1. The History of Computers

The first counting tools people used were sticks and stones. However, as the human mind developed over time, new computing devices were designed starting with the invention of the abacus in China, around 1300 BC. It was used to perform basic arithmetical operations – addition, subtraction, multiplication, division. The first mechanical adding machine, the Pascaline, was built by Blaise Pascal, a French mathematician and scientist, between 1642 and 1644. The Pascaline was able to perform addition and subtraction in short time. The device was basically a wooden box with a number of gears and wheels.

The first machine resembling today's modern computers was The Analytical Engine designed in the 1830s by British mathematician Charles Babbage who is often called the father of the computer. He showed his machine at the exhibition in Paris in 1855. The Analytical Engine contained an ALU (arithmetic logic unit), control unit, memory, and an input/output system. These are the essential p arts of a modern computer. Babbage never finished this work, but many of his ideas were the basis for building today's computers.

The 19th century was a period of a rapid evolution of comp uting theory and a number of calculating machines began to be used at that time. However, it wasn't until the middle of the 20th century that a major breakthrough in computing technology was made. In 1936 Konrad Zuse, a German engineer, developed the Z1 machine, the first programmable mechanical computing device, which was later followed by the Z2 and the Z3. This series of inventions led to the advent of the first fully-functioning programmable electro-mechanical computer.

Vacuum Tubes were employed in the first generation of computers to perform calculations. The first generation computer was ENIAC (Electronic Numerical Integrator and Calculator). This generation of computers was serious and huge. They performed arithmetic calculations by exploiting vacuum tubes. Although the first generation of computers has many disadvantages than its blessings. However, its importance can't be forgotten.

As a result, the second generation of computers was created. Transistors were utilized in the second generation of computers. The use of vacuum tubes within the

first generation of computers revolutionized the globe of technology.

Third generation computers start using integrated circuits instead of transistors. The integrated circuit is a semiconductor material, that contains thousands of transistors miniaturized in it. With the help of integrated circuit, the computer becomes more reliable, fast, required less maintenance and power consumption, small in size.

This generation of computers reduce the computational time. In the previous generation, the computational time was microsecond which was decreased to the nanosecond. In this generation, punch cards were replaced by mouse and keyboard. Integrated Circuits themselves include many transistors, capacitors, and resistors and because of this third generation computer systems are smaller in size, efficient, and extra reliable.

After third-generation computers, which mostly utilized microprocessors, fourth-generation computers were released in 1972. VLSI technology, or Very Large Scale Integrated (VLSI) circuits, was employed in these computers. As a result, they were dubbed microprocessors. A microprocessor is made up of thousands of integrated circuits that are assembled on a single chip known as a silicon chip.

Fifth-generation computers were introduced after the fourth-generation computers were invented. Fifth-generation computers, also known as modern computers, are still in the development stage and are based on artificial intelligence. In 1982, Japan was invented the FGCS (Fifth Generation Computer System). Computers of this generation are based on microelectronic technology with high computing power and parallel processing.

2. Types of Computers and their Use

Nowadays computers are available in different shapes and sizes and have different processing capabilities. As a result, the computers are classified based on size and purpose, functionality, and data handling capabilities.

Servers are computers designed to provide services to other computers or users on a network. They play a crucial role in managing and distributing data, applications, and other resources across a network or the internet. Servers are used in a wide range of industries, including finance, healthcare, education, e-commerce, government, and information technology.

A mainframe computer is a powerful machine designed to perform considerable computational tasks like enormous volumes of data and handling multiple users simultaneously. The central system is a large server connected to hundreds of terminals over a network. Mainframe computers can have multiple processors with different operating systems and allow many p rograms to run at the same time. Mainframes are characterized by high processing speed, great memory capacity, and excellent reliability. Industries where mainframes are still used today include financial institutions, government agencies, airlines, telecommunications, manufacturing industries, etc.

A Supercomputer is a computer with a high level of performance compared to a general purpose computer. Unlike mainframes, people typically only use them for one, complex task. So, the performance of the supercomputer is higher comp ared to the mainframe as supercomputers can execute billions of operations per second, processing one single but most complex problem at once. Mainframes, in turn, process thousands of queries simultaneously. As a result, their performance is slower. They are designed to process a huge amount of data, sometimes trillions of instructions per second due to the thousands of interconnected processors in them. It is basically used in scientific and engineering applications such as weather forecasting, scientific simulations, and nuclear energy research, oil and gas exploration, quantum mechanics. It was first developed by Roger Cray in 1976.

A desktop PC is basically a general-purpose computer designed for individual use. It consists of a microprocessor as a central processing unit(CPU), memory, inp ut

unit, and output unit, a tower (system unit). This kind of computer is suitable for personal work such as creating a document, making a p resentation, watching a movie, surfing the web or communicating with friends, etc.

A laptop computer is a portable personal computer that is small enough to rest on the user's lap hence its name. It includes a flip down screen and a keyboard with a touchpad, processor, memory and hard drive all in a battery-operated package. They offer a lot of connectivity options: USB ports for connecting p eripherals, slots for memory cards, etc. Users buy different types of laptops for different purposes – education, making reports, gaming, video editing and computational tasks as well.

A tablet is a wireless touchscreen PC that is slightly smaller and weighs less than the average laptop. It combines the best aspects of smartphones or laptops. However, they don't include all the same hardware components as a full desktop computer or laptop. Tablets don't have the internal fans that PCs have. They also have less storage capacity than traditional PCs. Tablets are commonly used for reading books, watching films, taking photos, playing games and drawing with a stylus.

These devices play a vital role in our everyday life and are of great help. As technology continues to advance, computers will continue to play an essential role in our lives.

3. Computer hardware

A computer is an electronic machine which can accept data in a certain form, process the data, and give the results of the processing in a specified format as information.

First, data is fed into the computer's memory. Then, when the program is run, the computer performs a set of instructions and processes the data. Finally, we can see the results (the output) on the screen or in printed form.

A computer system consists of two parts: hardware and software. Hardware is any electronic or mechanical part you can see or touch. Software is a set of instructions, called a program, which tells the computer what to do. There are three basic hardware sections: the central processing unit (CPU), main memory and peripherals.

The central processing unit (CPU) is built into a single chip which executes program instructions and coordinates the activities that take place within the computer system. The chip itself is a small piece of silicon with a complex electrical circuit called an integrated circuit.

The processor consists of three main parts:

■ The control unit examines the instructions in the user's program, interprets each instruction and causes the circuits and the rest of the components - monitor, disk drives, etc. -+ to execute the functions specified.

■ The arithmetic logic unit (ALU) performs mathematical calculations (+, -, etc.) and logical operations (AND, OR, NOT).

■ The registers are high-speed units of memory used to store and control data.

One of the registers (the program counter, or PC) keeps track of the next instruction to be performed in the main memory. The other (the instruction register, or IR) holds the instruction that is being executed.

The power and performance of a computer is partly determined by the speed of its processor. A system clock sends out signals at fixed intervals to measure and synchronize the flow of data. Clock speed is measured in gigahertz (GHz).

RAM and ROM

The main memory (a collection of RAM chips) holds the instructions and data

which are being processed by the CPU. The programs and data which p ass through the processor must be loaded into the main memory in order to be processed. Therefore, when the user runs a program, the CPU looks for it on the hard disk and transfers a copy into the RAM chips. RAM (random access memory) is volatile - that is, its information is lost when the computer is turned off. However, ROM (read only memory) is non-volatile, containing instructions and routines for the basic operations of the CPU. The BIOS (basic input/output system) uses ROM to control communication with peripherals. RAM capacity can be exp anded by adding extra chips.

Peripherals are the physical units attached to the computer. They include storage devices and input/output devices.

Storage devices (hard drives, DVD drives or flash drives) provide a permanent storage of both data and programs. Storage devices can be classified into three types: magnetic, optical and flash memory storage devices. Magnetic devices store data magnetically (floppy disk, internal or external hard disk drive HDD, magnetic tape).

Disk drives are used to read and write data on disks. Optical drives use a laser to read and write data, so they are not affected by magnetic fields (CD, DVD, Blu -ray disc, HD-DVD). Flash memory is solid-state, rewritable memory; it is non-volatile, so it retains data when the power is turned off (flash memory cards and flash drives (USB stick). Input devices enable data to go into the computer's memory. The most common input devices are the mouse and the keyboard. Output devices enable us to extract the finished product from the system. For example, the computer shows the output on the monitor or prints the results onto paper by means of a printer.

Buses and cards

The main circuit board inside your system is called the motherboard and contains the processor, the memory chips, expansions slots, and controllers for peripherals, connected by buses - electrical channels which allow devices inside the computer to communicate with each other. For example, the front side bus carries all data that passes from the CPU to other devices. The size of a bus, called bus width, determines how much data can be transmitted.

4. Primary storage

Data storage is one of the fundamental functions performed by a computer system. A computer stores data using various technologies, which creates different levels of data storage. Storage media are commonly classified into primary and secondary.

The term primary storage is used to describe internal storage devices, which can be directly accessed by the CPU with minimum or no delay. Primary storage is often referred to as primary memory and can be either volatile – RAM (Random Access Memory) and cache memory or non-volatile – ROM (Read Only Memory).

Read only memory chip is an integrated circuit which houses the instructions required to start the work of a computer. BIOS software is stored on a non -volatile ROM chip. The data in ROM can only be read by CPU, it cannot be modified. The CPU cannot directly access the ROM memory, the data has to be first transferred to the RAM, and then the CPU can access that data from the RAM. It is often used to store BIOS program on a computer motherboard. ROM was used as a storage media in a Nintendo, Gameboy, and Sega Genesis game cartridge. ROM chips store several MB (megabytes) of data, usually 4 to 8 MB per chip. It can vary in size from less than an inch in length to multiple inches in inches in length and width, depending on their use. ROM can be classified into• MROM, PROM, EPROM and EEPROM. • MROM: Masked read-only memory, it is as old as semiconductor technology and this type of ROM data is physically encoded in the circuit and only be programmed during fabrication. • PROM: Programmable ROM, it can be modified only once by the user. • EPROM: Erasable and Programmable ROM, the content of this 109 ROM can be erased using ultraviolet rays and ROM can be reprogrammed. • EEPROM: Electrically Erasable and Programmable ROM, it can be erased electrically and reprogrammed about ten thousand times. • FLASH ROM: Its modern designs have the feature of very high endurance, and flash memory can be erased and rewritten more quickly than conventional EEPROM (exceeding 1,000,000 cycles).

RAM stores the data which is currently processing by the CPU. The data which is easily modifiable are generally stored in the RAM. RAM is of two types:

1. Static Random Access Memory (SRAM)

2. Dynamic Random Access Memory (DRAM)

Static Random Access Memory (SRAM)

Data is stored in transistors and requires a constant power flow. Because of the continuous power, SRAM doesn't need to be refreshed to remember the data being stored. SRAM is called static as no change or action i.e. refreshing is not needed to keep the data intact. It is used in cache memories.

Dynamic Random Access Memory (DRAM)

Relatively less expensive RAM is DRAM, due to the use of one transistor and one capacitor in each cell. Data is stored in capacitors. Capacitors that store data in DRAM gradually discharge energy, no energy means the data has been lost. So, a periodic refresh of power is required in order to function. It is used to implement main memory. This memory is slower than S RAM.

Most PCs are held back not by the speed of the CPU, but by the time it takes to move data in and out of the memory. One of the most important techniques for getting around this bottleneck is the CPU cache. The cache is a smaller and fast memory component in the computer which is inserted between the CPU and the main memory.

To make this arrangement effective. The cache needs to be much faster than the main memory. This approach is more economical than the use of fast memory devices to implement the entire main memory. Cache is a storage device found on the CP U chip itself. It carries the copies of original data that has been accessed recently and therefore increases the speed at which data is accessed. When the processor needs to read or write a location in the main memory, it first checks for a corresponding entry in the cache. If the processor finds that the memory location is in the cache, a Cache Hit has occurred and data is read from the cache.

Only if the data is not in the cache does it need to access main memory, but it copies in the process whatever it finds into the cache so that it is there ready for the next time it is needed. The whole process is controlled by a group of logic circuits called the cache controller.

It is important to ensure that the cache and main memory contain consistent data. Two different techniques can be used to achieve this. In the write-through mode, data is simultaneously updated in cache and main memory. This method is

simpler and safer for data coherency. However, the write-through process is quite slow since modifications have to be written in both the cache and main memory. The main alternative is the write-back mode, which allows the processor to write changes only to the cache first. The main memory is not updated until the cache block needs to be replaced. Cache entries that have been changed are flagged as ‘dirty’ telling the cache controller to write their contents back to the main memory before using the space to cache new data. A write-back cache speeds up the write process but requires a more advanced cache controller. Most cache controllers move a ‘line’ of data rather than just a single item each time they need to transfer data between main memory and the cache, thus increasing the chance of a cache hit. The amount of data transferred each time is known as the ‘line size’.

5. Secondary Storage

Secondary storage devices are one of the solutions to keep data on the long-term basis. Secondary storage media are always non-volatile, considerably slow but offer greater storage capacity. Common examples of secondary storage devices are magnetic, optical devices and flash memory.

Magnetic storage devices store data by magnetizing particles on a disk or tape. It is covered with a magnetic coating and stores data in the form of tracks, sp ots and sectors. Hard disk drives and floppy disks are common examples of magnetic devices. A hard drive contains one or more platters housed inside an air-sealed casing. Data is written to the platters using a magnetic head, which moves rapi dly over them as they spin. When data is recorded on an HDD, it is converted from the digital form into the analogue form. Magnetized tiny area of the plate denotes a binary one; whereas, the demagnetized tiny area denotes a binary zero. The average time required for the read/write heads to move and find data is called seek time (or access time) and it is measured in milliseconds (ms); most hard drives have a seek time of 7 to 14 ms. While transfer rate means the average speed required to transmit data from the disk to the CPU, measured in megabytes per sec.

Traditionally, hard drives offer greater capacity and a lower price, but the situation is changing rapidly as solid state drives are replacing hard drives in laptops and desktop PCs. A solid-state drive (SSD) is a type of non-volatile storage media that uses integrated circuit assemblies to store data persistently. Two key components make up an SSD: a flash controller and flash memory chips. Whereas a spinning HDD reads and writes data magnetically, an SSD reads and writes the data to interconnected flash memory chips, which are fabricated out of silicon. Unlike a hard disk drive (HDD), an SSD has no moving parts and it is not so sensitive to shocks and vibrations.

Optical storage devices allow all read and write activities which are performed by laser beam. An optical disc is a flat disc that stores data in the form of p its. CDs, DVDs and Blue-ray discs are considered standards in today's optical storage market. One of the biggest advantages of optical storage over other storage media is durability. Among disadvantages of optical storage one can name its speed and

capacity.

Secondary storage plays a significant role in computer architecture for mul tiple reasons. There are many kinds of secondary storage, each with advantages and disadvantages. An emerging cloud computing is a remote server for data storage and backup that needs the Internet connection. It is up to you what to choose.

6. Software

Software is a set of instructions, rules or programs used to operate a comp uter system and instruct the system to carry out specific tasks. Software can be classified into two main categories: system software and application software. Some common system software examples include: operating systems, firmware, device drivers. The most common types of application software are word processors which are used to create documents as well as edit, format and output text (e.g. MS Word, Google Docs), database software which helps in creating and managing datab ases (e.g. Oracle, MySQL), web Browsers which are mainly used for surfing the Internet to help the user find specific web addresses or retrieve data across the web (e.g. Google Chrome, Internet Explorer), spreadsheets which are used for data organization, analysis and storage in tabular form (e.g. Excel).

Let's focus on an operating system which acts as an intermediary between application programs and computer hardware. An operating system has three main functions: manage the computer's resources, such as the central processing unit, disk drives, establish a computer interface and execute and provide services for application software.

OS can be single-tasking systems that can run only one program at a time, while a multi-tasking operating system allows more than one program to start simultaneously. Multi-tasking operating systems are also known as time-sharing systems since the available processor time is divided between multiple processes. Multitasking may be characterized in preemptive and cooperative types. In preemptive multi-tasking, the operating system shares the processor time and allocates a slot for each program. In cooperative multitasking, the operating system never initiates the switching between processes to share the CPU computing resources.

In a single-user operating system, only one user can have access to the computer system at a time. Single-user operating systems can be classified into 2 types: single-user single-tasking operating systems and single-user multi-tasking operating systems. A single-user single-tasking OS, as its name suggests, allows a single user to do only one task at a time. In a single-user multi-tasking OS, a single user can

perform multiple tasks simultaneously.

The desktop operating systems are designed to manage a personal computer. The purpose of a mobile OS is to provide environment for application software to run on mobile devices.

An open-source operating system means that a source code is visible p ublically and editable. In proprietary software, the source code is protected and the vendor controls software updates and users can't add features to proprietary software themselves.

Every operating system requires a user interface enabling users to interact with the OS in order to set up the operating system and its hardware. There are two primary types of user interface available: CLI and GUI. Applying Command Line Interface (CLI) means that the user runs a program by typing a command. Other operating systems have the GUI (Graphical User Interface) that allows the user to use a mouse to click on icons on the screen or choose commands from a list of choices known as a menu. The distinct feature of a GUI is the use of WIMP environment: windows, icons, menus and pointer.

7. Networks: types, topologies, hardware network components

A network is a collection of computers, servers and network devices connected to one another to allow the sharing of data. Networks can be classified according to different criteria.

Based on geographical area networks can be classified into three categories.

LANs (Local Area Networks) cover a small geographical area such as an office, a home, a building, or a group of buildings. MANs (Metropolitan Area Networks) span an entire city. WANs (Wide Area Networks) cover a country or a continent. The largest WAN in existence is the Internet, which connects millions of p eople all over the world.

Following network architecture two types, peer-to-peer and client-server architecture, are considered. In a client-server network, one computer acts as a server. It stores and distributes data to the other nodes, or clients. In a peer-to-peer network, all the computers have the same capabilities - that is, share files and peripherals without requiring a separate server computer.

A network topology is a configuration of the elements of a network. Typical network configurations include 6 topologies.

Star network: all nodes are connected to a special central node.

Bus network: all nodes are connected to a single cable that acts as the backbone of the entire network.

Ring topology: each device/node is connected with its neighboring node forming the shape of a ring, hence its name.

Tree topology: all the computers are connected like the branches of a tree. In computer networking, tree topology is known as a combination of a bus and star network topologies.

Mesh topology: a network topology in which the infrastructure nodes connect directly to as many other nodes as possible.

Hybrid topology: this type includes a mix of bus topology, mesh topology, ring topology, star topology, and tree topology. The combination of topologies depends on the need of a company.

On basis of physical medium there are two types of networks. In wired LAN, two or more personal computers are connected through such communication media as coaxial or twisted-pair cables. High-speed fiber optic cables are usually used to send data over longer distances. Wireless networks, on the other hand, use electromagnetic waves, such as radio waves, to transmit data.

In computer networks, we have multiple networking devices such as modems, routers, hubs, switches, bridges, gateways, etc. Each device has its own specification and is used for a particular purpose.

Computer networks are one of the important aspects of Computer Science. In the early days, they were used for data transmission on telep hone lines and had a very limited use, but nowadays, the integration of computers and other different devices allows users to communicate more easily.

8. The Internet

Digital Subscriber Line (DSL) is a high-speed Internet connection, which utilizes the standard telephone lines. It allows the full bandwidth of the copper twisted-pair telephone cabling to be utilized. The DSL signal is pulled out from the phone line as it enters the premises and is wired sep arately to a DSL modem. DSL service can be delivered simultaneously with wired telephone service through the same telephone line since DSL uses higher frequency bands for data transmission. The most commonly installed DSL technology for Internet access is ADSL (Asymmetric Digital Subscriber Line). It is asymmetric because the download speed is faster than upload speed.

Although DSL makes use of telephone cabling, it should not be confused with the dial-up connection of yesteryear. A dial-up connection to the Internet was set up by dialing a phone number, hence the name. It can carry voice or data signals over the copper telephone wire at a time and it was impossible to use the phone to make calls and browse the Internet at the same time.

Cable Internet is a form of broadband Internet access that uses the infrastructure of cable TV networks to provide Internet services. It is integrated into the cable television infrastructure analogously to DSL. Since TV itself takes up only a small portion of the cable's bandwidth, it leaves room for Internet access to be provided through the same network.

First, your Internet Service Provider sends a data signal through the coaxial cable into your home — specifically, to a cable modem. The cable modem then connects to your computer and other devices via an Ethernet cable or through Wi -Fi network using a Wi-Fi router.

A cable connection is highly reliable and is not subject to outages due to storms, like satellite Internet. However, since residential cable Internet access is provided through shared bandwidth, the speed can be slower during peak usage hours when a lot of Internet users are online. This does not happen with a DSL network, which keeps a consistent Internet signal because each subscriber has their own dedicated line.

Fiber-optic Internet uses fiber-optic cables instead of copper wires and it is

incredibly fast. Those cables send data to and from a computer by harnessing the power of light and can carry data over long distances with low attenuation and distortion of the light signal. That light signal uses binary system to communicate with computers. The presence of light indicates a binary one and the absence of light indicates a binary zero. Fiber-optic cables transfer data faster than copper wiring, which means faster load times and higher-quality streaming.

The three wireless technologies widely used today are Wi-Fi, cellular and satellite Internet. Wi-Fi uses radio waves to wirelessly connect devices and is commonly applied for local area networking. To get access to the Internet, a device (a tablet or a smartphone) has to be connected over Wi-Fi to a wireless router. Internet over Satellite usually allows a user to access the Net via a geostationary satellite that orbits the Earth. As signals must travel long distances from the Earth up to the satellite and back again, it may cause a delay between the request and the answer. However, modern technologies make it possible to minimize this latency. Satellite Internet access can provide high-speed Internet. To get access to the Internet, one needs a satellite dish for two-way (upload and download) data communications and a modem.

A cellular network is a communication network distributed over land areas called "cells". Each cell has at least one fixed-location transceiver, but more commonly, there are three cell sites. These base stations (cell towers) provide a cell with the network coverage, which can be used for transmission of voice and data. A cell typically uses a different set of frequencies from the neighboring cells to avoid interference and provide guaranteed service quality within each cell.

Circuit switching establishes a dedicated communication path before data transmission begins. So, no other devices can use this path while it’s reserved even if it’s idle, which leads to a waste of bandwidth. Data is not divided into units, so the complete data is to be transmitted through the same route. Circuit switching is mainly utilized in public switched telephone networks. Once you build the circuit, it is in place until you tear it down. Packet switching refers to a technique where data is divided into multiple units called packets. There are two different approaches used for packet switching: datagram packet switching and virtual circuit switching. In datagram packet switching technique, there is no dedicated channel for data

transmission and packets can be routed individually through different paths. The packets are later reassembled in the original order based on the sequence number of each packet. The major advantage of this technology is that it provides a more efficient use of Internet bandwidth.

Virtual circuit switching is a connection-oriented technique that combines the characteristics of circuit switching and datagram packet switching. In this type of packet switching technology, a virtual connection is first established between the source and destination and the packets are then routed along this path sequentially.

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

The number of layers is sometimes referred to as five or four. We'll study five layers. The Physical Layer and Data Link Layer are referred to as one single layer as the 'Physical Layer' or 'Network Interface Layer' in the 4-layer reference.

9. Search engines

A search engine is a software program that provides information according to the user query. It finds various websites or web pages that are available on the internet and gives related results according to the search. Today, there are many different search engines available on the Internet, each with its own abilities and features.

Search engines can be classified into the following three categories:

1) crawler-based search engines;

2) human-powered directories;

3) meta-search engines.

Crawler-based search engines such as Google and Yahoo, compile their listings automatically. There are three basic steps that every crawler-based search engine follows before displaying search results: crawling, indexing, ranking. Search engines crawl the whole web to fetch the web pages available. A piece of software called crawler or bot or spider, performs the crawling of the entire web. Various data mining techniques are used to define which pages should be crawled and the crawling frequency.

Indexing is next step after crawling which is a process of identifying the words and expressions that best describe the page. The identified words are referred as keywords and the page is assigned to the identified keywords.

Then, the ranking process involves determining which pieces of content are the best results for specific queries. When someone types a search query, the engine searches through the index to find relevant content. The search engine ranks these results according to how relevant they are. A website with a high ranking means the search engine thinks it is more relevant than other results.

Human-powered directories like Yahoo! Directory, Open Directory and LookSmart depend on human editors to compile their listings showing results that are added manually. Firstly, a short description along with the website URL is submitted to the directory for approval. Then submitted site is then manually reviewed and added in the appropriate category or rejected for listing. Keywords entered in the search box will be matched with the description of the site.

Meta-search engine like MetaCrawler or Dogpile do not have a database of indexed pages of its own. They combine the results of various search engines into one and give one result. They send users' queries to several other search engines and compiles top results from each into one overall list. These results are processed, ranked and presented to the user.

Search engines are designed to find answers for internet users. They organize the internet so that you can instantly discover relevant search results.

10. Programming languages

Programming is the process of writing a program using a computer language. A program is a set of instructions which a computer uses to do a specific task. The only language a PC can directly execute is machine code, which consists of 1s and 0s. This language is difficult to write, so we use symbolic languages that are easier to understand. For example, assembly languages use abbreviations such as ADD, SUB, MPY to represent instructions. The program is then translated into machine code by software called an assembler. Machine code and assembly languages are called low - level languages because they are closer to the hardware.

As they are quite complex and restricted to particular machines software developers designed high-level languages, which are closer to the English language to make the programs easier to write and to overcome the intercommunication problem between different types of computers. Here are some examples.

FORTRAN was one of the first high-level programming languages designed by IBM in mid-1950s for scientific and engineering computations. It introduced the concept of high-level abstraction allowing programmers to write a code closer to human language.

C was used to write system software, graphics and commercial programs.

Java was designed to run on the Web; Java applets are small programs that run automatically on web pages and let you watch animated characters, and p lay music and games. Java popularized object-oriented programming (OOP) denoting writing program code that's more intuitive and reusable; in other words, code that shortens program-development time.

Python was created in 1989 and has become popular for various applications, including web development, data analysis, and artificial intelligence.

Programs written in high-level languages must be translated into machine code by a compiler or an interpreter. A compiler translates the source code into object code - that is, it converts the entire program into machine code in one go. On the other hand, an interpreter translates the source code line by line as the program is running.

A programming language is the backbone of this digital world. Everything in this world from every electronic device to software programs and websites is

operating because of programming languages.

11. Basics of web design

Web design is the process of planning and arranging content online. The first web page was created at CERN by Tim Berners-Lee on August 6, 1991. Since then designing a website has changed a lot both in aesthetics and functionality. Web design also includes web apps, mobile apps and user interface design.

A web page is often used to provide information to viewers, including pictures or videos to help illustrate important topics. A web page may also be used as a method to sell products or services to viewers.

Web designers use Hyper Text Markup Language (HTML). HTML is a code used to describe the structure of information on a webpage. HTML consists of commands called tags which are placed around different kinds of contents (e.g. tables, paragraphs, lists, hyperlinks, images, videos, etc.) telling the web browser how to display them.

But you do not need to understand HTML to make your own personal home page. Many word-processing, desktop publishing programs will generate HTML tags for you. To upload or copy your web page use the server's File Transfer Protocol (FTP). Elements usually have an opening tag and a closing tag, and give information about the content they contain.

CSS also known as Cascading Style Sheets is a design mechanism whose primary function is to improve the appearance of a webpage by defining its styling and layout. CSS provides a way to define and apply styles across all pages of a website, making it easier for developers to maintain and update their designs. CSS is a core technology of the World Wide Web, alongside HTML and JavaScript.

JavaScript is another core technology of the World Wide Web. It is a cross-platform, object-oriented programming language used by develop ers to make web pages interactive and user-friendly. It allows developers to create dynamically updating content, use animations, pop-up menus, clickable buttons, etc. HTML & CSS are used to control presentation, formatting, and layout, JavaScript is used to control the behavior of different web elements.

Though webpages are different there are multiple webpage elements that most pages contain.

Text is the most significant element of any web site because users surf the web in search of information expressed in hypertext. Text is displayed in a variety of fonts and sizes. Most text files are available in two formats: HTML or PDF.

Background underlies colours and patterns of a webpage.

Tables with columns and rows are used to position images and text on a page.

Frames are a kind of independent box in which you can load a Web page.

A hyperlink is an element in an HTML document that links to either another portion of the document or to another document altogether. On webpages hyperlinks are usually colored purple or blue and are sometimes underlined.

An icon is a pictogram displayed on a computer screen in order to help us navigate a computer system using a mouse, pointer, finger or recently voice commands.

Graphics deals with generating images with the aid of computers, displaying art and image data effectively and meaningfully to the consumer, processing image data received from the physical world, such as photo and video content.

A web page can be accessed by entering a URL address into a browser's address bar. It may contain text, graphics, and hyperlinks to other web pages and files. When you click a link provided by a search engine, you are accessing a web page. T he Internet consists of millions of web pages, with more being added every day

12. Security and privacy on the Internet

There are many benefits from an open system like the Internet, but one of the risks is that we are often exposed to hackers, who break into computer systems.

To avoid risks, you should set all security alerts to high on your web browser.

Mozilla Firefox displays a lock when the website is secure and allows you to disable or delete cookies - small files placed on your hard drive by web servers so that t hey can recognize your PC when you return to their site.

If you use online banking services, make sure they use digital certificates - files that are like digital identification cards and that identify users and web servers.

Private networks can be attacked by intruders who attempt to obtain information such as Social Security numbers, bank accounts or research and business reports. To protect crucial data, companies hire security consultants who analyze the risks and provide solutions. The most common methods of protection are passwords for access control, firewalls, and encryption and decryption systems. Encryption changes data into a secret code so that only someone with a key can read it. Decryption converts encrypted data back into its original form.

Malware (malicious software) are programs designed to infiltrate or damage your computer, for example viruses, worms, Trojans and spyware. A virus can enter a PC via an infected USB flash drive or via the Internet. A comp uter virus is a very small program routine that infects a computer system and uses its resources to reproduce itself. It often does this by patching the op erating system to enable it to detect program files, such as COM or EXE files. It then copies itself into those files. This sometimes causes harm to the host computer system.

The virus remains dormant until the infected host file is activated. Only after the host file is activated, the virus can run, executing malicious code and replicating itself to infect other files on the computer.

When the user runs an infected program, it is loaded into memory carrying the virus. The virus uses a common programming technique to stay resident in memory. When it infects a file, the virus replaces the first instruction in the host p rogram with a command that changes the normal execution sequence. This type of command is known as a JUMP command and causes the virus instructions to be executed

before the host program. The virus then returns control to the host program which then continues with its normal sequence of instructions and is executed in the normal way.

Any virus has four main parts. A misdirection routine that enables it to hide itself; a reproduction routine that allows it to copy itself to other programs; a trigger that causes the payload to be activated at a particular time or when a particular event takes place; and a payload that may be a fairly harmless joke or may be very destructive. A program that has a payload but does not have a reproduction routine is known as a Trojan.

The main difference between a virus and a worm is that viruses must be triggered by the activation of their host, whereas worms are standalone malicious programs that can self-replicate and propagate independently through email attachments. Once a worm has entered the system, it can run, self-replicate and propagate without a triggering event. A worm makes multiple copies of itself, which then spread across the network. These copies will infect any inadequately p rotected computers and servers that connect - via the network or internet - to the originally infected device.

A Trojan horse is disguised as a useful program; it may affect data security.

Spyware collects information from your PC without your consent. Most spyware and adware (software that allows pop-ups - that is, advertisements that suddenly appear on your screen) is included with 'free' downloads.

If you want to protect your PC, don't open email attachments from strangers and take care when downloading files from the Web. Remember to update your anti-virus software as often as possible, since new viruses are being created all the time.

Viruses are often attached or concealed in downloaded files. When the host file is accepted by a system, the virus remains dormant until the infected host file is activated. Only after the host file is activated, the virus can run, executing malicious code and replicating itself to infect other files on the computer.

13. Data security

There are a variety of security measures that can be used to protect hardware and software including:

1. Installing a firewall to protect networks from external and internal attacks.

There are several ways that firewalls work. Most use a combination of methods. One common method is packet filtering. Incoming data is broken down into small chunks, or packets. The firewall then inspects each packet using a set of filters. Based on settings determined by the user, the firewall decides whether to deny or permit access. For example, filters can block all access to and from specific domain names. If a network administrator notices a particular IP address is generating a lot of traffic to or from the network, he or she could create a filter to block that IP address. Filters can also look for certain words or p hrases. For most users, the default settings of the program will provide enough protection. A user can always create an exception to allow an unauthorized program. This gives the program permission to communicate through the firewall, even if the program is normally blocked. The program accesses the Internet without lowering the settings for the whole firewall.

2. Backing up data and programs.

There are different types of backup including incremental backup which are copies all the selected files that have been created or changed since the last backup (full , differential or incremental). These files are identified by the fact that their archive bit would be on. The archivebit is a digital bit stored with a file indicating if the file has been backed up since it was edited. The archive bit is switched off when the file is backed up using a full or incremental backup. Differential backup which copies all the files created or modified since the last full backup. The archive bit is not set to “off” by a differential backup. Full backup which cop ies all the selected files on a system, whether or not they have been edited or backed up before.

3. Protecting against natural disasters by installing uninterruptible power

supplies and surge protectors.

4. Password-protect programs and data with passwords which cannot easily be cracked.

5. Encrypting data

Data encryption converts data into a different form (code) that can only be accessed by people who have a secret key (formally known as a decryp tion key) or password. Data that has not been encrypted is referred to as plaintext, and data that has been encrypted is referred to as ciphertext. Encryption is one of the most widely used and successful data protection technologies in today's corporate world. Encryption is a critical tool for maintaining data integrity, and its importance cannot be overstated. Almost everything on the internet has been encrypted at some point.

6. Use signature verification or biometric security devices to ensure user authorization.

7. Protect against viruses by using antivirus programs. Use only vendor-supplied software or public domain (free software) or shareware p roducts that are supplied by services that guarantee they are virus-free. Antivirus software is designed to detect, prevent and take action to disarm or remove malicious software from your computer such as viruses, worms and Trojan horses. Don't visit suspicious websites, hackers have much more nuanced ways of getting their viruses on your computers, which is why you need a robust antivirus to stay one step ahead of them. Some antivirus software will ask for your permission before "cleaning" a file to remove malicious code. If you prefer a hands-off approach, you can adjust the settings so the software automatically removes malicious files.

Every virus contains a signature, which is like its fingerprint. It's the distinguishing feature that sets it apart from other programs running on your computer, and it also makes the virus recognizable, and therefore a p otential target for antivirus software. Documents, programs and applications are generally scanned for viruses when they are being used. Once an executable file is downloaded, it is instantly scanned to check if it is infected with malware. As opposed to signature-based scanning, which matches signatures found in files with that of a database of known malware, heuristic scanning uses rules and algorithms to look for commands which may indicate malicious intent. This causes the antivirus programming to

recognize new malware without having the exact match in the database. Most antivirus programs use both signature and heuristic-based methods in combination, in order to catch any malware that may try to evade detection.

14. IT Trends. What to expect in the future?

The rapidly changing technologies often surpass our ability to foresee its advancements. However, let's have a look into the future of IT sphere. We will focus on two main IT trends - artificial neural networks and Internet of Things (IoT).

Artificial neural networks (ANN) are a type of Artificial Intelligence (AI) designed to mimic how the human brain processes information. ANN consists of interconnected nodes, or neurons, that process information similarly to the human brain. The artificial neurons receive input and then use the information to create the output or data. In between the input units and output units are one or more layers of hidden units, which, together, form the majority of the artificial brain. Most neural networks are fully connected, which means each unit in one layer is connected to every unit in another layer. The connections between one unit and another are represented by a number called a weight, which can be either positive or negative.

Convolutional neural networks (CNN) are one of the most popular models used today. This neural network computational model uses a variation of multilayer perceptrons and contains one or more convolutional layers that can be either entirely connected or pooled. These convolutional layers create feature map s that record a region of image which is ultimately broken into rectangles and sent out for nonlinear processing.

Recurrent neural networks (RNN) are more complex. They save the output of processing nodes and feed the result back into the model (they did not pass the information in one direction only). This is how the model is said to learn to predict the outcome of a layer. Each node in the RNN model acts as a memory cell, continuing the computation and implementation of operations. If the network's prediction is incorrect, then the system self-learns and continues working towards the correct prediction during backpropagation.

Neural network can accomplish many tasks: from face recognition and making cars drive autonomously on the roads, to generating shockingly realistic CGI (Computer-Generated Image) faces, to

machine translation, to fraud detection,
clustering, pattern recognition and to predict
outcomes. Neural networks are trained.
Neural networks learn things by a
feedback process called backpropagation.
This involves comparing the output a network produces with the output it was meant to produce, and using the difference between them to modify the weights of the connections between the units in the network, working from the output units through the hidden units to the input units — going backward, in other words.
On a technical level, one of the main challenges is the amount of time it takes to train networks. Another big issue is that neural networks are 'black boxes', in which the user feeds in data and receives answers. We can fine-tune the answers, but we don't have access to the exact decision-making process. This is the problem a number of researchers are working on today, but it will only become more important as artificial neural networks play a bigger and bigger role in our lives.
The Internet of Things, or IoT, is a system of interrelated physical objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT can also use artificial intelligence (AI) and machine learning to make data collecting processes easier and more dynamic.
IoT is essential to business. IoT enables companies to automate p rocesses and reduce labor costs. It also cuts down on waste and improves service delivery, making it less expensive to manufacture and deliver goods.
IoT is developing and needs improvement. Among disadvantages are the risk that a hacker could steal confidential information also increases, IoT challenges to collect and manage the data from multiple devices, problems with bugs in a network, absence of international standard of compatibility for IoT. It can be comp ensated by its ability to access information from anywhere at any time on any device, transferring data packets over a connected network saving time and money, automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

15. Types of Computers and their Use

Information Technology is a broad field that includes a lot of sp ecialties. You can work in computer support, hardware and software engineering, cybersecurity, cloud computing or web development. Information technology professionals study, design, support, manage, implement computer-based information systems including both software applications and computer hardware. Let's have a look at some of th e IT professions.

Hardware engineers draw on computer engineering to develop, design and test various physical components related to computer systems. Their job also involves designing and creating prototypes as well as overseeing the manufacturing and installation process to ensure the hardware meets the existing standards and functions properly.

Software engineers research, design and write new software programs and computer operating systems. They apply engineering p rinciples and knowledge of programming languages to build software solutions for end users.

A system administrator is responsible for maintaining an organization's computer systems and providing a reliable work environment. They perform ongoing monitoring of all servers to make sure the systems function properly, install and upgrade computer components and software, troubleshoot technical issues.

Data scientists should be good at manipulating and analyzing large amounts of data to categorize it by patterns and trends.

An IT security specialist should have an in-depth understanding of a variety of cyber security threats that may affect the company they work in. They are responsible for implementing and overseeing an organization's security systems.

Database administrators employ specialized software to organize and keep track of data. Responsibilities can vary according to a company's needs but typically include: archiving data, implementing security measures, troubleshooting, keeping the database up to date, ensuring that the database is correctly backed up and can recovered in case of data loss.

A network engineer is responsible for designing, implementing, monitoring and managing the local and wide area networks, giving technical support to staff, fixing

network faults.

Full-stack developers should be creative, graphically inclined, and have excellent attention to details. They are responsible for both front -end and back-end development.

IT directors ensure that department tasks correspond to the company's goals and development, implement IT policy, provide direction for IT team members, running regular checks on network and data security.

These professions play a vital role in our everyday life. Information technology is an appealing career field for young people. As technology continues to advance, IT specialists will be of high demand in the future.