International Journal of Advanced Science and Research
www.allsciencejournal.com
ISSN: 2455-4227
Received: 20-11-2025, Accepted: 25-12-2025, Published: 10-01-2026
Volume 11, Issue 1, 2026, Page No. 22-24

A systematic review of cybersecurity threats in the banking sector

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

Abstract
The rapid digital transformation of the banking sector has significantly enhanced financial accessibility, operational efficiency, and customer convenience worldwide. However, this transformation has simultaneously expanded the cybersecurity threat landscape, exposing banking institutions to sophisticated and evolving cyber risks. Cyber attacks on banking systems have emerged as a major challenge, affecting financial stability, customer trust, and national economic security. This research paper presents a systematic review of cybersecurity threats in the banking sector, with a focus on identifying key threat categories, attack vectors, and governance challenges. The study systematically analyzes existing literature, policy documents, cybersecurity reports, and academic research to classify major cyber threats such as phishing, malware, ransomware, insider threats, identity theft, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs). The review highlights the increasing role of human behavior, ethical erosion, and governance gaps in amplifying cybersecurity risks. The paper further emphasizes the need for integrated cybersecurity strategies combining technological safeguards, ethical governance, regulatory frameworks, and awareness initiatives. The findings of this study contribute to a comprehensive understanding of cybersecurity challenges in the banking sector and provide valuable insights for policymakers, financial institutions, and researchers. The paper concludes by emphasizing the importance of proactive cybersecurity governance and continuous risk assessment to ensure the resilience and sustainability of digital banking systems.

Keywords: Cybersecurity, banking sector, cyber threats, digital, banking, risk management, information security, governance

Introduction

The banking sector has undergone a profound transformation due to rapid advancements in information and communication technologies. Digital banking platforms, mobile banking applications, online payment systems, and electronic financial services have revolutionized traditional banking operations. These innovations have improved efficiency, reduced operational costs, and expanded financial inclusion. However, increased reliance on digital technologies has also exposed the banking sector to complex cybersecurity threats. Cybersecurity has become a critical concern for financial institutions due to the sensitive nature of financial data and the high financial incentives for cybercriminals. Banking systems store vast amounts of confidential customer information, including personal identities, transaction records, and financial credentials. Any compromise of such information can result in financial loss, reputational damage, and erosion of public trust. In recent years, cyber attacks targeting banks have grown in frequency, sophistication, and scale. Cybercriminals increasingly use advanced techniques such as social engineering, malware injection, ransomware attacks, and coordinated cyber campaigns. The interconnected nature of financial networks further amplifies the impact of cyber incidents, making cybersecurity a matter of national and global importance.

This research paper aims to systematically review existing studies on cybersecurity threats in the banking sector to identify prevailing threat patterns, vulnerabilities, and mitigation challenges. By synthesizing current knowledge, the study seeks to provide a structured understanding of cyber risks and support the development of effective cybersecurity strategies.

Research Objectives: The primary objectives of this systematic review are:

- To identify major cybersecurity threats affecting the banking sector.
- To classify cyber threats based on their nature, origin, and impact.
- To analyze technological, human, and governance-related vulnerabilities in banking systems.
- To examine existing cybersecurity frameworks and mitigation strategies.
- To highlight research gaps and future directions in banking cybersecurity.

Research Methodology

This study adopts a systematic literature review methodology, which ensures a structured, transparent, and comprehensive analysis of existing research. Secondary data has been collected from peer-reviewed journals, conference proceedings, government publications, cybersecurity reports, and banking sector studies. The review process involved the following steps:Identification of relevant databases and sourcesSelection of keywords such as cybersecurity threats, banking cyber attacks, digital banking risks, and information securityScreening of studies based on relevance, credibility, and publication qualityCategorization of cyber threats and vulnerabilities Thematic analysis and synthesis of findingsThis methodology enables a comprehensive understanding of cybersecurity challenges while ensuring academic rigor and reliability.

Overview of Cybersecurity in the Banking Sector

Cybersecurity in the banking sector encompasses the protection of digital assets, financial data, customer information, and transaction systems from unauthorized access, attacks, and misuse. Banks rely on complex IT infrastructures, including core banking systems, cloud platforms, and digital interfaces, which require robust

security mechanisms. Despite advancements in security technologies, banks remain attractive targets for cybercriminals due to high financial rewards and the critical nature of banking operations. Cybersecurity in banking is therefore not limited to technical controls but also includes governance policies, regulatory compliance, employee training, and ethical responsibility.

Classification of Cybersecurity Threats in the Banking Sector

Phishing and Social Engineering AttacksPhishing attacks involve deceptive communication techniques used to manipulate individuals into revealing sensitive information such as passwords, PINs, and account details. Social engineering exploits human psychology rather than technical vulnerabilities, making it one of the most effective cyber attack methods. Malware and Ransomware Attacks Malware attacks involve malicious software designed to infiltrate banking systems, steal data, or disrupt operations. Ransomware encrypts critical data and demands payment for its release, posing serious operational and financial risks.

Insider Threats

Insider threats originate from employees or authorized individuals who misuse their access privileges intentionally or unintentionally. Such threats are difficult to detect and can result in significant data breaches.

Governance and Ethical Challenges in Banking Cybersecurity

Cybersecurity threats are not solely technical issues; they reflect broader governance and ethical challenges. Weak regulatory enforcement, lack of ethical awareness, and insufficient accountability mechanisms increase the vulnerability of banking institutions. Ethical erosion in digital practices contributes to irresponsible behavior, increasing cyber risks.

Impact of Cyber Attacks on the Banking Sector

Cyber attacks have far-reaching consequences for the banking sector, affecting not only financial assets but also institutional credibility, customer trust, and national economic stability. As banks increasingly rely on digital platforms, cyber incidents can disrupt core banking operations, payment systems, and customer services. Even a single successful cyber attack may result in large-scale financial losses and long-term reputational damage. One of the most immediate impacts of cyber attacks is financial loss. Fraudulent transactions, ransomware payments, system recovery costs, and legal penalties impose significant financial burdens on banking institutions. In addition, cyber incidents often require banks to invest heavily in forensic investigations, system upgrades, and cybersecurity audits, increasing operational costs. Cyber attacks also lead to erosion of customer trust, which is particularly damaging in the banking sector where trust is fundamental. Data breaches involving personal and financialinformation reduce customers' confidence in digital banking platforms and discourage the adoption of online financial services. Loss of trust can result in customer attrition and long-term reputational harm. At a broader level, cyber attacks pose risks to financial stability and national security. Disruption of banking services can affect payment systems, credit availability, and economic activities. In extreme cases, coordinated cyber attacks may undermine confidence in the financial system and create systemic risks. Therefore, cybersecurity in banking is not merely an organizational concern but a matter of public interest.

Human Factors and Ethical Dimensions of Cyber Threats

While technological vulnerabilities are significant, human behavior remains one of the most critical factors contributing to cybersecurity threats in the banking sector. Employees, customers, and third-party service providers often become the weakest links in the cybersecurity chain due to lack of awareness, negligence, or unethical behavior. Phishing and social engineering attacks primarily exploit human psychology rather than system weaknesses. Employees may unknowingly disclose credentials, click malicious links, or fall victim to fraudulent communications. Similarly, customers with limited cyber awareness are more susceptible to online fraud and identity theft. Ethical decline in the digital environment further intensifies cyber risks. Unethical practices such as misuse of access privileges, data manipulation, and lack of accountability increase internal vulnerabilities. The absence of strong ethical culture within organizations can normalize risky behavior and weaken cybersecurity governance. Promoting ethical responsibility, transparency, and digital discipline among employees and users is therefore essential. Ethical training and awareness programs play a crucial role in strengthening the human firewall against cyber threats.

Cyber Laws and Regulatory

Frameworks in the Banking SectorLegal and regulatory frameworks play a vital role in shaping cybersecurity practices in the banking sector. Governments and regulatory authorities have introduced various cyber laws, data protection regulations, and compliance standards to address cyber risks. These frameworks aim to ensure data confidentiality, system integrity, and accountability. Despite the presence of regulatory mechanisms, enforcement challenges remain. Rapid technological advancements often outpace legal frameworks, creating regulatory gaps. Inconsistent implementation, lack of coordination among agencies, and limited institutional capacity further weaken regulatory effectiveness.

Banks are required to comply with multiple regulations related to data protection, cyber incident reporting, and risk management. However, compliance alone is insufficient without proactive cybersecurity governance. Strengthening cyber laws, improving enforcement mechanisms, and promoting regulatory harmonization are essential for effective risk mitigation.

Emerging Technologies and Future Cybersecurity Challenges

Emerging technologies such as artificial intelligence, cloud computing, blockchain, and the Internet of Things are reshaping the banking sector. While these technologies offer efficiency and innovation, they also introduce new cybersecurity challenges. Artificial intelligence can be misused for automated cyber attacks, deepfake frauds, and sophisticated phishing campaigns. Cloud-based banking systems raise concerns related to data privacy, shared responsibility, and cross-border data security. As technology evolves, cyber threats are likely to become more complex

and difficult to detect. Banks must therefore adopt adaptive and forward-looking cybersecurity strategies. Continuous risk assessment, investment in advanced security tools, and collaboration with cybersecurity experts are essential to address future threats.

Discussion

The systematic review reveals that cybersecurity threats in the banking sector are multidimensional, involving technological, human, ethical, and governance-related factors. While technological safeguards are necessary, they are insufficient in isolation. Human behavior, ethical awareness, and institutional governance play equally important roles in determining cybersecurity resilience. The findings highlight the need for an integrated approach that combines technical security measures with ethical governance, regulatory compliance, and continuous awareness programs. Addressing cybersecurity challenges requires collaboration among banks, policymakers, regulators, and society at large.

Conclusion

Cybersecurity threats pose a serious challenge to the stability and sustainability of the banking sector in the digital era. This systematic review has identified key threat categories, vulnerabilities, and governance gaps affecting banking institutions. The study emphasizes that cybersecurity is not solely a technical issue but a socio-technical and ethical challenge. Strengthening cybersecurity in banking requires a holistic strategy that integrates technology, human awareness, ethical responsibility, and effective governance. Proactive policies, ethical digital practices, and continuous capacity building are essential to ensure secure and resilient banking systems.

Future Scope of Research

Future research may focus on region-specific cybersecurity challenges, the role of artificial intelligence in cyber defense, and the effectiveness of ethical education in reducing cyber risks. Empirical studies and comparative analyses can further enrich understanding and support evidence-based policymaking.

References

1. Anderson R, Barton C, Böhme R, Clayton R, van Eeten M, Levi M, *et al*. Measuring the cost of cybercrime. Journal of Cybersecurity,2019:5(1):1–17. https://doi.org/10.1093/cybsec/tyz003
2. Basel Committee on Banking Supervision. Principles for operational resilience. Bank for International Settlements, 2021.
3. ENISA. Threat landscape for the financial sector. European Union Agency for Cybersecurity, 2022.
4. Kshetri N. Cybersecurity management: An organizational and strategic approach. University of Toronto Press, 2021.
5. Maurushat A. Cybersecurity and human rights. Edward Elgar Publishing, 2018.
6. National Institute of Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce, 2020.
7. OECD. Digital security risk management for economic and social prosperity. OECD Publishing, 2020.
8. Reserve Bank of India. Cyber security framework in banks. RBI Publications, 2022.
9. Sharma S, Gupta J. Cyber threats and security challenges in the Indian banking sector. International Journal of Information Security Science,2020:9(2):45–58.
10. World Economic Forum. Global cybersecurity outlook. World Economic Forum, 2023.