Securing Internet of Things

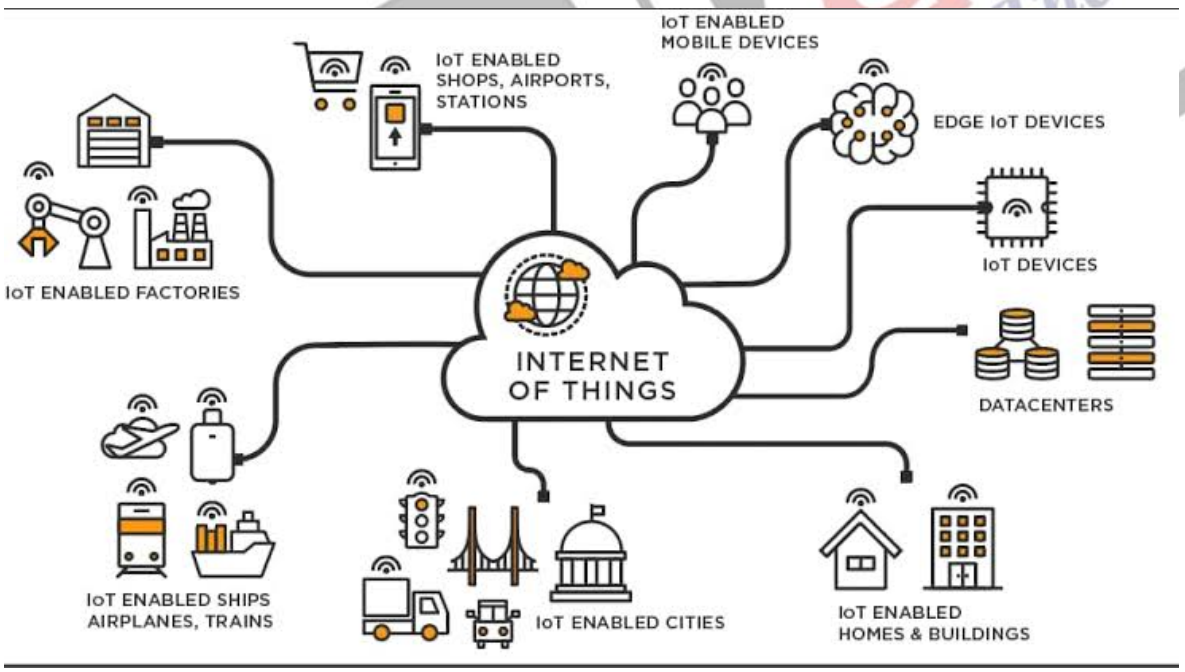
For Prelims: Internet of Things(IoT), Artificial intelligence/ Machine Learning, Cloud / Edge computing

For Mains: Code of Practice for Securing Consumer Internet of Things(IoT), Cyber-Security, Internet of Things and its uses.

Why in News

Recently, in order to secure **Consumer** Internet of Things (IoT) devices, **Telecommunication Engineering Centre (TEC)**, under Department of Telecommunications, Ministry of Communications, has released a report "**Code of Practice for Securing Consumer Internet of Things(IoT)".**

- These guidelines will **help in securing consumer IoT devices & ecosystem** as well as managing vulnerabilities.



Key Points

- **Internet of Things:**
  - **Definition:** It is a **computing concept** that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices.
  - **One of Fasting Growing Technology:** It is one of the **fastest emerging technologies across the globe**, providing enormous beneficial opportunities for society, industry, and

consumers.
    - **Use of IoT:** It is being used to create smart infrastructure in various verticals such as **Power, Automotive, Safety & Surveillance, Remote Health Management, Agriculture, Smart Homes and Smart Cities etc,** using connected devices.
        - A smart device is a context-aware electronic device capable of performing autonomous computing and connecting to other devices wire or wirelessly for data exchange.
    - **Supplementary Technologies:** IoT is benefitted by recent advances in several technologies such as sensors, communication technologies (Cellular and non-cellular), **Artificial intelligence**/ **Machine Learning**, **Cloud / Edge computing** etc.
- **Magnitude of IOT:** It has been projected that there would be around 11.4 billion consumer IoT devices and **13.3 billion enterprise IoT devices globally by 2025** i.e. consumer IoT devices would account for nearly 45% of all the IoT devices.
    - According to a market research report published by Markets and Markets, the global IoT security market size is expected to grow from **USD 8.2 billion in 2018 to USD 35.2 billion by 2023.**
- **Need For Guidelines:**
    - **Anticipated Growth:** In view of the anticipated growth of IoT devices, it is important to ensure that the IoT endpoints comply with the safety and security standards.
    - **Cyber-Security Attack:** The hacking of the devices/networks being used in daily life would harm companies, organisations, nations and more importantly people.
        - Therefore securing the IoT ecosystem end-to-end i.e. from devices to the applications is very important.
        - Ensuring end to end security for connected IoT devices is key to success in this market -without security, IoT will cease to exist.
    - **Privacy Concerns:** There is in this data-driven future, a growing concern about the potential for increased government surveillance and the resulting encroachment of civil rights, and the suppression of dissent or of marginalised communities
    - **Consequences of Cyber Security Attack:** Possible consequences of such attacks could include:
        - Discontinuity and interruption to critical services/infrastructure.
        - Infringement of privacy.
        - Loss of life, money, time, property, health, relationships, etc.
        - Disruptions of national scale including civil unrest.
- **Guidelines for securing consumer IoT:**
    - **No Universal Default Passwords:** All IoT device default passwords shall be unique per device and/or require the user to choose a password that follows best practises, during device provisioning.
    - **Implement a means to manage reports of vulnerabilities:** IoT developers should provide a dedicated public point of contact as part of a vulnerability disclosure policy.
    - **Keep software updated:** Software components in IoT devices should be securely updateable.
    - **Securely store sensitive security parameters:** IoT devices may need to store security parameters such as keys & credentials, certificates, device identity etc. which are critical for the secure operation of the device.
    - **Communicate securely:** Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage of the device.
    - **Minimise exposed attack surfaces:** Devices and services should operate on the ‘principle of least privilege’.
        - The Principle of Least Privilege states that a **subject should be given only those privileges** needed for it to **complete its task.**
    - **Ensure that personal data is secure:** In case the device collects or transmits personal data, such data should be securely stored.
    - **Make systems resilient to outages:** Resilience should be built into IoT devices and services where required by their usage or by other relying systems.

Way Forward

- **Addressing Data Security Concerns:** While IoT technology is clearly of significant advantage to citizens worldwide, along with greater advantage comes a potential risk to privacy.
    - This concern over data protection will need to be addressed and IoT manufacturers will have to build and sustain consumer trust in their devices.
    - In this context, **the Data Protection Bill,2019** is a step in the right direction.
- **Need for Global Deliberation:** Around the world, legislators, device manufacturers, and law enforcement agencies should come together to figure out how to benefit from IoT while mitigating risks.

Source: PIB