1. 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.

1.1. 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.

1.2. 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.

1.3. 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.

2. 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.

2.1. 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.

2.2. 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.

2.3. 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".

2.4. 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. Cyber Regulations Appellate Tribunal (CRAT)

- **Under the IT Act, 2000, Section 62,** the Central Government of India created the Cyber Regulations Appellate Tribunal (CRAT) as a chief governing body and authority for fact-finding, receiving cyber evidence, and examining witnesses.
- According to the Civil Court and Code of Civil Procedure, 1908, CRAT has the power to:
    - Receive evidence on affidavits.
    - Ensure that all electronic and cyber evidence and records are presented for court.
    - Enforce, summon, and issue regular commissions for examining witnesses, documents, and people under oath.
    - Review final decisions of the court to resolve incidents and cases.
    - Approve, dismiss, or declare the defaulter's applications as ex-parte.

3. 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).

Salient Features of the Digital Personal Data Protection Act, 2023

Applicability

- The Act applies to the **processing of digital personal data within India** where such data is collected online, or collected offline and is digitized.
- It will also apply to the processing of personal data **outside India** if it is for offering goods or services in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data.

Consent

- Personal data may be processed only for a lawful purpose after obtaining the consent of the individual. **A notice must be given before seeking consent.**
- The notice should contain details about the personal data to be collected and the purpose of processing. Consent may be withdrawn at any point in time.
- Consent will **not be required for 'legitimate uses'** including:
    - specified purpose for which data has been provided by an individual voluntarily,
    - provision of benefit or service by the government,
    - medical emergency, and
    - employment.
- For individuals **below 18 years of age, consent will be provided by the parent or the legal guardian.**

Rights of data principal

- Data principal is an **individual whose data is being processed.** He/She will have the right to:
    - obtain information about processing,
    - seek correction and erasure of personal data,
    - nominate another person to exercise rights in the event of death or incapacity, and
    - grievance redressal.

Duties of Data Principals

- Data principals will have certain duties. They must not:
    - register a false or frivolous complaint, and
    - furnish any false particulars or impersonate another person in specified cases.
- Violation of duties will be punishable with a penalty of up to Rs 10,000.

Obligations of data fiduciaries

- Data fiduciary is the **entity determining the purpose and means of processing.** Data fiduciary must:
    - make reasonable efforts to ensure the accuracy and completeness of data,
    - build reasonable security safeguards to prevent a data breach,

    - inform the Data Protection Board of India and affected persons in the event of a breach, and
    - erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes.
- In case of government entities, storage limitation and the right of the data principal to erasure will not apply.

Transfer of personal data outside India

- The Act allows transfer of personal data outside India, except to countries restricted by the central government through notification.

Exemptions

- Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases. These include:
    - prevention and investigation of offences, and
    - enforcement of legal rights or claims.
- The central government may, by notification, exempt certain activities from the application of the Act. These include:
    - processing by government entities in the interest of the security of the state and public order, and
    - research, archiving, or statistical purposes.

Data Protection Board of India

- The central government will establish the Data Protection Board of India. Key functions of the Board include:
    - monitoring compliance and imposing penalties,
    - directing data fiduciaries to take necessary measures in the event of a data breach, and
    - hearing grievances made by affected persons.

Penalties

- The schedule to the Act specifies penalties for various offences such as up to:
    - Rs 200 crore for non-fulfilment of obligations for children, and
    - Rs 250 crore for failure to take security measures to prevent data breaches.

Key Issues

- Exemptions to data processing by the State on grounds such as national security may lead to data collection, processing, and retention beyond what is necessary. This may violate the fundamental right to privacy.
- The Act does not regulate risks of harms arising from processing of personal data.
- The Act does not grant the right to data portability and the right to be forgotten to the data principal.
- The Act allows transfer of personal data outside India, except to countries notified by the central government. This mechanism may not ensure adequate evaluation of data protection standards in the countries where transfer of personal data is allowed.
- The members of the Data Protection Board of India will be appointed for two years and will be eligible for re-appointment. The short term with scope for re-appointment may affect the independent functioning of the Board.

1. 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.

1.1. 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.

1.2. 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.

1.3. 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.