Notes on Information and Communication Technology and Computing

Different Generations of Wireless Communication

Wireless telephones **started with 0G** (zero generation) systems, which became available after World War II. Mobile telephones were usually mounted in cars or trucks, briefcase models were also made. Technologies used in 0G systems included MTS (Mobile Telephone System), IMTS (Improved Mobile Telephone Service), AMTS (Advanced Mobile Telephone System) etc.

Generations	Details	Advantages	Limitations
1G	**In 1979,** the first cellular system in the world became operational **by Nippon Telephone and Telegraph (NTT) in Tokyo, Japan.** First-generation mobile systems used analog transmission for speech services. In a few years, cellular communication spread to other parts of the world too – reaching Europe in 1981 and the USA in 1982.	Use of multiple cell sites. Ability to transfer calls from one site to the next site. Allowed voice calls in one country.	Poor quality of voice. Poor life of battery. Size of the phone was very large. No security. Capacity was limited. Poor handoff reliability.
2G	Second generation of mobile telecommunication was **launched in Finland in 1991.** It was **based on the GSM** (Group Special Mobile) standard. It enables data transmission like text messaging (SMS - Short Message Service), transfer of photos or pictures (MMS-Multimedia Messaging Service), but not videos. The family of this technology includes 2.5G and 2.75G. **2.5G** stands for "second and a half generation." It is a 2G-systems that have implemented **General**	Text messages, image messages, SMS and MMS are all possible. Signals are digitally encoded, which increases speech quality and lowers line noise. Improved Spectrum Efficiency, Enhanced security, better quality and capacity. Voice and data service. Framework cap has been increased, as well as network coverage.	Unable to handle complex data such as video. Requires strong digital signals.

	Packet Radio Service (GPRS). **2.75G** is also called **"Enhanced Data rates for GSM Evolution".** It allows the clear and fast transmission of data and information.		
3G	The third generation was first **released in the early 2000s.** 3G technologies enable network operators to offer users a wider range of more advanced services. Services include wide area wireless voice telephony, video calls, and broadband wireless data, all in a mobile environment. The family of this technology includes 3.5G and 3.75G. **3.5G** is also called **High-Speed Downlink Packet Access.** It provides a smooth evolutionary path for 3G networks allowing for higher data transfer speeds. **3.75G** is also called high **speed uplink packet access** (HSUPA). It is an enhanced form of the 3rd G network that includes **high speed packet access plus** (HSPA+).	Streaming audio and video has been improved. Several times faster data transmission. Can deliver speeds of up to 3Mbps. Multimedia applications such as video and photography are supported. Higher-speed, web WAP browsing and more security. Broadband with Large Capacity. Global Positioning System, mobile television, phone calls, and live video conferencing are examples of value added services.	Costly. Requirement of high bandwidth. Expensive 3G phones. Size of cell phones was large.
4G	4G wireless systems are a packet switched wireless system with wide area coverage and high throughput. It is designed to be cost effective and to provide high spectral efficiency. The 4G wireless uses the technique of **Orthogonal Frequency Division Multiplexing** (OFDM), **Ultra Wide Radio Band** (UWB) and millimeter wireless. 4G refers to all-IP packet-switched networks, mobile ultra-broadband (gigabit speed) access and multi-carrier transmission. The word **"MAGIC"** also refers to 4G wireless technology which stands for Mobile multimedia, Any-where, Global mobility support, Integrated wireless solution and Customized services.	High Speed, more security, high capacity. Access to the internet, streaming media, and video conferencing with ease. Exceptional spectral efficiency. Provide any type of service to users at any time and in any place. High quality of service and low cost per bit.	Uses more battery. Difficult to implement. Expensive equipment is required.
5G	In 5th Generation wireless	Data transmission is	Obstructions

	systems, customers benefit from ultra-fast internet and multimedia experiences. 5G technology transmits data using millimeter waves and unlicensed spectrum to achieve higher data rates. 5G performance targets high data rate, reduced latency, energy saving, cost reduction, higher system capacity, and massive device connectivity. Machine to machine communication can be possible in 5G. It performs Internet of Things (IoT) for smart home and smart city, connected cars etc.	faster than in previous generations. Global connectivity and service portability are provided by 5G technology. Wide broadcasting bandwidth up to Gigabit, supporting approximately 75,000 simultaneous connections. Large phone memory, quick dialing, and audio/video clarity. A high-speed, high-capacity system that allows for large-scale data broadcasting at Gbps.	can impact connectivity. Weakening of gadget batteries. Cybersecurity. Lack of encryption. Upload speeds do not match download speeds.

Visible Light Communication (VLC)

- VLC is a wireless technology that **relies on optical intensity modulation** and is potentially a game changer for internet-of-things (IoT) connectivity.
- It enables **high-speed transmission of data with visible light.** This data is transmitted by modulating the intensity of light given off by a light source.
- It is a preferred communication technique because of its high bandwidth and immunity to interference from electromagnetic sources.
- VLC uses wavelengths between 380 nm to 750 nm (i.e. 430 THz to 790 THz) for communication.

Architecture of VLC Systems

- A VLC system is composed of **two parts: the transmitter and the receiver.**
- Light emitted from a LED light (transmitter) through rapid light modulation is received by a receiving device, which is then translated into usable data.
- This can then be separated into three layers:
    - the **physical layer,** which basically dictates the relationship between the device and the medium,
    - the **MAC layer,** which points the data received and processed to the direction in which they need to go, and
    - the **application layer.**

Applications of VLC

Li-Fi

- Li-Fi or **'Light Fidelity'** is a **wireless optical networking** technology that makes use of LED lights to communicate and transmit data between devices wirelessly.
- It is analogous to Wi-Fi, which uses radio frequency for communication.
- **LED lights form the basis** of a wireless network whereas Li-Fi enables the transmission of data **by modulating the intensity of these LED lights.**
- A photo sensor receives modulated light which is then demodulated into electronic form.

Vehicle to vehicle communication

- VLC can be used for vehicular communication due to the presence of the vehicle lights and the existing traffic light infrastructure.
- The high priority applications indicated by the Vehicle Safety Communications Project include cooperative forward collision warning, pre-crash sensing, emergency electronic brake lights, lane change warning, stop sign movement assistant, left turn assistant, traffic signal violation warning and curve speed warning.

Underwater communication

- RF waves do not travel well in sea water because of its good conductivity. Therefore, VLC communication should be used in underwater communication networks.
- The **Un Tethered Remotely Operated Vehicle** (UTROV) is another application of the VLC in underwater communication.
- The different jobs that can be performed using UTROV include observatory maintenance of the oceans and deployment opportunities from the ships.

Information displaying signboards

- Signboards are often made from an array of LEDs which in turn are modulated to convey information in airports, bus stops and other places where the broadcasting of data is necessary.

Healthcare Industry

- The use of Wi-Fi can interfere with medical devices such as MRI (magnetic resonance imaging) and even treatment of patients.

- Li-Fi, on the other hand, offers a feasible opportunity where visible light communication can enable data transfer in such EMI (Electromagnetic Interference) sensitive environments. It can further aid in robotic treatment and laparoscopy.

Power Plants and Other Sensitive Areas

- Sensitive areas like Power Plants need fast digital communication to monitor grid-integrity and demand. Nuclear Power Plants, instead, need to monitor core temperature and send it across quickly.
- Wi-Fi can negatively affect sensitive areas because of its radiation; however, the implementation of Li-Fi in such areas can provide a safer and faster measure.

Educational Institutes

- Universities and schools need to have uninterrupted internet access for a plethora of reasons.
- By installing LED lights, universities and schools can not only save energy cost but also provide high-speed internet access. Li-Fi can completely replace Wi-Fi in educational institutes.

Entertainment and Advertisement Industry

- A single LED light can be used for transmission and reception as well as providing the visualization to entertain kids.
- Another use of VLC could be in the advertising industry, where large billboards made of LEDs are used for advertisement.

Advantages of VLC communication

- **Supports larger bandwidth:** Hence overcome bandwidth limitation of RF communication.
- **Secure communication:** VLC based data communication can not be intercepted by any one from the other room. It provides secured communication unlike RF communication.
- **Power efficient:** VLC source is used for both illumination and communication, it has low power consumption.
- **EM radiation:** Light based communication, hence, not affected due to EM radiation from RF systems.
- **Health and installation:** It does not have any health risks to human beings and is easy to install.

Disadvantages of VLC communication

- Interference issues from other ambient light sources.
- Supports short coverage range.
- Challenges to integrate with the WiFi system.
- Other drawbacks include atmospheric absorption, shadowing, beam dispersion etc.

Types of Web

- **Web 1.0:** Refers to the early days of the dial-up Internet when websites and web pages were static, and their primary purpose was to share information.
- **Web 2.0:** Characterized by social media platforms, blogs, wikis, and other user-generated content platforms delivered over the internet.
- **Web 3.0:** A version of the internet that focuses on **intelligent automation, context-aware applications, and enhanced privacy and security measures.**
    - This new technological dimension believes in leveraging the power of Artificial Intelligence, machine learning, and the latest technologies like blockchain to solve the problems of the present-day online ecosystem.
    - With Web 3.0, the data generated by disparate and increasingly powerful computing resources, including mobile phones, desktops, appliances, vehicles, and sensors, will be sold by users through decentralized data networks, ensuring that users retain ownership control.

Optical Fibre

- Optical fibre is a data transmission method that **makes use of light pulses** traveling down a long fibre, often constructed of plastic or glass.
- The **total internal reflection of light** is used in the fibre optic cable.

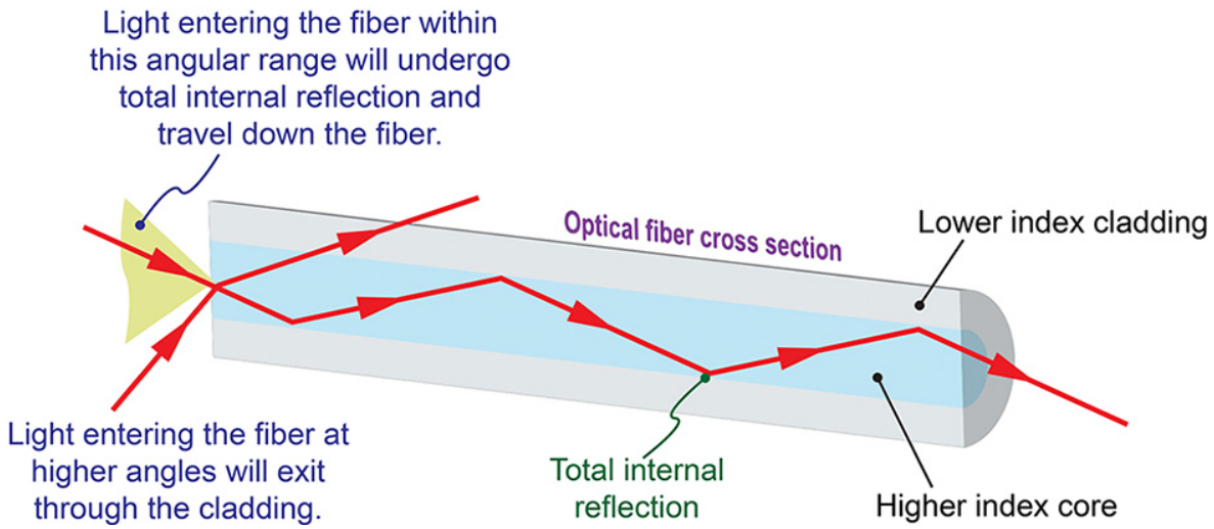

Figure.1. Operation of an Optical Fibre

Structure of Optical Fibre

- The **core, cladding, and outer coating** are all components of an optical fibre. While glass and plastic are commonly utilised, various materials can be used based on the desired transmission spectrum.
- The section of the fibre that transmits light is called the core.
- The material used for cladding often has a **lower refractive index than the core** (usually about 1 percent lower).
- Because of the index difference, total internal reflection occurs at the index border along the length of the fibre, preventing light from escaping through the sidewalls.

Applications of Optical Fibre

- **Medical Industry:** to view internal body parts by inserting into hollow spaces in the body.
- **Communication:** It increases the speed and accuracy of the transmission data. Compared to copper wires, fibre optics cables are lighter, more flexible and carry more data.
- **Defence:** data transmission in high-level data security fields of military and aerospace applications.
- **Industries:** for imaging in hard-to-reach places.
- **Broadcasting:** to transmit high-definition television signals which have greater bandwidth and speed.
- **Lighting and Decorations:** in festivals or homes.
- **Mechanical Inspections:** to detect damages and faults which are at hard-to-reach places.

BharatNet

- National Optical Fibre Network (NOFN) was **launched in October 2011** and was renamed as Bharat Net Project in 2015.
- The project is being executed by a **Special Purpose Vehicle (SPV) namely Bharat Broadband Network Limited** (BBNL), which was incorporated on February 25, 2012 under Indian Companies Act, 1956 with an authorized capital of Rs 1000 crore.

- The entire project is being funded by the **Universal Service Obligation Fund** (USOF), which was set up for improving telecom services in rural and remote areas of the country.
- The project is a **Centre-State collaborative project,** with the states contributing free Rights of Way for establishing the Optical Fibre Network.
- Non-discriminatory access to the NOFN was provided to all the service providers like Telecom Service Providers (TSPs), Cable TV operators and content providers to launch various services in rural areas.

Aim of BharatNet

- **To connect all the 2,50,000 Gram panchayats** in the country and **provide 100 Mbps connectivity** to all gram panchayats.
    - To achieve this, the existing unused fibres (dark fibre) of public sector undertakings (PSUs) (BSNL, Railtel and Power Grid) were utilised and incremental fibre was laid to connect to Gram Panchayats wherever necessary.
- To facilitate the delivery of e-governance, e-health, e-education, e-banking, Internet and other services to rural India.

Three-phase implementation

- **First Phase:** Provide one lakh gram panchayats with broadband connectivity by laying underground optic fibre cable (OFC) lines by December 2017.
- **Second Phase:** Provide connectivity to all the gram panchayats in the country using an optimal mix of underground fibre, fibre over power lines, radio and satellite media. It was to be completed by March 2019.
- **Third Phase:** From 2019 to 2023, a state-of-the-art, future-proof network, including fibre between districts and blocks, with ring topology to provide redundancy would be created.

Recent Development

- The Union Cabinet in August 2023 has approved an allotment of ₹1,39,579 crore for the next phase of BharatNet to make 5G network available to remote areas of the country.
- According to government sources, around 1.94 lakh villages have been connected at present and the rest of the villages are expected to be connected in the next 2.5 years.

National Broadband Mission

- The Ministry of Communications has launched the 'National Broadband Mission' (NBM), on **December 17, 2019, to facilitate universal and equitable access to broadband services** across the country, especially in rural and remote areas.
- It aimed to provide broadband access to all villages by 2022.
- It involves laying an incremental **30 lakh route km of Optical Fiber Cable** (OFC) and an increase in tower density from 0.42 to 1 tower per thousand of the population by 2024.

Vision of the National Broadband Mission

- To enable fast track growth of digital communications infrastructure, bridge the digital divide for digital empowerment and inclusion, provide affordable and universal access to broadband for all.

Objectives of the National Broadband Mission

- To address policy and regulatory changes required to accelerate the expansion and creation of digital infrastructure and services.
- Creation of a digital fiber map of the Digital Communications network and infrastructure, including Optical Fiber Cables and Towers, across the country.
- Work with all stakeholders including the concerned Ministries/ Departments/ Agencies, and the Ministry of Finance, for enabling investments for the Mission.
- Work with the Department of Space, to make available adequate resources required for extending connectivity to far flung areas of the country through satellite media.
- To encourage and promote adoption of innovative technologies for proliferation of broadband especially by the domestic industry.
- Seek cooperation from concerned stakeholders by developing innovative implementation models for Right of Way (RoW).
- To work with States/UTs for having consistent policies pertaining to expansion of digital infrastructure including for RoW approvals required for laying of OFC.
- To develop a Broadband Readiness Index (BRI) to measure the availability of digital communications infrastructure and conducive policy ecosystem within a State/UT.
- Promote direct and indirect employment as a result of development of Digital Communications infrastructure across the country and through the digital economy.

Progress of the National Broadband Mission (As of June 2022)

- **Broadband Connectivity to Villages:** Under the BharatNet Project 1,77,550 Gram Panchayats (GPs) have been made service ready till June 2022.
- **Availability of Broadband Speeds (Mbps):** Telecom Regulatory Authority of India (TRAI) has been obtaining Crowd-sourced data about download and upload speed for different service providers through TRAI My speed App. It is envisaged to achieve broadband speeds up to 50 Mbps by 2024-25.
- **Fiberization (Lakh Kms) Cumulative:** Total Optical Fibre Cable (OFC) laid is approximately 34.62 Lakh Km as on June 2022. It is envisaged to be increased up to 50 Lakh Km by 2024-25.
- **Towers (in Lakhs) Cumulative:** 7.23 Lakh towers have been installed up to June 2022. It is envisaged to increase up to 15 Lakh towers by 2024-25.
- **Fiberization of Telecom Towers/ Base Transceiver Station (BTS) (%) Cumulative:** Approximately 35.11% of Telecom Towers/ BTSs are fiberized as of June 2022. It is envisaged to be increased up to 70% by 2024-25.
- **Mapping of Fiber Cumulative:** 10 Lakh Route KMs of Optical Fibre Cable laid by the PSUs is mapped on the PM GatiShakti NMP Portal.

Recent Development

- The government has revised the definition of broadband connectivity in February 2023.

- The Centre has specified a **higher minimum download speed of 2 Mbps** (megabits per second). Earlier, the definition notified by the Telecom Department in July 2013 had benchmarked it to 512 kbps (kilobits per second) as minimum download speed.
- As of June, 2023, India had about **861.47 million broadband subscribers**.
- Top five service providers constituted 98.37 per cent market share of the total broadband subscribers at the end of June 2023.
- India's top-5 service providers are- Reliance Jio Infocomm Ltd (447.75 million), Bharti Airtel (248.06 million), Vodafone Idea (124.90 million), BSNL (24.59 million) and Atria Convergence (2.16 million).

Cloud Computing

- Cloud computing is the **delivery of computing services**—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.
- Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database.
- As long as an electronic device has access to the web, it has access to the data and the software programs to run it.

Operation of Cloud Computing

The salient features of cloud computing are as follows:

- **On-demand:** Computing services sold on demand generally by the minute or the hour.
- **Elastic:** A user can have as much or as little of a service as they want at any given time.
- **Fully managed by the provider:** The consumer requires nothing but a personal computer and internet connection.
- **Data-intensive:** The focus is on data rather than computation.
- **Scalability:** Cloud computing has the ability to scale-up or scale-down in order to meet a user's needs.

Types of Cloud Computing

Public cloud

- Public clouds are **owned and operated by third-party cloud service providers,** which deliver computing resources like servers and storage over the internet. Examples include Amazon Web Services, Microsoft Azure, etc.

Private cloud

- A private cloud refers to cloud computing resources **used exclusively by a single business or organization.** The services and infrastructure are maintained on a private network.
- It can be physically located on the company's onsite datacenter. Some companies also pay third-party service providers to host their private cloud.

Hybrid cloud

- Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them.
- By allowing **data and applications to move between private and public clouds,** hybrid cloud provides businesses greater flexibility and more deployment options and helps optimize existing infrastructure, security, and compliance.

Types of Cloud Computing Services

Infrastructure as a Service (IaaS)

- The most basic category of cloud computing services.
- With IaaS, a **user can rent IT infrastructure**—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider **on a pay-as-you-go basis.**

Platform as a Service (PaaS)

- Platform as a service (PaaS) refers to cloud computing services that supply an **on-demand environment** for developing, testing, delivering, and managing software applications.
- PaaS is designed to make it easier for developers **to quickly create web or mobile apps,** without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development.

Software as a service (SaaS)

- Software as a service (SaaS) is a method for delivering software applications over the internet, on demand and typically on a subscription basis.
- With SaaS, cloud providers **host and manage the software application and underlying infrastructure,** and handle any maintenance, like software upgrades and security patching.
- Users connect to the application over the internet, usually with a web browser on their phone, tablet, or PC.

Serverless computing

- Overlapping with PaaS, serverless computing focuses on building app functionality without spending time continually managing the servers and infrastructure required to do so.
- The cloud provider handles the setup, capacity planning, and server management.

Advantages of Cloud Computing

- Cloud computing services **minimize IT requirements and physical storage,** which helps small businesses cut significant business costs.
- Most cloud services are paid on a subscription basis, so capital expenditure is reduced.
- Cloud computing is also much **faster and easier to deploy,** so there are fewer start-up costs.
- Moving the business data to the cloud can make disaster recovery possible i.e., retrieving data in case of a hardware compromise.
- For many businesses, moving to the cloud enhances opportunities for collaboration between employees.
- It allows team members to work from anywhere.
- The cloud centralizes the data, meaning that the owner, employees and clients can access the company data from any location with internet access.
- Cloud computing **reduces a company's carbon footprint** by minimizing energy consumption and carbon emissions by more than 30%.

Limitations

- For cloud-based services, **consistent internet connection** is important.
- While the upfront or capital cost for the cloud-based server is very low , the cloud **server requires a significant amount to be paid each month** to maintain both servers as well as data.
- Companies with highly sensitive data may need their own IT department to keep data secure because when the data is stored in the cloud, the company is trusting a third party to keep it safe.

Cloud Storage

- Cloud storage is a cloud computing model that enables **storing data and files on the internet through a cloud computing provider** that a person can access either through the public internet or a dedicated private network connection.

Importance of Cloud Storage

Cost effectiveness

- With cloud storage, there is no hardware to purchase, no storage to provision, and no extra capital being used for business spikes.
- A person can add or remove storage capacity on demand, quickly change performance and retention characteristics, and only pay for storage that is actually used.

Increased agility

- With cloud storage, resources are only a click away. This results in an increase in agility of an organization.

Faster deployment

- Cloud storage services allow IT to quickly deliver the exact amount of storage needed, whenever and wherever it's needed.
- A developer can focus on solving complex application problems instead of having to manage storage systems.

Efficient data management

- By using cloud storage lifecycle management policies, users can perform powerful information management tasks including automated tiering or locking down data in support of compliance requirements.

Virtually unlimited scalability

- Cloud storage delivers virtually unlimited storage capacity. This removes the constraints of on-premises storage capacity.
- Users can efficiently scale cloud storage up and down as required for analytics, data lakes, backups, or cloud native applications.

Repair and recover

- Cloud storage services are designed to handle concurrent device failure by quickly detecting and repairing any lost redundancy.
- It can further protect data by using versioning and replication tools to more easily recover from both unintended user actions or application failures.

Limitations

Internet Dependency

- One can always save files while offline and access them later. However, an internet connection will be required for the update and sync.

Security and Privacy

- Confidential data must be given over to a third-party organization in order to be stored in the cloud. One must therefore have complete faith in the cloud vendor.

Costs

- There are additional costs for uploading and downloading files from the cloud. These can quickly add up if a user is trying to access lots of files often.

Limitations on Control

- After the user moves data to the cloud, the vendor is now in charge of it. This implies that users must rely on the vendors to maintain their services in a safe, stable, up-and-running, and fully functional manner. This limits the influence on data safety.

Cloud Computing in India

Cloud Computing and Data Centres

- The size of the digital population in India and the growth trajectory of the digital economy necessitates a strong growth of Data Centres.
- A Data Centre is a **dedicated secure space within a centralized location** where computing and networking equipment is concentrated for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of data.
- Cloud Service providers host their IT infrastructure in Data Centres to provide the Cloud Computing services to the end users.
- In the Union Budget 2022-23, the Union Minister for Finance and Corporate Affairs proposed that the Data Centres (along with Energy Storage Systems) would be included in the harmonized list of infrastructure.

Need for Data Centre

- Need for Data Centre infrastructure in India is necessitated by the data localization provisions of the Digital Personal Data Protection Act, 2023 and for protection of the digital sovereignty of the country in an increasingly connected world.
- As per various estimates, India has around 499 MW installed power capacity for Data Centres (till December 2022).
- The Ministry of Electronics & Information Technology also proposed a draft Data Centre Policy in 2020 with the vision of:
    - Making India a Global Data Centre hub,
    - Promoting investment in the sector,
    - Propelling digital economy growth,
    - Enabling the provisioning of trusted hosting infrastructure, and
    - Facilitating state of the art service delivery to citizens.

Growth of Data Centre in India

As per the draft Data Centre Policy 2020, for the long-term growth of the Data Centre sector in the country, it is critical to create a congenial, competitive and sustainable operating environment for the businesses. Some of the key policy thrust areas in this direction include:

- Availability of uninterrupted, clean and cost-effective electricity for Data Centres remains as one of the most important considerations for the Data Centre sector.
- MeitY to work with the Department of Telecommunications (DoT) to facilitate robust and cost-effective connectivity backhaul.
- Data Centres to be declared as an Essential Service under “The Essential Services Maintenance Act, 1968 (ESMA)”.
- Recognize Data Centres as a separate category under the National Building Code.
- Setting-up of Data Centre Economic Zones.
- Promote indigenous technology development, research and capacity building.

GI Cloud Initiative - MeghRaj

- In order to utilize and harness the benefits of Cloud Computing, Government of India has embarked upon an ambitious initiative - "GI Cloud" which has been named as 'MeghRaj' in **February 2014.**
- This initiative is to implement various components including governance mechanisms to ensure proliferation of Cloud in the government.
- The focus of this initiative is to **accelerate delivery of e-services** in the country while optimizing ICT spending of the Government.
- The architectural vision of GI Cloud encompasses a set of discrete cloud computing environments spread across multiple locations, built on existing or new (augmented) infrastructure, following a set of common protocols, guidelines and standards issued by the Government of India.

- The National Informatics Centre (NIC) is providing **National Cloud services** under the initiative MeghRaj. The services offered are Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Services (SaaS), Container as a Services (NCCaaS), Artificial Intelligence as a Service, Application Performance Management (APM) Service, Resource Monitoring as a Service, etc.

Advantages of MeghRaj

- Optimum utilization of existing infrastructure.
- Any software made available by any government department in India can be made available to other departments as well without additional costs.
- It provides a single point for maintaining Information & Communication Technology (ICT) infrastructure in India.
- According to the demands from the citizens of India, infrastructure of the government can be increased accordingly.
- Efficient service delivery.
- A security framework for the entire GI Cloud will lead to less environmental complexity and less potential vulnerability.
- Increased user mobility.
- Reduced effort in managing technology.
- Ease of first time IT solution deployment.
- Cost reduction.
- It prescribes the standards around interoperability, integration, security, data security and portability etc.

DigiLocker

- DigiLocker is a flagship initiative of the Ministry of Electronics & Information Technology (MeitY) as **part of the Digital India Programme.**
- **Launched in 2015,** the program **aims to make India go paperless** while providing a secure document access platform on a public cloud.
- It intends to provide citizens with 'Digital Empowerment' by allowing them to access authentic digital documents through a Digital Document Wallet.
- The stored documents can also be shared and verified through DigiLocker.

Three key layers

- The Government is aiming for the digital transformation with a philosophy 'Minimum Government and Maximum Governance', and it has identified three key layers- i) Cashless layer, ii) Paperless Layer and iii) Presenceless Layer.
- Cashless layer is taken care of by National Payments Corporations of India (NPCI) through the Digital Cashless transfer.
- Presenceless layer has been achieved by UIDAI.
- Paperless Layer has been addressed by DigiLocker addressing the eKYC, design and verification process.

Benefits to Citizens

- Important Documents Anytime, Anywhere.
- Authentic documents that are legally equal to originals.
- Citizen's consent is required for the exchange of digital documents.
- Faster service Delivery in the areas of Government Benefits, Employment, Financial Inclusion, Education and Health.

Benefits to Agencies

- **Reduced Administrative Overhead:** Aims towards paperless governance. It saves administrative costs by reducing the usage of paper and shortening the verification process.
- Trusted issued documents are provided as part of the digital transformation.
- Issued documents are retrieved in real-time from the issuing agency using DigiLocker.

Special Features and Achievements Under DigiLocker

- A total of Rs 452 crore documents have been made available to citizens.
- DigiLocker systems can be extremely useful in the event of a disaster. A successful example was demonstrated in the case of Kerala Flood, in which the IT department issued digital certificates to Kerala citizens during the Floods.
- Students in various states have access to more than 40 crore Educational Documents from school boards and higher education institutions.
- Digital DL/ RC (Driving Licence/Certificate of Registration) are made available to people.

Cyber Security

- Cybersecurity is the practice of **protecting systems, networks, and programs from digital attacks.**
- These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Concept of Cyber Threats

- Cyber threat is defined as any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority.
- A cyber threat can be **unintentional and intentional, targeted or non-targeted,** and can come from a variety of sources, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization.
- Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures and equipment failures that inadvertently disrupt computer systems or corrupt data.
- Intentional threats include both targeted and nontargeted attacks.
    - A targeted attack is when a group or individual specifically attacks a critical infrastructure system.
    - A non-targeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or malware is released on the Internet with no specific target.
- Repeatedly identified as the **most worrisome threat is the "insider"** — someone legitimately authorized access to a system or network.

Types of Cyber Threats

- **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks:** A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on a system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.
- **Man-in-the-middle (MitM) attack:** A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.
- **Phishing and spear phishing attacks:** Phishing attack is a type of email attack in which an attacker tries to find sensitive information of users in a fraudulent manner through electronic communication by pretending to be from a related trusted organization. Spear phishing targets specific organizations or individuals, and seeks unauthorized access to confidential data.
- **Drive-by attack:** Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might redirect the victim to a site controlled by the hackers.
- **Password attack:** Brute-force password guessing means using a random approach by trying different passwords and hoping that one works.
- **SQL injection attack:** SQL injection has become a common issue with database-driven websites.
- **Cross-site scripting (XSS) attack:** XSS attacks use third-party web resources to inject malicious JavaScript into a website's database.

- **Eavesdropping attack:** It occurs through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network.
- **Malware attack:** Malwares can be described as unwanted software that is installed in a system without consent. It can attach itself to legitimate code and propagate or replicate itself across the internet.
- **Ransomware:** Ransomware is a type of malware attack in which the attacker locks or encrypts the victim's data and threatens to publish or block access to data unless a ransom is paid.

Sources of Cyber Threats

- **Botnet operators:** Botnet operators use a network, or botnet, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets.
- **Criminal groups:** Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and criminal organizations also pose a threat through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
- **Foreign nation states:** Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. Also, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power.
- **Hackers:** Hackers break into networks for revenge, stalking others, and monetary gain. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites.
- **Hacktivists:** Those who make politically motivated attacks on publicly accessible web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into websites to send a political message.
- **Insiders:** The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
- **International corporate spies:** International corporate spies pose a threat through their ability to conduct economic and industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
- **Phishers:** Individuals, or small groups, execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
- **Spammers:** Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service attack).
- **Spyware/malware authors:** Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa virus, the Explore.Zip worm, the CIH (Chernobyl) virus, Nimda worm, Code Red, Slammer worm, and Blaster worm.

- **Terrorists:** Terrorists conduct cyber attacks to destroy, infiltrate, or exploit critical infrastructure to threaten national security, compromise military equipment, disrupt the economy, and cause mass casualties.

Cyber Security Scenario in India

- In India, cybersecurity has become a top priority in recent years due to the growing number of cyber-attacks on Indian businesses and government institutions.
- In India, phishing attacks have been on the rise in recent years. One notable example is the 2017 phishing attack on the Reserve Bank of India that resulted in the theft of over $1 million.
- Malware attacks are also common in India. In 2016, the WannaCry ransomware attack hit several Indian organizations, including the Andhra Pradesh police force and Bharat Sanchar Nigam Limited (BSNL).
- India witnessed **13.91 Lakh cyber security incidents in 2022.** The numbers still do not give an entire picture of cyberattacks on the country as these statistics only include information reported to and tracked by the CERT-In.
- Despite these challenges, there are positive trends emerging in India when it comes to cybersecurity.
- The Indian government has taken several steps to improve the country's cybersecurity posture, including establishing a National Critical Information Infrastructure Protection Centre (NCIIPC) and creating a National Cyber Coordination Centre (NCCC).
- In addition, the government has launched various awareness campaigns to educate citizens about cybersecurity threats and how to protect themselves.
- Approaches like R&D, legal framework, security incidents, early warning and response, best security policy compliance & assurance, international cooperation and security training are also followed in India to secure Indian Cyber Space.

Information Technology (IT) Act, 2000

- The IT Act of 2000 was enacted by the Parliament of India and **administered by the Indian Computer Emergency Response Team** (CERT-In) to guide Indian cybersecurity legislation, institute data protection policies, and govern cybercrime.
- It also protects e-governance, e-banking, e-commerce, and the private sector, among many others.
- While India does not have an exclusive, unitary cybersecurity law, it uses the IT Act and multiple other sector-specific regulations to promote cybersecurity standards. It also provides a legal framework for critical information infrastructure in India.
- This Act was amended through the Information Technology (Amendment) Act, 2008. The amendments were enforced and rules of important sections were notified in October, 2009 which addresses the needs of National Cyber Security.
- The Amendment inter alia added provisions to the IT Act, 2000 to deal with new forms of cyber crimes like publicizing sexually explicit material in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary and e-commerce frauds.
- The IT Act of 2008 applies to any individual, company, or organization (intermediaries) that uses computer resources, computer networks, or other information technology in India.

National Cyber Security Policy, 2013

- The Government of India on 1 July 2013 launched the National Cyber Security Policy 2013 with an aim **to protect information and build capabilities to prevent cyber attacks.**

- The policy is intended to cater for a broad spectrum of Information and Communications Technology users and providers including Government and non-Government entities.
- The National Cyber Security Policy 2013 is to safeguard both physical and business assets of the country.

Salient Features of the National Cyber Security Policy 2013

- The Policy outlines the roadmap for creation of a framework for comprehensive, collaborative and collective responsibility to deal with cyber security issues of the country.
- The policy lays out 14 objectives which include creation of a 5,00,000-strong professional, skilled workforce over the next five years through capacity building, skill development and training.
- The policy plans to create national and sectoral level 24×7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective, predictive, preventive, proactive response and recovery actions.
- The policy identifies eight different strategies for creating a secure cyber eco-system including the need for creating an assurance framework apart from encouraging open standards to facilitate interoperability and data exchange amongst different products or services.

Other Goals Include

- Creating a resilient and safe cyberspace for individuals, organizations, and the government.
- Creating frameworks, capabilities, and vulnerability management strategies for minimizing, faster prevention, or responding to cyber incidents and cyber threats.
- Encourage organizations to develop cybersecurity policies that align with strategic goals, business workflows, and general best practices.
- Simultaneously create institutional structures, people, processes, technology, and cooperation to minimize the damage caused by cybercrime.

Information Technology Rules

- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('2021 Rules') were released by the Central Government in February 2021.
- The 2021 Rules have been passed **under Sections 69A(2), 79(2)(c) and 87** of the Information Technology Act, 2000.
- The 2021 Rules supersede the previously enacted Information Technology (Intermediary Guidelines) Rules 2011.
- The 2021 Rules were introduced to update the regulatory framework in order to empower the ordinary users of social media and place obligations on Social Media Intermediaries ('SMIs') and Significant Social Media Intermediaries ('SSMI') for a safe and trusted online environment.
- It places special emphasis on the protection of women and children from sexual offences on social media.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 ('2023 Amendment')

- On April 6, 2023, the Ministry of Electronics and IT (MeitY) notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2023 to amend the IT Rules 2021.
- This amendment authorises the central government to **designate a "fact check unit" to identify "fake or false or misleading" information in respect of any business** of the central government.

- Initially, this amendment only contained provisions for regulating online gaming companies. But later MeitY published a new draft that included "fact-checking powers."
- The fact check unit can scrutinize any online comments, news reports or opinions about government officials and ministries and then notify online intermediaries for its censorship.
- Such intermediaries not only include online social media companies but also service providers such as internet service providers and file hosting companies.
- If any intermediary fails to comply, they will be at risk of losing their **safe harbour status under Section 79 of the IT Act, 2000.**
    - Safe harbour provision states that "an intermediary shall not be liable for any third-party information, data, or communication link made available or hosted by him".

National Cyber Security Strategy 2020

- The National Cyber Security Strategy 2020 was formulated by the Office of National Cyber Security Coordinator at the National Security Council Secretariat in March 2021.
- The strategy aims to **improve cybersecurity audit quality** so organizations can conduct better reviews of their cybersecurity architecture and knowledge.
- The plan's main goal is to serve as the official guidance for stakeholders, policymakers, and corporate leaders to prevent cyber incidents, cyber terrorism, and espionage in cyberspace.
- It also calls for an index of cyber preparedness, and attendant monitoring of performance.

Reserve Bank of India Act, 2018

The Reserve Bank of India introduced the RBI Act in 2018, which details cybersecurity guidelines and frameworks for UCBs (urban co-operative banks) and payment operators. The RBI Act of 2018 aims to:

- Create standards that equalize security frameworks of banks and payment operators according to how they adapt to new technologies and digitalization.
- Mandate banks to create and present their cyber crisis management plans.
- Encourage banks to regularly schedule threat assessment audits.
- Help banks implement their own email domains with anti-phishing and anti-malware technology.
- All Indian banks must follow these guidelines to standardize frameworks for payment processing cybersecurity and combat the ever-increasing business complications in a digital environment.

Indian Computer Emergency Response Team (CERT-In)

- Made **official in 2004,** CERT-In is the national nodal agency set up **under Section 70B of the Information Technology Act, 2000** to respond to computer security incidents as and when they occur.
- CERT-In creates awareness on security issues through dissemination of information on its website and **operates 24x7 Incident Response Help Desk.**
- It provides Incident Prevention and Response services as well as Security Quality Management Service.
- CERT-In perform the following functions in the area of cyber security:
    - Collection, analysis and dissemination of Information on cyber incidents;
    - Forecast and alerts of cyber security incidents;
    - Emergency measures for handling cyber security incidents;
    - Coordination of cyber incident response activities;

    - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security, practices, procedures, prevention, response and reporting of cyber incidents; and
    - Such other functions relating to cyber security as may be prescribed.

National Critical Information Infrastructure Protection Center (NCIIPC)

- The National Critical Information Infrastructure Protection Center (NCIIPC) was **established on January 16, 2014,** by the Indian government, **under Section 70A of the IT Act, 2000**.
- Based in New Delhi, the NCIIPC was appointed as the national nodal agency in terms of Critical Information Infrastructure Protection.
- Additionally, the NCIIPC is regarded as a unit of the National Technical Research Organization (NTRO) and therefore comes under the Prime Minister's Office (PMO).
- NCIIPC is required to monitor and report national-level threats to critical information infrastructure. The critical sectors include:
    - Power and energy
    - Banking, financial services, and insurance
    - Telecommunication and information
    - Transportation
    - Government
    - Strategic and public enterprises
- NCIIPC successfully implemented several guidelines for policy guidance, knowledge sharing, and cybersecurity awareness for organizations to conduct preemptive measures of these important sectors, especially in power and energy.

Digital Personal Data Protection (DPDP) Act, 2023

- On August 11, 2023 the Digital Personal Data Protection Act, 2023 (the Act) received the assent of the President of India and was published in the Official Gazette.
- The DPDP Act is **India's first data protection Act,** and it establishes a framework for the processing of personal data in India.
- It provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.
- The Act is concise and SARAL, that is, Simple, Accessible, Rational & Actionable Law, and used the word “she” instead of “he”, to acknowledge women in Parliamentary law-making.

Seven Principles

The Act is based on the following seven principles:

- The principle of consented, lawful and transparent use of personal data;
- The principle of purpose limitation (use of personal data only for the purpose specified at the time of obtaining consent of the Data Principal);
- The principle of data minimisation (collection of only as much personal data as is necessary to serve the specified purpose);
- The principle of data accuracy (ensuring data is correct and updated);
- The principle of storage limitation (storing data only till it is needed for the specified purpose);
- The principle of reasonable security safeguards; and
- The principle of accountability (through adjudication of data breaches and breaches of the provisions of the Bill and imposition of penalties for the breaches).

Internet of Things (IoT)

- The term Internet of Things refers to the collective network of connected devices and the technology that **facilitates communication between devices and the cloud,** as well as between the devices themselves.
- Basically, IoT integrates everyday “things” with the internet.

Working of IoT

- IoT systems work through the **real-time collection and exchange of data.** An IoT system has **three components: smart device, IoT application and a graphical user interface.**
- Smart device is a device, like a television, security camera, or exercise equipment that has been given **computing capabilities.** It collects data from its environment, user inputs, or usage patterns and communicates data over the internet to and from its IoT application.
- An IoT application is a **collection of services and software that integrates data received** from various IoT devices. It uses machine learning or artificial intelligence (AI) technology to analyze this data and make informed decisions.
- The decisions are communicated back to the IoT device and the IoT device then responds intelligently to inputs.
- The IoT device or fleet of devices can be managed through a graphical user interface.

Examples of IoT devices

Connected cars

- There are many ways vehicles, such as cars, can be connected to the internet. It can be through smart dashcams, infotainment systems, or even the vehicle's connected gateway.
- They collect data from the accelerator, brakes, speedometer, odometer, wheels, and fuel tanks to monitor both driver performance and vehicle health.

Connected homes

- Smart home devices are mainly focused on improving the efficiency and safety of the house, as well as improving home networking.
- Devices like smart outlets monitor electricity usage and smart thermostats provide better temperature control.
- Hydroponic systems can use IoT sensors to manage the garden while IoT smoke detectors can detect tobacco smoke.
- Home security systems like door locks, security cameras, and water leak detectors can detect and prevent threats, and send alerts to homeowners.

Smart cities

- IoT applications have made urban planning and infrastructure maintenance more efficient.
- IoT applications can be used for measuring air quality and radiation levels, reducing energy bills with smart lighting systems, detecting maintenance needs for critical infrastructures and increasing profits through efficient parking management.

Manufacturing

- IoT applications can predict machine failure before it happens, reducing production downtime.
- Wearables in helmets and wristbands, as well as computer vision cameras, are used to warn workers about potential hazards.

Logistics and transport

- Commercial and Industrial IoT devices can help with supply chain management, including inventory management, vendor relationships, fleet management, and scheduled maintenance.

- Shipping companies use Industrial IoT applications to keep track of assets and optimize fuel consumption on shipping routes.

Benefits of IoT

- Real-time resource visibility.
- Reduced costs.
- Improved operational efficiency.
- Data-driven insights for quick decision-making.
- End-to-end, remote monitoring and management of assets/resources.
- Real-time, predictive and prescriptive insights.
- Improve end-customer experience.

Big Data

- By definition, Big Data is data whose scale, diversity, and complexity require new architecture, techniques, algorithms, and analytics to manage it and extract value and hidden knowledge from it. Big Data is characterized by 6Vs:
    - **Volume:** amount of data from myriad sources.
    - **Variety:** types of data: structured, semi-structured, unstructured.
    - **Velocity:** speed at which big data is generated.
    - **Veracity:** degree to which big data can be trusted.
    - **Value:** business value of the data collected.
    - **Variability:** ways in which big data can be used and formatted.

Applications of Big Data

Governance

- Prevent cyber-attacks
- Enhance security systems
- Detect card-related fraud cases
- Predict criminal activities
- Improving the quality of education
- Disaster Management

Retail/Consumer

- Market based analysis
- Supply chain management and analytics
- Behaviour based targeting
- Market and consumer segmentation

Medical and Health

- Clinical trials data analysis
- Disease pattern analysis
- Campaign and sales program optimization
- Patient care quality and program analysis
- Medical device and pharmacy supply chain management
- Drug discovery and development analysis

Economy

- To manage financial data
- To capture the production, price statistics, and calculate the resultant GDP
- Evade risks and minimize losses for financial firms
- Catching hold of tax evaders
- Deregistration of shell companies
- Preventing money laundering and curbing terrorism financing

Finances and Fraud Services

- Compliance and regulatory reporting
- Risk analysis and management
- Fraud detection and security analysis
- Credit risk and scoring
- Trade surveillance
- High speed arbitrage trading

Web and Digital Media

- Large scale clickstream analysis
- Ad targeting, forecasting and optimization
- Social graph analysis and profile segmentation

Agriculture and Food

- Seed Selection
- Geo-Tagging to keep the track record of agricultural assets
- Weather Forecasting
- Effective water management
- Food Processing
- Identification of Crop Diseases

Telecommunications

- Revenue assurance and price optimization
- Call detail record analysis
- Network performance
- Mobile user location analysis

Government Initiatives and Interventions in India

- **National Data & Analytics Platform (NDAP):** NITI Aayog launched the National Data & Analytics Platform (NDAP) in May 2022. The platform uses cutting-edge methods to link diverse datasets from across the government and enables the use of several types of data at once. As of Feb 2023, NDAP hosts 885 datasets from across 15 sectors and 46 Ministries.
- **Big Data Management Policy:** It was drafted by CAG for auditing large chunks of data generated by the public sector in the states and the union territories.
- **National Data Warehouse on Official Statistics:** The Ministry of Statistics and Programme Implementation has proposed to establish a National Data Warehouse on Official Statistics with a view to leveraging big data analytical tools to further improve the quality of macro-economic aggregates.
- Use of Direct Benefit Transfer in MGNREGA (Mahatma Gandhi National Rural Employment Guarantee Act), Aadhaar for authentication and availing welfare scheme, Smart City Mission, Digital India, BHIM app etc. are important government initiatives that are using Big Data for achieving good governance in the country.