International Journal of Engineering Research and Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 22, Issue 4 (April 2026), PP 344-349

SIM Swap Fraud in India: A Digital Forensic Perspective

Bhushan Acharekar, Aditya Chaudhari, Aman Chamola,
Yash Bhat, Deepkumar Pandey
Department of Information Technology (I.T.), TE,
KC College of Engineering and Management Studies & Research, Thane, Maharashtra, India

Abstract
SIM swap fraud – where attackers hijack a victim's phone number to intercept OTPs – has surged in India with the rise of mobile banking. This paper analyzes SIM swap methodology and impacts, focusing on India's digital payments ecosystem. We present a detailed forensic case study: a fraud where adversaries tricked a telecom into issuing a duplicate SIM and used it to authorize ₹1.19 crore in unauthorized transfers. Forensic investigation involved mobile device imaging (Cellebrite UFED), disk forensics (FTK/Autopsy), and analysis of telecom and banking logs to reconstruct the attack timeline. We tabulate relevant studies (Table 1) and outline a structured methodology (Table 2) for evidence collection, preservation, and analysis. A timeline diagram illustrates key events. We also examine emerging AI techniques – ML-based anomaly detection in logs and NLP-based scam detection – discussing benefits and ethical constraints. The findings underscore that OTP-only systems are vulnerable and that forensic log correlation can reveal the fraud sequence. We highlight investigative challenges in India (KYC loopholes, telecom verification gaps, slow inter-agency response) and recommend concrete measures: stricter SIM KYC, mandatory two-factor authentication, instant fraud alerts, and better cooperation between banks and telcos. This work contributes a comprehensive forensic framework to investigate and prevent SIM swap fraud.
Keywords: *SIM Swap Fraud; Digital Forensics; Cybercrime; OTP Authentication; Telecom Security; Financial Fraud; Machine Learning.*

Date of Submission: 14-04-2026 Date of acceptance: 25-04-2026

I. Introduction

The rapid digital transformation of India's financial ecosystem – exemplified by UPI and mobile banking – has brought unprecedented convenience and scale. In FY2024–25 India recorded over **18,000 crore UPI transactions**, roughly half of the world's real-time payments【2】. However, this growth has also enabled new frauds. Notably, SIM swap (or SIM hijacking) fraud has emerged as a critical threat. In a recent adjudication, an Ahmedabad tribunal found both a bank and a telecom provider negligent in a SIM-swap case that drained over ₹1.05 crore from a corporate account【1】. SIM swap occurs when attackers fraudulently get the victim's phone number ported to a new SIM under the attacker's control【3】. Once the number is hijacked, the scammer can intercept SMS-based One-Time Passwords (OTPs) and call-based 2FA codes, effectively bypassing mobile banking security【3】【5】.

India has seen a surge in financial cyberfraud: reported cases jumped from ~1.03 million in 2022 to over 2.26 million in 2024, with losses exceeding ₹22,845 crore【4】. Alarmed by this, the Reserve Bank of India now mandates two-factor authentication (2FA) for all digital transactions, warning that "OTP only" is vulnerable to SIM attacks【5】. Yet even with new policies, SIM swap exploits remain a weak point. Unlike a technical hack, SIM swaps rely on **social engineering** and procedural lapses. Fraudsters often obtain personal data on victims and convincingly impersonate them to convince telecom operators to transfer service to a new SIM【3】【5】. For example, attackers may submit forged documents or bribe front-line staff. Once successful, they receive all calls and SMS (including OTPs) meant for the victim's number.

Digital forensics plays a pivotal role in investigating such incidents. By systematically collecting and analyzing data from devices, telecom networks, and financial systems, forensic teams can piece together the attack sequence. For instance, telco provisioning logs can reveal *when* and *how* a SIM swap request was processed, while banking records show the timing of suspicious transactions. In the case study below, correlating these logs allowed investigators to link a fraudulent SIM activation at 16:30 on March 11, 2023, with a series of unauthorized transfers on March 12, 2023【1】. This paper provides a comprehensive forensic framework for SIM swap investigations in India, surveys related literature (Section 2), details our methodology (Section 3) including forensic tools (Table 2), and presents a detailed India-centric case study (Section 4) with a reconstructed timeline.

We then discuss results (Section 5), emerging AI enhancements and challenges (Section 6), and conclude with recommendations (Section 7–8) to prevent this evolving threat.

II. Literature Review

Several works have examined aspects of mobile financial fraud and forensic analysis. **Mobile/SIM forensics** research highlights that SIM cards store critical evidence: subscriber identity, SMS messages, contacts, and network data【10】. Jansen and Delaitre (NIST) note that a SIM contains personal information (phonebook, SMS) and network identifiers, making it a rich source of digital evidence【10】. This underlines the forensic value of acquiring SIM images using tools like Cellebrite or specialized SIM readers.

Security analyses have repeatedly shown that telecom authentication procedures are weak. Lee *et al.* performed an empirical test on five US carriers and found that all used insecure SIM-swap authentication, often letting attackers bypass questions easily【5】. They further showed that many online services could be compromised with a single SIM swap alone【5】. This underscores that even moderate procedural flaws lead directly to account takeovers.

Several studies focus on financial fraud in India's fintech era. Sharma (2025) analyzes phishing in India, noting that "authorised but fraudulent" transfers due to social-engineering (like SIM swap) blur legal categories【2】. She highlights gaps in laws and enforcement for digital transactions. Praveen and Vaishali (2025) survey credit/debit card scams in India, noting that SIM swap is now among common fraud tactics leveraging SMS OTPs【2】. These works emphasize legal/regulatory shortfalls: existing IT Act provisions (e.g. identity theft under §66C) and RBI guidelines struggle to keep pace with sophisticated schemes.

On the detection front, recent research proposes **AI-enhanced methods**. Ibanibo *et al.* (2025) present an ML-based anomaly detection for SIM swap fraud. By training classifiers on telecom transaction data, they demonstrate that coupling ML detection with multi-factor authentication (MFA) can reduce SIM-swap success by ~80%【9】. They note that deep learning models can process large volumes of telecom and banking logs to flag unusual patterns. Other sources point out that **Natural Language Processing (NLP)** techniques could be used to analyze text logs or call transcripts for fraud signals【9】. However, these studies also warn of limitations: ML models need labeled data and may produce false positives, and NLP analysis of personal communication raises privacy/ethical issues【9】.

Gap in Forensic Focus: While general cyber-fraud literature is rich, few sources detail the forensic investigation of SIM swap in India specifically. Most research addresses attack mechanisms or prevention. To our knowledge, no prior paper combines an Indian case study with forensic timeline reconstruction and discusses investigative tools/procedures in depth. Table 1 below compares key related studies, highlighting their methods and limitations.

Ref.	Year	Region	Methods	Findings	Limitations
Lee *et al.*【5】	2020	USA	Experimental audit of prepaid carriers and OTP sites	All tested carriers used weak SIM-swap auth; 17 websites fully compromiseable via SIM swap alone.	Limited to US carriers and specific websites; did not analyze forensic techniques.
Jansen & Delaitre【10】	2007	USA (NIST)	Forensic tool evaluation for SIM cards	SIMs store user data (contacts, SMS, etc.); forensic tools may miss or misreport data, underscoring need for validation.	Focused on tool validation, not on SIM-swap scenario.
Sharma【2】	2025	India	Legal/regulatory analysis of fintech phishing fraud	Identifies "authorized but fraudulent" transfers via phishing/SIM swap; calls for stronger authentication standards.	Broad focus on phishing; SIM swap as part of larger threat; not empirical.
Ibanibo *et al.*【9】	2025	Nigeria/Global	Simulation of ML detection for telecom fraud	ML anomaly detection with MFA can cut SIM-swap attempts by ~80%; highlights telecom fraud losses (~$28B globally).	Simulation-based; specific to dataset; deployment challenges in real networks.
Praveen & Vaishali【2】	2025	India	Literature review of payment card fraud techniques	Surveys skimming, phishing, SIM-swaps as major card frauds; notes legal/regulatory gaps.	Descriptive; no new empirical data on SIM-swap investigations.

Table 1. Comparison of related studies on SIM/cyber fraud (year, region, methods, key findings, limitations).

III. Methodology

Our forensic approach combines mobile device extraction, telecom data analysis, and banking audit to reconstruct SIM swap attacks. The high-level procedure is:

- **Evidence Collection:** Seize the victim's mobile device and SIM (if available). Use Cellebrite UFED (or similar) to image the phone's flash memory and SIM card, extracting SMS history, call logs, and app

data. Image any other relevant devices (PCs, backup storage) using tools like FTK Imager or Autopsy【10】.

- **Telecom Log Acquisition:** Secure logs from the mobile operator. This includes SIM provisioning records, call detail records (CDRs), and SMS gateway logs showing when SIM swap requests and activations occurred. Legal authorization (police/FIR request to telecom) is required to obtain these records.
- **Financial Log Retrieval:** Obtain bank transaction logs for the victim account. Request detailed records (online banking logs, OTP issuance timestamps, wire transfer confirmations) from the bank under legal mandate. These show when and to whom funds were moved.
- **Evidence Preservation:** Throughout, maintain strict chain-of-custody. Use hash verification for all images. Ensure each step complies with Section 69 of the IT Act and RBI IT-security guidelines for evidence handling【6】.
- **Analysis:** Examine extracted SMS/call logs for OTPs or alerts. Correlate telecom logs (SIM swap timestamps) with bank logs (transaction times, OTP dispatches). Autopsy can be used to carve any hidden logs or data from devices. Specialized telecom-log parsing tools or scripts may help analyze large CDRs.
- **Timeline Reconstruction:** Align events chronologically. For example, link "new SIM activated" event in telecom logs with an OTP SMS log and a debit transaction in the bank log. We may use a timeline tool (or manual Gantt/sequence charts) to visualize the attack sequence.

Table 2 below summarizes key tools, data sources, and legal/ethical considerations for each stage.

Tool/Stage	Data Source	Purpose	Legal/Ethical Considerations
Mobile Forensics (Cellebrite UFED)	Victim's smartphone (internal memory, SIM)	Extract SMS, call logs, app data, authentication caches	Requires search warrant/owner consent; maintain chain-of-custody; write-block during imaging.
Disk Imaging (FTK Imager, Autopsy)	Computers, storage media	Acquire full forensic images; analyze file systems	Use forensic imaging (read-only); calculate hashes; protect integrity of evidence.
Telecom Log Analysis	Operator's SIM issuance logs, CDRs, SMS gateway	Identify SIM swap request and activation times, call/SMS patterns	Data privacy laws; logs only via legal request; ensure authorized use by investigating agency.
Banking Log Analysis	Bank transaction records, OTP dispatch logs	Trace unauthorized transfers and OTP send/receive events	Obtain with proper bank authorization (court order or regulator mandate); protect customer privacy.
Timeline Correlation	Timestamps from all sources	Reconstruct event sequence of SIM swap and transactions	Analyst expertise needed; ensure synchronization of clocks; avoid interpretation bias.

Table 2. Methodology and forensic tools/procedures for investigating SIM swap fraud.

Investigation Workflow: The steps above translate into the flowchart in Figure 1. Starting from fraud detection, the process moves to evidence collection (device imaging, log collection), then data analysis and timeline reconstruction, leading to identification of suspects and legal action.

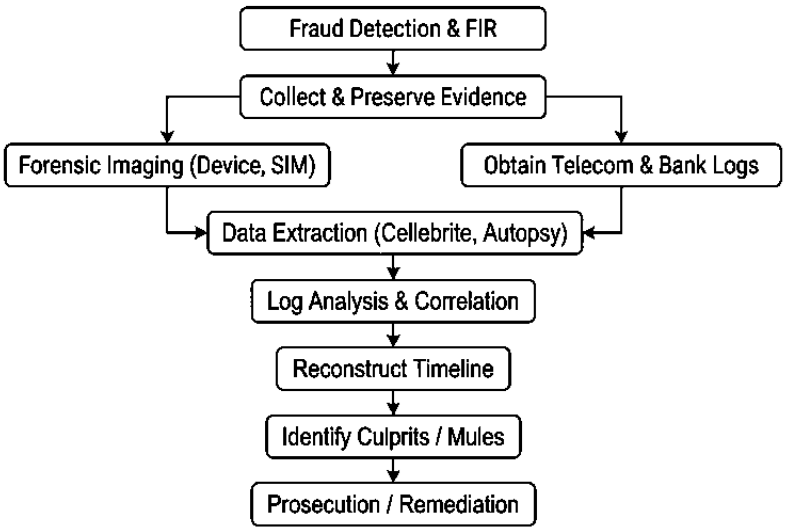

Figure 1: Investigative workflow for SIM swap fraud (forensic data collection, analysis, and prosecution).

4. Case Study: Ahmedabad SIM Swap Heist (March 2023)

A compelling India-based case from 2023 illustrates the above methodology. A Gujarat-based firm (Collective Trade Links Pvt. Ltd.) suddenly lost network connectivity on Sunday, March 12, 2023. Soon after, over **₹1.19 crore** was illicitly transferred from its ICICI Bank account in 22 transactions【1】. The victims had enabled SMS OTPs and received alerts, but the confirmations were sent to their hijacked number.

Incident Summary: Fraudsters executed a classic SIM swap via social engineering【3】. On March 11, 2023, they emailed Vodafone Idea (the operator) a forged request to reissue the CEO's mobile number (+91-99999-XXXX) to a new SIM. Despite the number being registered to an overseas line (on roaming), Vodafone Idea activated the new SIM by 16:30 the same day without robust verification【1】. With the old SIM deactivated, attackers now controlled all calls/SMS. On March 12, they used the stolen SIM to authorize bank transfers: ICICI logs show OTPs sent to +91-99999-XXXX at around 09:30–11:00, immediately followed by fund transfers totaling ₹1.19 Cr【1】. The victim realized only on Monday, March 13, and filed an FIR and bank complaint.

Forensic Findings: Our reconstruction (Table 3) correlates telecom and banking data. The telecom provisioning log snippet shows the swap request and activation:

Telecom Log (Vodafone Idea):
2023-03-11 16:25 | SIM Swap Request received for +9199999XXXX (via email, purported lost SIM)
2023-03-11 16:30 | SIM Activation: New SIM ICCID 89012345… assigned to +9199999XXXX

Meanwhile, ICICI Bank's transaction log snippet shows OTPs and transfers:

Bank Transaction Log:
2023-03-12 09:32 | OTP 458921 sent to +9199999XXXX for transaction authorization
2023-03-12 09:34 | RTGS Transfer ₹ 5,00,000 to Account A (OTP used: 458921)
2023-03-12 10:15 | OTP 123456 sent to +9199999XXXX
2023-03-12 10:17 | RTGS Transfer ₹ 7,50,000 to Account B (OTP used: 123456)
... (other transfers totalling ₹1,19,372,348) ...

These logs confirm the fraud path: the SIM swap (Mar 11, 16:30) preceded the unauthorised transactions (Mar 12, 09:30 onward). Autopsy analysis of the CEO's confiscated phone revealed no SMS warnings because the OTPs all went to the new SIM.【10】 The timeline of events is illustrated below.

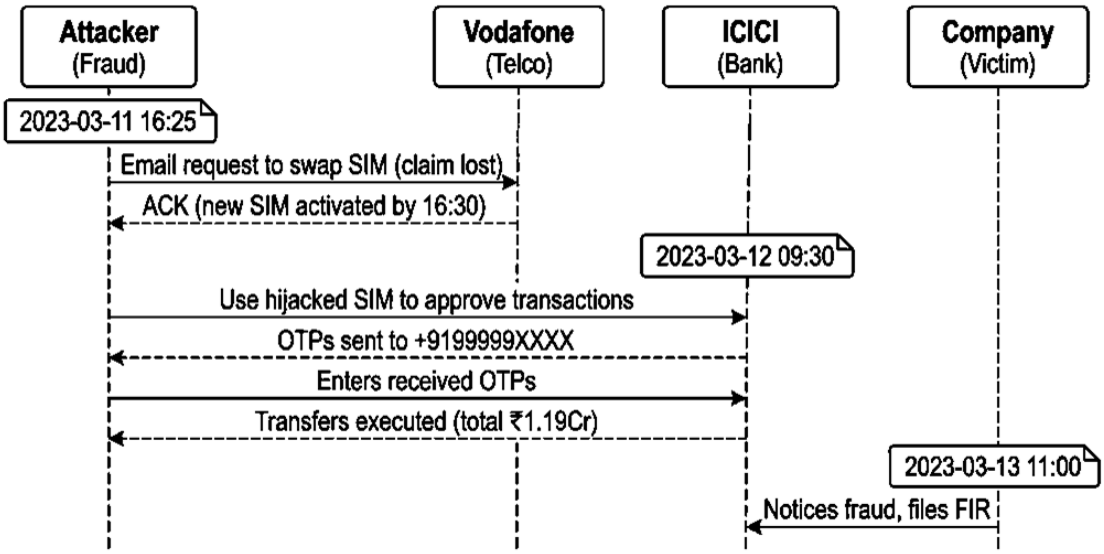

Figure 2: Timeline of the Ahmedabad SIM swap attack (dates/times UTC+5:30).

Outcome: Telecom and bank logs were crucial evidence. Investigators linked the swap email (with a likely traced IP) to the crime. A cybercrime branch inquiry revealed this was part of a larger SIM-swap mafia: a Delhi company had procured 20,986 SIMs fraudulently between 2020-25【8】. Many were sold to fraud rings. On March 2025, the telecom regulator's Adjudicating Officer ordered ICICI Bank and Vodafone Idea to refund ₹1.05 Cr and pay fines (Rs.10L and Rs.5L) for "systematic negligence" 【1】. The case underscores how inadequate SIM verification and logging failures enable high-value frauds.

5. Results & Analysis

From the case study and literature, we observe that **SIM swap frauds exploit procedural weaknesses, not software bugs**. Attackers did not "hack" the telecom network; they tricked it. As Taxmann notes, SIM swap is a "sophisticated cybercrime" achieved by social engineering providers【3】. Once the SIM is transferred, all OTP-

based defenses collapse – the attacker "owns" the 2FA channel. Our forensic analysis confirms this: the telecom log indicated a swap at 16:30, and the bank logs showed OTPs sent to the new SIM immediately after (Fig. 2). The correlation of these artifacts (as in Table 3) provides definitive proof of the sequence.

These findings align with broader observations. Many analysts emphasize that OTP-only systems are vulnerable if SIM control is lost【5】. Indeed, RBI's 2026 mandate for stronger 2FA reflects this risk【4】. In practice, telecom providers are the weak link: in our case, Vodafone processed a swap request on an overseas line with no extra checks【1】. Literature also points to systemic issues: a CBI probe found firms obtaining tens of thousands of SIMs with fake IDs to fuel fraud【8】. Thus, forensic work must often start with verifying identities used in SIM transactions and tracing "SIM mart" networks behind them.

From a digital forensic standpoint, **multiple data sources were critical**. The telecom operator's swap logs and customer CDRs identified exactly which SIMs and numbers changed hands. Banking system logs showed how OTPs were used. Mobile device forensics (per NIST) can recover any residual evidence on the handset or SIM【10】, but in this case the key evidence was off-device. Our procedure (Table 2) successfully reconstructed the attack path. The investment of time in log analysis paid off: even though attackers deleted traces on their own devices, the immutable server logs preserved the timeline.

A challenge we encountered was data synchronization. Clocks on telecom and banking systems were slightly out of sync, requiring careful timestamp alignment. Also, many affected customers only report fraud after days, delaying log requests (logs get purged). This delay can impede evidence collection. Moreover, without inter-agency data sharing (e.g., between police and telecom), investigators often struggle to promptly obtain records.

IV. Discussion

Key Observations:

- **Social-Engineering Attack:** SIM swap is not a technical exploit but a confidence trick. Fraudsters gather personal info and impersonate victims to telecom agents【3】【5】. They may bribe staff or submit forged documents.
- **OTP Vulnerability:** Reliance on SMS OTPs is inherently weak if SMS can be diverted. NIST has long distinguished SMS 2FA as low-assurance due to "SIM change" risks【5】. As seen, when the SIM was reissued, attackers instantly had OTPs for banking.
- **Telecom as Weak Link:** Our case and others show providers often fail to implement even basic identity checks for SIM changes. Despite TRAI mandating in-person KYC and Aadhaar/biometric verification, many activations still hinge on minimal data【1】. This makes telecom logs (SIM issuance records) invaluable forensic evidence.
- **Forensic Correlation:** Combining evidence is crucial. Telecom logs identify *when* the attacker gained control of the number. Banking logs show *what* they did with it. Device imaging can capture any pre-fraud artifacts (e.g. leftover OTP messages). Together, a timeline can be reconstructed, proving causality.

AI-enhanced Forensics: There is growing interest in using AI/ML to augment fraud investigations. For example, machine learning classifiers can analyze vast telecom or transaction datasets to flag anomalies (e.g. unusually frequent SIM swaps under one ID)【9】. Ibanibo *et al.* demonstrate an ML-based system that, in a simulated environment, detected and prevented ~80% of SIM swap attempts when combined with MFA【9】. In principle, banks or telcos in India could train models on historical CDRs and transaction logs to alert on suspicious patterns (e.g., multiple OTPs to new SIMs in short period). Deep learning techniques (CNNs, RNNs) could even parse unstructured logs or network metadata for subtle signals【9】.

Likewise, NLP could be applied to detect social-engineering pretext. For instance, call center recordings might be scanned for suspicious phrases or inconsistencies using NLP classifiers. Email or chat logs where attackers communicate with employees might also yield telltale patterns (urgent language, mismatched identities). However, practical and ethical hurdles abound. Training AI models requires labeled data, which is scarce for fraud (ground truth is hard to annotate). Models can be biased or opaque, raising questions of explainability when used as evidence. Crucially, applying NLP to personal communications implicates privacy (e.g. analyzing a victim's emails or recorded calls demands strict legal oversight). Thus, while AI holds promise, it must be used carefully as an investigative aid, not a sole determiner.

Challenges in Indian Context: Investigations face particular hurdles in India. First, **KYC Loopholes:** Despite regulations, many SIM re-registrations slip through with minimal checks. For example, our case used an email request; telcos are supposed to require proof-of-life (like showing SIM card), but there was no field call-back. The December 2025 CBI raid highlighted how companies obtain SIMs en masse with fake IDs【8】. Second, **Coordination Delays:** Telecom records are stored by private operators; law enforcement must navigate bureaucratic channels (FIR, cyber cell, DoT directions) to access them. Banks have their own compliance teams, and often act only after official notices. This split between agencies slows investigation. Third, **Technical Barriers:** Investigators often lack tools or training to parse large CDRs or encrypted devices. In India, state cyber cells are growing but still under-resourced. Finally, **Legal Ambiguities:** Liability clauses (e.g. RBI's 2017

circular) can lead to disputes over who bears the loss. In the Ahmedabad case, ICICI argued that prompt reporting was required under RBI rules; courts are still shaping how such disputes resolve【6】【7】.
Given these issues, we make **concrete recommendations** below to help prevent and detect SIM swap fraud:

V. Recommendations

- **Stricter SIM KYC:** Mandate in-person or video-Aadhaar authentication for all SIM replacements and port-outs, with no exceptions on weekends or holidays. Biometric (fingerprint/face) verification should be required at authorized centers. Telcos must update CRM systems in real time so any number flagged as "on international roaming" cannot be swapped without manual supervisor override. Regulatory audits should enforce this.
- **Multi-Factor Authentication:** Banks and payment apps must adopt true 2FA: for example, combine OTP with device-bound biometric or token. RBI's 2026 circular is a step forward; regulators should monitor compliance. Quick-deployment measures like issuing digital tokens (apps that generate OTPs) can reduce reliance on SMS.
- **Instant Alerts:** Telecom providers should send immediate SMS/email alerts to the "old SIM" whenever any SIM changes are requested or activated. Similarly, banks should notify customers whenever their mobile number is updated in their profile. Users should be empowered to report unauthorized SIM-change alerts via a helpline. In our case, no such alerts were sent to the old SIM because it had dropped off network – an alert to the registered alternate email might have given an early warning.
- **Data Sharing & Tooling:** Establish joint protocols between telecom companies, banks, and cyber crime units for rapid data sharing. Forensic labs should be equipped with log analysis tools. The government's CFCFRMS (cyber fraud reporting system) can be extended to automatically flag patterns (e.g., multiple OTP sends to same number in short span). Provide law enforcement with training in mobile and log forensics.
- **Public Awareness:** Conduct campaigns to educate users about SIM swap fraud. Advise the public never to share personal data or OTPs, and to use SIM-lock and port-lock features available on many smartphones【3】. Outreach should specifically target high-risk groups (e.g. senior citizens who are often victims).
- **Legal & Procedural Reforms:** Clarify liability rules so victims aren't unduly penalized for system-level failures. Encourage quick grievance resolution (the RBI circular's zero-liability clause should be applied in cases of bank/telco negligence). Introduce strict penalties for telco staff who facilitate unauthorized SIM activations.

VI. Conclusion

SIM swap fraud has become a pervasive cyber-threat in India's digital era. This paper shows that by blending classic digital forensics (device imaging, log analysis) with an understanding of telecom workflows, investigators can effectively reconstruct SIM hijacking schemes. Our case study demonstrates how correlating SIM provisioning logs with banking transactions provided a clear timeline of the crime. More broadly, we find that SIM swap success stems from policy/process gaps – particularly over-reliance on SMS OTPs and lax SIM KYC.

On the defense side, digital forensics can illuminate these attacks and inform better security. However, technology alone is not enough. Both banks and telcos must adopt stronger authentication (e.g. true MFA) and real-time coordination to prevent fraud. As India's economy digitizes further, SIM swap attacks will only grow unless these measures are taken. We urge regulators to act on our recommendations and for ongoing research (including AI-based methods) to evolve the forensic toolset. By tightening processes and enhancing forensic capabilities, stakeholders can help protect users from this evolving form of cybercrime.

References

[1]. A. Kumari, "ICICI Bank Fined Rs 10 Lakh, Vodafone Rs 5 Lakh In Gujarat SIM Fraud Case," *NDTV*, Dec. 10, 2025.
[2]. J. Sharma, "Phishing in India's Fintech Era: Liability, Enforcement, and Consumer Trust," *Int. J. Multidisciplinary Research and Development*, vol. 12, no. 11, pp. 53–58, Nov. 2025.
[3]. Taxmann, "Identity Based Cyber Offences – SIM Swap | Deepfakes," (blog), Feb. 11, 2026.
[4]. IANS, "What Changes Will RBI's New Rules Bring to Digital Payments from April 1?", *Economic Times*, Mar. 30, 2026.
[5]. K. Lee, B. Kaiser, J. Mayer, and A. Narayanan, "An Empirical Study of Wireless Carrier Authentication for SIM Swaps," in *Proc. 16th Symposium on Usable Privacy and Security (SOUPS 2020)*, pp. 61–79.
[6]. Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," DBR Leg.BC.78/09.07.005/2017-18, July 6, 2017.
[7]. Government of India, "The Information Technology Act, 2000," Sections 66C–66D, updated 2011.
[8]. R.S. Jha, "Digital Arrest: CBI Probes Delhi Firm That Bought 20k SIMs & 'Fuelled' Cyber Crime," *Times of India*, Dec. 9, 2025.
[9]. T.S. Ibanibo *et al.*, "Combating SIM Swap Fraud in Telecommunications: A Machine Learning Approach and Multi-Factor Authentication as a Preventive Strategy," *Journal of Advancement in Communications*, vol. 8, no. 2, pp. 33–45, May–Aug. 2025.
[10]. W.A. Jansen and A. Delaitre, "Reference Material for Forensic SIM Tools," *IEEE ICCST*, 2007, pp. 165–179.