How ASTR Works

Data Collection: TSPs provide the list of all the connections (not suspected connections) to ASTR which includes photographs of individuals taken during the SIM registration process.

Image Matching: ASTR extracts facial features from subscriber images and compares them against the entire database to identify multiple SIM connections linked to the same individual.

Fraud Detection: On detection of multiple connections linked to the same person, the system flags them as potentially fraudulent, prompting further investigation.

Action: LEAs/ Operators can take appropriate actions, such as blocking the fraudulent mobile connections and preventing further misuse.

Technologies Used

ASTR uses next-generation AI/ML algorithms for generating accurate results.

सी-डॉट
C-DOT

Centre for Development of Telematics

Telecom Technology Centre of
Govt. of India

www.cdot.in

C-DOT Campus, Mehrauli,
New Delhi - 110030, India
+91 11 2659 8262 | +91 9821488871

C-DOT Campus, Electronics City Phase
1, Bengaluru - 56100, India
+91 80 2852 0050

export@cdot.in

CDOT_India

Centre for Development of Telematics

सी-डॉट
C-DOT

ASTR

AI and Facial Recognition powered Solution for Telecom SIM Subscriber VeRification

The next-gen AI/ML solution for neutralising cyber crimes.

About ASTR

AI and Facial Recognition powered Solution for Telecom SIM Subscriber VeRification (ASTR) is an advanced solution developed by India's Centre for Development of Telematics (C-DOT), a premier R&D centre of Ministry of Communication, Government of India.

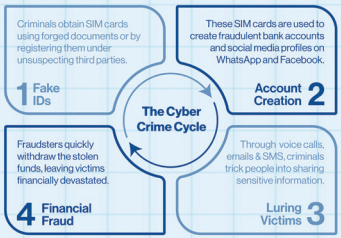
ASTR harnesses the power of artificial intelligence (AI) and facial recognition technology to revolutionise the verification of Subscriber Identity Module (SIM) significantly reducing the risk of fraudulent activities. The solution employs next-generation advanced algorithms and proactive intelligence to analyse vast databases of subscriber images, swiftly identifying connections obtained through forged documentation. This enables telecom operators and law enforcement agencies to take proactive measures against fraudulent mobile connections, protecting both consumers and the integrity of the telecom ecosystem.

Objectives

To carry out 100% SIM verification across all TSP.

Prevention of cyber-crimes and frauds.

Assisting the LEAs in the investigation of financial frauds and cyber crimes.



ASTR Breaks the Chain:

Facial Recognition
ASTR identifies multiple SIM cards linked to the same person, even if fake IDs were used during registration.

1

Early Detection
It allows authorities to block fraudulent SIM cards before they can be used to create fake accounts

2

Prevention
By preventing the creation of fraudulent accounts, ASTR disrupts the entire cybercrime cycle.

3

Investigation
When fraudulent SIMs are detected, ASTR's data can be used by law enforcement to trace criminals

4

Sample Case :

213 SIMs across different TSPs
100 Names
100 Forged PoI/PoA

ASTR detects Fraud
ONE PERSON

Benefits of ASTR

Enhanced Fraud Detection: ASTR's AI-powered facial recognition accurately identifies multiple SIM connections associated with a single individual, enabling early detection & prevention of fraudulent activities.

Increased Security: By reducing the prevalence of fraudulent SIM cards, ASTR strengthens the overall security of the telecom network, protecting consumers from identity theft, financial fraud, and other cybercrimes.

Improved Efficiency: ASTR's automated processes streamline the verification of SIM card subscribers, reducing the need for manual intervention & minimising the time and resources required for fraud detection.

Cost Savings: By preventing fraudulent activities, ASTR helps telecom operators avoid financial losses associated with fraudulent SIM card usage, such as unauthorised calls, SMS scams, and data theft.