IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

# Cyber Security in Banking and Financial Institutions in Telangana: A Comprehensive Analysis of Threats, Initiatives, and Strategic Frameworks (2024-2026)

**A.Suresh Babu**, Lecturer in Computer Application/Comp.science

Government Degree college, Badangpet, Rangareddy District – Hyderabad

**DOI**: https://doi.org/10.56975/ijrar.v13i1.330544

**Abstract**

The rapid digital transformation of the banking and financial sector in Telangana has brought significant economic benefits but has also exposed institutions to sophisticated cyber threats. This paper examines the current cybersecurity landscape in Telangana, focusing on the unique challenges faced by financial institutions. It analyzes recent trends in cybercrime, the effectiveness of state-led initiatives such as the Telangana Cyber Security Bureau (TGCSB), and the regulatory frameworks governing the sector. Through a review of recent data from 2024 to 2026, the study highlights the shift from traditional financial fraud to complex schemes involving mule accounts and social engineering. The paper concludes with strategic recommendations for strengthening the cyber resilience of Telangana's financial ecosystem.

**Keywords:**

Cybersecurity, Banking Sector, Telangana, Digital Fraud, RBI, Financial Institutions, AI Security, Cyber Threats

## 1. Introduction

Telangana, particularly its capital Hyderabad, has emerged as a global hub for Information Technology and Financial Services. As the state pushes for unprecedented financial inclusion through digital platforms, the security of these systems has become a matter of national importance. The banking sector, being the backbone of the economy, is a primary target for cybercriminals seeking high-value gains. This paper explores the intersection of technological advancement and cyber risk within the specific socio-economic context of Telangana.

## 2. The Cybersecurity Landscape in Telangana (2024-2026)

Recent reports, including the *India Cyber Threat Report 2025* by the Data Security Council of India (DSCI), indicate that Telangana remains at the forefront of cyber- attack targets in India. However, the state has also shown remarkable resilience and proactive management.

### 2.1 Statistical Trends

The following table summarizes the cybercrime trends in major urban centers of Telangana during 2025:

| Region | Case Trend (2025 vs 2024) | Financial Loss (2025) | Recovery/Refund (2025) |
|---|---|---|---|
| Cyberabad | 36% Decrease | Rs 404.61 Crore | ~Rs 200 Crore |
| Hyderabad | 7.6% Decrease | Rs 319 Crore | Rs 150 Crore |
| Statewide | 10% Dip (Financial) | ~Rs 1,200 Crore (Est.) | Rs 246 Crore |

While the number of reported financial cybercrimes has seen a slight decline, the complexity of these crimes has increased. Non-financial cybercrimes, such as identity theft and cyber-stalking, saw a 23% increase in the same period, indicating a diversification of attacker tactics.

## 3. Key Cyber Threats to the Banking Sector

The banking and financial institutions (BFIs) in Telangana face a multi-faceted threat environment. The most prominent threats identified in 2025-2026 include:

### 3.1 Mule Account Networks and "Operation Crackdown"

One of the most significant challenges is the proliferation of "mule accounts"—bank accounts used to launder stolen money. In early 2026, the Telangana Cyber Security Bureau (TGCSB) launched *Operation Crackdown 1.0*, which revealed extensive networks of mule accounts. Investigations suggested that in some cases, there was

suspected connivance of bank officials in facilitating the opening of these accounts without proper KYC verification.

### 3.2 Social Engineering and Investment Frauds

Social engineering remains the most effective tool for cybercriminals. In Telangana, investment schemes and part-time job frauds topped the list of complaints in 2025. These schemes often leverage the high digital presence of the state's population to lure victims into sharing sensitive financial information or transferring funds voluntarily.

### 3.3 Digital Arrest and Credit Card Scams

"Digital arrest" scams, where victims are intimidated by callers posing as law enforcement officers, accounted for approximately 8% of total financial losses in 2025. Credit card frauds followed closely at 7%, highlighting the need for better consumer awareness and more robust transaction monitoring systems.

## 4. Institutional and Policy Frameworks

Telangana has established a robust institutional framework to combat cyber threats, led by the state government and law enforcement agencies.

### 4.1 Telangana Cyber Security Bureau (TGCSB)

The TGCSB serves as the apex body for cybersecurity in the state. It coordinates between various stakeholders, including the Reserve Bank of India (RBI), commercial banks, and the central government's Indian Computer Emergency Response Team (CERT-In).

### 4.2 State Initiatives and Programs

- **Shield 2.0 Program:** Launched in February 2026, this program focuses on enhancing the technical capabilities of law enforcement and financial institutions to detect and respond to cyber incidents in real-time.
- **Law Enforcement CISO Council:** This initiative brings together Chief Information Security Officers (CISOs) from various sectors to share threat intelligence and best practices.
- **SBI Cyber Defender Program:** A collaborative effort between the State Bank of India and TGCSB to provide specialized training to banking personnel on identifying and preventing digital fraud.

### 4.3 Regulatory Compliance

Financial institutions in Telangana operate under the dual oversight of national regulations (IT Act 2000, RBI Cyber Security Framework) and state-level policies. The *Telangana Cyber Security Policy (2016)* laid the groundwork for the protection of Critical Information Infrastructure (CII) and the establishment of dedicated Cyber Crime Cells.

## 5. Challenges and Strategic Recommendations

Despite the progress made, several challenges persist:

- **Insider Threats:** The suspected involvement of bank staff in fraudulent activities necessitates stricter internal audits and behavioral monitoring.
- **Digital Literacy Gap:** While urban areas are highly connected, rural populations remain vulnerable to basic social engineering tactics.
- **Rapid Technological Evolution:** The rise of AI-driven deepfakes and automated phishing requires institutions to adopt advanced AI-based defense mechanisms.

**Recommendations:**

1. **Implementation of Zero-Trust Architecture:** BFIs should move away from perimeter-based security to a zero-trust model where every access request is verified.
2. **Enhanced Public-Private Partnerships:** Regular threat-sharing sessions between TGCSB and private banks can significantly reduce response times.
3. **Mandatory Cyber Hygiene Training:** Continuous education for both bank employees and customers is essential to mitigate the risk of social engineering.

## 6. Conclusion

Cybersecurity in the banking and financial sector of Telangana is a dynamic and evolving field. While the state has made significant strides in reducing the overall volume of cybercrime through proactive operations like *Crackdown 1.0* and *Shield 2.0*, the emergence of new threat vectors requires constant vigilance. By fostering a culture of security, investing in advanced technology, and maintaining strong regulatory oversight, Telangana can continue to protect its financial integrity in the digital age.

## References

1. Data Security Council of India (DSCI). (2025). *India Cyber Threat Report 2025*.
2. Telangana Cyber Security Bureau (TGCSB). (2026). *Annual Report on Cybercrime Trends and Operations*.
3. Government of Telangana. (2016). *Telangana Cyber Security Policy*.
4. Reserve Bank of India (RBI). (2024). *Cyber Security Framework for Banks: Updated Guidelines*.
5. Siasat Daily. (2025). "Cybercrime cases decrease in Hyderabad in 2025".
6. Times of India. (2026). "Operation Crackdown: TGCSB targets mule account networks".