e-ISSN 2582-4570

PREVENTING CYBER CRIMES AND FRAUDS USING PRO-ACTIVE COMMUNICATION INTELLIGENCE AND NEUTRALIZING THE CYBER CRIME SYNDICATES : A CASE STUDY OF MEWAT DISTRICT, HARYANA, INDIA

Naveen Jakhar[*]

ABSTRACT

The last three decades have seen a revolution in the field of Information and Communication Technology (ICT). Mobile phones have played the role of a catalyst in this digital transformation. The journey which started with voice calls have reached to huge data consumption, group calls and payment transfers on the go using UPI, Banking APPs and other payment APPs. As per TRAI Telecom Subscription Data as on 31st December 2021, there are approximately 115.4 crore wireless users and 76.5 crore broadband users in India.[1]This huge and vulnerable subscriber base provides a very large attack surface to the malicious elements. These malicious elements carry out various frauds like SIM swap, fake OTP, KYC updation, installing remote access APPs like Any Desk,Lottery Scam, online Transactions Frauds, Fake Calls Frauds, Email Frauds,Vishing, Phishing, SMiShing etc. The Law Enforcement Agencies (LEAs) and Ministry of Home Affairs (MHA) have reported that major cyber-crime fraud networks are operating from regions like Mewat, Jamtara etc. areas of the country. SIMs subscribed on forged/fake documents are involved in majority of these cybercrimes as well as conventional crimes like extortion, dacoity, kidnapping, hoax and threat calls etc., owing to anonymity and untraceability of such SIMs. Such syndicates are a direct threat to national security, public law and order. Once a mobile number is reported to be involved in any cyber fraud, the LEAs start investigation and the mobile number is also shared with Department of Telecom (DoT) for checking Customer Acquisition Form (CAF) and Proof of Identity/Address (PoI/PoA) documents used for taking the SIM connection. Majority of the times it is observed that the PoI/PoA documents are in order for these Fake SIMs.So, an alternative system was required which should be agnostic of any PoI/PoA. This paper presents a case study on an indigenous and innovative system designed by DoT Haryana LSA unit for carrying out pro-active analysis using communication intelligence for identifying non bonafide mobile numbers and weeding them out from the telecom ecosystem even before they carry out any cyber fraud. The tool has been proven so successful that entire cyber crime syndicates of Mewat have been neutralized, disconnecting 4.96 lakh SIMs across all TSPs, which is approximately 30% of total SIMs.

[*]ITS, Assistant Director General (Security), Department of Telecom, Government of India
Email ID: naveen.jakhar50@gov.in

[1] TRAI Telecom Subscription Data as on 31st December 2021, https://www.trai.gov.in/sites/default/files/PR_No.12of2022_0.pdf last visited on 4th April 2022.

I. INTRODUCTION AND PROBLEM STATEMENT

National Crime Records Bureau (NCRB) *Crime in India 2020 Report* has revealed that India recorded 50,035 cases of cyber crime in 2020, with an 11.8% surge in such offences over the previous year. In terms of motive, the maximum 60.2% cyber-crimes lodged in 2020 were done for fraud (30,142 out of 50,035 cases).[2] India lost Rs 1.25 lakh crores due to cyber crimes in year 2019-20.[3]More than 7 lakh complaints have been lodged on National Cyber Crime Reporting portal in last 3 years[4]. 135 crore Indian citizens are vulnerable to such frauds.

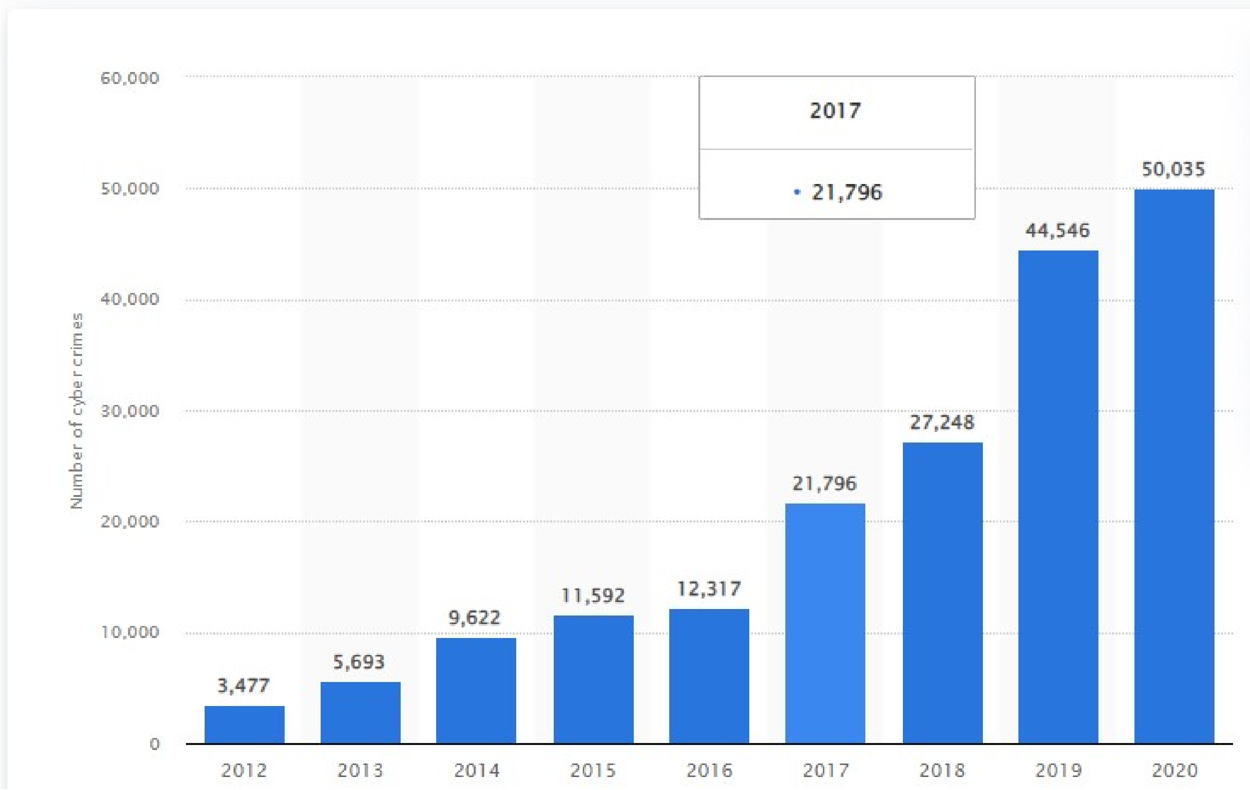


Fig.1 Number of cyber crimes in India from year 2012 to 2020 *Source: Statista 2022*[5]

Let us try to understand the Modus Operandi of a cyber crime syndicate. This is how any cyber crime syndicate works – the first person arranges fake SIM card, the second person gets bank accounts and payment APPs opened on fake SIM cards, thethird person impersonating as an agent of telecom service provider, bank or any other service agency, makes the fraud calls using another set of fake SIM cards to citizens for seeking their details like Aadhaar

[2] National Crime Records Bureau (NCRB), MHA Crime in India 2020 Report https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf last visited on 4 April 2022.

[3] *ibid*

[4] www.cybercrime.gov.in

[5] Number of cyber crimes reported across India from 2012 to 2020 https://www.statista.com/statistics/309435/india-cyber-crime-it-act/ last visited on 4th April 2022.

number, OTP, PIN, CVV debit/credit card details, bank details and the fourth person withdraws the money once they have duped the innocent citizen. Fake SIMs is the main link in the chain. The untraced-ability and anonymity in the SIMs make cyber crime investigation very complex.

The list of suspected mobile numbers is shared by MHA with DoT on regular basis. But when the documents of these suspected mobile numbers were analyzed, they were found to be genuine in all respects because each verification case was being dealt separately. An in-depth analysis and investigation was carried out by DoT Haryana LSA and it was observed that such is the expertise level of fraudsters that they have created fake Proof of Identity/Address documents which can never be detected by human beings by analyzing a single case in isolation – so even after being reported by LEAs – such SIMs come out be compliant during DoT audit – and cyber crime gangs remain functional. The fraudsters are creating fake/forged documents with such advanced techniques and keep on changing the Name, Guardian's Name, Date of Birth etc that conventional text based analysis can never catch them.

DoT and LEAs carry out conventional text based analysis on regular basis. But due to these changes in Name and other details, such Fake SIMs are never caught during text based analysis.

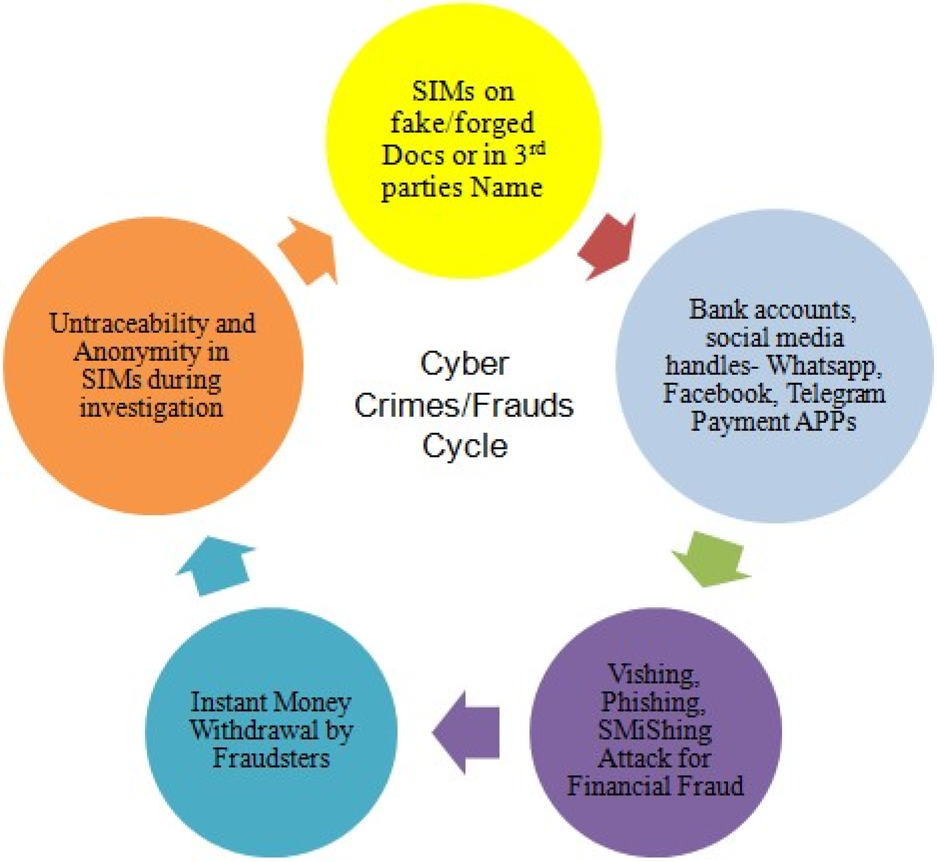

SIMs on fake/forged Docs or in 3rd parties Name
Bank accounts, social media handles- Whatsapp, Facebook, Telegram Payment APPs
Vishing, Phishing, SMiShing Attack for Financial Fraud
Instant Money Withdrawal by Fraudsters
Untraceability and Anonymity in SIMs during investigation
Cyber Crimes/Frauds Cycle

Fig.2Modus operandi of cyber crime syndicates -cyber crime/frauds cycle

The above mentioned issues crystallize into following problem statements:

i. The TSPs maintain their individual database and work in silos.

ii. There are more than 30 PoI/PoA documents on which a person can take a new SIM connection.[6] The database of the issuing organizations of these PoI/PoA does not have connectivity with SIM subscriber database. So, there exists no cross checking mechanism at the TSP end if a person uses a fake/forged PoI/PoA for taking a new SIM connection.

iii. The field units of the DoT were carrying out text based analysis of the entire subscriber base. The fraudsters are creating fake/forged documents with different Names Date of Birth; with such advanced techniques that conventional text based analysis can never catch them.

iv. More than 7 lakh complaints have been filed on NCRP portal in last 3 years. India recorded 50,035 cases of cyber crime in 2020, maximum 60.2% cyber-crimes were done for fraud. Fake SIMs are the main link in all such crimes[7].

v. The number of registered cyber-crimes has increased more than five-fold since 2014 and crossed 50000 for the first time in 2020. Cases of fraud accounted for more than 60% of these cases in 2020. The pendency of these cases at the police crossed 70% by the end of 2020.[8]

[6] https://dot.gov.in/

[7] www.cybercrime.gov.in

[8] https://factly.in/data-the-number-of-registered-cyber-crimes-cross-50000-in-2020-20-of-these-are-fraud-cases/

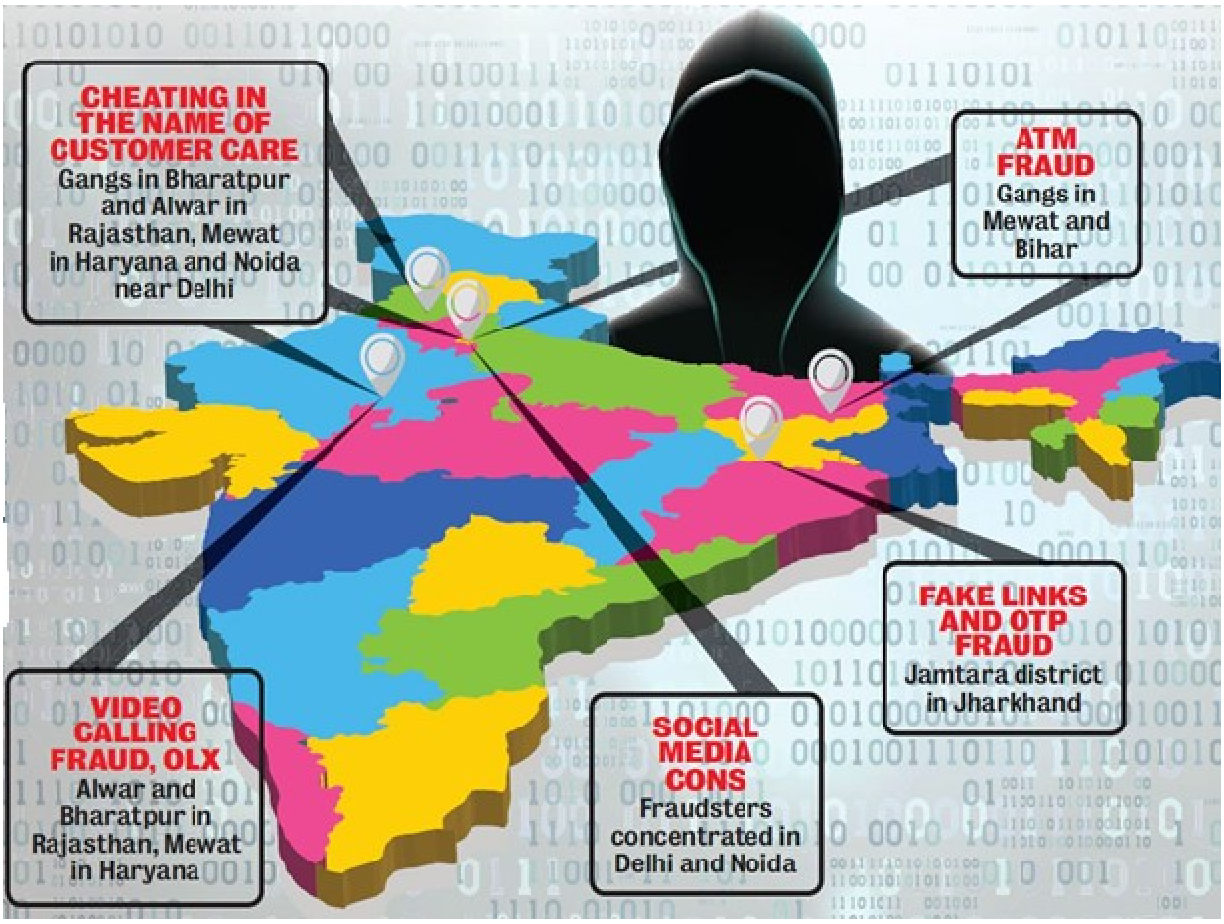

CHEATING IN THE NAME OF CUSTOMER CARE
Gangs in Bharatpur and Alwar in Rajasthan, Mewat in Haryana and Noida near Delhi
ATM FRAUD
Gangs in Mewat and Bihar
FAKE LINKS AND OTP FRAUD
Jamtara district in Jharkhand
SOCIAL MEDIA CONS
Fraudsters concentrated in Delhi and Noida
VIDEO CALLING FRAUD, OLX
Alwar and Bharatpur in Rajasthan, Mewat in Haryana

Fig.3 Cyber crime hotspots in India

II. INNOVATION AND METHODOLOGY ADOPTED

These above mentioned figures of cyber crimes cases and pendency of investigation are not only scary but also pose a strong threat to the vision of Digital India and Digital Economy. As they say "*Prevention is better than cure*." The aim of the field study was to detect the non bonafide SIMs before incident of cyber crime or fraud. The study was descriptive and was carried out in Mewat District, Haryana. So, a team of officers in DoT Haryana LSA took this challenge of detecting the potential non bonafide SIMs and weeding them out from the telecom ecosystem even before they carry out any cyber fraud/crime. This gave birth to ASTR (अस्त्र)–Artificial Intelligence and Facial Recognition powered Solution for Telecom SIM Subscriber Verification. It is an indigenous and innovative system designed by an in house team of ITS officers in DoT Haryana LSA.

Innovative Research Approach

ASTR project was conceptualized and designed during the period April 2021 to July 2021. The subscriber images were taken from the TSPs and algorithms were trained using this dataset. The first version of the system was ready in the last week of July 2021. As a pilot project, ASTR was launched in Mewat region. The vision of the ASTR project is to analyze the whole subscriber base of all TSP combine and cleanse the database by identifying on bonafide mobile numbers even before they carry out any cyber fraud and the case reporting by LEAs.

As per DoT instructions, a person can have at max nine SIMs in his name in India. For people staying in Jammu & Kashmir and Northeast, a person can have at max six SIMs.

During SIM subscription process, live image of the subscriber is taken by the Point of Sale agent of the TSPs. DoT has issued instructions to all the Telecom Service Providers (TSPs) for submitting the images of the subscribers taken during SIM subscription process. ASTR utilizes these captured images of the subscribers and tries to find similarity among them with very high grade of accuracy using face recognition and Artificial Intelligence. The images from all the TSPs are merged for carrying a comprehensive analysis. In second step, Big Data Analytics was performed on the name of the subscribers for checking similarity of names using Fuzzy logic.

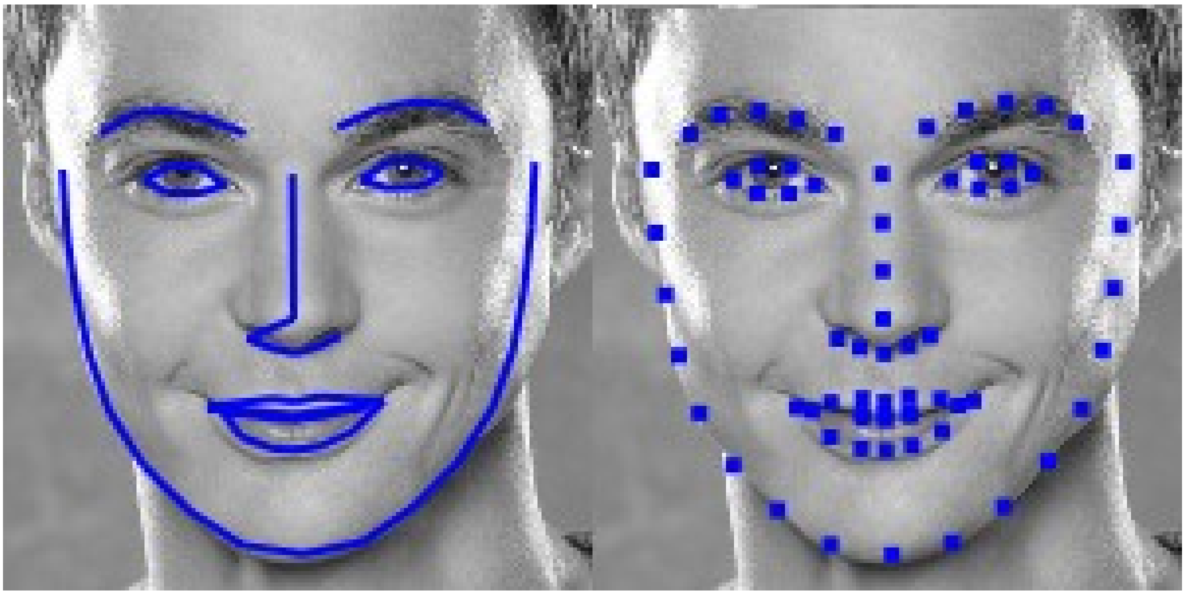
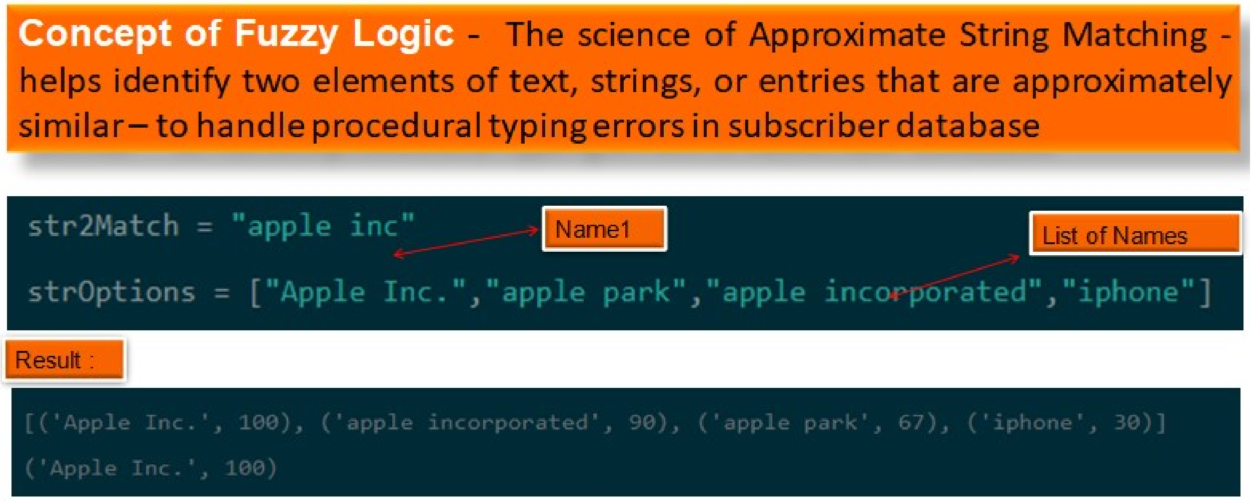


Fig4. Genesis of ASTR: 68-point Frontal Facial Landmark Model



Concept of Fuzzy Logic - The science of Approximate String Matching - helps identify two elements of text, strings, or entries that are approximately similar – to handle procedural typing errors in subscriber database

```
str2Match = "apple inc"

strOptions = ["Apple Inc.","apple park","apple incorporated","iphone"]
```

```
[('Apple Inc.', 100), ('apple incorporated', 90), ('apple park', 67), ('iphone', 30)]
('Apple Inc.', 100)
```

Fig5. Concept of Fuzzy Logic in ASTR

The innovative elements of ASTR are as follows:

(i) The subscriber images are taken from all the TSPs and stored as aggregated images.

(ii) In second step, the human faces are encoded using multi staged and layered HOG model and Convolutional Neural Network (CNN) models. Multi layered and integrated HOG and CNN models have been used for handling the tilt and angle of face, opaqueness and dark colour of the images.

(iii) In third step, face comparison is carried out for each face against all faces. Similar faces are grouped under one directory. Multi threading and cosine vector comparison have been used for ensuring face comparisons with very high grade of accuracy. Vectorized comparisons have been used for handling huge calculations of 16.69 lakh * 16.69 lakh i.e. 2.785 lakh crore comparisons.

(iv) Two faces are said to be identical by ASTR if they match 97.5% or more.

(v) In fourth step, Fuzzy logic is used for finding similarity / approximate match for the subscriber names. It is capable of handling all type of typographical mistakes and provides unique sets of names. Depending upon the output, it is derived whether the same person has acquired two or more SIMs under different names using forged Proof of Identity/ Proof of Address documents.

(vi) In the final step, all similar faces under one directory are mapped to a collage and important details like Mobile Number, CAF Number, Name of Subscriber and TSP are stamped on the collage for easy identification and further analysis like hotspot of Point of Sales and retailers which are involved in selling these fraudulent SIMs etc.

(vii) ASTR is capable of detecting all SIMs against a suspected face in less than 10 seconds from a database of 1 crore images.

III. LEGAL PROVISIONS

Indian Telegraph Rules 1951 has laid down rules for handling improper or illegal use of telephone. The relevant rules are reproduced below:

S. No.	Rule under Indian Telegraph Rules, 1951	Description
1	Rule 416A - Special Powers of Telegraph Authority	Notwithstanding anything contained in rule 416 where the Telegraph Authority is satisfied that any person is engaged, in any smuggling activity or is acting in violation of any law relating to the conservation of the foreign exchange resources of the country or is acting prejudicially to the public safety and interest or the Defence of India, Civil Defence or Internal Security, the Telegraphy Authority shall- (a) where such person is an applicant, refuses to grant any telephone connection or any similar service or to provide any alteration of any existing service; and (b) where such person is a subscriber, withdraws, either totally or partially, any telephone or similar service provided under these rules
2	Rule 419 - Interception or monitoring of telephone messages	It shall be lawful for the Telegraph Authority to monitor or intercept a message transmitted through telephone, for the purpose of verification of any violation of these rules or for the maintenance of the equipment.
3	Rule 427 - Illegal or improper use of telephone	A subscriber shall be personally responsible for the use of his telephone. No telephone shall be used to disturb or irritate any persons or for the transmission of any message or communication which is of an indecent or absence nature orris calculated to annoy any person or to disrupt the maintenance of public

		order or in any other manner contrary to any provision of law

Relevant Sections in Indian Penal Code, 1860

Impersonation, cheating, creating forged/fake documents is an illegal act under Indian Penal Code, 1860. Section 415 to 420 of Indian Penal Code, 1860 deal withcheating, impersonation and their punishment. Section 463 to 476 Indian Penal Code, 1860deal with creating fake documents, using fake documents as genuine one, false document or electronic record. The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "*forgery for the purpose of cheating*", may also be applicable in a case of identity theft.

The cyber crimes also find mention in Information Technology Act, 2000. The relevant sections for identity theft and impersonation are as follows:

S. No.	Section under Information Technology Act,2000	Description
1	Section 66C - Punishment for identity theft	Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
2	Section 66D - Punishment for cheating by personation by using computer resource	Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

IV. Conclusion and Impact of ASTR project in Mewat, Haryana

(i) Before ASTR project, there were approx 16.69 lakh SIMs in Mewat region, Haryana. The tool has been proven so successful that entire cyber crime syndicates of Mewat have been neutralized, disconnecting 4.96 lakh SIMs across all TSPs, which is approximately 30% of total SIMs.

(ii) The project which was launched in Mewat, Haryana has been expanded in complete Haryana LSA. On monthly basis, the activity of 100% SIM subscriber verification for new SIMs is carried out using ASTR system. The list of suspected mobile numbers is generated by ASTR. Immediate action for re-verification of suspected mobile numbers is taken and the mobile numbers are disconnected if found non-bonafide.

(iii)Also, all the suspected mobile numbers of Haryana which are being reported on National Cyber Crime Reporting Portal are analyzed using ASTR for finding all other SIMs which have been taken using similar faces. The re-verification and disconnection of all non bonafide SIMs involved in the criminal syndicates is carried out.

(iv)ASTR project is directly benefitting 135 crores Indian citizens using mobile devices or telecom services by creating a robust telecommunication ecosystem and keeping the fraudsters away from the telecom network. The project is acting as a catalyst for providing a robust and secure telecommunication ecosystem for achieving the goal of Digital India. The ASTR project is directly instilling confidence among the citizens for using digital services and giving a push to the digital economy.

(v) ASTR Project has directly helped the LEAs, banking/financial institutions by detecting the fake/forged SIMs using pro active analysis. The cyber crime syndicates which were operational in Mewat, Haryana have been completely neutralized. The cyber frauds, crimes and other illegal activities using SIMs, have drastically reduced in Mewat, Haryana.The effectiveness of ASTR system is evident as approx 4.96 lakh potential fraud SIMs have been disconnected.

(vi)ASTR is acting as a tool for e-governance and ease of doing business by ensuring a trusted and verified digital telecommunication ecosystem where every subscriber will be uniquely identifiable and traceable.The ASTR project is directly instilling confidence among the citizens for using digital services and giving a push to the digital economy.

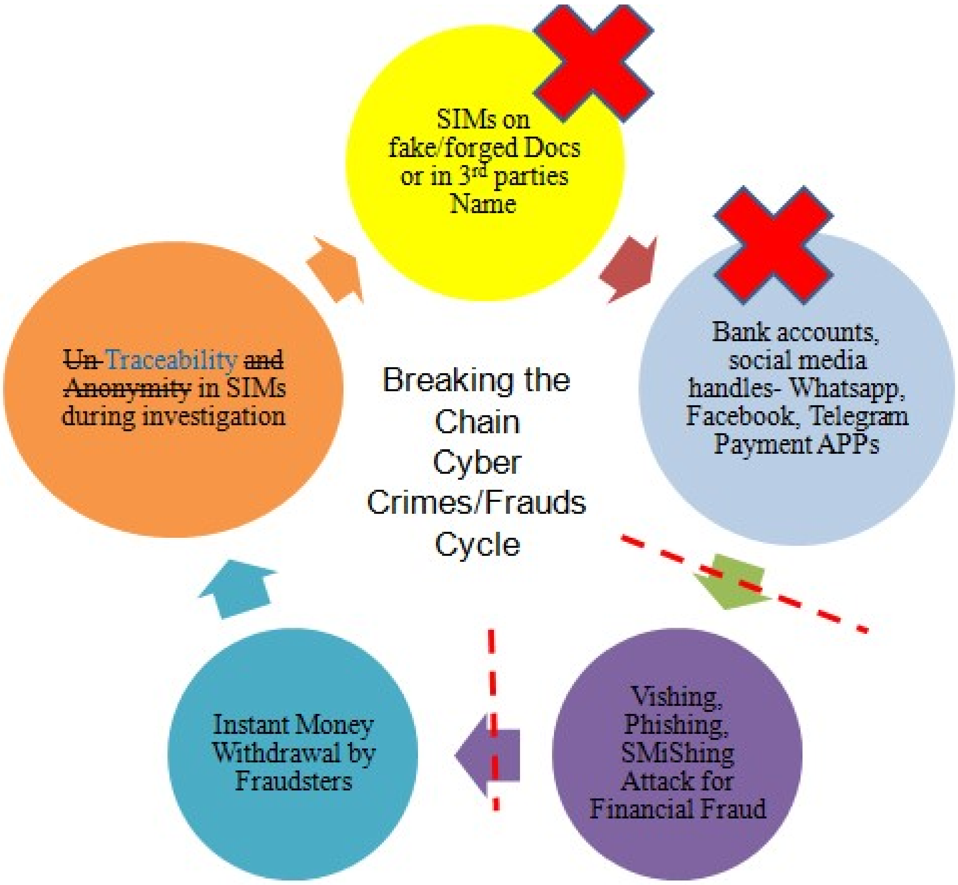

SIMs on fake/forged Docs or in 3rd parties Name
Bank accounts, social media handles- Whatsapp, Facebook, Telegram Payment APPs
Vishing, Phishing, SMiShing Attack for Financial Fraud
Instant Money Withdrawal by Fraudsters
~~Un~~ Traceability ~~and Anonymity~~ in SIMs during investigation
Breaking the Chain Cyber Crimes/Frauds Cycle

Fig.6ASTR – breaking the Chain of Cyber Crimes/Frauds cycle

V. WAY FORWARD FOR CURBING CYBER FRAUDS IN INDIA

DoT Haryana LSA aims to curb the cyber crimes/frauds across India using communication intelligence and pro-active analysis. The feedback and result of ASTR may be integrated in the SIM subscriber on boarding APPs of all the Telecom Service Providers, thereby making the entire telecom ecosystem more robust and secure as envisaged in National Digital Communication Policy 2018[9].

The cyber laws are still in nascent stage in India and stricter regulations are required for dealing financial frauds and cyber frauds.

There is an urgent requirement of finding all hotspots where fake SIMs are being sold and from where these syndicates operate. Utilizing ASTR, targeted operations may be launched in these hotspots for effectively neutralizing the cyber crime syndicates operating anywhere in India.

A Standard Operating Procedure (SoP)may be developed and integrated version of ASTR

[9] National Digital Communication Policy, 2018 *available at* https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf

in coordination with MHA for re-verification of the social media accounts like Facebook, Whatsapp, Telegram etc. and bank accounts & payment APPsof suspected disconnected mobile numbers. Their removal from these suspected entities from the social media platforms and bank, Payment APPs will further cleanse the system and will play a key role in ensuring a secure and robust telecom and digital ecosystem.