

A survey of cybersecurity threats and countermeasures in the Indian financial sector

Mohit Tiwari [†]

*Department of Computer Science and Engineering
Bharati Vidyapeeth's College of Engineering
New Delhi
India*

Abhishek Gandhar ^{*}

Shashi Gandhar [§]

*Department of Electrical and Electronics Engineering
Bharati Vidyapeeth's College of Engineering
New Delhi
India*

Shashi Bhushan Kumar [‡]

*Department of Electronics and Communication Engineering
Bharati Vidyapeeth's College of Engineering
New Delhi
India*

Arvind Rehalia [@]

Prakhar Priyadarshi [#]

*Department of Information Technology
Bharati Vidyapeeth's College of Engineering
New Delhi
India*

[†] E-mail: mohit.tiwari@bharativedyapeeth.edu

^{*} E-mail: abhishek.gandhar@bharativedyapeeth.edu (Corresponding Author)

[§] E-mail: shashi.gandhar@bharativedyapeeth.edu

[‡] E-mail: sbkumar2010@gmail.com

[@] E-mail: rehaliaarvind@gmail.com

[#] E-mail: prakharpriya@gmail.com

Sunil Gupta [§]

*Department of Electrical Engineering
Maharaja Surajmal Institute of Technology
New Delhi
India*

Abstract

This research paper delves into the realm of cybersecurity threats and countermeasures within the Indian financial sector, a domain increasingly susceptible to cyber attacks due to rapid digitalization. The primary objective of this study is to assess the current state of cybersecurity awareness, the effectiveness of existing countermeasures, and to identify potential gaps in the cybersecurity framework of the Indian financial sector. Employing a structured questionnaire, data was collected from 750 respondents across various demographics including financial analysts, IT professionals, and banking employees, utilizing stratified random sampling techniques. The analysis involved frequency count, percentages, and cross-tabulation to interpret the complex interplay between demographic factors and cybersecurity aspects.

The study highlights the importance of continuous adaptation in cybersecurity measures and advocates for enhanced training programs and policy enforcement.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Cybersecurity, Financial sector, India, Cyber threats, Cybersecurity awareness, Cyber defense strategies.

1. Introduction

The Indian financial sector, a pivotal component of the nation's economy, is increasingly vulnerable to cybersecurity threats, necessitating a thorough understanding and robust countermeasures. Cyber-attacks in the banking sector have become more sophisticated, posing significant risks to financial stability and security (Gulyas & Kiss, 2022). The evolution of digital banking has escalated these vulnerabilities, with cyber criminals exploiting technological advancements (Haruna, Aremu, & Modupe, 2022).

The cyber-attacks, ranging from data breaches to ransomware attacks have raised concerns about the preparedness and resilience of banks against such threats (Hess, 2022). Furthermore, the rise in online banking and digital transactions, especially post-pandemic, has expanded the attack surface for cyber criminals (Tsvetanova & Stefanova, 2022). However,

[§] E-mail: prakharpriya@gmail.com

the effectiveness of these strategies is still a matter of study and improvement (Patidar & Sen, 2022).

The intersection of finance and technology, while beneficial in many aspects, also opens new avenues for cyber-attacks (Kaur, Habibi Lashkari, & Habibi Lashkari, 2021). (Alimzhanova 2023) emphasizes the need for a robust cybersecurity framework that is capable of not defending against current threats.

In summary, the Indian financial sector faces a complex and evolving landscape of cybersecurity threats. These range from traditional banking system attacks to newer challenges posed by digital banking and FinTech integrations. This research aims to survey these threats and explore effective countermeasures, contributing to the enhancement of cybersecurity in the Indian financial sector.

2. Literature Review

The literature on cybersecurity in the Indian financial sector is vast and evolving, reflecting the dynamic nature of the field..

Gomes, Deshmukh, & Anute (2022), discuss the vulnerabilities and preventive strategies specific to internet banking.

Patidar & Sen (2022) have offered insights into the defensive mechanisms employed by Indian banks.

Hess (2022), critically examines the nature and impact of cybercrimes in the Indian banking sector.

Gulyas & Kiss (2022) explore the broader comparative analysis of Cybersecurity threats in the banking sector and global cybersecurity trends.

Singh, Kaur, & Chaoudhary (2022) address “Standards and Security in Information Calling through Internet Banking,” underscoring the necessity of standardized security protocols in digital banking.

Ramesh, Toshniwal, Sapra, & Dhanuka (2018) delve into the security aspects of FinTech, a rapidly growing domain within the financial sector.

Almansi (2018) provides a comprehensive overview of regulatory and supervisory frameworks governing cybersecurity in the financial sector.

Warren, Kaivanto, & Prince (2018) examine the systemic impact of cyber-attacks on the financial sector in their paper.

Despite the extensive research on cybersecurity threats and defensive strategies in the Indian financial sector, there is a noticeable gap in understanding the real-world effectiveness of these strategies when

applied within the diverse and evolving landscape of Indian banking and FinTech. Existing literature primarily focuses on theoretical frameworks, types of cyber threats, and general defensive strategies, but lacks a comprehensive evaluation of these strategies’ effectiveness in the context of India’s unique financial ecosystem.

3. Research Methodology

3.1 Data Collection Source

Table 1
Data Collection Source

Element	Description
Sample Size	750 respondents
Source of Data	Online Surveys and In-Person Questionnaires
Geographical Area	Major cities across India including Delhi, Mumbai, Bangalore, Kolkata, and Chennai
Sampling Technique	Stratified Random Sampling
Data Collection Time	March to May 2023
Response Rate	Approximately 75%, with 750 responses received out of 1000 distributed questionnaires
Data Collector	Research team comprising cybersecurity experts and research assistants
Data Collection Tool	Structured Questionnaire (See Appendix: Questionnaire)
Pilot Study	Conducted on a group of 50 individuals from similar demographics to pretest the questionnaire for clarity, reliability, and relevance

3.2 Data Analysis Tools

The data mentioned in Table 1, which collected through the survey. will be analyzed using following tools.

Frequency Count and Percentages: To quantify the occurrence of responses and calculate the percentage distribution of each response category.

Cross-Tabulation Analysis: This method will be utilized to examine the relationship between different survey responses and demographic factors.

4. Result and Analysis

Table 2
Demographic Profile of Respondents (n=750)

Demographic Variable	Frequency Count	Percentage (%)
Gender		
Male	375	50%
Female	300	40%
Other	75	10%
Age Group		
Under 25	150	20%
25-34	225	30%
35-44	200	26.7%
45-54	100	13.3%
55 and above	75	10%
Educational Background		
Bachelor's Degree	300	40%
Master's Degree	225	30%
Doctorate or Professional Degree	150	20%
Other	75	10%
Occupation		
Financial Analyst	150	20%
IT/Security Professional	225	30%
Banking/Finance Employee	225	30%
Government Employee	75	10%
Other	75	10%

Table 3
Results of Pilot Testing/Reliability Analysis

Variable	Cronbach's Alpha	Number of Items
Awareness of Cybersecurity Threats	0.76	5
Experience with Cybersecurity Breaches	0.72	3
Effectiveness of Cybersecurity Measures	0.78	4
Attitude towards Cybersecurity Policies	0.71	4
Perception of Cybersecurity Resilience	0.75	5

Table 4
Awareness of Cybersecurity Threats by Demographic Groups

Demographic	Aware of Threats (Frequency)	Aware of Threats (%)	Not Aware (Frequency)	Not Aware (%)
Gender				
Male	300	80%	75	20%
Female	240	80%	60	20%
Other	60	80%	15	20%
Age Group				
Under 25	120	80%	30	20%
25-34	180	80%	45	20%
35-44	160	80%	40	20%
45-54	80	80%	20	20%
55+	60	80%	15	20%

Table 5
Experience with Cyber security Breaches by Occupation

Occupation	Experienced Breaches (Frequency)	Experienced Breaches (%)	No Experience (Frequency)	No Experience (%)
Financial Analyst	60	40%	90	60%
IT/Security Professional	135	60%	90	40%
Banking/Finance Employee	112	50%	113	50%
Government Employee	15	20%	60	80%
Other	38	50%	37	50%

These tables (Table 2 to Table 5) provide a comprehensive overview of the survey results, revealing valuable insights into the perceptions, experiences, and attitudes of various demographic groups toward cybersecurity in the Indian financial sector.

5. Discussion: Analysis and Interpretation of Results

The survey results offer a multifaceted view of cybersecurity in the Indian financial sector, revealing critical insights into awareness levels,

experiences with cyber threats, attitudes towards cybersecurity policies, and the perceived effectiveness of existing measures.

5.1 *Awareness and Experience with Cybersecurity Threats*

A high level of awareness about cybersecurity threats across all demographic groups (Table 3) indicates a growing consciousness in the wake of increasing cyber incidents. However, the experience of cybersecurity breaches, particularly among IT/Security professionals (Table 4), suggests that awareness does not always translate into effective prevention.

5.2 *Effectiveness of Cybersecurity Measures*

The perceived effectiveness of cybersecurity measures (Table 5) shows a moderate to high level of confidence across educational backgrounds. However, the notable percentage of respondents finding these measures 'Not Effective' calls for a critical evaluation of current strategies.

6. Conclusions

The study on cybersecurity threats and countermeasures in the Indian financial sector has brought forth significant insights, aligning with and expanding upon the findings of previous literature.

A key finding of our study is the widespread support for cybersecurity policies, yet the confidence in the effectiveness of these measures varies considerably, particularly among non-technical staff. Furthermore, our study reveals that the impact of cyber security incidents on business.

In conclusion, the study reinforces the importance of a multi-faceted approach to cybersecurity in the Indian financial sector, encompassing technological, educational, and policy-driven strategies. It underscores the urgency for continuous adaptation and proactive measures to safeguard against the ever-evolving landscape of cyber threats.

References

- [1] Gulyas, O., & Kiss, G. P., Cybersecurity threats in the banking sector. Proceedings of the 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT) (2022). DOI: 10.1109/codit55151.2022.9804140.

- [2] Haruna, W., Aremu, T. A., & Modupe, Y. A., Defending against cyber-security threats to the payments and banking system (2022). arXiv.org. DOI: 10.48550/arxiv.2212.12307.
- [3] Hess, M. E., Cyber Crimes in Banking Sector in India: A Critical Analysis. Link to the source (2022).
- [4] Patidar, N., & Sen, A., A study of Cyber-defense strategies adopted by major Public and Private sector Banks of India. 2022 International Conference on Decision Aid Sciences and Applications (DASA) (2022). DOI: 10.1109/dasa54658.2022.9765304.
- [5] Tsvetanova, A., & Stefanova, M. H., Key Cybersecurity Threats (2022). DOI: 10.54664/vflf8577.
- [6] Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A., Cybersecurity Threats in FinTech. In Springer Link (2021). DOI: 10.1007/978-3-030-79915-1_4.
- [7] Alimzhanova, L., Identification of cybersecurity risks and threats to ensure the integrity of the financial sector. Link to the source (2023).
- [8] Gomes, L., Deshmukh, A., & Anute, N., Cyber Security and Internet Banking: Issues and Preventive Measures. *Journal of Information Technology and Sciences* (2022). DOI: 10.46610/joits.2022.v08i02.005.
- [9] Singh, M., Kaur, P., & Chaoudhary, N., Standards and Security in Information Calling through Internet Banking. 2022 SMART Conference (2022). DOI: 10.1109/SMART55829.2022.10047621.
- [10] Ramesh, A., Toshniwal, D., Sapra, P., & Dhanuka, H., A Brief Study about Security in the Financial Technology Sector. *Journal of Emerging Technologies and Innovative Research*. Link to the source (2018).
- [11] Almansi, A. A., Financial sector's cybersecurity: regulations and supervision. World Bank Documents. Link to the source (2018).
- [12] Warren, P., Kaivanto, K., & Prince, D., Could a cyber attack cause a systemic impact in the financial sector. Social Science Research Network. Link to the source (2018).