



Reconstructing Telecom Fraud Networks: Operational Insights from CID

Sundaram Vishal^{1*}, Vinay K A² ¹Brainware University, Barasat, Kolkata, vishalsundaram2023@gmail.com,

²National Forensic Sciences University Goa Campus, Curti, Ponda, Goa, vinayshetty22122@gmail.com

Abstract- One of the most critical emerging threat to India's digital economy is the Telecom-enabled fraud with estimated losses exceeding ₹50,000 crore over the past six years. The paper provides a functional model of forensic network reconstruction, which is based on field level investigations at Criminal Investigation Department (CID). The paper not only explores the technical anatomy of SMS interception malware, but also investigates the dynamics of fraud in the real world, specifically utilizing the cryptocurrency vectors, and offers a specialized forensic tool, CDRAnalyze, to analyze Call Detail Records (CDRs). These technical findings are contextualized in the research with references to the legal provisions on Section 63 of the Bharatiya Sakshya Adhiniyam (BSA) 2023 [1], which pertains to the admissibility of electronic evidence. The proposed system incorporates malware reverse engineering, network topology analysis, and legal compliance systems to improve investigation systems in fighting high-tech telecom based fraud ecosystems.

Keywords- Telecom-enabled fraud, SMS malware, CDR analysis, Network mapping, BSA 2023, Cryptocurrency fraud.

I. INTRODUCTION

A. Background and Motivation

The telecommunications infrastructure and the digital payment systems that have been developed in India have triggered remarkable economic growth, which has led to the financial inclusion of millions of citizens. Nevertheless, this digital revolution has also provided new attack surfaces to the advanced criminal organizations. Financial frauds that are telecom-facilitated are a form of social engineering, malware deployment and abuse of a telecommunications network to commit massive financial offences. The magnitude of this risk is enormous: during the last six years Indian citizens and organizations have experienced losses amounting to more than 52,000 crores [3] in different kinds of telecom-mediated fraud. These frauds have become a complicated multi-phase affair involving SMS interception malware, SIM swapping schemes, and money laundering with crypto-

currencies to a large extent [15].

B. More recent Interventions by Regulators

The alarming nature of this threat has inspired the Department of Telecommunications (DoT) to implement two high-risk projects in 2025: the Digital Intelligence Platform (DIP) and Financial Fraud Risk Indicator (FRI) [2]. These systems utilise real-time monitoring, machine learning algorithms and inter- agency data sharing to detect and prevent fraudulent transactions. These platforms have prevented losses between May and December 2025 of ₹660 crore [2], demonstrating the effectiveness of active, technology-based measures. Nevertheless, the reactive nature of existing investigation frameworks is a major challenge because forensic analysis is conducted after the fact, when the financial damage is already done and, in most cases, after a lot of money has been lost.

C. Legal Framework Evolution

In July 2024, India's legal framework governing digital evidence changed fundamentally when the Bharatiya Sakshya Adhiniyam (BSA) was enacted [1] to replace the Indian Evidence Act of 1872. The admissibility of electronic records has now been regulated under Section 63 of the BSA, replacing the procedural requirements laid down in Section 65B of the Indian Evidence Act [1]. The forensic practitioners have been greatly affected by this change of legislation, and there is a need to revise the protocols of collecting and documenting evidence, as well as giving testimony in court by experts to ensure that the evidence is admissible in the legal court.

D. Research Objectives and Scope

The paper fills the gap that is present in the field of telecom- enabled fraud forensics, primarily through regard to the lack of scholarly research that can be used to compare qualified operational investigative practice with academic research. Based on field level research studies carried out at the Criminal Investigation Department (CID), Ranchi, Jharkhand, this study will attempt to achieve the following aims:

- i. Technical Analysis: Break or dissect the architecture and mechanics of the SMS interception malware you come across in the real world and locate certain vulnerabilities used and the evasion techniques used.
- ii. Operational Framework: Capture investigative processes, obstacles and best practices of successful fraud cases in action, to the law enforcement agencies.
- iii. Tool Development: Current tool 'CDRAnalyze' , a forensic application specific to Call Detail Record analysis which uses graph-theoretic algorithms to rebuild criminal networks and extract actors of interest.
- iv. Legal Compliance: Have evidence handling and documentation protocols to meet the requirements of BSA 2023 Section 63 which ensure that the output of the investigation of the case is admissible in the court of law.
- v. Strategic Roadmap: Suggest an extensive research and policy agenda to improve the capability of India to prevent, detect and prosecute telecom enabled financial frauds.

II. LITERATURE REVIEW

A. History of Telecom-Based Fraud

Fraud using telecom has developed in different stages, with each stage being more sophisticated and technologically complicated. Initial forms were basic voice phishing (vishing) and SMS phishing (smishing) attacks, which were mostly based on social

engineering. It has been recorded that the movement of these primitive methods has progressed to sophisticated continuous threats that use malware [16], compromise of network infrastructure, and multi-jurisdictions money laundering. Research has highlighted the fact that telecommunications fraud is ceasing to be the province of the lone perilous individuals and instead it has become an organized criminal business with advanced technical skills and operational security measures.

B. SMS Interception and OTP Bypass Methods

It is recorded in the literature that there are several vectors of attack on SMS interception such as exploitation of SS7 protocols, SIM swap fraud, malware-based interception and social engineering of telecommunication staff. Another type of particular insidiousness is malware-based SMS interception that runs silently on infected computers transmitting incoming SMS messages to attacks servers without the user noticing. Studies have single out typical malware families that attack Android-based devices [16] by taking advantage of Android vulnerabilities including Janus signature bypass (CVE-2017- 13156) [5] and cleartext traffic transfer.

C. Fraud Vector: Cryptocurrency

The introduction of cryptocurrency into the fraud plots has completely changed the world of money laundering. Banking systems as they are traditionally implemented have audit trails and regulatory controls that are hard to compromise, which are useful in forensic investigation. Some of the fraud ecosystems have been using blockchain platforms like TRON because of the low cost of transactions and the short duration of transactions confirmation [6]. Cryptocurrencies (especially those that focus on privacy and low transaction fees) provide criminals with a tool to send money quickly across borders in pseudonymous mode [17], [18].

D. Network Forensics Analysis and Call Detail Records

Call Detail Records (CDRs) form an important source of data that is used to recreate criminal networks and determine patterns of communication between co-conspirators. Graph-theoretic methods of CDR analysis have been widely studied in the academic literature, and the telecommunications networks are viewed as mathematical graphs [7] in which nodes are people (phone numbers) and edges are communication events (calls, SMS). CDR temporal analysis can be effectively used to identify changes in criminal networks, recruitment trends, and future crime [14]. Degree, betweenness, and eigenvector centrality have been commonly used as centrality measures to analyze criminal networks [10], [11], community detection algorithms include Louvain and modularity optimization have been used to enhance structural identification [8], [9], [12], [13].

E. Jurisdiction of Digital Evidence

Section 65B of the Indian Evidence Act has regulated the admissibility of digital

evidence in the Indian courts by providing procedures such as the computer system being certified by an individual who holds lawful possession of the computer system. The switching to the Bharatiya Sakshya Adhiniyam 2023 is an evolution of the evidentiary standards, where Section 63 offers new regulations about electronic records. The wider cyber governance system of India is also enforced with the help of the National Cyber Security Policy 2023 [4].

F. Gaps in Existing Research

Although the literature on telecom fraud is increasing, the gaps are still quite large. To begin with, conducting research to close the gap existing between operational investigative practices and academic frameworks has not been extensively researched thus creating a gap between the theoretical model and the realities on the field. Second, the majority of available tools to analyse CDR are commercial and costly and do not fit the particular requirements of law enforcement organisations. Third, the BSA 2023 has not been explored in relation to its legal implications on the digital forensic practices. The paper fills such gaps by incorporating field-level knowledge and suggests an open-source forensic tool.

III. FRAUD MALWARE ENABLED BY TELECOM

A. Architecture and Functionality of Malware

The SMS interception malware that was under scrutiny in CID Ranchi investigations has a complex multi-layered code structure with the aim of ensuring that it is not caught without leaving a lasting access to the victim devices. The malware runs on a variety of different modules, which perform individual malicious functions: Defects affecting the integrity of the system and its state, including the presence of viral code in a file, data, or binary code.

B. Infection Vector and First Compromise: Considering the integrity of the system and its condition, such as the presence of viral code in a file, data or binary code. The malware usually gets first entry into the system via social engineering campaigns, usually in the form of a legitimate application which could be banking apps, government service portals, or the use of common utility software. Distribution channels encompass malicious links via SMS or WhatsApp, maliciously compromised third-party applications stores, drive-by downloads on maliciously compromised websites. The first dropper will typically have little to no malicious code, a dropper application that is configured to circumnavigate the simplest security scanners and create a presence on the computer.

C. SMS Interception Module: The malware is built around the main functionality of the malware as the SMS interception module, which is the registration of broadcast receivers to SMS messages sent to it. On Android phones, SMS messages cause system-wide broadcasts which may be intercepted by applications given the permission to read

SMS messages, using the READ_SMS permission. The malware uses this to intercept any incoming messages and fully obtains them prior to being shown to the user with the capability to selectively hide or delete messages so that the victim knows nothing. Intruded SMS messages, especially those with OTPs sent by banking and financial institutions, are sent instantaneously to Command and Control (C2)-controlled by the attackers. The malware makes use of a variety of exfiltration mechanisms, including HTTP/ HTTPS POSTs, SMS forwarding to premium-rate numbers under attacker control and encrypted messaging protocols to avoid network-level detection.

D. Other Evil Capabilities: In addition to SMS interception, the malware under analysis has a number of other features that make it more useful in committing financial fraud, namely, contact list harvesting, call logs monitoring, keylogging, screen recording, remote control execution etc.

E. Android Vulnerabilities Exploitation.

The malware exploits various classes of Android vulnerabilities in order to realize its goals:

1. Janus Vulnerability (CVE-2017-13156): Janus vulnerability takes advantage of difference in Android checking signature of APK. Android APK files may be viewed as ZIP archives as well as DEX executables. Attackers can put up a malicious DEX code that will be executed by crafting a file that is valid in both formats: having a valid signature by a genuine application in the ZIP part of the file. This enables the malware to bypass signature checks and look like a genuine application.
2. Transmission of Cleartext traffic: TLS/SSL has become common in setting up secure communications, Android applications, of which the ones that are popular enough to attract older API levels continue to transmit sensitive data over plaintext HTTP traffic. The malware will also be able to carry out man-in-the-middle attacks on the traffic over the local network, stealing credentials and session tokens. Such weaknesses are quite often applied in man in the middle interception techniques [15].
3. Exploitation by permission model: This is a vulnerability that can be exploited by attackers without modification. Users often give broad permissions without knowing what they entail especially when there is some form of urgency or a misleading message. The malware takes advantage of this by soliciting hazardous permissions in the guise of service and these hazardous permissions are often presented as essential to some acceptable functionality.

IV. CID RANCHI OPERATIONAL INSIGHTS.

A. Case Study Situation and Design

The working experiences in this section are based on working research undertaken in the Criminal Investigation Department (CID), Ranchi, Jharkhand. Such inquiries comprised various instances of telecom-based financial fraud, and the amount of money stolen by

individuals was between ₹50,000 and ₹35 lakhs. Similarities could be found in the cases in terms of modus operandi, technical infrastructure, and structure of criminal enterprises. This was in line with the state-level crime trends that are reported by Jharkhand CID [19].

B.General Fraud Patterns and Modus Operandi.

1) Impersonation Tactics: Most of them concerned fraudsters who posed as bank officials, law enforcement agents or government officials. Common scenarios included:

- Bank security alert scam: The victim is contacted in this issue with details that the suspect is attempting to steal their account, and the scammers will offer to keep the account secure by installing security software (the virus).
- Twitter Scam: This type of scam is committed by fraudsters who tell a victim that the existing KYC (Know Your Customer) is expired and that he/she must fill in the information presently or lose the account.
- Digital Arrest Scam: The scammers inform the victims that they have participated in a criminal act (money laundering, drug trafficking) and require their cooperation with a digital investigation so they can be arrested, and pushed into downloading malware and provide their banking details.
- Refund/Reward Scam: In the case with refund/reward scam, the victim is to get the refund on a wrongly charged item or even reward on a loyalty program but you have to install a program to get this done.

i. **Multi-Stage Social Engineering:** Advanced social engineering frauds have a multi-stage process, and there are actors that can be assigned various roles:

Initial Contact: This is the initial approach, at a low level, whereby a pretext is established and vulnerability in the victim is checked.

Authority Figure: In case the victim is interested, the call is passed onto a more senior operative who poses as a bank manager, police officer or government official which adds credibility to the hoax.

Technical Support: A technical support threat actor takes the victim through the process of malware downloading, which is usually conducted using screen-sharing software to gain access to the victim device and control it remotely.

Closer: Once malware has been installed with the credentials, a rogue agent runs the fraudulent transactions that ensures that the victim is kept on the phone.

i. Temporal Patterns: Case time analysis showed that there were certain trends of time:

Peak Activity Hours: Fraudulent calls are mostly made during working days i.e 10 AM -5 PM when the victims are at risk of thinking that they are receiving valid business contacts.

Weekend Targeting: Large percentage of attempts of the fraud is done on weekends, when banks are closed and it is hard to check their claims, calling directly to the bank.

Quick Process: Fraudulent transactions can be carried out within a few minutes after malware is installed and credentials have been obtained and this ensures that there is limited time within which the victim can intercept the transaction.

b. Technical infrastructure and structure of the organization

The telecommunications infrastructure is referred to as the first category. It was found out that scammers use advanced telecommunication networks to conceal their identities and locations:

VoIP Services: VoIP services are the cause of many fraudulent calls, which are usually those of international providers that have loose identity checks or those that have no identity checks.

SIM Farms: SIM farms are large scale operations; arrays of mobile devices with multiple SIM cards which allocate calls to many phone numbers making it difficult to trace and block calls.

Caller Id Spoofing: Caller id spoofing is a technique of fraudsters to display phone numbers that seem legitimate like official helpline numbers of banks and government numbers of agencies so that the impersonation makes more sense.

Organizational Hierarchy: The assessment of records of the arrested suspects and the interrogation proved the hierarchical structure of the organization:

Masterminds/Financiers: High-level people that provide funds, infrastructure and strategy. Such individuals do not turn into real offenders too frequently and keep the safety of their activities secreted with the help of compartmentalization.

Technical Specialists: These are individuals which deal with malware development, server infrastructure control, and cryptocurrencies. These professionals are remote and could be located in different jurisdictions.

Call Center Operators: Mid-level operators, calling on the actual fraud, typically work out of rented office space or residential premises which have VoIP systems and scripts. On the one hand, money mules are low-tier persons that offer bank accounts or crypto wallets to accept and send stolen money.

Money mules themselves are usually hired based on advertisements in which they are promised easy money to work at the job involving financial processing.

- iii. **Geographic Distribution:** Although the victims were concentrated around the state of Jharkhand and other neighbouring states, the criminal infrastructure was geographically spread:

Call Centers: Found in various states such as Rajasthan, Gujarat, Maharashtra and West Bengal and most frequently in the tier-2 and tier-3 cities with less law enforcement.

Technical Infrastructure: The servers used to store malware and C2 infrastructure tended to be based in other countries, especially ones with lax cybercrime legislation and with less co-operation with Indian counterparts.

Money Laundering Networks: Money exchanges and money mules were spread all over India and abroad, and the funds were commonly transferred to the Southeast Asian countries, where the money would be cashed out.

c. Investigative Problems and Restrictions

Jurisdictional Complexity: Telecom fraud operations have a high level of jurisdictional problems due to their distributed nature. The victims, offenders, technical infrastructure, and financial intermediaries are frequently in dissimilar states or countries and this demands a lot of inter-agency coordination. Lagging in getting the cooperation of other jurisdictions tend to enable criminals to destroy evidence or move business.

Technical Expertise Gaps: Not all law enforcement agencies have employees who have specialized training on digital forensics, malware scanning, and cryptocurrency tracking. This is due to the lack of expertise which hampers with investigations especially during the volatile initial stages of investigations where quick technical identification can help determine the suspect and stop further victimization.

Resource Constraints: Forensic tools and infrastructure are not inexpensive and need constant maintenance and changes. Most of the agencies are low-budget and use manual analysis that are inefficient compared to automated solutions, which have time-consuming approaches to analysis.

Cooperation and Awareness of the Victims: Most of the victims do not report fraud because they are embarrassed, fear legal hassles or are under the opinion that it is

impossible to recover. This underreporting interferes with the attempts to identify the patterns, monitor criminal networks, and efficiently distribute resources. Also, due to the lack of digital literacy in some demographic categories, they are especially vulnerable to social engineering attacks.

Problems of cryptocurrency tracing: Although blockchain transactions should be transparent in theory, their practical tracing is complicated by a variety of factors:

Mixing Services: Criminals would utilize cryptocurrency mixing services (tumblers) which combine money sent by various sources and send it back breaking the trail of transactions.

Privacy Coins: There are crypto-operations involving privacy-oriented cryptocurrencies (Monero, Zcash) that are based on cryptographic methods to keep the contents of transaction hidden.

Exchange Cooperation: A significant portion of cryptocurrency exchanges, especially ones located in a jurisdiction with lax regulations, will not cooperate to provide the law enforcer with user data.

Setting: Advanced attackers make use of address poisoning techniques, which consist of generating wallet addresses that have a cosmetic appearance of valid addresses to swindle victims and make it difficult to conduct forensic analysis.

d. Favourable Investigative Strategies

Nevertheless, several investigative techniques have been found to work:

- i. Rapid Response and Seizure of Devices: The police have gained significant capacity to swiftly respond to and confiscate devices in an emergency. The police have been able to develop considerable capacity to respond and seize devices swiftly during an emergency. Real-time seizure of the victim devices immediately a complaint is filed means that the malware can be forensically analyzed and removed before being remotely uninstalled or evidence erased.
- ii. Proactive CDR Analysis: Instead of monitoring the complaints to get to accumulated numbers, active analysis of the CDRs related to familiar numbers of frauds will enable investigators to establish co-conspirators, organizational structures and anticipate prospective victims.
- iii. Co-working with Telecommunications Providers: The formation of direct communication with telecommunications service providers will allow blocking fraud numbers quickly, identifying the information of SIM cards registration, and tracking suspicious conversations in real-time.
- iv. Financial Institutions Co-ordination: The cooperation with banks and payment processors makes it possible to freeze the account that received a fraudulent transfer quickly, which increases the chances of retrieving the funds and disrupting the operations of money laundering.

v. Public Awareness Campaigns: The proactive public awareness campaigns that are carried out on social media, local media, and community-based outreach have been successful in lowering the rates of victimization by educating citizens on the prevalent methods of fraud and warning signs.

j. CDRAnalyze: A FORENSIC SOLUTION

a. Philosophy of Motivation and Design

It was the unique requirements and limitations of the Indian law enforcement agencies in the investigation of telecom fraud that led to the development of CDRAnalyze. The available commercial products to aid the CDR analysis are usually cost-prohibitive, need more than sufficient training, and do not have the option of the features that address the peculiarities of the telecommunications networks and fraud patterns in India.

b. System Architecture and Components

The architecture adopted by CDRAnalyze is a modular architecture comprising of few integrated components:

Data Ingestion Module: The data ingestion module covers the importation of CDR data of a number of different telecommunications service providers, each of which might utilise a different format and schema. The module includes:

Format Parsers: Parsing of popular CDR formats such as CSV, Excel, XML of big Indian telecom providers.

- **Data Validation:** Automatic validation is done to identify incomplete records, formatting errors and inconsistencies if any.
- **Normalization:** Transform all data imported into a common internal schema that will help to perform analysis across various data sources.
- **Metadata Extraction:** Automated extraction of metadata when it comes to date ranges, records count, unique phone numbers, and type of call.

i. Data Processing and Analysis Engine

The core analysis engine applies several methods of analysis:

- **Temporal Analysis:** The recognition of communication patterns across time like the most active points, time clustering, and anomalies.
- **Frequency Analysis:** Metric calculations of frequency of calls and SMSs between sets of numbers, discovery of high frequency communicators.
- **Geographic Analysis:** Map based analysis of cell towers locations to represent geographic distribution of criminal networks and determine operational bases.

ii. Visualization Module

Investigative analysis and presentation in the courtroom are impossible without good visualization:

- **Timeline Visualizations:** Temporal charts using the patterns of communication, sequence of events and operational periods.
- **Geographic Maps:** Reintegration with mapping services to be able to visualize the locations of cell towers, locations of suspects, and geographic patterns of the occurrence of criminal activities.
- **Statistical Dashboards:** Summary statistics, charts, and graphs giving analysis of the network characteristics and the findings.

iii. Report and Evidence Documentation Module.

CDRAnalyze has extensive evidence documentation capabilities in order to be legally admissible:

- Automated Report Generation: Generation of organized reports of investigations such as method, findings, visualization and conclusions in formats acceptable in court.Chain of Custody Tracking: Chain of custody logs of every import or export of data, and analytical operation performed on data with timestamps, user identities, and hashes. However, the next thing is evidence packaging, the export of results of the analysis, source information, and documentation in tamper- evident formats (with digital signatures).

c. Technical Implementation

The technology stack which is used to implement CDRAnalyze is as follows:

- Programming Language: Python 3.x to core analyse the engine, with its comprehensive data science and network analysis Library.
- Processings: Pandas to work with data, NumPy to compute numbers.
- Visualisation: Matplotlib, statistical visualisations, Plotly, Statistical visualisations, Gephi, Advanced network visualisations.
- Database: SQLite is used as the local storage of data, which can be supported by PostgreSQL in a big-scale implementation.
- User Interface: Web-based interface Web-based using Flask, or can be accessed by any standard web browser without special software.
- Security: Data stored is encrypted, controlled (role-based access control), and log is audited.

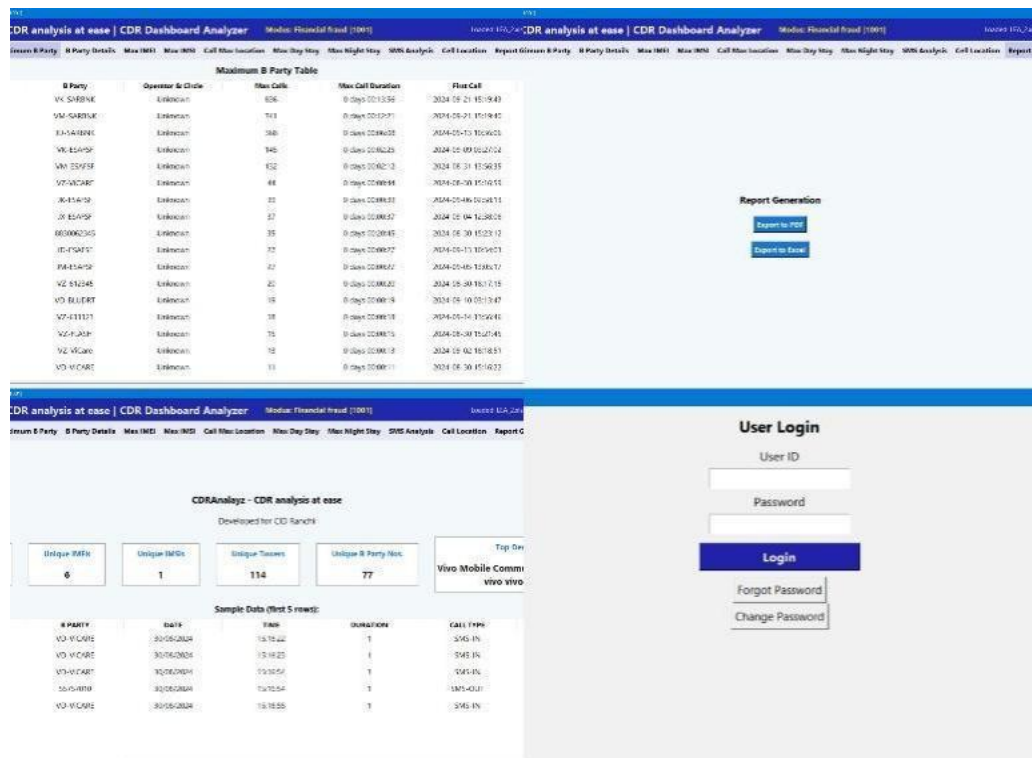


Fig. 1. Integrated interface of CDRAnalyze illustrating key functionalities: Maximum B-Party, automated court-ready report export (PDF/Excel), dashboard-level summaries and role- based secure login system.

d. Future Development Roadmap

CDRAnalyze is planned to undergo some development, which will be:

- **Machine Learning Integration:** Supervised learning models learn automated techniques to detect any fraud pattern based on past cases of fraud.
- **Real-Time Analysis:** Real-time monitoring of suspect communication with the capability to stream.
- **Multi-Modal Data Integration:** CDR data integrated with other types of data, such as financial transactions data, social media data, and cryptocurrency blockchain data.
- **Collaborative Features:** Multi-user support and role-based access control, which allows collaborative work of many agencies in investigations.
- **Mobile Application:** A mobile interface where field investigators can get information about analysis results and receive real-time updates through a mobile interface.

V. CONCLUSION

The telecom-enabled financial fraud is among the critical and changing dangers to the Indian digital economy and financial stability of the population upheld by the operational framework of the present paper, which is built on field-level investigations in CID Ranchi. The creation of CDRAnalyze indicates that specialized and accessible forensic tools can be used to improve the investigation processes, and the strategic research roadmap will be the detailed agenda to enhance the ability of India to prevent, detect and prosecute telecom-based fraud.

Technical Characterization, SMS interception malware architecture, techniques of exploiting, and evasion mechanisms are technically characterized in a detailed manner, and offer useful information to both defensive and forensic study.

Operational Insights, Reporting actual fraud trends, criminological organization, and investigative issues, the gap between academia and practice at the field level.

Analytical Approach, CDR analysis used to reconstruct the network, which shows the effectiveness of degree, betweenness, and network flow centrality measures on network of actors and organizational structure identification [10], [11], [13] and community detection algorithms.

Tool Development, Groundbreaking releases of CDRAnalyze, a customized forensic tool based on the requirements of the Indian law enforcement agencies and with the facility of automated analysis, visualization, and evidence recording that complies with the BSA.

Strategic Vision, Suggestion of a research roadmap going over the technical dimension, operational dimension, institutional dimension, policy dimension and public awareness dimension of the telecom fraud problem.

The issue of telecom-enable fraud is not only a problem of the law enforcement but also a problem of society that impacts economic growth, confidence of people in the digital machinery, and financial stability of millions of individuals. In finding a solution to this challenge, it will be necessary not just to be able to demonstrate technical and operational prowess, but also to demonstrate a commitment to safeguard civil liberties, provide due process, and create a digital ecosystem that is innovative and secure. The field-level knowledge and analytical models discussed in this paper constitute one of the steps towards a more well-rounded evidence-based response to telecom-enabling fraud.

This forces our criminal defensive and investigative abilities to keep up with the changing tactics of the criminal enterprises. With continued investigation, concerted effort, and dedication, India will be able to establish a strong framework of defense against this ubiquitous menace to its people and its digital economy.

RESEARCH GAPS

Notwithstanding all the recent development, there are still crucial loopholes in the ability of India to fight fraud over telecoms:

- **Technical Skills:** Digital forensics, malware analysis, and tracking of cryptocurrency require a highly skilled employee, which not all law enforcement agencies have at their disposal.
- **Tool Availability:** Commercial forensic tools are usually prohibitively costly and the open-source versions do not offer functions that would suit Indian contexts.
- **Inter-Agency Coordination:** Jurisdiction Inter- Agency Dividing investigations between states or nations are impeded by fractured jurisdiction.
- **Implementation of the Legal Frameworks:** Although the BSA 2023 offers a contemporary legal landscape, the practice faces a number of problems, such as judicial familiarity with digital evidence and their inconsistent application of the standards of evidence.
- **Public Awareness:** Low digital literacy and little awareness on fraud techniques have led to the high rates of victimization.

REFERENCES

- [1] Government of India, Ministry of Home Affairs, "The Bharatiya Sakshya Adhiniyam, 2023," Act No. 47 of 2023, enacted July 2024.
- [2] Department of Telecommunications, Government of India, "Digital Intelligence Platform (DIP) and Financial Fraud Risk Indicator (FRI): Implementation and Impact Report," December 2025.
- [3] Reserve Bank of India, "Report on Trend and Progress of Banking in India 2024-25," Annual Report, 2025.
- [4] Ministry of Electronics and Information Technology, Government of India, "National Cyber Security Policy 2023," Policy Document, 2023.
- [5] Android Open Source Project, "Android Security Bulletin—CVE- 2017-13156 (Janus Vulnerability)," December 2017. Available: <https://source.android.com/security/bulletin>
- [6] TRON Foundation, "TRON Protocol Documentation," Technical Documentation, 2025. Available: <https://developers.tron.network>
- [7] M. E. J. Newman, "Networks: An Introduction," Oxford University Press, 2010.
- [8] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2008, no. 10, p. P10008, 2008.
- [9] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proceedings of the National Academy of Sciences*, vol. 99, no. 12, pp. 7821-7826, 2002.
- [10] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, no. 3, pp. 215-239, 1978-1979.

- [11] S. P. Borgatti, "Centrality and network flow," *Social Networks*, vol. 27, no. 1, pp. 55-71, 2005.
- [12] A. Clauset, M. E. J. Newman, and C. Moore, "Finding community structure in very large networks," *Physical Review E*, vol. 70, no. 6, p. 066111, 2004.
- [13] U. Brandes, "A faster algorithm for betweenness centrality," *Journal of Mathematical Sociology*, vol. 25, no. 2, pp. 163-177, 2001.
- [14] P. Holme and J. Saramäki, "Temporal networks," *Physics Reports*, vol. 519, no. 3, pp. 97-125, 2012.
- [15] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027-2051, 2016.
- [16] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, 2012, pp. 95-109.
- [17] M. Moser, R. Bohme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in *Proceedings of the 2013 APWG eCrime Researchers Summit*, 2013, pp. 1-14.
- [18] S. Meiklejohn et al., "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 Internet Measurement Conference*, 2013, pp. 127-140.
- [19] Criminal Investigation Department, Jharkhand Police, "Annual Crime Statistics Report 2024-25," Internal Report, 2025.