on the Sharing tab of the file's or folder's properties sheet.

However, these share-level permissions won't apply to someone who is using the local computer on which the data is stored. If you share the computer with someone else, you'll have to use file-level

permissions (also called NTFS permissions, because they're available only for files/folders stored on NTFS-formatted partitions). File-level permissions are set using the Security tab on the properties sheet and are much more granular than share-level permissions.

In both cases, you can set permissions for either user accounts or groups, and you can allow or deny various levels of access from read-only to full control.

3: Password-protect documents

Many productivity applications, such as Microsoft Office applications and Adobe Acrobat, will allow you to set passwords on individual documents. To open the document, you must enter the password. To password-protect a document in Microsoft Word 2003, go to Tools | Options and click the Security tab. You can require a password to open the file and/or to make changes to it. You can also set the type of encryption to be used.

Unfortunately, Microsoft's password protection is relatively easy to crack. There are programs on the market designed to recover Office passwords, such as Elcomsoft's Advanced Office Password Recovery (AOPR). This type of password protection, like a standard (non-deadbolt) lock on a door, will deter casual would-be intruders but can be fairly easily circumvented by a determined intruder with the right tools.

You can also use zipping software such as WinZip or PKZip to compress and encrypt documents.

4: Use EFS encryption

Windows 2000, XP Pro, and Server 2003 support the Encrypting File System (EFS). You can use this built-in certificate-based encryption method to protect individual files and folders stored on NTFS-formatted partitions. Encrypting a file or folder is as easy as selecting a check box; just click the Advanced button on the General tab of its properties sheet. Note that you can't use EFS encryption and NTFS compression at the same time.

EFS uses a combination of asymmetric and symmetric encryption, for both security and performance. To encrypt files with EFS, a user must have an EFS certificate, which can be issued by a Windows certification authority or self-signed if there is no CA on the network. EFS files can be opened by the user whose account encrypted them or by a designated recovery agent. With Windows XP/2003, but not Windows 2000, you can also designate other user accounts that are authorized to access your EFS-encrypted files.

Note that EFS is for protecting data on the disk. If you send an EFS file across the network and someone uses a sniffer to capture the data packets, they'll be able to read the data in the files.

5: Use disk encryption

There are many third-party products available that will allow you to encrypt an entire disk. Whole disk encryption locks down the entire contents of a disk drive/partition and is transparent to the user. Data is automatically encrypted when it's written to the hard disk and automatically decrypted before being loaded into memory. Some of these programs can create invisible containers inside a partition that act like a hidden disk within a disk. Other users see only the data in the "outer" disk.

Disk encryption products can be used to encrypt removable USB drives, flash drives, etc. Some allow creation of a master password along with secondary passwords with lower rights you can give to other users. Examples include PGP Whole Disk Encryption and DriveCrypt, among many others.

6: Make use of a public key infrastructure

A public key infrastructure (PKI) is a system for managing public/private key pairs and digital certificates. Because keys and certificates are issued by a trusted third party (a certification authority, either an internal one installed on a certificate server on your network or a public one, such as Verisign), certificate-based security is stronger.

You can protect data you want to share with someone else by encrypting it with the public key of its intended recipient, which is available to anyone. The only person who will be able to decrypt it is the holder of the private key that corresponds to that public key.

7: Hide data with steganography

You can use a steganography program to hide data inside other data. For example, you could hide a text message within a .JPG graphics file or an MP3 music file, or even inside another text file (although the latter is difficult because text files don't contain much redundant data that can be replaced with the hidden message). Steganography does not encrypt the message, so it's often used in conjunction with encryption software. The data is encrypted first and then hidden inside another file with the steganography software.

Some steganographic techniques require the exchange of a secret key and others use public/private key cryptography. A popular example of

steganography software is StegoMagic, a freeware download that will encrypt messages and hide them in .TXT, .WAV, or .BMP files.

8: Protect data in transit with IP security

Your data can be captured while it's traveling over the network by a hacker with sniffer software (also called network monitoring or protocol analysis software). To protect your data when it's in transit, you can use Internet Protocol Security (IPsec)–but both the sending and receiving systems have to support it. Windows 2000 and later Microsoft operating systems have built-in support for IPsec. Applications don't have to be aware of IPsec because it operates at a lower level of the networking model.

Encapsulating Security Payload (ESP) is the protocol IPsec uses to encrypt data for confidentiality. It can operate in tunnel mode, for gateway-to-gateway protection, or in transport mode, for end-to-end protection. To use IPsec in Windows, you have to create an IPsec policy and choose the authentication method and IP filters it will use. IPsec settings are configured through the properties sheet for the TCP/IP protocol, on the Options tab of Advanced TCP/IP Settings.

9: Secure wireless transmissions

Data that you send over a wireless network is even more subject to interception than that sent over an Ethernet network. Hackers don't need physical access to the network or its devices; anyone with a wireless-enabled portable computer and a high gain antenna can capture data and/or get into the network and access data stored there if the wireless access point isn't configured securely.

You should send or store data only on wireless networks that use encryption, preferably Wi-Fi Protected Access (WPA), which is stronger than Wired Equivalent Protocol (WEP).

10: Use rights management to retain control

If you need to send data to others but are worried about protecting it once it leaves your own system, you can use Windows Rights Management Services (RMS) to control what the recipients are able to do with it. For instance, you can set rights so that the recipient can read the Word document you sent but can't change, copy, or save it. You can prevent recipients from forwarding e-mail messages you send them and you can even set documents or messages to expire on a certain date/time so that the recipient can no longer access them after that time.

Disclaimer

All the above contents are taken from mention below references. As an author I'm not obtaining any copyrights/Patent for this work.

References

1.https://www.techrepublic.com/article/10-things-you-can-do-to-protect-your-data/
2.https://www.cybintsolutions.com/7-easy-steps-to-protect-your-data/
3.https://cloudian.com/guides/data-protection/data-protection-and-privacy-12-ways-to-protect-user-data/
4.https://www.tutorialspoint.com/computer_fundamentals/index.htm
5.https://www.tutorialspoint.com/basics_of_computers/basics_of_computers_introduction.htm

TABLE OF CONTENTS

CHAPTER – I
Basic Things of Computer.....1

CHAPTER - II
Computer Components.....9

CHAPTER – III
Browser.....19

CHAPTER – IV
Middleware.....23

CHAPTER – V
Protection.....35

CHAPTER- VI
Steps to Protect Your Data.....37