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

A paradigm shift of Cyber security Management in Indian Banks since 2015: A Critical analysis on Literature Review

Ms. Smitha Ramachandran[1], Dr. Babu Vinothkumar Y[2]

[1]Assistant Professor, School of Management Studies, Palakkad, University of Calicut
[2]Associate Professor, Department of Management Studies and Research, Coimbatore Institute of Management and Technology, Coimbatore 641109

Abstract

Indian banks had witnessed a major shift in its operations since a decade. With the advent of digital revolution, the banking sector has witnessed a massive change from its traditional mode of operations. The rise in the usage of digital banking and the vulnerabilities of the digital banking system has exposed the system into witnessing a rise of cyber threats. A well-equipped system for prevention of cybersecurity in Banks is still a challenge.

This paper tries to study about the paradigm shift the Indian banks have adopted in the management of cyber treats and attacks based on the published research papers, articles and writings. A critical analysis of the relevant articles is done. The common threat factors and the area where the focus for threat management has been identified. The strategies to be adopted so as to minimise the risk is brought out after the analysis. Some strategic recommendation based on the findings is provided

Keywords: Cybersecurity, Banking, Cyber fraud, digital banking, Cyber threat

1. Introduction

Indian banks had witnessed a major shift in its operations since a decade. With the advent of digital revolution, the banking sector has witnessed a massive change from its traditional mode of operations. Earlier the banking industry focussed much on relationship banking, the modern era is focussing on the ease of doing business with the help of technology at the same time giving importance to customer satisfaction too. The traditional way of banking operations have given way for the digitised era.

Earlier the Indian banking industry was dominated by manpower but slowly it is giving way to AI & ML. The transition of banking industry in using chatbots and other AI tools is significantly slow compared to other service industry

The digital revolution with it has brought about numerous benefits but at the same time a major threat in the form of security issue has risen.

This paper aims to have a look into various literature on how the nature of cyber frauds have changed and the various factors contributing to the cyber security and the technological advances that are employed for the management of cyber security.

Articles in the relevant area is collected for past ten years. These articles are reviewed and analysed critically to find out the various contributing factors for cyber frauds and how equipped Indian banks are to fight against these frauds.

The changing nature of banking operations, the use and high dependency on technology and lack of digital awareness is making it difficult for the banks to handle the customers and build trust.

- How have the cyber security management changed over the past decade?
- What were the contributing factors for the cyber frauds?
- Is the technology helpful in managing the crime?
- Steps needed in improving the cyber security management in Indian banking industry
- The relevance on AI and ML in cyber security management and how effectively it is used to manage cyber threat

The researcher has collected relevant literatures/articles related to cyber security management in Indian banking industry. The articles reviewed are from the period 2015-2025 which are published in various journals.

The details of the articles are given below:

Title	**Authors**	**Publication Details**
Perceived Risk Factors Influence on Intention to Continue Using Internet Banking among Malaysians	*Normalini Md Kassim & T. Ramayah*	JO - Global Business Review, Vol 16, 2015
Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation	*Ariana L. Johnson*	Banking Institute Journal > Vol. 20 (2016) > Iss. 1 North Carolina Banking Institute
Cyber Security Management Model For Critical Infrastructure	*Limba, Tadas Plėta, Tomas Agafonov, Konstantin Damkus, Martynas*	June 2017 Journal of Entrepreneurship and Sustainability Issues 4(4):559-573
Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator	*Artie W. Ng and Benny K.B. Kwok*	JO - Journal of Financial Regulation and Compliance, Vol 25, 2017
Regulation of Cyber Security In The Banking Sector	*Ludek Novak, Petr Doucek*	Pg49-54, https://idimt.org/wp-content/uploads/proceedings/IDIMT_proceedings_2017.pdf
Data Protection As A Part Of Cyber Security	*Jan Capek*	Pg 289-296 https://idimt.org/wp-content/uploads/proceedings/IDIMT_proceedings_2017.pdf
CyberSecurity in Banks	*Burra Butchi Babu*	Pg 26-32 , The Journal of Indian Institute of Banking & Finance Jan – March 2018 VOl 89/No 1

		https://www.iibf.org.in/documents/BankQuest/Bank-Quest-Jan-Mar-2018-Final-200418.pdf
The Cyber Threat Landscape: Confronting Challenges to the Financial System	*Adrian Nish and Saher Naumann*	Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #3, 2019 https://carnegieendowment.org/files/02_19_Nish_Naumaan_Fin_Threats_final.pdf
Government regulations in cyber security: Framework, standards and recommendations	*Jangirala Srinivas, Ashok Kumar Das, Neeraj Kumar*	Future Generation Computer Systems 92 (2019) 178–188 Future Generation Computer Systems | Journal | ScienceDirect.com by Elsevier
The Times of Cyber Attacks	*Sakshi Singh, Suresh Kumar*	ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering [e–ISSN: 2067–3809] TOME XIII [2020] | FASCICULE 3 [July – September] https://acta.fih.upt.ro/pdf/2020-3/ACTA-2020-3-25.pdf
Cybersecurity in the Indian banking industry: Will 2020 redefine the cybersecurity ecosystem?	*Datta S, et.al*	https://www.deloitte.com/in/en/about/press-room/cybersecurity-in-the-indian-banking-industry-part-1.html
Assessing The Factors of Cybersecurity Awareness in the Banking Sector	*Adel Ismail Al-Alawi* *Sara Al-Bassam*	*AGJSR* 37 (4) 2019: 17-32 Adel Ismail Al-Alawi *et al* https://www.researchgate.net/publication/352855616_Assessing_The_Factors_of_Cybersecurity_Awareness_in_the_Banking_Sector
Artificial intelligence in cyber security: research advances, challenges, and opportunities	*Zhimin Zhang et al*	JO - Artificial Intelligence Review, vol 55,2022 https://www.researchgate.net/publication/350040089_Artificial_intelligence_in_cyber_security_research_advances_challenges_and_opportunities
Cyber Security Challenges in Indian Banks	*Kalpana Nayar, Priyanka Rathod*	Shodh Sarita, Quarterly Bilingual research Journal, Vol8 ,Issue 29, Jan-March 2021 https://vpmthane.org/jbcapp/upload/m6/496.pdf
Challenges of Digital Privacy in Banking Organizations	Okechukwu Innocent Ogudebe	Part of the Databases and Information Systems Commons

		https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=14936&context=dissertations
An Overview on Cyber Crime and Cyber Security	*Bhumika Tuli, Santosh Kumar and Neha Gautam*	Asian Journal of Engineering and Applied Technology, Vol 11,2022
Cyber Security and Internet Banking: Issues and Preventive Measures	*Leandre Gomes,Abhinav Deshmukh,Nilesh Balvant Anute*	Journal of Information Technology and Sciences www.matjournals.com e-ISSN: 2581-849X Volume-8, Issue-2 (May-August, 2022)
Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking	*Diptiben Ghelani, Tan Kian Hua, Surendra Kumar Reddy Koduru*	TY - BOOK https://www.researchgate.net/publication/363786499_Cyber_Security_Threats_Vulnerabilities_and_Security_Solutions_Models_in_Banking/link/637b6f6554eb5f547cf03da0/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation	*Amar Johri and Shailendra Kumar*	Hindawi Human Behavior and Emerging Technologies Volume 2023, Article ID 2103442, 10 pages
Fraud Prevention In Digital Payment Systems And Cybersecurity Education For Customers Of Nationalized Financial Institutions	*Kushwant Singh, et al.,*	TY - BOOK Virtual International Scientific Conference "Development Through Research And Innovation - 2023", IVth Edition, Pg no - 98 – 115
Industry 4.0 Adaption in Indian Banking Sector—A Review and Agenda for Future Research	*Gupta, R.*	Vision 27(1) 24–32, Feb 2023 https://journals.sagepub.com/doi/abs/10.1177/0972262921996829
Cyber Security of Banks in India	*Medicherla Sri Sivathmika et al*	International Journal of Enhanced Research in Management & Computer Applications ISSN: 2319-7471, Vol. 12 Issue 5, May, 2023,
Data privacy and cybersecurity challenges in the digital transformation of the banking sector	*Shuang Wang et al*	Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & Security, 147,

		104051. https://doi.org/10.1016/j.cose.2024.104051
Assessment of Cybersecurity Risks and threats on Banking and Financial Services	*Rami Shehab et. al*	Journal of Internet Services and Information Security (JISIS), volume: 14, number: 3 (August), pp. 167-190.
Risk Management in Commercial Banking Institutions: An Examination of the Cybersecurity Challenges for Commercial Banks in India: Recommendations for Guyana's Banking Sector	*La donna Delon*	Journal of Financial Risk Management, 2024, 13, 549-575
Cyber-Financial (Cy-Fi) Fraud in India: A Case Study of COVID-19 Induced Cybercrime in Mewat Region	*Kundan Kumar & Naresh Kumar Verma*	Journal of Asian and African Studies 00(0) 1–17, 2024
Cybersecurity in Banking: Threats, Solutions & Best Practices	*Claire dela Luna*	https://www.esecurityplanet.com/cloud/cyber-security-in-banking/
A critical review of emerging cybersecurity threats in financial technologies	*Uchenna Joseph Umoga et al*	International Journal of Science and Research Archive, 2024, 11(01), 1810–1817
Digital Risk and Financial Inclusion: Balance between Auxiliary Innovation and Protecting Digital Banking Customers	*Ahmed et al.*	TY - BOOK https://www.researchgate.net/publication/380034396_Digital_Risk_and_Financial_Inclusion_Balance_between_Auxiliary_Innovation_and_Protecting_Digital_Banking_Customers/link/6645baa80b0d28457436fd59/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
What Is Cyber Security Management?	*Anne Gomez*	https://www.ollusa.edu/blog/cyber-security-management.html#:~:text=By%20Anne%20Gomez,risks%20from%20sophisticated%20cyber%20threats.
Cybersecurity risks in online banking: A detailed review and	*Adedoyin Tolulope Oyewole et al*	World Journal of Advanced Research and Reviews, 2024, 21(03), 625–643

preventive strategies application		
Safeguarding India's Financial Infrastructure: Strategies and Techniques for Cybersecurity Risk Mitigation	*Dr. Amey Rajiv Naik and Dr. Trilok Singh*	International Journal of Engineering Applied Science and Management ISSN (Online): 2582-6948 Vol. 5 Issue 10, October 2024
A Study on Cyber Security Issues Affecting Online Banking and Transactions	*Vishnupriya et al*	Vol-9 Issue-6 2023 IJARIIE-ISSN(O)-2395-4396
Cybersecurity in Indian Banking: Addressing Emerging Threats and Solutions	*Ankita Mishra*	*IJALR, Vol. 5, Issue 3, Feb 2025*

2. Literature Review

(Normalini Md Kassim & T. Ramayah, 2015) Their study emphasise the need for banking institutions to refine security, usability and customer engagement strategies in terms of building trust and promoting perceived usefulness for the adoption of internet banking. Though the study was exclusively done in Malaysian banking industry, their findings can be generalised for the users of banking operations elsewhere.

(**Ariana L. Johnson 2016)** Financial institutions are prime targets for cybercriminals due to the sensitive and valuable data they hold. Threats are becoming more sophisticated, including phishing, ransomware, insider threats, and supply chain attacks. Regulators emphasize risk management, reporting, and continuous improvement of security postures. Cybersecurity is no longer just an IT concern but a core business issue. Boards and executives must integrate Cybersecurity into organizational strategy and governance. Regular security assessments, penetration testing, and employee training are crucial. Adoption of technologies like AI, machine learning, encryption, and multi-factor authentication. Stronger Cybersecurity frameworks, intelligence sharing, and regulatory alignment are crucial for FIs to protect against evolving cyber threats

(Tadas Limba, 2017) Cybersecurity is more than a technological issue. It is a strategic management issue. A Cybersecurity models with six dimension and each dimension with three level were proposed. The six dimension identified were Legal Regulation, Good Governance, Risk Management, Security Culture, Technology Management, Incident Management and the three level in each dimensions are initial, moderate and full integration. This model will helps in Reduce the impact of cyber-attacks, Improve internal security awareness and Enhance reputation and resilience

(Artie W. Ng & Benny K.B. Kwok ,2017) In Honkong's financial system, FinTech plays an important role but at the same time, the mass adoption of this system has brought with it the risk and security concerns. The need for real-time alerts and pattern analysis is to be adapted. Also fortification initiatives for Cybersecurity like the cyber resilience assessment, professional Development Program, cyber intelligence sharing platform have to be considered.

(Ludek Novak, Petr Doucek 2017) Regulatory compliance and risk prevention are interlinked. Must prepare for both known and emerging cyber threats using flexible, hybrid models. The need for a comprehensive cybersecurity strategy that includes employee training, awareness, and a strong organizational culture is emphasized.

(Jan Capek 2017) Information overload makes it difficult to protect data. Hence some of the proposed solution to protect data are Keyless Signature Infrastructure (KSI) and blockchain which offer decentralized, tamper-evident alternatives to secure data. Some of the Benefits of Blockchain are High data integrity, Decentralization, Scalable trust.

(Burra Butchi Babu, 2018) Coordination across banks, regulators and legal enforcement are essential and a necessity

(Adrian Nish and Saher Naumann, 2019) A significant incident from July 2016, where cyber attackers attempted to steal $150 million from banks in South Asia and West Africa, showcasing the potential for coordinated attacks across continents has been highlighted in the article. The changing landscape of cyber-attacks identified were Advanced Capabilities, Aggressive Disruption Tactics, and Collaboration among Criminals. Financial institutions must adopt collaborative approaches, simplify security measures, and proactively address the capabilities of cybercriminals to safeguard their operations and maintain public trust

(Jangirala Srinivas,et.al 2019) The essential cybersecurity requirements: Confidentiality, integrity, availability, Authentication (e.g., biometrics, smart cards), Authorization, Non-repudiation, Data freshness and Protection from physical theft. The authors also emphasises on Cybersecurity Incident Management Framework (CIMF) which helps to coordinate and manage cyber threats nationally. Also emphasizes public-private collaboration and defined responsibilities. The standardisation challenges faced by the banks are: rganizational fragmentation (e.g., multiple SDOs), Limited coverage of privacy in existing standards, Slow pace of standard development, Economic and proprietary pressures and lack of awareness among consumers and public sector. The document provides a comprehensive overview of cyber security, emphasizing the importance of standards, frameworks, and policies to safeguard digital systems against various cyber threats.

(Sakshi Singh, Suresh Kumar, 2020) Cybersecurity is a critical challenge in the digital era. Here the authors' project future cyber risks, including IoT vulnerabilities and cloud security concerns, and suggests designing future technologies with built-in security measures. It advocates for smart security solutions, including AI-driven continuous monitoring, encryption, and block-chain-based protection to mitigate threats. As threats evolve rapidly, both technological innovation and human awareness must keep pace. Strong governance, advanced tools, and proactive design are essential to protect sensitive data and critical infrastructure

(Datta S, et.al 2020) The study have identified strategies like leadership-driven prioritisation, strategic budgeting and a culture of continuous vigilance is to be proactively adopted by Indian banks to mitigate the risk of cyber threat

(Adel Ismail Al-Alawi and Sara Abdurrahman Al-Balsam 2021) The study identified that the key factors that contribute to Cybersecurity awareness were Top management commitment and support, budgeting for cyber security, Cybersecurity compliance and Cybersecurity culture

(Zhimin Zhang, 2021) Though AI significantly enhances cybersecurity through automation, precision, and scalability, along with decision transparency, data reliability, large data requirements and model vulnerabilities are to be addressed. The study proposes a conceptual human-in-the-loop cybersecurity model that integrates machine learning with human expertise to enhance security resilience. This approach aims to mitigate AI limitations and improve response accuracy against cyber threats.

(Kalpana Nayar, Priyanka Rathod 2021) The research paper focuses on how the shift towards digital banking after covid-19 and public awareness about the same. As the shift is towards the increasing usage

of digital banking, so is the cyber security challenges. The most commonly found threats are Low awareness among employees and customers, Inadequate budgets and lack of top management support, Poor identity and access management, Rise in ransomware attacks, mobile malware, and DDoS attacks, Exploitation via social media and mobile banking apps. Indian banks face a rising tide of cyber threats due to rapid digitization. There is an urgent need for enhanced awareness, rigid security practices, and strong regulatory frameworks to safeguard the financial ecosystem and public trust

(Okechukwu Innocent Ogudebe 2022) In his doctoral thesis have suggested the necessity of social change and its implication can reduce digital fraud affecting vulnerable groups (elderly, disabled, illiterate),Promotes a culture of cybersecurity among users and bank employees and enhances overall trust and security in digital banking systems.

(Bhumika Tuli, Santosh Kumar, Neha Gautam 2022) Cybersecurity measures like a) Technical Controls: COMSEC (communication security), network & information security, and emission and transmission protection. b) Operational Security (OPSEC): Identifying critical data, assessing risk, applying countermeasures. c) Cyber Risk Management: Managing threats (hackers), vulnerabilities (system flaws), and viruses (e.g., Melissa, Code Red) are to be taken to tackle the issue of cyber threats

(Leandre Gomes, Abhinav Deshmukh, and Nilesh Anute 2022) The study identifies the Prevalence of Cyber Threats: consistently highlight phishing, identity theft, and UPI/OTP fraud as common in Indian digital banking. The Awareness & Behaviour: Respondents show good awareness, but behavioural gaps (like not changing passwords) persist. Also suggests to have a Preventive Frameworks: Prior research stresses technical measures (2FA, antivirus) and education campaigns by banks. The importance of user awareness and robust security policies. Legal and technical measures are both essential. There's a notable gap in cyber literacy and behaviour among users.

(**Diptiben Ghelani, Tan Kian Hua, Surendra Kumar Reddy Koduru 2022)** With the adoption of technology by banking sector the data handled by them has become massive or in technology terms, it is the 'Big Data' we are dealing in the present day banking operations. With the high data handling the risk of cyber-attack is in the increase. Multi-layered dynamic approach, adopting hybrid approaches that combine machine learning, ontology-based security, and block-chain for robust banking cyber security. Denial-of- Service (DoS) attacks,Third-party Platform Risks, Advanced Persistent Threats (APTs) are in the rise.

(Amar Johri and Shailendra Kumar 2022) The study on the Customer Awareness towards Their Cybersecurity in the Kingdom of Saudi Arabia found that banks need to enhance their Cybersecurity policies and provide more comprehensive training to customers. Regular Cybersecurity awareness programs are essential to improve customer knowledge and satisfaction. The findings suggest that banks can achieve long-term sustainability by prioritizing Cybersecurity management.

(Kushwant Singh, et al., 2023) Digital banking usage is increasing worldwide. Phishing, malware, and data breaches are increasing day by day.

(Gupta, R., 2023) The efficiency of banking operations and reduction of cost is possible with the adoption of newer technologies like the AI-driven processes or Internet of Things (IoT) or cloud computing but at the same time Cybersecurity risks, regulatory hurdles, customer resistance is causing hurdles to the adoption of digital banking.

(Medicherla Sri Sivathmika et al 2023) Despite increasing digitization, many Indian banking customers remain unaware or negligent of basic Cybersecurity practices. There's an urgent need for personalized,

proactive, and educational interventions by banks and regulatory authorities to protect consumers from rising cyber threats.

(Shuang Wang, Muhammad Asif, Muhammad Farrukh Shahzad, Muhammad Ashfaq 2024) A study on the challenges, perceptions, and strategies related to data privacy and Cybersecurity with respect to Pakistani banking sector identified that though digital banking creates a competitive advantage adhering to regulatory compliance and building customer trust a challenging part. Meanwhile risk mitigation strategies like Robust Access Controls, Continuous Threat Monitoring, Employee Training, Compliance Governance, and Data Encryption have to be given importance.

(Rami Shehab et al. 2024) A systematic review of 35 literature related to the cyber threats have helped to identify that the malware attack is the common form of threat that is damaging and attacking frequently. Some of the models were also identified but they could not give a fool-proof security. The authors suggest that Effective strategies for mitigating cyber risks include sharing information between institutions, adopting best practices, and implementing robust security measures

(La donna Delon, 2024) in his article points out that India's outdated cyber laws and limited awareness among both employees and customers exacerbate Cybersecurity challenges. He advises for fostering public-private partnerships for better threat intelligence sharing

(Kundan Kumar & Naresh Kumar Verma 2024) Case of cyber-crime in Mewat region in India had pointed out Operational, Developmental, Institutional, Psychological, Technological issues.

(Claire dela Luna 2024) Cybersecurity is Critical for Banks for Customer Data Protection, Maintaining Trust, Regulatory Compliance, Preventing Financial Loss, Protecting Infrastructure, and Business Continuity. Some Effective Cybersecurity Solutions are Multi-Factor Authentication, End-to-End Encryption, AI-Powered Threat Detection, Zero Trust Architecture, Security Incident and Event Management (SIEM). Some of the Best Practices identified for Cybersecurity are Regular employee training on security protocols, conducting routine security audits to identify vulnerabilities, keeping software updated to close security gaps, implementing strong password policies, and developing a robust incident response plan. Increasing reliance on advanced technologies like AI, block chain, and quantum computing and stricter regulatory frameworks to enhance data protection and compliance are to be adopted by the banks.

(Uchenna Joseph Umoga et al, 2024) The paper reviews the evolving Cybersecurity challenges facing financial technologies (FinTech), emphasizing the urgency of addressing traditional and sophisticated cyber threats to safeguard financial systems. The study offers insights into technical vulnerabilities, human factors, and regulatory shortcomings that threaten FinTech ecosystems. Advanced and emerging threats identified were Ransomware, AI-driven attacks, and supply chain vulnerabilities and Cloud systems are particularly targeted, requiring hypervisor-level monitoring and defense mechanisms. Regulatory frameworks are often fragmented or outdated. There's a need for more cohesive and culturally aware Cybersecurity governance models. The future Calls for quantum-safe cryptography, blockchain security, and regulatory evolution. Emphasizes integration of AI, machine learning, and collaborative threat intelligence for proactive security.

(Ahmed et al. 2024) The research identifies five key factors influencing customer protection: authentication mechanisms, data privacy policies, encryption methods, information transparency, and responsiveness

(Anne Gomez 2024) The articles defines cyber security management as a systematic approach to protecting digital infrastructure from unauthorized access and cyber-attacks. It highlights key aspects such

as risk assessment, vulnerability management, incident response, and security awareness training to mitigate cyber threats. The types of cybersecurity management covers risk management, incident response, compliance enforcement, Security Operations Center (SOC) management, and Identity & Access Management (IAM). Organizations must adopt comprehensive security frameworks to protect their digital infrastructure effectively.

(Adedoyin Tolulope Oyewole et al. 2024) The study focusses on cybersecurity risks in online banking. Due to the increasing growth of digital banking, threats posed by cybercrimes are also on the rise. The current security framework was analysed with recent cyber incidents. It emphasises the need for dynamic cybersecurity strategies that integrate advanced technologies like Big Data analytics, AI, and continuous risk assessment. Also banks need to adopt holistic security approaches, combining regulatory compliance, employee awareness programs, and proactive monitoring. The study concludes that strengthening cybersecurity resilience requires strategic investments in technology, education, and cross-industry collaboration to protect financial assets and maintain customer trust.

(Dr. Amey Rajiv Naik, Dr. Trilok Singh 2024) The digitization of India's financial sector—including banking, insurance, and payment systems—has expanded operational efficiency but simultaneously heightened vulnerability to cyberattacks. These attacks can lead to data breaches, financial fraud, and loss of public trust. The confidentiality, integrity, and availability of customer data are now more critical than ever due to the large-scale handling of sensitive information. CERT-In (2022) and RBI (2020) have highlighted that the frequency and impact of such incidents are growing. The literature highlights the urgent need for a robust, multi-layered approach to cybersecurity in India's financial sector. Technological innovation, regulatory reform, and employee empowerment must work in tandem to build resilient institutions. While notable progress has been made, significant gaps persist in terms of legacy integration, regulatory compliance, and skilled manpower. Future efforts must focus on the scalable deployment of AI and blockchain technologies, while fostering a culture of continuous security awareness and adaptability.

(Vishnupriya et al. 2024) cybersecurity in online banking is a dynamic and multifaceted issue. While technological advancements like AI, blockchain, and cryptography hold promise for strengthening defenses, human awareness, regulatory compliance, and continuous institutional adaptation remain crucial. The literature consistently calls for an integrated approach combining advanced tools, legal safeguards, employee training, and public awareness to build a resilient digital financial ecosystem. Future studies should focus on practical implementations, consumer education, regulatory frameworks, and the evolving nature of cyber threats to improve the resilience of financial institutions. While technological defenses are essential, the literature underscores the importance of designing holistic frameworks that integrate user perception, behavioural motivation, and institutional support to mitigate cyber risks in online banking.

(Ankita Mishra 2025) The study examines the evolving cybersecurity landscape in India's banking sector, emphasizing the dual nature of digital transformation—enhancing accessibility and efficiency while exposing financial institutions to complex cyber threats. It states cybersecurity as both a technological and governance issue essential to financial stability and consumer protection. Sophisticated attacks now exploit legacy systems, third-party software, and integration gaps. Digital payment fraud has surged, with a fivefold increase in recent years and Global cybercrime trends amplify domestic vulnerabilities. The author recommends Modernizing cyber laws to address new threats, Creating centralized reporting portals and inter-agency task forces for incident response. More recommendations are about allocating more resources to RBI and enforcement bodies, Promoting advanced security

technologies (AI-driven detection, multi-factor authentication, block-chain), Conducting regular security audits, Fostering public-private national and international partnerships and Leading national digital literacy campaigns and improving transparency in banking security practices

3. Methodology

Data Collection

Articles are collected from published journals, magazines and websites.

Samples

Literature pertaining to ten years is collected. The no of articles in each year varies as the literature pertaining to the research questions are few in the earlier years.

Analysis

Critical analysis is applied to find out the parameters/factor used in cyber security management and Strategies applied by banks to manage cyber security and its impact on banking operations.

Analysis of literature/articles published in various journals and conference proceedings over a period of ten years i.e from 2015-2025 is taken for the study.

Articles appropriate to the research questions is taken and is limited to Indian context only. Review of these articles/literature gives a clear picture of the elements/factors presently adopted by the banks. How for the past decade the factors and the mechanism of cybersecurity management has changed. The no of articles for each year is not the same. This is due to the lack of articles pertaining to the research under question. Though there are numerous articles in the field of cyber security, the number are far more less when the area is limited to Banking industry. Further it is very much limited for the Indian context. This may be due the slower adoption of digital banking in India or research in this perspective may have just started picking up.

4. Critical Analysis

It can be seen that the no of articles appropriate for the research questions is increasing yearly. This can be due to the reason that banks may not have seriously thought about the cyber security issues and solutions earlier. Also there may be an occasional incident of security breaches in the earlier times and the no of digital users were also not high at that point of time.

The number of articles and case related to cyber frauds in banking sector is increasing day by day.

The key areas where the cyber-crime happens is operational, developmental, institutional, psychological, technical shown in figure1

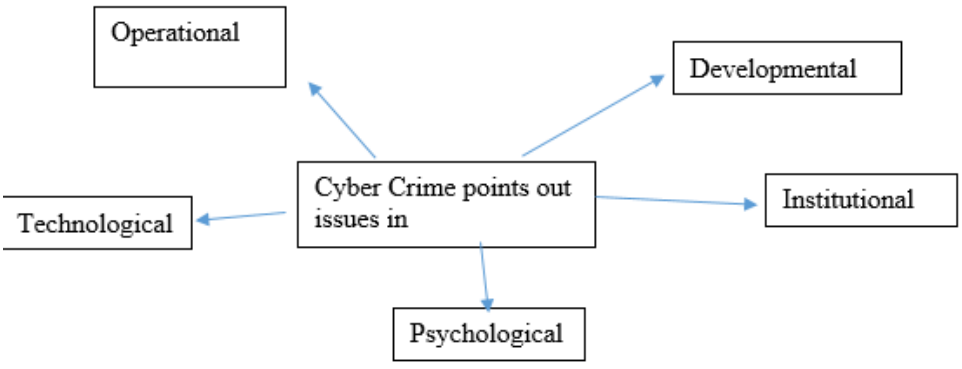


Figure 1: Areas of Cyber Crime in Banks

The most common factors that affect the cyber security are shown in figure 2

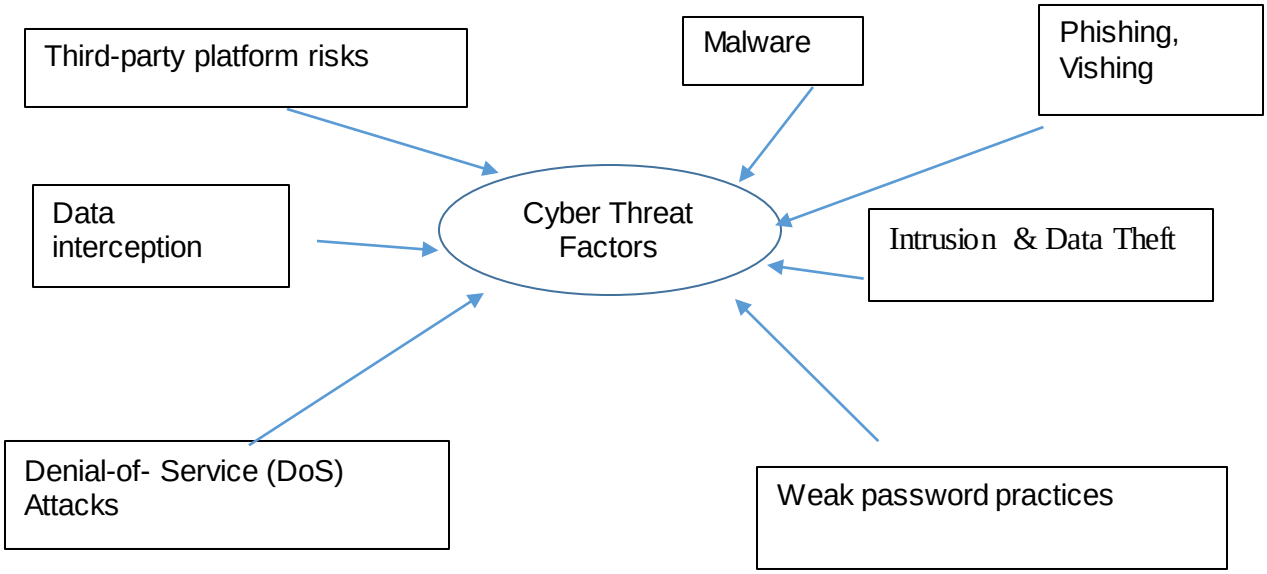


Figure 2: Cyber Threat Factors

Analysis of the literatures points out some of the cybersecurity strategies adopted by the banks. But strategies like the use of AI, Machine Learning, Block-chain technology are not fully implemented by the banks. Some of the banks are yet to embrace these technology. The most common strategy applied by the banks are Multi-factor authentication, training employees.

Customer awareness are mainly done through text messages or whatsApp messages. But how far this is successful is a question and studies have to be conducted in this area.

Some of the strategies presently adopted by the banks and to be implemented are depicted in figure 3

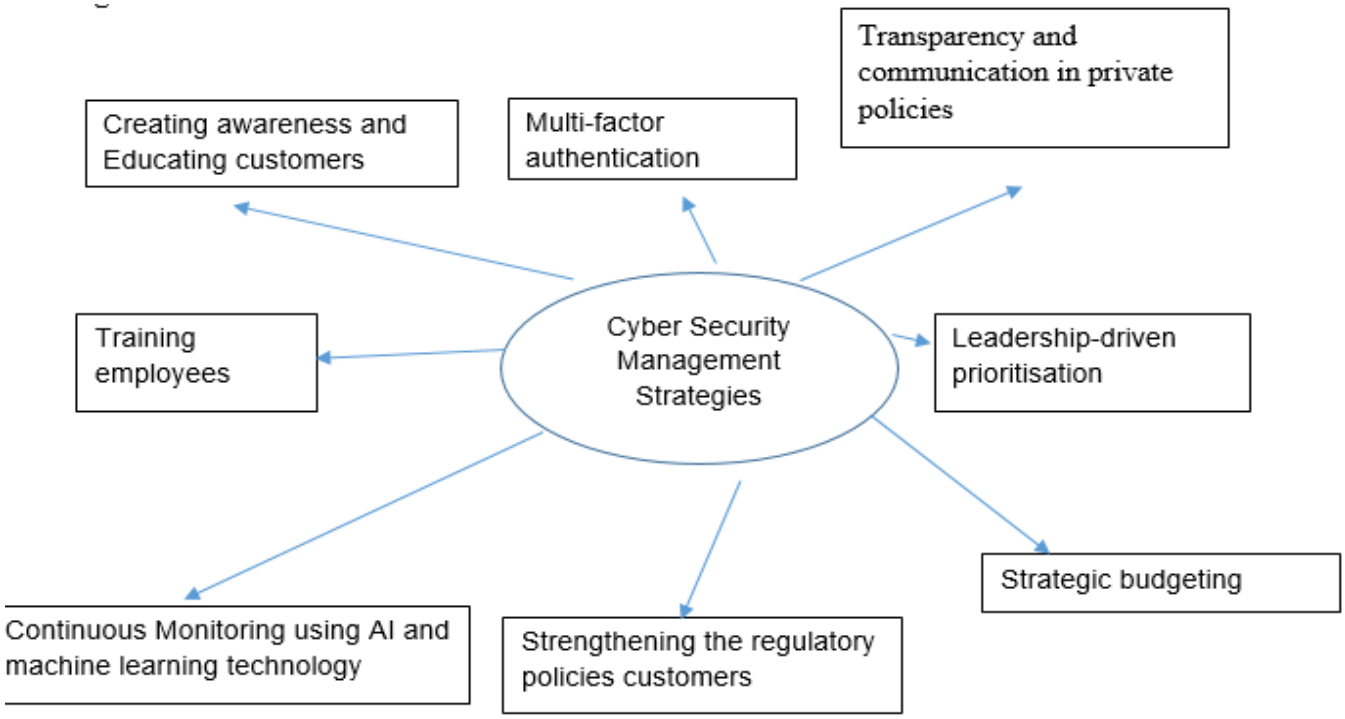
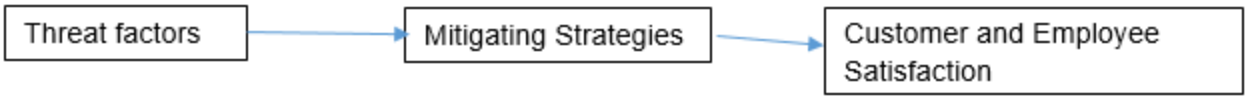


Figure 3: Cyber Security Management Strategies

A model can be drafted from these analysis where the input factors can be threat factors and the relevant mitigating strategies like the adoption and adaptation of newer stronger technologies, polices and regulations ultimately giving the customer and employee satisfaction



5. Findings and Suggestions

It can be seen that the security measures adopted by banks are exponentially increasing within no time. This may be due to the growing number of digital banking users. Associated with the increasing use of digital banking, the no of frauds are also in the rise.

Some of the most common threat factors are phishing and Malware, though data theft and third-party platform risks are in the rise. Weak password policies were another factor of threat but this is being replaced by strong password policies and second factor authentication by the banks.

Analysis have shown the areas where the cyber frauds are happening. It includes Operational, Developmental, Institutional, Psychological and Technological area. This points out that emphasise should be given to the said areas for cyber protection and prevent the frauds. Strategies in the respective areas like policy framing and implementation, employee training, customer awareness, adopting newer technologies like Block-chain, AI & ML tools

6. Conclusion

The nature of banking operations from personal trust building to the virtual mode is rising in all parts of the world. The concept of brick and mortar and human factor is being slowly replaced by various technologies for the day-to-day operations in banking industry.

With the rise of adoption of digital banking, the cyber frauds are also increasing. Banks along with the government have to adopt best practices in mitigating the risk associated with the cyber threats.

The paper shows the analysis of various published articles, research papers and writings about the cyber security management in Indian Banks. The critical analysis points out the major areas where the emphasis has to be given for prevention of cyber frauds and ensuring the smooth operations of digital banking.

The common threat factors and the implemented strategies are also discussed. The author points out the need of adopting and adapting to the newer technologies for mitigating the cyber threat in Indian banking sector.

References

1. Kassim, N. M., & Ramayah, T. (2015). Perceived risk factors influence on intention to continue using internet banking among Malaysians. *Global Business Review*, *16*(3), 393-414.
2. Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. *North Carolina Banking Institute, 20*, 277–306.
3. Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues, 4*(4), 559–573.
4. Ng, A., & Kwok, B. (2017). Emergence of fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance, 25*(4)
5. Novák, L., & Doucek, P. (2017). Regulation of cyber security in the banking sector. In *IDIMT-2017 Digitalization in Management, Society and Economy* (pp. 49–54)

6. Čapek, J. (2017). Data protection as a part of cyber security. In *IDIMT-2017 Digitalization in Management, Society and Economy: 25th Interdisciplinary Information Management Talks* (pp. 289–296)
7. Babu, B. B. (2018). Cybersecurity in banks. *The Journal of Indian Institute of Banking & Finance, 89*(1), 26–32.
8. Nish, A., & Naumann, S. (2019). The cyber threat landscape: Confronting challenges to the financial system. *Cyber Policy Initiative Working Paper Series: Cybersecurity and the Financial System* (No. 3). Carnegie Endowment for International Peace.
9. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178–188
10. Singh, S., & Kumar, S. (2020). The times of cyber attacks. *Acta Technica Corviniensis – Bulletin of Engineering, 13*(3), July–September.
11. Deloitte. (2020). Cybersecurity in the Indian banking industry: Part 1 – Will 2020 redefine the cybersecurity ecosystem? Retrieved from https://www.deloitte.com/in/en/about/press-room/cybersecurity-in-the-indian-banking-industry-part-1.html
12. Al-Alawi, A. I., & Al-Bassam, S. (2019). Assessing the factors of cybersecurity awareness in the banking sector. *Arab Gulf Journal of Scientific Research, 37*(4), 17–32.
13. Zhang, Z., et al. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review, 55*, 1–30.
14. Nayar, K., & Rathod, P. (2021). Cyber security challenges in Indian banks. *Shodh Sarita: Quarterly Bilingual Research Journal, 8*(29), January–March
15. Ogudebe, O. I. (2022). *Challenges of digital privacy in banking organizations* (Doctoral dissertation, Walden University). Walden Dissertations and Doctoral Studies, 13665.
16. Tuli, B., Kumar, S., & Gautam, N. (2022). An overview on cyber crime and cyber security. *Asian Journal of Engineering and Applied Technology, 11*(1), 36–45.
17. Gomes, L., Deshmukh, A., & Anute, N. B. (2022). Cyber security and internet banking: Issues and preventive measures. *Journal of Information Technology and Sciences, 8*(2), May–August. e-ISSN: 2581-849X.
18. Ghelani, D., Hua, T., & Koduru, S. K. R. (2022). *Cyber security threats, vulnerabilities, and security solutions models in banking*. Advance preprint.
19. Johri, A., & Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Human Behavior and Emerging Technologies, 2023*, Article ID 2103442, 10 pages. Hindawi.
20. Singh, K., Mistrean, L., Singh, Y., Dhwaj, D., & Parashar, A. (2024). *Fraud prevention in digital payment systems and cybersecurity education for customers of nationalized financial institutions*
21. Gupta, R. (2021). Industry 4.0 adaption in Indian banking sector—A review and agenda for future research. *Vision: The Journal of Business Perspective, 27*(1), 97–109.
22. Sri Sivathmika, M., Satyanarayana, J. V., & Manogna, J. S. (2023). Cyber security of banks in India. *International Journal of Enhanced Research in Management & Computer Applications, 12*(5), 34–41. ISSN: 2319-7471.
23. Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security, 147*
24. Shehab, R., et al. (2023). Assessment of cybersecurity risks and threats on banking and financial serv-

ices. *Journal of Internet Services and Information Security, 14(3)*

25. Delon, L. (2024). Risk management in commercial banking institutions: An examination of the cybersecurity challenges for commercial banks in India: Recommendations for Guyana's banking sector. *Journal of Financial Risk Management, 13,* 549–575.
26. Kumar, K., & Verma, N. K. (2024). Cyber-financial (Cy-Fi) fraud in India: A case study of COVID-19 induced cybercrime in Mewat region. *Journal of Asian and African Studies, 00*(0), 1–17.
27. dela Luna, C. (2024, September 13). Cybersecurity in banking: Threats, solutions & best practices. *eSecurity Planet*. https://www.esecurityplanet.com/cloud/cyber-security-in-banking
28. Umoga, U. J., et al. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive, 11*
29. Ahmed, F., Hussain, A., Khan, S., Malik, A., Asim, M., Ahmad, S., & Elaffendi, M. (2024). *Digital risk and financial inclusion: Balance between auxiliary innovation and protecting digital banking customers*
30. Gomez, A. (2024, April 9). What is cyber security management? *Our Lady of the Lake University Blog*. https://www.ollusa.edu/blog/cyber-security-management.html
31. Oyewole, A. T., et al. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews, 21*(3), 625–643.
32. Naik, A. R., & Singh, T. (2024). Safeguarding India's financial infrastructure: Strategies and techniques for cybersecurity risk mitigation. *International Journal of Engineering Applied Science and Management, 5*(10), 1–26. ISSN 2582-6948.
33. Vishnupriya, et al. (2023). A study on cyber security issues affecting online banking and transactions. *International Journal of Advance Research and Innovative Ideas in Education (IJARIIE), 9*(6), 2395–4396.
34. Mishra, A. (2025). Cybersecurity in Indian banking: Addressing emerging threats and solutions. *International Journal of Advanced Legal Research (IJALR), 5*(3), 1–15.