Information Technology

Introduction

The study and use of systems that store, retrieve, and distribute information is known as information technology (IT). Software, hardware, and many software and hardware-based applications make up the system. Information technology benefits businesses, education, government, and even healthcare.
India's economy and jobs have benefited greatly from this industry. According to NASSCOM, the IT industry earned $180-billion in sales in 2019, with export revenue of $99-billion and domestic revenue of $48-billion, representing a 13 percent increase. India's IT workforce is expected to number 4.36-million by 2020.

Information Technology (IT) Act 2000

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) published the model law on electronic commerce (e-commerce) to promote uniformity in national laws. India's primary law covering cybercrime and electronic commerce is the Information Technology Act of 2000 (ITA-2000, or the IT Act).

- The Information Technology Act of 2000 legitimises activities using electronic data transmission and other forms of electronic communication, as well as electronic business transactions.
- Aim: To provide legal recognition for transactions using electronic data exchange.

Features of the Information Technology Act, 2000

- It is legal to engage electronic contracts over secure electronic channels.
- Digital signatures are legally recognised.
- There are security precautions in place for electronic records, as well as digital signatures.
- The mechanism for appointing adjudicating officers to conduct investigations under the Act is outlined in the Act.
- The Act includes a provision for the establishment of a Cyber Appellate Tribunal. All appeals against the Controller's or Adjudicating Officer's orders will be heard by the Tribunal.
- The Act includes a provision for the establishment of a Cyber Appellate Tribunal. All appeals against the Controller's or Adjudicating Officer's orders will be heard by the Tribunal.
- There is a provision for the appointment of a Controller of Certifying Authorities (CCA) to licence and control the activities of Certifying Authorities. The Controller is the central location for all digital signatures.
- The Act covers actions and violations committed outside of India.
- Senior police officers and other authorities may enter any public location without a warrant, search and arrest anybody for offences listed in this legislation.
- Provisions for the formation of a Cyber Regulations Advisory Committee to provide advice to the Controller and the Central Government.

Section 66A and Restrictions on Freedom of Speech

Since its inception as an addition to the original statute in 2008, Section 66A has sparked debate regarding its constitutionality.

Section 66A

Any person who communicates by any means of a computer resource, any material that is excessively offensive or threatening in nature; or any information that he knows to be false but intends to cause irritation, discomfort, danger, obstruction, or insult is subject to a three-year jail sentence and a fine.

Shreya Singhal Case

- Shreya Singhal, a Delhi-based law student, filed a Public Interest Litigation (PIL) before the Supreme Court of India, claiming that Section 66A should be repealed. As a consequence, it violated the Constitution's Article 14, 19 (1) (a), and Article 21.
- Section 66A was declared illegal by the Supreme Court in 2015. The court found that Section 66A of the Information Technology Act of 2000 "arbitrarily, excessively, and disproportionately" infringes on Article 19(1) of the Indian Constitution's right to free speech. A plea to invalidate sections 69A and 79 of the Act, which regulates the process and safeguards for banning particular websites, was denied by the Court.
- The Centre may limit public access to an intermediary under Section 69A of the IT Act of 2000. "Telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, and other intermediaries" are examples of intermediaries.

National Knowledge Network (NKN)

The National Information Network (NKN) is a high-speed data transmission network that aims to connect all higher education and research institutions in order to facilitate information sharing and collaborative research.

- The National Knowledge Network was authorised by the Cabinet Committee on Infrastructure (CCI) in March 2010.
- Frontier research and innovation are shifting towards interdisciplinary and collaborative techniques throughout the world, which needs effective communication, and processing capability.
- To address such paradigm changes in India, NKN, with its multi-gigabit potential, wants to link all universities, research institutes, libraries, labs, hospitals, and agricultural organisations.
- NKN also includes the top mission-oriented agencies in nuclear, space, and military research.
- The network solves the important problem of access by enabling the flow of information and knowledge. It establishes a new model of partnership to benefit the country's scientific endeavours.
- The network is designed with a proactive mindset in mind. It takes into account future needs and new opportunities, both in terms of consumption and possible rewards.
- It will usher in a new era of knowledge. It will play a crucial role in changing society and supporting inclusive development.

Features of NKN

- Establishing high-speed network connectivity will enable knowledge and information sharing.
- Enabling collaborative research, development, and Innovation.
- Facilitating advanced distance education in specialised fields such as engineering, science, medicine, space, law, etc.
- Facilitating an ultra-high-speed backbone for e-Governance.
- Facilitating integration of different sectoral networks in research, education, health, commerce, and governance.
- Link to Global Networks to collaborate with research communities across the globe.

Stakeholders in the Internet Space

It's crucial to recognise the four main types of online stakeholders. They are:

- Any internet service's customers

- The Telecom Service Providers (TSPs) or Internet Service Providers (ISPs)
- Over-the-top (OTT) service providers (those who offer internet access services such as websites and apps)
- The government, which has the power to control and define these actors' interactions.
- The Telecom Regulatory Authority of India (TRAI) is an independent telecom regulator that primarily supervises TSPs and their licence criteria.

The Indian Computer Emergency Response Team (CERT-IN)

- The Indian Computer Emergency Response Team (CERT-In) is a government of India institution under the Ministry of Electronics and Information Technology. It serves as the focal point for cyber security risks such as hacking and phishing. It increases the security defences of the Indian Internet domain. CERT-In discovered a major issue in Android Jelly-Bean's VPN functionality in March 2014.
- CERT-In has been operational since January 2004. The constituency of CERT-In is the Indian Cyber Community.
- CERT-In has been appointed as the national agency in charge of performing the following cyber security duties.
  - Information about cyber events is collected, analysed, and disseminated.
  - Cyber security issues are forecasted and alerted.
  - Measures should be taken in the event of a cyber-security incident.
  - Cyber incident response operations must be coordinated.
  - Recommendations, advisories, vulnerability notifications, and whitepapers on information security policies, processes, prevention, response, and reporting of cyber events
  - Other cyber security-related responsibilities may be required.

Optical Communication

- Optical communication is a method of communication in which light, rather than electrical current, is utilised to deliver the signal to the distant end. Optical fibres are used to deliver signals to their destinations in optical communication. Optical fibres have essentially supplanted copper wire communications in the industrialised world's core networks due to their various benefits over electrical transmission.
- Optical communications have been one of the most common communication modalities since the invention of low-loss optical fibre lines in the 1970s.

Advantages of Optical Fiber Cable

- **Bandwidth:** Metal cables have a substantially lower bandwidth than fibre optic lines. The major benefit of fibre over other transmission mediums is the quantity of information that can be sent per unit of time.
- **Low power loss:** Low power loss is provided by the optical fibre, allowing for greater transmission lengths. The longest approved copper distance is 100m, and the maximum suggested fibre distance is 2 km.
- **Interference:** Electromagnetic interference is not a problem with fibre optic lines. It may even be used in electrically loud areas since the fibre is unaffected by the noise.
- **Size:** A fibre optic cable has 4.5 times the capacity of a wire cable and a cross-sectional area 30 times that of copper.

- **Weight:** Metal wire is much thicker and heavier than fibre optic cables. They also take up less space with the same capacity cables. When fibre is lighter, it is easier to install.
- **Security:** Optical fibres are difficult to tap. Emissions cannot be intercepted since they do not emit electromagnetic radiation. Fibre is the most secure media available for conveying sensitive data since tapping it is impossible.
- **Flexibility:** An optical fibre has greater tensile strength than copper or steel fibres of the same diameter. It is more pliable, bends more readily, and is resistant to most corrosive substances. As a consequence, the copper wire becomes vulnerable.
- **Cost:** Glass, unlike copper, has a great supply of raw materials. It indicates that glass is less expensive to make than copper.

Disadvantages of Optical Fiber Cable

- **Difficult to splice:** Splicing optical fibres is difficult, and there is a light loss in the fibre owing to scattering. They just have a little physical cable arc. They will shatter if we bend them too much.
- **Expensive to install:** Optical fibres are more costly to install, and they must be done by professionals. They aren't as strong as wires. Optical fibre testing often necessitates the use of specialised equipment.
- **Highly susceptible:** Because fibre optic cable is so thin and compact, it is very susceptible to being cut or damaged during installation or construction. The data transmission possibilities of fibre optic cables are enormous. When fibre optic cable is selected as the transmission medium, restoration, backup, and survival must all be considered.
- **Can't be curved:** The optical fibre transmission must be repeated at regular intervals. When fibres are twisted around curves of just a few centimetres radius, they might be damaged

National Optical Fibre Network (NOFN)

- The optical fibre transmission must be repeated at regular intervals. When fibres are twisted around curves of just a few centimetres radius, they might be damaged or suffer transmission losses.
- The government intends to link NOFN to all of the country's 2,50,000 Gram Panchayats. This will be accomplished by leveraging existing PSU fibres (BSNL, Railtel, and Power Grid), as well as laying additional fibre to link to Gram Panchayats as needed.
- The resulting dark fibre network will be lighted by suitable technology, providing adequate bandwidth to Gram Panchayats. The National Optical Fibre Network will be the name of this project (NOFN). As a result, the gap in connection between Gram Panchayats and Blocks would be closed.
- All Service Providers shall have access to the NOFN without discrimination. Telecom Service Providers (TSPs), Internet Service Providers (ISPs), Cable TV operators, and Content Providers, for example, may establish a variety of services in rural regions.
- These operators may offer a variety of services such as e-health, e-education, and e-governance, among others.
- The cost of the NOFN project is projected to be over Rs. 20,000 crores. It is expected to be finished in two years. The Universal Service Obligation Finance will fund the project (USOF).

Visible Light Communication Technology

Light Fidelity (Li-Fi)

Li-Fi, or light fidelity, is a wireless technology designed by the German scientist Harald Haas that uses visible light instead of radio waves to send data at terabits per second speeds—more than 100 times faster than Wi-Fi. Despite the fact that it was found in the previous decade, it was only in 2015 that proofs of concept for commercial use began to emerge.

Working: A Visible Light Communications (VLC) system is Li-Fi. It has a photo-detector for receiving light signals and a signal processing device for converting the data into streamable information. Unlike Wi-Fi, which is powered by radio waves, Li-Fi is powered by visible light.

Applications: Traffic management: Traffic lights can communicate with each other through traffic lights. Traffic control may be made sophisticated and flexible in real-time by incorporating Li-Fi technology. Roadsides can also be turned into wireless hotspots by converting traffic and street light posts into access points.

- **Safe zones:** Because visible light is safer than radio waves, it can be utilised in situations where radio waves are prohibited, such as petrochemical and nuclear plants, as well as hospitals.
- **Accident prevention:** Vehicles with LED-based headlights and taillights can connect with one another and exchange information, preventing accidents.
- **Underwater communication:** Li-Fi can also work underwater, where Wi-Fi is unavailable, opening up a world of possibilities for military and navigational operations.
- **Power transmission:** It also opens up another innovative possibility: wireless power transmission, in which the smartphone not only receives data but also receives power to charge itself.

Limitations:

- External light sources, such as daylight and bulbs, as well as barriers in the way of transmission, are likely to create communication pauses with Li-Fi.
- Because visual light cannot penetrate through opaque objects and requires a line of sight for transmission, its range will be initially limited. More capable LED bulbs will need to be placed at various locations in order to experience full connectivity.
- To enable connectivity, Li-Fi requires that the lightbulb be turned on at all times, which means that the lights will have to be turned on during the day.
- Visual light communication systems as an add-on to lighting systems will also have significant installation costs at first.
- If Li-Fi can be made to work in practice, any LED bulb (indoor or outdoor) can be converted into a hotspot that transmits data to any mobile device, allowing for universal broadband connection between devices.

Radio Frequency Identification (RFID)

The term RFID refers to a technique of encoding digital data in RFID tags or smart labels that may be read by a reader. In the same way that a device takes data from a tag, it's similar to barcoding. RFID is a kind of technology that also incorporates automated data collecting and identification. Such technology recognises things, gathers data about them, and feeds it straight into the computer with little or no human involvement.

How RFID Works

RFID scanners work similarly to barcode scanners in which they acquire and store data using low-power radio waves rather than scanning laser light reflections from printed barcode labels. This technology is used to automate data collection in a warehouse or distribution centre. Radio frequencies are read by the transceiver and sent to an RFID tag. The identifying information is subsequently sent to the RFID reader through a tiny computer chip included within the tag.

Constituents of RFID

The three components are an RFID tag or label, a reader, and an antenna. To convey data to the reader, the tag has a circuit and an antenna integrated it. The reader then converts the waves that have been sent into a usable type of data. The data is subsequently transferred to a host computer system, where it may be analysed and stored.

Types of RFID

RFID can be divided into two categories:

Near Field RFID includes a small, omnidirectional reader antenna with a tag reading range of 5 mm to 10 cm based on frequency and antenna.

- Far-Field RFID uses a set of directed, resonant antennas and tags that can reach distances of up to 22.1 meters.

Applications of RFID

- **Supply chain and logistics management:** By giving visibility, RFID may help enhance efficiency, reduce mistakes, and improve quality in the supply chain. With RFID applications, you can instantly know how many of each sort of item you have, as well as their position and stage in the process.
- **Real-time location:** One can trace the whereabouts of personnel and assets in real-time using this technology. It aids in determining the efficacy of a floor-based plan and keeping track of resource locations. RFID applications can automatically track the movement of goods and upload the information to the ERP or financial management system.
- **Smart home controls:** Energy consumption/production management systems for homes and businesses.
- **Environmental:** Energy, ozone & pollution measuring equipment.
- **Traffic signals:** The usage of RFID for traffic signals on the road (Road Beacon System). It is based on the use of RFID transponders (radio beacons) placed on the floor that are read by a vehicle-carrying unit (OBU) that filters the various traffic signals and, if necessary, warns the driver.

Benefits of RFID

- When tags are moved, they can set off alarms.
- Data can be automatically read and saved by readers and tags without regard to their orientation.
- On tags, product codes may be unique or standardised.
- Items can be labelled individually, but they must be read in bulk.
- Tag data may be accessed by WMS and ERP systems.
- Counterfeiting/reproducing tags is tough.

Cloud Computing

Cloud computing refers to the distribution of computer services such as servers, storage, databases, networking, software, analytics, and intelligence via the internet ("the cloud") in order to provide quicker innovation, more flexible resources, and cost savings. Cloud computing refers to the on-demand distribution of computer system resources, such as data storage (cloud storage) and processing power, without the involvement of a direct user or active administration.

Clouds may be restricted to a single business (enterprise clouds) or made open to a large number of companies (public clouds) (public cloud). To achieve coherence and economies of scale, cloud computing depends on resource sharing.

Benefits of Cloud Computing

- **Cost:** It saves money on hardware and software, as well as the cost of setting up and maintaining on-site data centres, as well as the cost of 24/7 electricity and cooling, and the expense of paying IT professionals to administer the infrastructure.
- **Speed:** Most cloud computing services are self-service and on-demand, which means that even massive quantities of computing resources may be deployed in minutes, usually with only a few mouse clicks, offering enterprises a lot of flexibility and relieving capacity planning strain.
- **Global scale:** Most cloud computing services are self-service and on-demand, which means that even massive quantities of computing resources may be deployed in minutes, usually with only a few mouse clicks, offering enterprises a lot of flexibility and relieving capacity planning strain.
- **Productivity:** Hardware installation, software patching, and other time-consuming IT administration tasks are common in on-site data centres. IT departments may devote more effort to achieve more critical business objectives.
- **Performance:** The most popular cloud computing services are housed on a secure worldwide network of data centres that are upgraded to the latest generation of fast and efficient computer technology on a regular basis. It provides a number of benefits over a single corporate data center, including reduced application network latency and more scalability.
- **Reliability:** Data backup, disaster recovery, and business continuity are all simpler and less costly with cloud computing. Because data may be duplicated throughout the cloud provider's network at several redundant locations.
- **Security:** A wide range of policies, technologies, and controls are available from several cloud providers. It improves your entire security posture by assisting in the protection of your data, applications, and infrastructure from possible attacks.

Major types of Cloud Services

- **Software as a Service (SAAS):** Software as a service (or SaaS) is a method of delivering software as a service through the Internet. Instead of installing and maintaining software, one simply uses the Internet to access it, liberating oneself from the hassles of software and device maintenance. Previously, if a company wanted to use software, it had to be installed on local systems and then properly maintained. However, under SAAS, the software can be accessed directly through thin clients such as a browser.
- **Infrastructure as a Service (IAAS):** Infrastructure as a service (IaaS) is a pay-as-you-go cloud computing service that delivers on-demand compute, storage, and networking capabilities. IaaS helps you to save money and time by not having to buy and maintain your own servers and data centre infrastructure. Each resource is sold separately as a service component, and you only pay for what you

use. The infrastructure is managed by a cloud computing service provider, while one, installs, configures, and manages its own software, which includes operating systems, middleware, and applications.

- **Platform as a Service (PAAS):** PaaS is a full cloud development and deployment environment that includes tools that allow you to create anything from basic cloud-based applications to complex cloud-enabled commercial systems. Using PaaS, one may save money and time by not having to buy and manage software licences, underlying application architecture and middleware, container orchestrators, and other resources. One is in charge of the apps and services they develop, while the other is in control of the cloud service provide

Uses of Cloud Computing

- **Create cloud-native applications:** Online and mobile app creation, deployment, and scalability are all aided by cloud computing.
- **Test and build applications:** You may save money and time on application development by using cloud infrastructures. Scaling up or down is straightforward.
- **Store, back up and recover data:** Transferring data to an offsite cloud storage system through the Internet is a more cost-effective solution to secure big amounts of data. It is accessible from any device and from any location.
- **Analyse data:** Unify data across several teams, divisions, departments, and geographic areas on the cloud. Utilise cloud technologies such as machine learning and artificial intelligence to uncover insights that can assist you in making better decisions.
- **Stream audio and video:** You can connect with your audience anywhere, at any time, on any device, thanks to high-definition video and audio that is transmitted internationally. Examples include netflix, amazon prime, hotstar, and other streaming services.
- **Deliver software on demand:** On-demand software, often known as software as a service (SaaS), enables businesses to give customers the most up-to-date software versions and updates.