3 EMERGING TRENDS
(NCERT CLASS 11)

INTRODUCTION

Many emerging trends in computer science involve various technologies that have grown at a faster pace. Emerging trends could be identified by simply being updated with journals and newspapers, and social gatherings. Technology has been increasing tremendously over the years. The infrastructure provided by various companies for their growth has been an excellent resource for innovating new technologies. The emerging trends in the information technology industry like Artificial Intelligence (AI), Robotics, Data Analytics, Cyber Security, Bioinformatics, Education involving technological assistance, etc., have seen a positive trend in recent years. These trends also have the potential of growing exponentially to the foreseeable future.

ARTIFICIAL INTELLIGENCE (AI)

- Artificial Intelligence is comprised of two words Artificial and Intelligence, where Artificial means "man-made," and intelligence means "thinking power", hence AI means "a man-made thinking power.
- "Artificial Intelligence exists there ,where a machine can have human based skills such as learning, reasoning, and solving problems.
- According to the father of Artificial Intelligence, John McCarthy, it is "The science and engineering of making intelligent machines.
- **Goals of AI :**
  - (I) To Create Expert Systems ? The systems which holds intelligent behavior, learn, demonstrate, explain, and advice its users.
  - (II) To Implement Human Intelligence in Machines? Creating systems that can understand, think, learn, and behave like humans.

Applications of AI :- AI has been dominant in various fields such as –

(I) Gaming
(II) Natural Language Processing
(III) Expert Systems
(IV) Vision Systems
(V) Speech Recognition
(VI) Handwriting Recognition
(VII) Intelligent Robots

Artificial intelligence is a science and technology based on disciplines such as Computer Science, Biology, Psychology, Linguistics, Mathematics, and Engineering.

Difference between Normal Programming and AI Programming :

	NORMAL/REGULAR PROGRAMMING	AI PROGRAMMING
INPUT	Input is a sequence of alphanumeric symbols presented and stored as per some given set of previously stipulated rules and that uses a limited set of communication media such as keyboard, mouse, disc, etc.	Input may be a sight, sound, touch, smell or taste. Sight means one dimensional symbols such as typed text, two dimensional objects or three dimensional scenes.
PROCESSIN	Processing means manipulation of the stored symbols by a set of previously defined algorithms.	Processing includes knowledge representation and pattern matching, search, logic, problem solving and learning.
OUTPUT	output is a sequence of alphanumeric symbols, may be in a given set of colors that is placed on such a medium as a CRT screen, paper, or magnetic disk.	Output can be in the form of printed language and synthesized speech, manipulation of physical objects or locomotion i.e., movement in space.

- **Advantages of Artificial Intelligence :**
  - (I) **High Accuracy with less errors :** it takes decisions as per preexperience or information.
  - (II) **High-Speed.**

(III) **High reliability :** can perform the same action multiple times with high accuracy.

(IV) **Useful for risky areas :** helpful in situations such as defusing a bomb, exploring the ocean floor, where to employ a human can be risky.

(V) **Digital Assistant :** Such as used by various E-commerce websites to show the products as per customer requirement.

(VI) **Useful as a public utility :** such as a self-driving car which can make our journey safer and hassle-free, facial recognition for security purpose, Natural language processing to communicate with the human in human-language, etc.

Artificial intelligence can be divided into three subfields:

(I) Artificial intelligence

(II) Machine learning

(III) Deep learning

MACHINE LEARNING

Machine Learning is a system that can learn from example through self-improvement and without being explicitly coded by programmer. As its name, it gives the computer that makes it more similar to humans: The ability to learn.

- Applications of Machine Learning:-
  - (I) Image Recognition.
  - (II) Speech Recognition.
  - (III) Traffic prediction.
  - (IV) Product recommendations.
  - (V) Self-driving cars.
  - (VI) Email Spam and Malware Filtering.
  - (VII) Virtual Personal Assistant.
  - (VIII) Online Fraud Detection.
  - (IX) Stock Market trading.
  - (X) Medical Diagnosis.
  - (XI) Automatic Language Translation.
- **WORKING OF MACHINE LEARNING :**
  - (I) Clustering is the most common unsupervised learning technique. It is used for exploratory data analysis to find hidden patterns or groupings in data. Applications for cluster analysis include gene sequence analysis, market research, and object recognition.
  - (II) Classification techniques predict discrete responses—for example, whethera n email is genuine or spam, or whether a tumor is cancerous or benign.
  - (III) Regression techniques predict continuous responses—for example, changes in temperature or fluctuations in power demand.

NATURAL LANGUAGE PROCESSING (NLP)

NLP is a way of computers to analyze, understand and derive meaning from a human languages such as English, Spanish, Hindi, etc. It is the technology that is used by machines to understand, analyse, manipulate, and interpret human's languages.

- **Components of NLP :** There are the following two components of NLP:-
  - (I) Natural Language Understanding (NLU).
  - (II) Natural Language Generation (NLG).
- Applications of NLP:-
  - (I) Question Answering
  - (II) Spam Detection
  - (III) Sentiment Analysis
  - (IV) Machine Translation
  - (V) Spelling correction
  - (VI) Speech Recognition
  - (VII) Chatbot
  - (VIII) Information extraction
- An "immersive experience" pulls a person into a new or augmented reality, enhancing everyday life via technology. It often use one or more technologies linked together. The three pillars of immersive experiences are visual quality, sound quality, and intuitive interactions. Full immersion can only be achieved by simultaneously applied all these three.
- **How does Augmented Reality work :** It involves technologies like S.L.A.M. (simultaneous localization and mapping), depth tracking (briefly, a sensor data calculating the distance to the objects), and the following components:
  - (I) **Cameras and sensors :** Collecting data about user's interactions and sending it for processing.
  - (II) **Processing :** AR devices eventually should act like little computersto be able to measure speed, angle, direction, orientation in space, and so on.
  - (III) **Projection :** This refers to a miniature projector on AR headsets, which takes data from sensors and projects digital content.
  - (IV) **Reflection :** Some AR devices have mirrors to assist human eyes to view virtual images.
- **Applications of AR :**
  - (I) Most popular applications of AR is gaming. New AR games provide much better experiences to players, some even promote a more active outgoing way of life (PokemonGo, Ingress).

(II) AR in retail may act to bring better customer engagement and retention, as well as brand awareness and more sales. Some features may also help customers make wiser purchases – providing product data with 3D models of any size or color.

- Virtual Reality (VR) is use of computer technology to create a simulated environment. Unlike traditional user interfaces, VR places the user inside an experience. Instead of viewing a screen in front of them, users are immersed and able to interact with 3D worlds/objects.
- **The Basics of how VR Works :** Every headset is used to perfect their approach to creating an immersive 3D environment. Each VR headset puts up a screen in front of eyes thus, eliminating any interaction with the real world. Two autofocus lenses are generally placed between the screen and the eyes that adjust based on individual eye movement and positioning.

  The visuals on the screen are rendered either by using a mobile phone or HDMI cable connected to a PC. A frame rate of minimum 60fps, an equally competent refresh rate and minimum 100-degree field of view (FOV) is required for true VR.
- **Applications of VR :**
  (I) Automotive industry.
  (II) Healthcare.
  (III) Retail
  (IV) Tourism
  (V) Real estate
  (VI) Architecture
  (VII) Gambling
  (VIII) Learning and Development.

BIG DATA

Big Data is also data but with a huge size/volume and yet growing exponentially with time. In short such data is so large and complex that none of the traditional data management tools are able to store it or process it efficiently.

- **Benefits of Big Data Processing :**
  (I) Businesses can utilize outside intelligence while taking decisions.
  (II) Improved customer service.
  (III) Early identification of risk to the product/ services, if any.
  (IV) Better operational efficiency.
- **Characteristics Of Big Data :**
  (I) **Volume :** The name Big Data itself is related to a size which is enormous.
  (II) **Variety :** Variety refers to heterogeneous sources and the nature of data, both structured and unstructured. During earlier days, spread sheets and databases were the only sources of data considered by most of the applications as structured big data type. Nowadays, data in the form of emails, photos, videos, monitoring devices, PDFs, audio, etc. are also being considered in the analysis applications. This variety of unstructured data poses certain issues for storage, mining and analyzing data.
  (III) **Velocity :** It means speed of generation of data. How fast the data is generated and processed to meet the demands, determines real potential in the data.
  (IV) **Variability :** This refers to the inconsistency which can be shown by the data at times.

INTERNET OF THINGS (IOT)

- The IOT concept was initially proposed by a member of the Radio Frequency Identification (RFID) development community in 1999, and now it has become more relevant to the practical world as the use of mobile devices, embedded devices, communication, cloud computing and data analytics has increased. Internet connects all people means "Internet of People" IoT connects all things means "Internet of Things".
- Interconnection of Things/Objects/Machines, e.g., sensors, mobilephones, electronic devices, home appliances, any existing items and interact with each other via Internet.
- Internet of Things technology can include any sensor, electronic devices or software which are connected to the internet and can be utilized remotely and can exchange data. Here devices works themselves without human intervention for the welfare of humans.
- **MAJOR CHARACTERISTICS OF IOT :**
  (I) Very Large Scale.
  (II) Heterogeneity.
  (III) Pervasivity : Computing and Communication technologies embedded in our environments.
- **How Does the Internet of Things Work?**

  The Internet of Things is an aggregation of internet enabled sensors, smart devices and software that can be manipulated by scripts, applications and user interfaces across long distances.

- **Applications of IOT :**

(I) **Smart house :** Suppose we are not at home and doubts starts in our mind. Did I turn the coffee maker off? Did I set the security alarm? etc. With a smart home,we can quiet all of these worries with a quick glance at smartphone/tablet. we can connect the devices and appliances in our home so they can communicate with each other and with us and can work with the commands given over smartphone remotely.

(II) **Smart car :** the driverless car (now a prototype) where taxis work based on AI and take the passengers safely and accurately to the desired destination.

(III) **Elderly care :** Patient surveillance can be life-saving; automatically detecting when someone falls down or when they begin to experience a heart attack so that emergency care can be sent immediately.

(IV) **Disaster warning :** Sensors can collect critical information about the environment, allowing for early detection of environmental disasters like earthquakes, tsunamis, etc., thus saving lives.

(V) **Delivery Drones :** drones being used to deliver item with the help of smart grid/geospatial data.

(VI) A smart city is a framework, predominantly composed of Information and Communication Technologies (ICT), to develop, deploy, and promote sustainable development practices to address growing urbanization challenges. A big part of this ICT framework is essentially an intelligent network of connected objects and machines that transmit data using wireless technology and the cloud.

- **IoT Platform :** It is an integrated service which offers the things to bring physical objects online. It easily allow to configure devices for machine-to-machine communication through millions of devices connects simultaneously .

Sensors are useful and very important for the devices in order to fetch the data. The data can be real-time, which includes the current temperature, pressure or humidity.

List of Sensors most commonly used in the IoT devices:-

(I) Temperature Sensor

(II) Pressure Sensor

(III) Proximity Sensor

(IV) Accelerometer and Gyroscope Sensor

(V) IR Sensor

(VI) Optical Sensor

(VII) Gas Sensor

(VIII) Smoke Sensor

- **IoT Platform Types :**

(I) **End-to-end IoT Platforms :** provide the hardware, software, connectivity, security, and device management tools to handle connection of millions of concurrent device.

(II) **Connectivity Management Platforms :** It offer low power and low cost connectivity management solutions through Wi-Fi and cellular technologies.

(III) **IoT Cloud Platforms :** It's aim to get rid of the complexity of building our own complex network .

(IV) **Data Platform –** It deals with data in some way with the tools we need to route device data and manage / visualize data analytics.

CLOUD COMPUTING

Cloud refers to a Internet or Network or present at remote location. Cloud Computing refers to remote access of hardware/software resources for access, configuration, manipulation. Cloud computing offers online data storage, infrastructure, and application. Applications such as customer relationship management (CRM) ,e-mail, web conferencing, execute on cloud. It can work on public and private networks, i.e., WAN, LAN or VPN.

Cloud computing offers platform independency, because software is not required to be installed locally on the PC.Thus applications are being mobile and collaborative.

- **Uses of cloud computing :**

(I) Create new apps and services.

(II) Store, back up and recover data.

(III) Host websites and blogs.

(IV) Stream audio and video.

(V) Deliver software on demand.

(VI) Analyze data for patterns and make predictions.

DIFFERENCE BETWEEN PUBLIC AND PRIVATE CLOUD	
PUBLIC CLOUD	**PRIVATE CLOUD**
Hosted at service provider site.	Hosted at Enterprise or service provider server.
Cheaper than private cloud.	Costlier than public cloud.
Utilizes shared infrastructure.	Utilizes own infrastructure.
Supports connectivity over internet.	Supports connectivity over internet/Private WAN.
Require higher level of security.	Require medium level of security.
Supports multiple customers.	Supports one customer.
Shared server.	Dedicated server.
Fixed cost. Multitenant architecture.	Variable cost. Dedicated customer architecture.
Example - ESDS's eNlight Cloud, Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.	Hewlett Packard Enterprise (HPE) — offers the Helion Cloud Suite software, Helion CloudSystem hardware, Helion Managed Private Cloud and Managed Virtual Private Cloud services

SOFTWARE AS A SERVICE (SaaS)

SaaS is a fully-developed software solution ready for purchase and use over the internet on a subscription basis. The SaaS provider manages the infrastructure, operating systems, middleware, and data necessary to deliver the program, ensuring that the software is available whenever and wherever customers need it. Many SaaS applications run directly through web browsers, eliminating the need for downloads or installations. This greatly reduces software management issues for internal IT teams. Examples of SaaS: Microsoft Office 365, Salesforce, Cisco WebEx, Google Apps.

PLATFORM AS A SERVICE (PaaS)

PaaS is extremely helpful for any company that develops software and web-based applications. Many of the tools needed to develop for multiple platforms (computers, mobile devices, browsers, etc) can be quite expensive. By using PaaS, customers can access the development tools they need, when they need them, without having to purchase them outright. Since the platform is accessible over the internet, remote development teams can all access the same assets to speed up product development. Examples of PaaS: AWS Elastic Beanstalk, Apache Stratos, Google App Engine, Microsoft Azure.

INFRASTRUCTURE AS A SERVICE (IaaS)

It provides a completely virtualized computing infrastructure that is provisioned and managed over the internet. An IaaS provider manages the physical end of the infrastructure (servers, data storage space, etc) in a data center, but allows customers to fully customize those virtualized resources to suit their specific needs. Examples of IaaS: Microsoft Azure, Amazon Web Services (AWS), Cisco Metacloud, Google Compute Engine (GCE).

BLOCKCHAIN TECHNOLOGY

It typically refers to the transparent, trustless, publicly accessible ledger that allows us to securely transfer the ownership of units of value using public key encryption and proof of work methods. The technology uses decentralized consensus to maintain the network, means not centrally controlled by a bank, corporation, or government. In fact, the larger the network grows and becomes increasingly decentralized, the more secure it becomes. The potential for blockchain technology is not limited to bitcoin. As such, it has gained a lot of attention in a variety of industries including: financial services, charities and nonprofits, the arts, and e-commerce.

Grid computing

- It is a computer network in which each computer's resources are shared with every other computer in the system. Processing power, memory and data storage are all community resources that authorized users can tap into and work/use for specific tasks.
- **Grid can be of two types**
  (i) Data grid, used tomanage large and distributed data having required multi-user access, and
  (ii) CPU or Processor grid, where processing is moved from one PC to another as needed or a large task is divided into subtasks and divided to various nodes for parallel processing.
- To set up a grid, by connecting numerous nodes in terms of data as well as CPU, a middleware is required to implement the distributed processor architecture. The Globus toolkit (http://toolkit.globus.org/toolkit) is one such software toolkit used for building grids, and it is open source. It includes software for security, resource management, data management, communication, fault detection, etc. ❐❐❐

11 SOCIETAL IMPACT
(NCERT CLASS 11)

INTRODUCTION

In recent years, the world around us has seen a lot of changes due to use of 'Digital Technologies'. These changes have made a dramatic impact on our lives, making things more convenient, faster, and easier to handle. The introduction of personal computers (PCs) and Internet followed by smartphones has brought these technologies to the common man.

While we reap the benefits of digital technologies, these technologies can also be misused. Let's look at the impact of these technologies on our society and the best practices that can ensure a productive and safe digital environment for us.

DIGITAL FOOTPRINTS

A digital footprint is data that is left behind when users have been online. There are two types of digital footprints which are active and passive.

(I) An active digital footprint is where the user has deliberately shared information about themselves either by using social media sites or by using websites.

Examples of active digital footprints

- Posting on Instagram,Facebook, Instagram, Twitter, and other social media platforms.
- Filling out online forms, i.e. when signing up to receive emails or texts
- Agreeing to install cookies on our devices when prompted by the browser

(II) A passive digital footprint is made when information is collected from the user without the person knowing this is happening.

Examples of passive digital footprints

- Websites that install cookies in our device without disclosing it to us.
- Apps and websites that use geolocation to pinpoint our location .
- Social media news channels and advertisers that use our likes, shares, and comments to profile us and to serve up advertisements based on our interests.

How digital footprint is being used for marketing purposes?

- Digital footprints are also known as cyber shadow, electronic footprint, or digital shadow are generally collected with the help of tracking cookies. These cookies are created while using popular sites. Whatever we search is stored in these along with our dates, GPS relevant data. These are shared by actual site we are visiting to the popular sites.
- Popular sites in tern analyze these data and revert back in the form of advertise later on. For e.g. we search for a flight from x location to y location for a particular date. Next day if we open search engine ,ads automatically popups even if we have booked out tickets.

For the following four reasons we should care about managing our digital footprint :

(I) To protect our reputation.
(II) To make safe personal information.
(III) To prevent financial loss.
(IV) To preserve our freedom

Risk due to digital footprint :

- Privacy concern
- Scam
- Identity theft
- Fake websites

How to manage digital footprints ?

(I) Enter name into several search engines.
(II) Double-check privacy settings, but don't trust them.
(III) Create strong, memorable passwords.
(IV) Keep all our software up to date.
(V) Review our mobile use. Delete useless files(temp.).
(VI) Build reputation through behavior.

DIGITAL SOCIETY AND NETIZEN

Digital society reflects the growing trend of using digital technologies in all spheres of human activities. But while online, all of us need to be aware of how to conduct ourselves, how best to relate with others and what ethics, morals and values to maintain.Being a good netizen means practicing safe, ethical and legal use of digital technology. A responsible netizen must abide by net etiquettes, communication etiquettes and social media etiquettes.

- **Net or communication etiquettes :** Netiquette is short for "Internet etiquette" or communication etiquettes over internet. It is Just like etiquette - a code of polite behavior in society, netiquette is a code of good behavior on the Internet. It includes several aspects of the Internet, social media, email, online chat, web forums, website comments, multiplayer gaming, and other types of online communication.

Do	Don't
❖ Keep Messages and Posts Brief. ❖ Use Discretion. ❖ Protect Personal Information. ❖ Obey Copyright Laws. ❖ Help Others. ❖ Respect other people's privacy. ❖ Verify facts before reposting. ❖ Check messages and respond promptly. ❖ Thank others who help you online.	❖ posting inflammatory /offensive comments shout. ❖ respond to Internet Trollers. ❖ Post private or embarrassing images/comments. ❖ Name-call or express offensive opinions. ❖ Exclude people or talk behind their backs. ❖ Stick to the topic. ❖ spam others by sending large amounts of unsolicited email.

DATA PROTECTION

Refers to the practices, safeguards, and binding rules put in place to protect our personal information and ensure that it remain in control. In short, we should be able to decide whether or not we want to share some information, who has access to it, for how long, for what reason, and be able to modify some of this information, and more.

Consequences of Unprotected Data/Data breaches:-

(I) Suffer from security breach/attack.
(II) Physical data loss.
(III) Hit with a virus .
(IV) Targeted by hackers .
(V) Suffer from DDoS(Distributed denial of service).
(VI) Lose of money.
(VII) Intellectual property at risk .
(VIII) Damage downtime.

How we can protect our personal data online:-

(I) Through Encrypt our Data.
(II) Keep Passwords Private.
(III) Don't Overshare on Social Networking Sites.
(IV) Use Security Software.
(V) Avoid Phishing Emails.
(VI) Be Wise About Wi-Fi .
(VII) Be Alert to Impersonators .
(VIII) Safely Dispose of Personal Information.

INTELLECTUAL PROPERTY (IP)

Is a property created by a person or group of persons using their own intellect for ultimate use in commerce and which is already not available in the public domain.

Examples of IP Property which are, an invention relating to a product or any process, a new design, a literary or artistic work and a trademark (a word, a symbol and / or a logo, etc.),

Intellectual Property Right (IPR) is the statutory right granted by the Government, to the owner(s) of the intellectual property or applicant(s) of an intellectual property (IP) to exclude others from exploiting the IP commercially for a given period of time, in lieu of the discloser of his/her IP in an IPR application.

Why should an IP be protected?

- IP is an assets and can be exploited by the owner for commercial gains any manner.
- IP owner may intend to stop others from manufacturing and selling products and services which are dully protected by him.
- IP owner can sell and/or license the IP for commercial gains.
- IP can be used to establish the goodwill and brand value in the market.
- IP can be mention in resumes of it's creator and thus show competence of it's creator.
- IPR certificate establishes legal and valid ownership about an intellectual property.

Kinds of IPRs

- Patent (to protect technologies - The Patent Act).
- Trade Mark (to protect words, signs, logos, labels – The Trade Mark Act).
- Design (to protect outer ornamental configuration –The Designs Act).
- Geographical Indications (GI) (to protect region specific product –The Geographical Indications of Goods Act).
- Copyright (to protect literary and artistic work – The Copyright Act).

IPRs are protected in accordance with the provisions of legislations of a country specific. In India, IPRs can be protected and monopolized as per the act. Some of them are :

1. The Patent Act, 1970
2. The Designs Act, 2000
3. The Trade Mark Act, 1999
4. The Geographical Indications of Goods Act, 1999,
5. The Copyright Act, 1957
6. Protection of Integrated Circuits Layout and Designs Act, 2000
7. Protection of Plant Varieties and Farmers Rights Act, 2001, and also Trade Secret

PLAGIARISM

It is "the act of presenting the words, ideas, images, sounds, or the creative expression of others as it is your creation or your own." The word plagiarism is derived from the Latin word plagiare, which means to kidnap or abduct.

Why is it important to understand Plagiarism?

- Plagiarism is stealing of intellectual property.
- Plagiarism is cheating.
- Plagiarism is an Academic offence.
- Plagiarism is Academic theft!

Two Types of Plagiarism:

Intentional Plagiarism	Unintentional Plagiarism
Copying other's work	Not knowing how to acknowledge or incorporate sources of information through proper paraphrasing, summarizing and quotation
Borrowing/buying assignments	Careless copying or cutting and pasting from electronic databases
Cut , paste from electronic resources	Quoting excessively
Downloading essays/text from the Internet and presenting as our own work	Failure to use our own "voice"

How to avoid plagiarism

1. Use your own ideas
2. Cite the sources-When someone else's ideas are used, always acknowledge the sources and tell your reader WHERE THE IDEAS ARE FROM.
3. Rewrite other's ideas in your own words
4. Take careful notes
5. Develop your writing skills

SOFTWARE LICENSE

A software license is a document that provides legally binding guidelines to the person who holds it for the use and distribution of software. It typically provide end users with the right to make one or more copies of the software without violating copyrights. It also defines the responsibilities of the parties entering into the license agreement and may impose restrictions on how the software can be used. Software licensing terms and conditions usually include fair use of the software, the limitations of liability, warranties and disclaimers and protections.

Benefits of Using Licensed Software:-

- Using Unlicensed Software Against the Law.
- The Right Software License Can Save our Money.
- We can Receive Around-The-Clock License Support.

Software copyright is used by software developers/ software companies/proprietary software companies to prevent the unauthorized copying of their softwares. Free and open source licenses also rely on copyright law to enforce their terms.

Reason for copyright our software

(I) Our work(software development) is an asset Protect our rights.

(II) It protects our software structures.

(III) It protects software code,sequencing and organization.

(IV) It enhances protection against license agreements.

- Difference between licensing and copyright:- Copyright is a type of intellectual property protection and licensing is a kind of risk control measure that can be applied to control copyright loss exposure, so the licensor (copyright owner) can grant permission that usually takes the form of a licensing agreement to use its copyrighted material. This agreement specifies the exact material to be used, purposes the work could be used for and the duration of the license.
- Free and Open Source software(FOSS) FOSS is a kind of software that all allows users to not only freely run the program for any purpose, but also provides users access to its source code. Moreover, it also allows us to modify as we wish, as well as freely distribute copies of the original version or their altered version.

Following criteria must be met for FOSS:

- Source code must be included.
- Anyone must be allowed to modify the source code.
- Modified versions can be redistributed.
- The license must not require the exclusion of other.
- It must be free.

Example of Free and Open source software:-

- As Operating system – linux,Ubuntu
- As dbms – mysql,mongodb,SQlite
- As Programming language – java,php,python
- As internet browser/webserver – chromium,firfox/ apache http server,apache tomcat.

Types of Software based on use:

(I) **Free Software :** Free Software are those which are freely accessible, freely accessible, freely used, changed,improved, copied and distributed. It provides all types of freedom. The term 'Free' means'Freedom' at very little or No cost. The Source Code is also available with Free Software.

(II) **Open Source Software :** Open Source Software can be freely used, changed, improved, copied and Re-distributed but it may have some cost for the

media and support for further development.Source Code is also available with OSS. It can be modified and redistributed with some guidelines. The License may restrict source-code from being distributed and modification to maintain the Author's integrity. A software which is FREE as well as OPEN, called Free & Open Source Software (FOSS) or Free Libre & Open Source Software (FLOSS).

CYBER CRIME

Any crime that involves a computer and a network is called a "Computer Crime" or "Cyber Crime. Or in other term ,it is a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

STEPS TO PROTECT YOURSELF AGAINST CYBER CRIME

1. Make sure your security software is current – and update it regularly.
2. Lock or log off your computer when you step away.
3. Go offline when you don't need an internet connection.
4. Consider sharing less online.
5. Think twice about using public Wi-Fi.
6. When in doubt, don't click.

Types of Cyber Crime

(I) A computer is the target of the attack—for example, a data breach on a bank site.

(II) A computer is the weapon for an attack—for example, a denial of service (DoS) attack.

(III) A computer is an accessory to a criminal act—for example, digital identity theft which leads to theft of funds from a bank account.

HACKING

Hacking is the process of gaining unauthorized access into a computing device, or group of computer systems. This is done through cracking of passwords and codes which gives access to the systems.

Difference between hacker and cracker is that a cracker breaks the security of computer systems, and a hacker is a person who likes to explore computer systems and master them.

Types of Hackers

(I) Black hat hackers or crackers are individuals with extraordinary computing skills, resorting to malicious / destructive activities. Black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

(II) White hat hackers are those individuals who use their hacking skills for defensive purposes. This means that the white hat hackers use their knowledge and skill for the good of others and for the common good. Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use,but with one major difference that Ethical hacking is legal.

(III) **Grey-Hat Hackers :** These are individuals who work both offensively and defensively at different times. Their behavior can't be predicted. Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.

Hacking Process :

- Foot Printing - Whois lookup,NS lookup,IP lookup
- Scanning - Port Scanning,Network Scanning
- Gaining Access-Password Attacks,Social Engineering,Viruses
- Maintaining Access - Os BackDoors,Trojans,Clears Tracks.

Required Skills of an Ethical Hacker:

(I) **Microsoft:** skills in operation, configuration and management.

(II) **Linux:** knowledge of Linux/Unix;security setting, configuration, services.

(III) **Network Protocols:** TCP/IP; how they function and can be manipulated.

(IV) **Firewalls:** configurations, and operation of intrusion detection systems.

(V) **Project Management:** leading, planning, organizing, and controlling a penetration testing team.

(VI) **Routers:** knowledge of routers, routing protocols, access control lists.

(VII) Mainframes

CYBERBULLYING

It is the use of technology to harass, threaten or humiliate a target. Examples of cyberbullying is sending mean texts, posting false information about a person online, or sharing embarrassing photos or videos.

Cyberbullying differs from in-person bullying :

- **More difficult to recognize** – Bullying conducted via text or online medium can more easily go unnoticed.
- **More relentless** – Cyberbullying doesn't end at school, and can reach at child home.
- **More enduring** –It leaves a paper trail that can follow both the bully and the victim for years.

Different Types of Cyber Bullying

- **Doxing** – publishing revealing personal information about an individual online, for purposes of defaming,humiliating, or harassing the victim .
- **Harassment** – posting threatening,hurtful, or intimidating messages online, or sending them directly to someone, with the intention of harming that person.
- **Impersonation** – creating fake accounts or gaining access to a person's real social media accounts

and posting things to damage the victim's reputation.

- **Cyberstalking** – tracking and monitoring a person's online activity, and using the internet to stalk or harass an individual.

How to Prevent Cyber Bullying?

- Be aware of child's online activities
- Watch for the following signs of cyberbullying in children:
  - Refusal to allow to see what they are doing online
  - Avoidance of discussing what they are doing online
  - Sudden, unexplained increase or decrease in online activity
  - Deactivating social media accounts
  - Emotional responses (including sadness, anger, happiness) linked to their device usage Adults should also teach children to recognize and be aware of the signs of cyberbullying themselves..

CYBER LAW

Cyber law as it is the part of the legal systems that deals with the cyberspace,Internet and with the legal issues. It covers a broad area, like freedom of expressions, access to and utilization of the Internet, and online security or online privacy. Generically, it is known as the law of the web.

- **What is the importance of Cyber Law?**

Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views.

- The Information Technology Act of India, 2000 According to Wikipedia "The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cyber crimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.
- **Some key points of the Information Technology (IT) Act 2000 are as follows :**
  - (I) Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
  - (II) This Act allows the government to issue notices on internet through egovernance.
  - (III) E-mail is now considered as a valid and legal form of communication.
  - (IV) Digital signatures are given legal validity within the Act.
  - (V) The communication between the companies or between the company and the government can be done through internet.
  - (VI) Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
  - (VII) In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company.

The Information Technology Act, 2000 provides legal recognition to the transaction done via an electronic exchange of data and other electronic means of communication or electronic commerce transactions.Some of sections under it act 2000 are given below:-

SECTION	OFFENCE	PENALITY
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to Rs. 1,000,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to Rs.1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to Rs.1,000,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine
68	Failure/refusal to comply with orders	Imprisonment up to three years, or/and with fine up to Rs.200,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to three years, or/and with fine up to Rs.100,000

E-WASTE

Whenever an electronic device covers up its working life, or becomes non-usable due to technological advancements or becomes non-functional, it is not used anymore and comes under the category of e-waste or electronic waste. As the technology is changing day by day, more and more electronic devices are becoming non-functional and turning into e-waste. Managing such non-functional electronic devices is termed as e-waste management.

Ewaste Hazards

(I) **On environment**

- Acidification of soil
- Air pollution
- Pollution of ground water
- Landfills with lead and heavy metals

(II) **On Human Health :**

- Lung cancer
- DNA damage
- Asthmatic bronchitis
- Chronic damage to the brain
- Damage to heart, liver and spleen

- E-waste management can be defined as the practical and holistic approach and the founding pillar of cutting down waste from our mother earth. It is reusing and recycling of e-waste which is no longer in use and can be salved for some of its components. We are on the verge of a technological breakthrough with the introduction of AI and we need to dispose off toxic e-waste from our home before we pile up more and more e-waste. We are is dire need of introducing a customer awareness campaign because of lack of interest and knowledge regarding e-waste.
- Proper disposal of used electronic gadgets:- E-waste is a growing problem for us in India. As an 132cr strong economy, we produce e-waste in large quantities. It is very important to dispose off waste in a pragmatic manner.
- Ways to dispose off e-waste:
  1. Give Back to Your Electronic Companies and Drop Off Points
  2. Visit Civic Institutions
  3. Donating Your Outdated Technology
  4. Sell Off Your Outdated Technology
  5. Give Your Electronic Waste to a Certified E-Waste Recycler.

Awareness of Health concerns related to the usage of technology

(I) **Physical Problems:**

- **Repetitive Strain Injury:** the pain exists even when resting and that the lightest work becomes hard to do.
- **Carpal Tunnel Syndrome:** This is an illness caused by injuries that occur due to force on the median nerve found in the wrist.Its symptoms can occur as tingling in hands and fingers and the feeling of lethargy, sudden pain in wrists and arms and sometimes even in shoulders, neck and in the body.
- **Computer Vision Syndrome:** Experts stated that people blink their eyes more frequently while using a computer than they do at other times and that they face some problems related to this situation.
- **Radiation:** Computer screens produce radiations of various types. There have always been doubts that Individuals will have illnesses such as headaches and inattentiveness.
- Sleeping Disorders and Decrease in Productivity.
- Loss of Attention and Stress.

(II) **Psychological Problems:**

- Fear of technology
- Computer anxiety
- Internet addiction
- **Egosurfing:** An illness of regularly searching for one's own name on the web and checking what information is available about one's own on the net.
- **Infornography:** The word, derived from pornography and information, describes the state of "trying to soothe hunger for information on the net."
- **Blog streaking:** A desire to spread information online that shouldn't be known by everybody.
- **Youtube-Narcissism:** Constantly uploading one's own videos in order to introduce and make himself or herself known tooth ers.
- **Google-Stalking:** Trying to get information about all his or her relatives or acquaintances in the web.
- **Photolurking:** Looking at the photo albums of others' on the net.
- **Wikipediholism:** Contributing to the internet encyclopedia, Wikipedia, sending some one's own writings, and revising the present texts.

❑❑❑

24 SECURITY ASPECT
(NCERT CLASS 12)

THREATS AND PREVENTION

Network security is concerned with protection of our device as well as data from illegitimate access or misuse. Threats include all the ways in which one can exploit any vulnerability or weakness in a network or communication system in order to cause harm or damage one's reputation.

MALWARE

Malware is a short term used for Malicious software. It is any software developed with an intention to damage hardware devices, steal data, or cause any other trouble to the user. Various types of malware have been created from time-to-time, and large-scale damages have been inflicted. Many of these malware programs have been identified and counter measures have been initiated. However, different types of malware keep on coming on a regular basis that compromise the security of computer systems and cause intangible damages. Besides, each year, malware incur financial damages worth billions of dollars worldwide. Viruses, Worms, Ransomware, Trojans, and Spyware are some of the kinds of malware.

(I) **VIRUS :** If you observe that your system
(a) takes longer time to load applications
(b) shows unpredictable program behaviour
(c) shows inexplicable changes in file sizes
(d) has inability to boot,
(e) has strange graphics appearing on your screen

This could be because of your computer being infected by a virus.

Virus is a malicious program that attaches itself to the host program. It is designed to infect the host program and gain control over the system without the owner's knowledge. The virus gets executed eachtime the host program is executed. Also it has the tendency to replicate. They can spread through external media such as CDs, browsing infected internet sites and from email attachments.

Types of Viruses

(a) **File Virus :** These viruses infect and replicate when it gets attached to MS-DOS program files with EXE or COM extensions.

(b) **Boot sector virus :** These viruses infect the boot sector of floppy disks or hard drives. Boot sector of a drive contains program that participates in booting the system. A virus can infect the system by replacing or attaching itself to these programs.

(c) **Macro virus :** These viruses infect and replicate using the MS Office program suite, mainly MS Word and MS Excel. The virus inserts unwanted words or phrases in the document.

(II) **WORM :** Worm is also a malicious program like a virus. But unlike viruses, it does not need to attach itself to a host program. A worm works by itself as an independent object.It uses security holes in a computer networks to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

(III) **Ransomware :** It is a type of malware that targets user data. It either blocks the user from accessing their own data or threatens to publish the personal data online and demands ransom payment against the same. Some ransomware simply block the access to the data while others encrypt data making it very difficult to access.

It worked by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It literally made its victims "cry" and hence the name.

(IV) **Trojan horse :** A Trojan horse is a program that contains hidden malicious functions. Trojan Horses trick users intoinstalling them by appearing to be legitimate programs. Once installed on a system, they reveal their true nature and cause damage. Some Trojan horses will contact a central server and report back information such as passwords, user IDs, and captured keystrokes. Trojans lack a replication routine and thus are not viruses by definition.

(V) **SPYWARE :** It is a type of malware that spies on a person or an organisation by gathering information about them, without the knowledge of the user. It records and sends the collected information to an external entity without consent or knowledge of the user.

Spyware usually tracks internet usage data and sells them to advertisers. They can also be used to track and capture credit card or bank account information, login and password information or user's personal identity.

(VI) **ADWARE:** An Adware is a malware that is created to generate revenue for its developer. An adware displays online advertisements using pop-ups, web pages, or installation screens. Once an adware has infected a substantial number of computer systems, it generates revenue either by displaying

advertisements or using "pay per click" mechanism to charge its clients against the number of clicks on their displayed ads. Adwareis usually annoying, but harmless. However, it often paves way for other malware by displaying unsafe links as advertisements.

(VII) **Keyloggers :** A keylogger can either be malware or hardware. The main purpose of this malware is to record the keys pressed by a user on the keyboard. A keylogger makes logs of daily keyboard usage and may send it to an external entity as well. In this way, very sensitive and personal information like passwords, emails, private conversations, etc. can be revealed to an external entity without the knowledge of the user. One strategy to avoid the threat of password leaks by keyloggers is to use a virtual keyboard while signing into your online accounts from an unknown computer.

- **Modes of Malware distribution :**

A malware once designed, can take many routes to reach your computer. Some of the common distribution channels for malware are:

(I) **Downloaded from the Internet :** Most of the time, malware is unintentionally downloaded into the hard drive of a computer by the user. Of course, the malware designers are smart enough to disguise their malware, but we should be very careful while downloading files from the Internet (especially those highlighted as free stuff).

(II) **Spam Email :** We often receive an unsolicited email with embedded hyperlinks or attachment files. These links or attached files can be malware.

(III) **Removable Storage Devices :** Often, the replicating malware targets the removable storage media like pen drives, SSD cards, music players, mobile phones, etc. and infect them with malware that gets transferred to other systems that they are plugged into.

(IV) **Network Propagation :** Some malware like Worms have the ability to propagate from one computer to another through a network connection.

- **Combating Malware**

Common signs of some malware infection include the following:

(I) frequent pop-up windows prompting you to visit some website and/or download some software;

(II) changes to the default homepage of your web browser;

(III) mass emails being sent from your email account;

(IV) unusually slow computer with frequent crashes;

(V) unknown programs startup as you turn on your computer;

(VI) programs opening and closing automatically;

(VII) sudden lack of storage space, random messages, sounds, or music start to appear;

(VIII) programs or files appear or disappear without your knowledge.

ANTIVIRUS

Antivirus is a software, also known as anti-malware. Initially, antivirus software was developed to detect and remove viruses only and hence the name anti-virus. However, with time it has evolved and now comes bundled with the prevention, detection, and removal of a wide range of malware.

Methods of Malware Identification used by Antivirus:-

(I) **Signature-based detection :** In this method, an antivirus works with the help of a signature database known as "Virus Definition File (VDF)". This file consists of virus signatures and is updated continuously on a real-time basis. This makes the regular update of the antivirus software a must. If there is an antivirus software with an outdated VDF, it is as good as having no antivirus software installed, as the new malware will infect the system without getting detected. This method also fails to detect malware that has an ability to change its signature (polymorphic) and the malware that has some portion of its code encrypted.

(II) **Sandbox detection :** In this method, a new application or file is executed in a virtual environment (sandbox) and its behavioural fingerprint is observed for a possible malware. Depending on its behaviour, the antivirus engine determines if it is a potential threat or not and proceeds accordingly. Although this method is a little slow, it is very safe as the new unknown application is not given access to actual resources of the system.

(III) **Data mining techniques :** This method employs various data mining and machine learning techniques to classify the behaviour of a file as either benign or malicious.

(IV) **Heuristics :** Often, a malware infection follows a certain pattern. Here, the source code of a suspected program is compared to viruses that are already known and are in the heuristic database. If the majority of the source code matches with any code in the heuristic database, the code is flagged as a possible threat.

(V) **Real-time protection :** Some malware remains dormant or gets activated after some time. Such malware needs to be checked on a real-time basis. In this technique, the anti-malware software keeps running in the background and observes the behavior of an application or file for any suspicious activity while it is being executed i.e. when it resides in the active (main) memory of the computer system.

SPAM

The term spam means endless repetition of worthless text. In other words, unwanted messages or mails are known as Spam. At times internet is flooded with multiple copies of the same message, it is nothing but spam. Most spam is commercial advertising. In addition to wasting people's time, spam also eats up a lot of network bandwidth.

HTTP vs HTTPS

Both the HTTP (Hyper Text Transfer Protocol) and its variant HTTPS (Hyper Text Transfer Protocol Secure) are a set of rules (protocol) that govern how data can be transmitted over the WWW (World Wide Web). In other words, they provide rules for the client web browser and servers to communicate.

HTTP sends information over the network as it is. It does not scramble the data to be transmitted, leaving it vulnerable to attacks from hackers. Hence, HTTP is sufficient for websites with public information sharing like news portals, blogs, etc. However, when it comes to dealing with personal information, banking credentials and passwords, we need to communicate data more securely over the network using HTTPS. HTTPS encrypts the data before transmission. At the receiver end, it decrypts to recover the original data. The HTTPS based websites require SSL Digital Certificate.

FIREWALL

A firewall is hardware or software based network security system. It prevents unauthorized access(hackers, viruses, worms etc.) to or from a network.

Firewalls are used to prevent unauthorized internet users to access private networks connected to the Internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and out bound traffic. A firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria.

Types of Firewall :

(I) **Network Firewall :** If the firewall is placed between two or more networks and monitors the network traffic between different networks, it is termed as Network Firewall.

(II) **Host-based Firewall :** If the firewall is placed on a computer and monitors the network traffic to and from that computer, it is called a host-based firewall.

COOKIES

When the user browses a website, the web server sends a text file to the web browser.This small text file is a cookie. Generally a cookie contains the name of the website from which it has come from and a unique ID tag.

Some cookies last only until the browser is closed. They are not stored on your hard drive. They are usually used to track the pages that you visit so that information can be customised for you for that visit. On the other hand, some cookies are stored on your hard drive until you delete them or they reach their expiry date. These may, for example, be used to remember your preferences when you use the website.

HACKERS AND CRACKERS

The term hacking was first used at M.I.T during 1950s and 1960s. The term was used for people whoengaged themselves in harmless technical experiments and fun learning activities.

A computer enthusiast, who uses his computer programming skills to intentionally access a computer without authorization is known as hacking. The computer enthusiast involved in this activity is known as a hacker. A hacker accesses the computer without the intention of destroying data or maliciously harming the computer.

Another term commonly used with hacking is cracking. Cracking can be defined as a method by which a person who gains unauthorized access to a computer with the intention of causing damage.

Depending on the intent, there are different types of hackers :

(I) **White Hats: Ethical Hacker :** If a hacker uses its knowledge to find and help in fixing the security flaws in the system, its termed as White Hat hacker. These are the hackers with good intentions. They are actually security experts. Organisations hire ethical or white hat hackers to check and fix their systems for potential security threats and loopholes. Technically, white hats work against black hats.

(II) **Black Hats: Crackers :** If hackers use their knowledge unethically to break the law and disrupt security by exploiting the flaws and loopholes in a system, then they are called black hat hackers.

(III) **Grey Hats :** The distinction between different hackers is not always clear. There exists a grey area in between, which represents the class of hackers that are neutral, they hack systems by exploiting its vulnerabilities, but they don't do so for monetary or political gains. The grey hats take system security as a challenge and just hack systems for the fun of it.

NETWORK SECURITY THREATS

(I) **Denial of Service :** Denial of Service (DoS) is a scenario, wherein an attacker (Hacker) limits or stops an authorised user to access a service, device, or any such resource by overloading that resource with illegitimate requests. The DoS attack floods the victim resource with traffic, making the resource appear busy. If attackers carry out a DoS attack on a website, they will flood it with a very large number of network packets by using different IP addresses. This way, the web server would be overloaded and will not be able to provide service to a legitimate user. The users will think that the website is not working, causing damage to the victim's organisation. Same way, DoS attacks can be done on resources like email servers, network storage, disrupting connection between two machines or disrupting the state of information (resetting of sessions).

If a DoS attack makes a server crash, the server or resource can be restarted to recover from the attack. However, a flooding attack is difficult to recover from, as there can be some genuine legitimate requests in it as well.

A variant of DoS, known as Distributed Denial of Service (DDoS) is an attack, where the flooded requests come from compromised computer (Zombies) systems distributed across the globe or over a very large area. The attacker installs a malicious software known as Bot on the Zombie machines, which gives it control over these machines. Depending upon the requirement and availability, the attacker activates a network of these Zombie computers known as Bot-Net to carry out the DDoS attack. While as a simple DoS attack may be countered by blocking requests or network packets from a single source, DDoS is very difficult to resolve, as the attack is carried from multiple distributed locations.

(II) **Intrusion Problems :** Network Intrusion refers to any unauthorised activity on a computer network. These activities may involve unauthorised use of network resources (DoS) or threatening the security of the network and the data. Network intrusion is a very serious problem and the network administrator needs to devise strategy and implement various security measures to protect the network.

(a) **Asymmetric Routing :** The attacker tends to avoid detection by sending the intrusion packets through multiple paths, thereby bypassing the network intrusion sensors.

(b) **Buffer Overflow Attacks :** In this attack, the attacker overwrites certain memory areas of the computers within the network with code (set of commands) that will be executed later when the buffer overflow (programming error) occurs. Once the malicious code is executed, an attacker can initiate a DoS attack or gain access to the network.

(c) **Traffic Flooding :** It is one of the most trivial methods of network intrusion. It involves flooding the network intrusion detection system with message packets. This huge load leaves the network detection system incapable of monitoring the packets adequately. The hacker takes advantage of this congested and chaotic network environment to sneak into the system undetected.

(III) **Snooping :** Snooping means secretly listening to a conversation. In the context of networking, it refers to the process of secret capture and analysis of network traffic. It is a computer program or utility that has a network traffic monitoring capability. In this attack, the hacker taps or listens to a channel of communication by picking all of the traffic passing through it. Once the network packets are analysed by the snooping device or software, it reproduces the exact traffic packets and places them back in the channel, as if nothing has happened. So, if the data that is being sent over the network is not encrypted, it is vulnerable to snooping and eventuallymay cause serious damage, depending upon the type of information leak. However, snooping is not always an attack, at times it is also used by network administrators for troubleshooting various network issues. Snooping is also known as Sniffing.

Various snooping software exist that act as network traffic analyser. Besides, various network hubs and switches have a SPAN (Sniffer Port Analyser) port function for snooping.

(IV) **Eavesdropping :** The term eavesdropping has been derived from the literal practice of secretly listening to the conversations of people by standing under the eaves of a house. Unlike snooping, where the network traffic can be stored for later analysis, eavesdropping is an unauthorised real-time interception or monitoring of private communication between two entities over a network. Also, the targetsphone calls (VoIP), instant messages, video conference, fax transmission, etc. In older days, eavesdropping was performed on the conventional telephone line and was known as wiretapping. Digital devices like laptops and cell phones that have a built-in microphone or camera can be easily hacked and eavesdropped using rootkit malware.

□□□