International Journal of Research in Advanced Engineering and Technology
www.allengineeringjournal.in
ISSN: 2455-0876
Received: 11-11-2025, Accepted: 10-12-2025, Published: 25-12-2025
Volume 11, Issue 2, 2025, Page No. 27-30

A regional taxonomy of cyber threats in the banking sector: Evidence from Jammu & Kashmir

Tanzilla Shahid
Research Scholar, Jyoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

Abstract
The rapid digitization of the Indian banking sector has transformed financial services by enhancing accessibility, efficiency, and inclusion. However, this digital transition has simultaneously increased exposure to sophisticated cyber threats. These risks become significantly more complex in conflict-affected and politically sensitive regions such as Jammu & Kashmir (J&K). The region's unique socio-political environment, infrastructural limitations, and evolving digital literacy landscape present distinct cybersecurity challenges for both public and private banking institutions.This research paper proposes a regional taxonomy of cyber threats affecting the banking sector in Jammu & Kashmir. The study systematically categorizes cyber threats based on their nature, origin, targets, and impact, while also examining regional vulnerabilities that intensify these threats. Using a descriptive and analytical research methodology, the paper draws upon secondary data sources including reports from regulatory bodies, cybersecurity frameworks, academic literature, and documented cyber incidents.The findings reveal that phishing, social engineering, malware, insider threats, mobile banking frauds, and politically motivated cyber attacks are the most prominent threats in the region. Additionally, the study highlights the role of youth behavior, ethical awareness, and governance mechanisms in shaping the cybersecurity landscape. The paper emphasizes the need for region-specific cybersecurity policies, ethical digital education, and collaborative governance models to strengthen cyber resilience in the banking sector of Jammu & Kashmir.

Keywords: Cyber threats, banking sector, jammu and kashmir, cybersecurity, regional taxonomy, digital governance

Introduction

The banking sector forms the backbone of any modern economy, facilitating financial transactions, economic growth, and public trust. In India, digital banking initiatives such as core banking systems, internet banking, mobile wallets, and Unified Payments Interface (UPI) have revolutionized financial services. While these innovations have promoted financial inclusion, they have also exposed banks to an expanding range of cyber threats.Jammu & Kashmir occupies a strategically sensitive position within India, marked by prolonged political instability, security concerns, and infrastructural challenges. As digital banking services expand in the region, cyber threats have emerged as a critical concern for financial institutions. Unlike other regions, cyber attacks in J&K are influenced not only by financial motives but also by political, ideological, and regional factors.This research attempts to develop a regional taxonomy of cyber threats specific to the banking sector in Jammu & Kashmir. By categorizing threats systematically, the study seeks to provide a structured understanding that can assistpolicymakers, banking professionals, and cybersecurity experts in developing targeted defense strategies.

Objectives of the Study The primary objectives of this research are

- To identify major cyber threats affecting public and private banks in Jammu & Kashmir.
- To develop a regional taxonomy of cyber threats based on nature, source, and impact.
- To analyze regional socio-political and technological factors influencing cybersecurity risks.
- To examine governance and ethical challenges related to cyber threats in the banking sector.
- To suggest policy and institutional measures for strengthening cybersecurity resilience.

Research Methodology

This study adopts a descriptive and analytical research methodology, relying primarily on secondary data. The sources of data include: Reports published by the Reserve Bank of India (RBI) Government publications and cybersecurity guidelinesAcademic journals, books, and conference papers Reports from cybersecurity agencies and thinktanksDocumented case studies of cyber incidents in bankingThe qualitative analysis focuses on identifying patterns, categorizing threats, and interpreting their implications within the regional context of Jammu & Kashmir. Overview of Cybersecurity in the Indian Banking Sector Cybersecurity in Indian banking has become a critical priority due to increasing incidents of financial fraud, data breaches, and service disruptions. Banks are attractive targets for cybercriminals because they store sensitive financial and personal data. Common cybersecurity challenges faced by banks across India include outdated infrastructure, lack of skilled cybersecurity professionals, and increasing sophistication of cyber attacks.Regulatory bodies such as the Reserve Bank of India have issued cybersecurity frameworks mandating banks to adopt robust risk management practices. However, implementation varies across regions, particularly in areas with infrastructural and administrative constraints such as Jammu & Kashmir.

Regional Context Jammu & KashmirJammu & Kashmir presents a unique cybersecurity environment shaped by several regional factors: Socio-Political Sensitivity Jammu & Kashmir occupies a uniquely sensitive position within the socio-political landscape of India. The region's historical complexities, prolonged political instability, security concerns, and periodic disruptions in governance have created a fragile socio-political environment. These conditions significantly influence the functioning of public

institutions, including the banking sector, and have direct implications for cybersecurity preparedness and resilience.The socio-political sensitivity of the region is rooted in long-standing political disputes, cross-border tensions, and internal security challenges. Frequent curfews, communication restrictions, and internet shutdowns have disrupted normal civic and economic activities. While such measures are often implemented for security reasons, they unintentionally affect digital banking operations, cybersecurity monitoring, and timely incident response. Banking institutions operating in this environment face operational constraints that differ substantially from those in more stable regions.From a societal perspective, trust in institutions plays a crucial role in digital banking adoption. In conflict-affected regions, public trust is often fragile due to political uncertainty, perceived marginalization, and limited engagement between institutions and local communities. This lack of trust can make individuals more susceptible to cyber fraud, misinformation, and social engineering attacks. Cybercriminals frequently exploit social anxiety, political unrest, and economic uncertainty to manipulate users into revealing sensitive financial information.The socio-political sensitivity of Jammu & Kashmir also contributes to a distinct cyber threat profile. Cyber attacks in the region are not always financially motivated; some are driven by ideological, political, or disruptive intentions. Banks, as symbols of state authority and economic stability, become attractive targets for politically motivated cyber actors. Distributed denial-of-service (DDoS) attacks, website defacements, and data breaches in the banking sector can be used to spread fear, disrupt financial systems, and undermine public confidence.Governance challenges further intensify cybersecurity risks. Periods of administrative transition and policy restructuring can lead to gaps in regulatory enforcement and coordination among institutions. In such environments, cybersecurity governance often becomes reactive rather than proactive. Limited regional autonomy in cybersecurity decision-making can also restrict the implementation of localized security strategies tailored to the socio-political realities of the region.Another critical dimension of socio-political sensitivity is its impact on human capital and digital literacy. Prolonged instability affects education systems, employment opportunities, and skill development, particularly among youth. Although young people in Jammu & Kashmir are increasingly digitally connected, uneven access to structured cybersecurity education and ethical digital training increases vulnerability to cyber exploitation. Youth may unknowingly become victims of cyber crime or, in some cases, participants in unethical cyber activities due to lack of awareness and socio-economic pressures.Despite these challenges, the region also presents opportunities for strengthening cyber governance through inclusive and participatory approaches. Youth engagement, community-based digital awareness programs, and region-specific cybersecurity policies can transform socio-political sensitivity into a catalyst for resilience. Empowering local stakeholders and integrating socio-political awareness into cybersecurity frameworks can enhance trust, accountability, and institutional effectiveness.

In conclusion, the socio-political sensitivity of Jammu & Kashmir plays a Decisive role in shaping the cybersecurity landscape of the banking sector. Cyber threats in the region cannot be understood or addressed in isolation from their broader socio-political context. A comprehensive cybersecurity strategy must therefore integrate technological safeguards with ethical governance, social trust-building, and region-specific policy interventions. Recognizing and addressing socio-political sensitivity is essential for ensuring secure, inclusive, and sustainable digital banking systems in Jammu & Kashmir.

Digital Infrastructure Constraints and Cybersecurity Risks in the Banking Sector: Digital infrastructure forms the backbone of modern banking systems, enabling online transactions, mobile banking, digital payments, and real-time financial services. However, in regions such as Jammu & Kashmir, persistent digital infrastructure constraints significantly affect the security and reliability of banking operations. Limited internet connectivity, uneven network coverage, and dependence on fragile communication systems create structural vulnerabilities that increase cybersecurity risks for public and private banking institutions.One of the major challenges in the region is the lack of stable and high-speed internet access, particularly in remote and rural areas. Frequent network disruptions, low bandwidth availability, and reliance on outdated communication technologies hinder secure digital banking practices. Under such conditions, banks are often unable to maintain continuous cybersecurity monitoring, timely software updates, and real-time threat detection. These limitations weaken institutional defenses and provide opportunities for cyber attackers to exploit system gaps.Dependence on vulnerable communication networks further amplifies cybersecurity risks. When banking services operate on insecure or poorly protected networks, the probability of data interception, unauthorized access, and malware infiltration increases. Public Wi-Fi usage, shared network environments, and unsecured mobile connections expose customers to phishing attacks, identity theft, and financial fraud. Cybercriminals frequently target users in low-connectivity regions by exploiting their limited awareness of secure digital practices.Digital infrastructure constraints also affect incident response and recovery mechanisms. Inadequate connectivity delays reporting of cyber incidents, disrupts coordination between banks and regulatory authorities, and slows down containment efforts. In sensitive regions, where rapid response is critical, such delays can escalate the impact of cyber attacks, resulting in financial losses and erosion of public trust in digital banking systems.Moreover, inconsistent digital infrastructure impacts cybersecurity training and awareness initiatives. Limited access to reliable digital platforms restricts the reach of cyber awareness programs, especially among rural populations and small banking outlets. This digital divide creates an environment where users remain unaware of evolving cyber threats, ethical digital behavior, and safe online banking practices.In conclusion, digital infrastructure constraints in Jammu & Kashmir represent a critical challenge to effective cybersecurity in the banking sector. Addressing cyber threats in such regions requires not only technological upgrades but also investments in resilient digital infrastructure, secure communication networks, and inclusive connectivity. Strengthening digital infrastructure is essential for enhancing cyber resilience, protecting financial data, and ensuring secure and sustainable digital banking services in the region.

Digital Literacy and Awareness

A significant section of the population lacks adequate awareness of cyber hygiene, making them susceptible to phishing and fraud.Rapid Digital InclusionGovernment-led digital inclusion initiatives have expanded banking access, but cybersecurity preparedness has not grown at the same pace. Concept of Regional Taxonomy of Cyber ThreatsA regional taxonomy of cyber threats refers to the systematic classification of cyber risks based on region-specific characteristics. Unlike generic cybersecurity models, regional taxonomy considers: Local socio-political conditionsTechnological infrastructureUser behavior and awareness Governance and regulatory effectiveness such a taxonomy enables banks to prioritize threats and allocate resources effectively. Classification of Cyber Threats in J&K Banking Sector Phishing and Social Engineering Attacks Phishing remains the most prevalent cyber threat in J&K. Fraudulent messages, emails, and calls target customers and bank employees to extract confidential information. Malware and Ransomware Attacks Malware attacks compromise banking systems and customer devices, while ransomware disrupts services by encrypting critical data. Insider Threats Employees with authorized access may intentionally or unintentionally cause data breaches, posing a serious internal risk. ATM and Card-Based Frauds Skimming devices and card cloning incidents have been reported, particularly in semi-urban and rural areas.Mobile Banking and UPI Frauds With increased smartphone usage, mobile banking frauds have risen due to fake applications and weak authentication practices.Politically Motivated Cyber Attacks In J&K, some cyber incidents are influenced by ideological or political motives, targeting banking infrastructure to disrupt services.

Impact of Cyber Threats on Banking Institutions Cyber threats result in: Financial losses Loss of customer trustOperational disruptionsLegal and regulatory penalties Reputational damage

For banks in J&K, these impacts are magnified due to regional instability and limited recovery resources.Youth, Cyber Behavior, and Banking SecurityYouth play a crucial role in the cybersecurity ecosystem. While technologically skilled, lack of ethical awareness and exposure to cyber misuse can increase risks. At the same time, youth can act as cybersecurity ambassadors through awareness programs, ethical hacking initiatives, and digital governance participation.

Cyber Governance and Regulatory Challenges Effective cyber governance in J&K is challenged by: Inconsistent policy implementation Limited coordination between agenciesShortage of cybersecurity professionalsLack of region-specific frameworksStrengthening governance requires collaboration between banks, government agencies, and educational institutions.

Ethical Dimensions of Cyber Threats

Cyber crimes reflect not only technical failures but also ethical decline. Promoting ethical digital behavior through education and awareness is essential for long-term cybersecurity resilience.Role of Public and Private BanksPublic sector banks face challenges related to legacy systems, while private banks deal with advanced yet complex digital platforms. Both require region-specific cybersecurity strategies. Risk Mitigation Strategies Cyber awareness programs Strong authentication mechanismsRegular security audits Employee training Incident response planning Policy RecommendationsDevelopment of region-specific cybersecurity policiesIntegration of ethical digital educationStrengthening public-private partnershipsInvestment in local cybersecurity talentFindings of the Study The study finds that cyber threats in J&K banking are multidimensional, influenced by technological, social, political, and ethical factors. A regional taxonomy approach is essential for effective risk management.

Conclusion

The increasing digitization of the banking sector has undeniably transformed financial services in India by enhancing efficiency, accessibility, and inclusion. However, this transformation has also expanded the cyber threat landscape, making banks increasingly vulnerable to complex and evolving cyber risks. In conflict-affected and politically sensitive regions such as Jammu & Kashmir, these challenges become more pronounced due to unique regional, socio-political, infrastructural, and governance-related factors.This study has attempted to develop a regional taxonomy of cyber threats affecting public and private banking institutions in Jammu & Kashmir. By categorizing cyber threats based on their nature, origin, and impact, the research highlights that cybersecurity challenges in the region extend beyond conventional financial cyber crimes. Threats such as phishing, social engineering, malware attacks, insider threats, mobile banking frauds, and politically motivated cyber attacks are deeply influenced by regional vulnerabilities, limited digital awareness, and governance gaps.The findings of the study emphasize that cybersecurity in Jammu & Kashmir cannot be addressed solely through technological solutions. While advanced security tools and frameworks are essential, equal importance must be given to ethical governance, digital awareness, and human behavior, particularly among youth. Youth, as digital natives, occupy a dual position in the cyber ecosystem—they can either contribute to cyber vulnerabilities through unethical practices or serve as key agents of change by promoting ethical digital behavior, cybersecurity awareness, and participatory governance.The research further reveals that existing cybersecurity policies and regulatory frameworks often lack region-specific sensitivity. Uniform national-level cybersecurity strategies may not fully address the unique challenges faced by banking institutions in Jammu & Kashmir.

Therefore, the study strongly advocates the development of region-specific cybersecurity policies, strengthened public–private collaboration, and localized capacity-building initiatives to enhance cyber resilience.Moreover, the study underlines the critical role of ethical education and cyber governance in mitigating long-term cyber risks. Cyber crimes are not merely technical failures but reflections of ethical erosion in the digital space. Integrating ethical values, digital responsibility, and cybersecurity education into academic and institutional frameworks can significantly contribute to sustainable cyber risk mitigation.In conclusion, this research establishes that a regional taxonomy-based approach provides a comprehensive and structured understanding of cyber threats in the banking sector of Jammu & Kashmir. Strengthening cybersecurity in the region requires a holistic strategy that combines technological safeguards, ethical governance, youth

participation, and inclusive policy implementation. Such an integrated approach can not only protect banking institutions from cyber threats but also contribute to national security, economic stability, and public trust in the digital financial ecosystem.

References

1. Reserve Bank of India – Cyber Security Framework for Banks
2. Government of India – Digital India Initiative
3. National Cyber Security Policy, India
4. Academic Journals on Cybersecurity and Banking