Sanchar Saathi Initiative

written by iasexam.com | 18/05/2023

Context- Union Minister of Communications launched the Sanchar Saathi portal in order to ensure Safety and security of the users.

Key Highlights

- Sanchar Saathi is a citizen-centered portal created by the Department of Telecom.
- The following are its modules:
  - Know your mobile connections – to know mobile connections registered in your name.
  - CEIR (Central Equipment Identity Register) – for blocking stolen/lost mobiles.
  - Telecom Analytics for Fraud Management and Consumer Protection (TAFCOP)
  - ASTR (Artificial Intelligence and Facial Recognition powered Solution for Telecom SIM Subscriber Verification) – to identify fraudulent subscribers.

Know Your Mobile

- It works with the residents to really look at the validity of IMEI of their cell phone.
- The **International Mobile Equipment Identity (IMEI)** is the 15-digit number that exceptionally recognizes every cell phone.
- There are two IMEI numbers on dual-SIM phones, one for each SIM card. In the event that a device is lost or stolen, the IMEI number can assist network providers in locating it.
- Manufacturers of mobile phones are now required by the Department of Telecommunications (DoT) to register the IMEI of each handset produced in India with the government.

Centralized Equipment Identity Register (CEIR)

- The Department of Telecommunications’ citizen-centric portal for tracking down stolen or lost mobile devices is called the Centralized Equipment Identity Register (CEIR).
- This also makes it easier to prevent lost or stolen mobile devices from being used in India by blocking them in the networks of all telecom providers.
- In the event that anybody attempts to utilize the taken gadget, the framework permits Policing to follow the gadget. Once a phone is found, citizens can use it normally by unlocking it on the portal.
- Additionally, it prevents the use of mobile devices in Indian networks that have forged or inaccurate IMEIs.

Telecom Analytics for Fraud Management and Consumer Protection (TAFCOP)

- The Telecom Analytics for Fraud Management and Consumer Protection (TAFCOP) module lets a mobile subscriber see how many mobile connections have been taken in his or her name using paper documents.
- Users are able to report bogus connections through the system. Additionally, it permits users to block unnecessary connections.

ASTR

- **“Artificial Intelligence and Facial Recognition powered Solution for Telecom SIM Subscriber Verification”** is the acronym for ASTR.
- This computerized reasoning based facial acknowledgment device has the capacity of running keeps an eye on supporter data sets of telecom administrators to derive whether it contains numerous associations related with a similar individual.
- With a single identity document, the Department of Telecommunications (DoT) permits nine legitimate mobile phone connections. In this manner, fundamentally, the ASTR turns upward on the off chance that there are in excess of nine associations against a solitary person’s photo.
- By spotting and preventing potential bogus mobile connections, it has the potential to reduce cyber fraud.

Working of ASTR

- Convolutional neural network (CNN) models are used to encode human faces in subscribers’ images to account for the images’ opaqueness, dark color, and tilt and angle.
- After that, each face is compared to all of the faces in the database, and similar faces are put into a single directory. Two appearances are closed to be indistinguishable by ASTR on the off chance that they match to the degree of somewhere around 97.5 percent.
- The ASTR algorithm uses what it calls “fuzzy logic” to find similarity or approximate matches for the subscriber names after the faces have been matched.

Significance

- Need for this initiative India has become the second largest telecom ecosystem in the world thanks to its 117 crore subscribers. Notwithstanding correspondence, cell phones are being utilized for banking, amusement, e-learning, medical care, profiting taxpayer supported organizations, and so on.

- Therefore, it is essential that users are safeguarded against a variety of frauds, including identity theft, forged KYC, device theft, banking fraud, and others.