International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Importance of Sanchar Saathi Mobile Application for Cybersecurity of Indian Citizens

Mr. Onkar Sanjay Shelke[1], Ms. Rupali Kharat[2]

Assistant Professor, Dr. D. Y. Patil ACS Women's College, Pimpri, Pune

Abstract

The Sanchar Saathi mobile application by the Department of Telecommunications is a critical intervention for Indian citizens facing increasing telecom fraud and cybersecurity threats. This paper analyses its significance, functionality, and impact as a citizen-focused cybersecurity tool. The application has proven its effectiveness by recovering over 700,000 lost devices, preventing identity theft, and enabling millions of fraud reports. Additionally, it discusses privacy issues, addresses adoption obstacles, and recommends strategies to strengthen telecom security for Indian users.

Keywords: Cybersecurity, Telecom Fraud, Digital Identity, IMEI Verification, Identity Theft, Government Initiative, Cyber Threats, Mobile Security

1. INTRODUCTION

1.1 Background

India's telecommunications sector has experienced exponential growth, with over 900 million mobile subscribers making it the world's largest mobile user base [1]. However, this rapid expansion has created a parallel growth in cybersecurity threats, including device theft, SIM fraud, identity theft through forged KYC (Know Your Customer) documents, banking fraud, and malicious communications [2]. The Department of Telecommunications (DoT), Government of India, recognized the urgent need to address these escalating cyber threats through a citizen-centric approach.

In response to these security challenges, the DoT launched the Sanchar Saathi initiative—a comprehensive telecom security program that includes both a web portal (launched May 16, 2023) and a mobile application (launched January 17, 2025) [2]. The Sanchar Saathi mobile application represents the government's commitment to bringing robust security features and fraud-reporting capabilities directly to citizens' smartphones, empowering them to protect their digital identity and take swift action against potential fraud.

1.2 Problem Statement

Indian citizens face multifaceted cybersecurity threats in their telecom usage:

1. **Device Theft and Loss**: With over 700,000 mobile devices reported lost or stolen annually, users lack immediate tools to protect their devices [1]
2. **Identity Theft**: Fraudulent KYC registrations and forged documents enable criminals to misuse citizens' identities for various illicit activities [2]
3. **Fraudulent Communications**: Spam calls, phishing SMS messages, and malicious links delivered through multiple platforms pose significant threats
4. **Financial Fraud**: Telecom fraud frequently precedes banking fraud, making comprehensive

protection essential

5. **Limited Awareness**: Many citizens lack knowledge about verifying device authenticity or checking unauthorized mobile connections in their name

1.3 Research Objectives

This research paper aims to:

1. Analyze the functionality and features of the Sanchar Saathi mobile application.
2. Evaluate its role in protecting Indian citizens' cybersecurity.
3. Assess the impact and effectiveness of the application in addressing telecom fraud.
4. Discuss privacy and implementation considerations.
5. Provide recommendations for improving adoption and effectiveness.

1.4 Significance of the Study

This study is significant as it:

- Provides comprehensive documentation of India's first government-backed telecom security mobile application
- Analyzes the effectiveness of citizen-centric cybersecurity initiatives
- Contributes to understanding digital security policies in emerging economies
- Offers insights into balancing security and privacy in government applications
- Provides recommendations for other nations implementing similar initiatives

2. Literature Review and Context

2.1 Telecom Security Landscape in India

India's telecommunications sector faces unprecedented security challenges due to its massive user base and digital adoption rate [2]. Cybercriminals exploit telecom infrastructure for:

- Identity theft through unauthorized SIM activations
- Device cloning and counterfeiting
- Spam and phishing attacks
- Financial fraud schemes
- Unauthorized data access and privacy violations
- Malware distribution through compromised devices

2.2 Government's Role in Cybersecurity

The DoT's approach reflects international best practices where government agencies:

- Establish regulatory frameworks for telecom security
- Provide citizen-centric tools for self-protection
- Collaborate with service providers for implementation
- Create awareness about digital threats and safety measures

The Sanchar Saathi initiative aligns with India's broader cybersecurity strategy and Digital India mission to create a secure digital ecosystem [3].

2.3 Global Context of Mobile Security Applications

Other nations have implemented government-backed mobile security solutions:

- Singapore's cybersecurity initiatives.
- Australia's government-backed security programs.
- European Union's regulatory frameworks (GDPR).

The Sanchar Saathi application distinguishes itself through its multilingual support (English, Hindi, and 21 regional languages), making it accessible to India's diverse population [2].

3. Features and Functionality of Sanchar Saathi Mobile Application

3.1 Core Features

The Sanchar Saathi mobile application provides six primary security features designed to empower users:

3.1.1 Know Mobile Connections in Your Name

This feature enables users to:

- Verify all mobile connections registered in their name.
- Identify unauthorized or fraudulent connections [4].
- Report suspicious connections immediately.
- Prevent misuse of their identity for telecom services.

Significance: This feature directly addresses identity theft by enabling users to detect whether criminals have opened connections using forged KYC documents [2].

3.1.2 Know Genuineness of Your Mobile Handset (IMEI Verification)

Users can verify device authenticity by:

- Entering the International Mobile Equipment Identity (IMEI) number.
- Checking if the device is blacklisted, duplicated, or already in use.
- Retrieving IMEI from device packaging, invoices, or by dialing *#06#[4].
- Accessing the CEIR (Central Equipment Identity Register) database.

Significance: This feature prevents citizens from purchasing counterfeit devices and protects against device cloning attacks [1].

3.1.3 Chakshu—Report Suspected Fraud Communications (SFC)

This feature allows users to report:

- Fraudulent calls through direct selection from call logs.
- Phishing SMS messages.
- Malicious web links.
- Unverified APKs (application packages).
- Device cloning attempts [2].

Users can report fraud through multiple channels:

- Direct in-app reporting.
- Call and SMS logs integration.
- WhatsApp and Telegram integration.
- Social media-based fraud reporting.

Significance: This creates a crowdsourced database of fraud patterns, helping authorities identify and block malicious actors [1].

3.1.4 Block Lost/Stolen Mobile Devices

Users can:

- Register their device as lost or stolen.
- Request immediate blocking through CEIR.
- Unblock the device when recovered [4].
- Check the status of blocking requests using the request ID.

Impact: Since the initiative's launch, over 700,000 lost mobile phones have been recovered, including 50,000 devices in October 2025 alone [1].

3.1.5 Multi-language Support

The application is available in:

- English and Hindi (primary languages).
- 21 regional languages (Tamil, Telugu, Kannada, Malayalam, Marathi, Gujarati, Punjabi, Assamese, Bengali, Oriya, Konkani, Manipuri, Nagamese, etc.) [2].

Significance: This ensures accessibility for India's linguistically diverse population, democratizing cybersecurity awareness and protection.

3.1.6 User-Friendly Reporting Interface

The application features:

- Automatic call/SMS log fetching.
- Quick tap reporting mechanism.
- Auto-population of communication details.
- Minimal data transmission (only reported details sent to DoT) [4].

3.2 Technical Architecture and Data Privacy

3.2.1 Permission Management

The Sanchar Saathi app requires specific permissions [4]:

Permission	Purpose	
Call/SMS Logs Access	To fetch communication details for reporting fraudulent calls/SMS. Logs remain on-device; only reported details transmitted to DoT	
Make	Manage Phone Calls	Device number detection during registration
Send SMS	One-time SMS registration to 14522 for DoT verification	

Table 1: Sanchar Saathi App Permissions and Purposes

3.2.2 Data Security Measures

- On-device call/SMS log storage (not sent to servers).
- Selective data transmission (only reported communications).
- One-time SMS verification during registration.
- DoT-owned infrastructure ensures government oversight.
- Compliance with Indian data protection frameworks.

4. Impact and Effectiveness

4.1 Adoption and Reach

4.1.1 Download Statistics

Metric	Value
Downloads (as of August 2025)	50+ lakh (5 million+)
Platform Availability	Android and iOS
Regional Language Support	21 regional languages
Device Recovery Rate (October 2025)	50,000 devices
Total Device Recovery (cumulative)	700,000+ devices

Table 2: Sanchar Saathi Application Adoption Statistics (as of December 2025)

4.1.2 Recent Mandates and Implementation

On November 28, 2025, the Department of Telecommunications issued directions requiring:

- All smartphone manufacturers and importers are to pre-install Sanchar Saathi on new devices.
- 90-day implementation period for compliance.
- Prevention of user deletion or disabling of the application [1].

This mandate significantly accelerates adoption, ensuring that new device users have access to security features regardless of initial awareness or choice.

4.2 Real-World Impact

4.2.1 Device Recovery and Theft Prevention

The application has demonstrated significant effectiveness in device recovery:

- **700,000+ devices recovered** since initiative launch [1]
- **50,000 devices recovered in October 2025 alone**, indicating accelerating recovery rates
- **IMEI blacklisting** prevents the sale of stolen devices in secondary markets [4]
- **Reduced the incentive for device theft** due to the rapid blocking capability.

4.2.2 Identity Theft Prevention

The app enables users to:

- Detect fraudulent KYC registrations in real-time.
- Report unauthorized mobile connections immediately.
- Prevent criminals from establishing telecom identities for financial fraud [2].
- Reduce identity theft-enabled banking fraud.

4.2.3 Fraud Reporting and Cybercriminal Tracking

Through the Chakshu feature, citizens contribute to:

- Building crowdsourced databases of fraud patterns.
- Enabling law enforcement agencies to identify and track cybercriminals.
- Creating early warning systems for emerging fraud schemes.
- Reducing response time for blocking malicious communications [2].

4.3 Comparative Effectiveness

Compared to traditional approaches:

Parameter	Traditional Method	Sanchar Saathi
Device Blocking Speed	1-3 weeks	Real-time
User Awareness	Limited	Direct notification
Fraud Reporting Channel	Police/official	In-app submission
Language Accessibility	Limited	23 languages
Accessibility (Cost/Time)	High	Free/on-device

Table 3: Effectiveness Comparison: Traditional vs. Sanchar Saathi Approach

5. Cybersecurity Implications for Indian Citizens

5.1 Multi-layered Protection

The Sanchar Saathi application provides layered cybersecurity defense:

1. **Device Authentication**: IMEI verification prevents counterfeiting and cloning
2. **Identity Verification**: Mobile connection tracking prevents fraudulent registrations
3. **Communication Security**: Spam/phishing reporting reduces fraud delivery mechanisms
4. **Active Recovery**: Device blocking prevents unauthorized access post-theft
5. **Collective Intelligence**: Crowdsourced fraud data protects a broader user base

5.2 Empowerment Through Knowledge

The application empowers citizens through:

- **Immediate threat detection**: Real-time alerts for unauthorized activities
- **Proactive protection**: Ability to verify devices before purchase
- **Informed reporting**: Understanding which communications constitute fraud
- **Digital literacy**: Building awareness about cybersecurity best practices

5.3 Protection Against Emerging Threats

The application addresses contemporary cybersecurity threats:

- **SIM Swap Attacks**: Detection of unauthorized connections enables rapid response [2]
- **Device Cloning**: IMEI verification prevents device duplication attacks
- **Phishing and Smishing**: SMS-based fraud reporting through Chakshu
- **Financial Fraud Chains**: Telecom security prevents preliminary steps in financial fraud [2]
- **Identity Theft**: Real-time monitoring of connections registered in the user's name

6. Privacy Considerations and Concerns

6.1 Privacy Framework

The application operates within India's privacy framework:

- Alignment with the Information Technology Act, 2000
- Compliance with India's proposed Digital Personal Data Protection Act
- DoT-operated infrastructure with government oversight
- Limited data transmission (only reported details) [4]

6.2 Identified Concerns

Technology experts and privacy advocates have raised concerns regarding:

6.2.1 Extensive Permissions

The application requests permissions for:

- Call and SMS log access.
- Phone call management.
- SMS sending capability.

While these permissions serve stated security functions, critics argue the potential for scope expansion [5].

6.2.2 Non-Deletable Installation

The mandatory pre-installation directive with the prevention of deletion raises concerns about:

- User autonomy and choice
- Potential for surveillance expansion
- Distinction between voluntary and mandatory security tools

6.2.3 Data Access Potential

Analysts note that while current implementation limits data transmission, the infrastructure could potentially be expanded for broader data access[5].

6.3 Mitigation Strategies

The DoT has implemented safeguards:

- Transparent disclosure of required permissions
- On-device data storage for call/SMS logs
- Limited server-side data transmission
- Government accountability mechanisms
- Clear communication about data usage

6.4 Privacy-Security Balance

The application represents a deliberate choice to prioritize:

- Collective security benefits (fraud prevention, device recovery)
- Individual empowerment (verification tools, reporting capabilities)
- Public health protection (rapid response to telecom misuse)

This balance reflects policy decisions about acceptable privacy trade-offs for enhanced security.

7. Implementation Challenges and Solutions

7.1 Adoption Barriers

Challenge 1: Digital Literacy Gaps

- **Problem**: Not all Indian citizens possess advanced technical knowledge
- **Solution**: Simple, intuitive interface with multilingual support
- **Solution**: In-app guidance and educational content

Challenge 2: Smartphone Penetration Disparity

- **Problem**: Significant populations in India lack smartphones
- **Solution**: Web-based Sanchar Saathi portal for non-app users
- **Solution**: SMS-based services (e.g., IMEI verification via SMS)

Challenge 3: Device Manufacturer Compliance

- **Problem**: Coordination required with multiple manufacturers and importers
- **Solution**: Clear 90-day mandate with compliance requirements

- **Solution**: Technical specifications provided by DoT

7.2 Addressing Privacy Concerns

Concern	Mitigation Strategy
Data Misuse	Transparent permission framework, on-device storage
Unauthorized Access	Government-operated infrastructure, audit trails
Scope Expansion	Legislative oversight, citizen awareness

Table 4: Privacy Concern Mitigation Strategies

8. Recommendations and Future Directions

8.1 Enhancing Effectiveness

Recommendation 1: Advanced Analytics

Implement machine learning algorithms to:

- Identify fraud patterns in real-time.
- Predict emerging cybersecurity threats.
- Provide personalized security recommendations to users.
- Enhance targeting of cybercriminal networks.

Recommendation 2: Multi-agency Integration

Facilitate seamless integration with:

- Law enforcement agencies (police, CBI)
- Financial regulatory authorities (RBI)
- Telecom service providers
- Cybercrime reporting centers

Recommendation 3: Awareness Campaigns

Develop comprehensive awareness initiatives:

- School and college cybersecurity education
- Community outreach programs in regional languages
- Integration with telecom provider customer communications
- Corporate training programs for businesses

8.2 Addressing Privacy and Governance

Recommendation 1: Transparent Governance Framework

Establish:

- Public accountability mechanisms
- Regular privacy audits and impact assessments
- Citizen oversight committees
- Published anonymized statistics on data usage

Recommendation 2: Legislative Safeguards

Support development of:

- Clear data protection legislation for government apps
- User rights and deletion policies

- Scope limitation clauses preventing unauthorized expansion
- International standards alignment (GDPR-like provisions)

Recommendation 3: User Empowerment

Provide citizens with:

- Full transparency on data collection and usage
- Choice mechanisms were feasible
- Easy opt-out procedures for voluntary features
- Clear communication about mandatory vs. optional components

8.3 Expansion Possibilities

Geographic and Sectoral Expansion

The Sanchar Saathi model could be extended to:

- Financial services cybersecurity
- E-commerce fraud prevention
- IoT device security
- Critical infrastructure protection

International Collaboration

Partner with:

- ASEAN nations for regional cybersecurity cooperation
- International Telecommunications Union (ITU)
- Global cybersecurity organizations
- Other emerging economies are implementing similar initiatives

9. Case Studies and Real-World Scenarios

9.1 Scenario 1: Device Theft Prevention and Recovery

Situation: A citizen's smartphone is stolen from a public location.

Sanchar Saathi Response:

1. User immediately accesses the app and marks the device as lost/stolen.
2. IMEI is registered with CEIR as blacklisted
3. The device is blocked across the telecom network.
4. If device surfaces in the secondary market, IMEI verification reveals blacklist status.
5. The device is recovered and returned to the citizen.

Outcome: Reduced incentive for device theft; improved device recovery rate.

9.2 Scenario 2: Identity Theft Prevention

Situation: A criminal attempts to open unauthorized mobile connections using a citizen's forged KYC documents.

Sanchar Saathi Response:

1. Citizen receives an alert through the telecom provider or notices unusual activity.
2. User checks mobile connections in the Sanchar Saathi app.
3. Unauthorized connections are identified immediately.
4. User reports fraudulent connections through the app.
5. DoT takes action to deactivate unauthorized connections.

Outcome: Prevented financial fraud chains that typically follow identity theft.

9.3 Scenario 3: Phishing and Spam Prevention

Situation: A citizen receives a phishing SMS claiming to be from their bank, requesting account details.

Sanchar Saathi Response:

1. User recognizes the suspicious nature of the message.
2. User reports the SMS directly from the message thread using the Chakshu feature.
3. Report includes automatic SMS details (sender, content, timestamp)
4. DoT adds SMS sender to fraud database.
5. Other users are alerted about this fraud pattern.
6. Telecom provider blocks sender number.

Outcome: Rapid prevention of phishing campaign affecting broader user base.

10. Conclusion

The Sanchar Saathi mobile application represents a significant advancement in India's cybersecurity infrastructure, offering citizen-centric protection against multifaceted telecom threats. By combining device verification, identity tracking, fraud reporting, and device recovery capabilities, the application creates a comprehensive defense system against the evolving cybersecurity landscape affecting Indian citizens.

Key Findings

1. **Comprehensive Security**: The application addresses identity theft, device theft, fraud communications, and unauthorized account creation through integrated features [1][2]
2. **Proven Effectiveness**: Recovery of 700,000+ stolen devices and prevention of millions of fraud attempts demonstrate significant real-world impact [1]
3. **Accessibility and Inclusivity**: Support for 23 languages ensures democratic access to security tools across India's diverse population [2]
4. **Citizen Empowerment**: Features enabling real-time verification and reporting transform citizens from passive victims to active participants in cybersecurity [2]
5. **Policy Innovation**: Government-backed, citizen-centric approach provides a model for emerging economies implementing digital security initiatives [1]
6. **Privacy-Security Trade-off**: While concerns about data permissions and mandatory installation exist, implemented safeguards and transparency mechanisms address key concerns [5]
7. **Scalability**: The application's success creates a foundation for expanding government cybersecurity initiatives to other sectors and international markets [1]

Strategic Importance

For Indian citizens, the Sanchar Saathi application provides:

- **Immediate protection** against contemporary cybersecurity threats
- **Proactive verification tools** enabling informed digital decisions
- **Collective defense mechanisms** leveraging crowdsourced fraud intelligence
- **Empowerment through knowledge** of digital identity and device authenticity

For India's digital ecosystem, the initiative represents:

- **Government leadership** in citizen-centric cybersecurity
- **Regulatory innovation** adapting to emerging telecom threats.
- **Public-private collaboration model** coordinating with service providers and manufacturers
- **A Foundation for digital confidence** is essential for e-commerce, fintech, and digital services growth

Future Scope

As the application scales through mandatory pre-installation and expanded features, its impact will likely increase substantially. The combination of technical capability, user accessibility, and official mandate positions Sanchar Saathi as a cornerstone of India's cybersecurity infrastructure for the coming decade.

The research demonstrates that with appropriate privacy safeguards, transparency mechanisms, and governance frameworks, government-backed cybersecurity applications can effectively address contemporary threats while maintaining citizen trust and democratic principles.

References

1. Press Information Bureau. (2025, December 1). Sanchar Saathi App: Telecom Empowerment at Citizens' Fingertips. Government of India, Department of Telecommunications. https://www.pib.gov.in/
2. Press Information Bureau. (2025, December 1). The Sanchar Saathi App has emerged as a powerful tool for securing India's growing telecom ecosystem. Government of India, Department of Telecommunications. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=156294
3. BBC News. (2025, December 2). Sanchar Saathi: India mandates state-owned cyber safety app on all smartphones. https://www.bbc.com/news/articles/cedxyvx74p4o
4. Google Play Store. (2025, October 4). Sanchar Saathi – Apps on Google Play. Retrieved from https://play.google.com/store/apps/details?id=com.dot.app.sancharsaathi
5. The Hacker News. (2025, December 2). India Orders Phone Makers to Pre-Install Government App for Cybersecurity. https://thehackernews.com/2025/12/india-orders-phone-makers-to-pre.html
6. Indian Express. (2025, December 1). What is Sanchar Saathi, the app govt has asked phone makers to preinstall? Retrieved from https://indianexpress.com/article/explained/explained-sci-tech/govt-smartphone-preinstall-sanchar-saathi-what-is-it-10396227/
7. Wikipedia. (2023, September 21). The Sanchar Saathi. Retrieved from https://en.wikipedia.org/wiki/Sanchar_Saathi
8. Press Information Bureau. (2025, August 8). Downloads of Sanchar Saathi Mobile App crossed 50 lakh. Government of India, Department of Telecommunications. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154606
9. Services India. (n.d.). Verify Mobile Device Using IMEI number. https://services.india.gov.in/service/detail/verify-mobile-device-using-imei-number
10. CEIR - Sanchar Saathi. (n.d.). Know Your Equipment Identity. Retrieved from https://www.sancharsaathi.gov.in/