www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 344-349

e-ISSN : 2583-1062
Impact Factor : 7.001

A STUDY ON ANALYSIS OF CYBERSECURITY ISSUES IN MODERN BANKING

Bino B[1], Mrs Keerthi S[2]

[1]MBA Student, School of Arts, Humanities and Management, Jeppiaar University, Chennai, India.

[2]Assistant Professor, School of Arts, Humanities and Management, Jeppiaar University, Chennai, India.

DOI: https://www.doi.org/10.58257/IJPREMS39676

ABSTRACT

The widespread use of digitalization, mobile banking, and online payment systems in the modern banking industry has increased cybersecurity challenges while also bringing unparalleled convenience. This study focuses on issues such as traditional methods, employee and customer ignorance, and the need for advanced security measures. The main goals of this research are to identify and analyze cybersecurity challenges in modern banking, assess the role of emerging technologies in enhancing cybersecurity, identify the difficulties public and private banks face in putting strong cybersecurity measures in place, and evaluate the efficacy of regulatory frameworks while offering workable solutions. It emphasizes the vital role of emerging technologies like artificial intelligence, blockchain, and real-time threat detection systems in risk mitigation.In order to find gaps and opportunities for development, the study also looks at the regulatory environment, including guidelines set by the Reserve Bank of India and international norms. The report emphasizes the necessity for banks to take a proactive stance by thoroughly examining these issues and suggesting remedies, which may include improving cybersecurity infrastructure, strengthening public-private cooperation, and promoting extensive awareness campaigns. Building a safe and robust financial environment that can survive the ever-changing panorama of cyberthreats in the digital era requires addressing these issues.

Keywords: Artificial intelligence (AI), Mobile banking, and Cybersecurity

1. INTRODUCTION

The technique of preventing unwanted access, theft, and damage to digital systems, networks, and data is known as cybersecurity. Cybersecurity in the context of contemporary banking guarantees the protection of transactional data, customer information, and financial assets.As digital platforms proliferate, cybersecurity has emerged as a crucial component of banking operations, protecting against ransomware, insider fraud, phishing, and malware. The utilization of cutting-edge technology and digital platforms to provide clients with cutting-edge financial services is referred to as modern banking. These consist of digital wallets, mobile banking applications, online banking, and automated teller machines (ATMs).

Cyber threats in banking have changed in tandem with the technological revolution in the sector. At first, the main issues were fraud and actual theft. However, the emphasis switched to defending against digital attacks as banks embraced online technologies. Simple viruses and unauthorized account access were the main components of early cyberattacks, but these have now developed into intricate, multi-layered operations including hacker collectives, state-sponsored cybercriminals, and AI-driven attacks. Potential defenses like blockchain and artificial intelligence have surfaced, but hackers are still adjusting and using techniques like ransomware, deepfakes, and social engineering.Technological developments have fueled the modernization of banking services, enabling financial institutions to provide individualized customer experiences, real-time data access, and smooth digital transactions. However, because of the enormous importance of financial and personal customer data, this change has made banks more appealing targets for hackers. Modern banking has cybersecurity issues from both internal and external sources, including staff carelessness and inadequate cybersecurity training, as well as external threats like malware and hackers. Strong cybersecurity measures are more important than ever in light of rising regulatory requirements and rising consumer expectations for safe digital services. This article explores these issues, potential solutions to lessen dangers, and public sentiment toward the adoption of cyber security in India.

2. REASERCH OBJECTIVES

1. To determine the obstacles that both public and private banks encounter when putting strong cybersecurity measures into place.
2. To Determine and Examine Cybersecurity Issues in Contemporary Banking,
3. To Assess New Technologies' Contribution to Strengthening Cybersecurity

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 344-349

e-ISSN : 2583-1062
Impact Factor : 7.001

3. REVIEW OF LITERATURE

1. Smith and colleagues (2020): Cyberthreats in Online Banking
   Data breaches have increased by 35% annually, according to this report, which examined the growing frequency of cyberattacks in the banking industry.
   The authors underlined the vital necessity of AI-based threat detection systems and multi-layered security mechanisms.
2. Gupta et al. (2019): Cyber Vulnerability and Legacy Systems
   Gupta et al. investigated the ways in which banks' antiquated IT systems increase risks. They pointed out that 60% of the institutions polled said that implementing cutting-edge security measures was hampered by outdated systems.
3. Williams and Zhao (2022): Artificial Intelligence in Banking Security
   The use of artificial intelligence in identifying and reducing cyberthreats was investigated in this study. According to the study, banks that used AI-driven systems saw a 30% decrease in successful attacks when compared to those that used conventional techniques.
4. Patel and Johnson (2021): New Risks in Cybersecurity for Banks
   The authors noted new dangers including ransomware and deepfake fraud and emphasized the value of blockchain technology and predictive analytics in reducing these risks.
5. Chen et al. (2022): Cybersecurity and Employee Awareness
   Chen et al. looked into how employee training might stop cyberattacks. Regular cybersecurity training programs decreased phishing success rates by 40%, according to the report.
6. Regulatory Difficulties in Cybersecurity Davis (2020)
   Davis examined the challenges of adhering to global cybersecurity laws such as PCI DSS and GDPR. The operational difficulties banks encounter in adhering to these guidelines while preserving profitability were brought to light by the study.
7. Kumar and Verma (2018): Security of Mobile Banking
   Vulnerabilities in mobile banking, like inadequate user authentication and unsafe app design, were the main focus of this study. It suggested fixes like biometric verification and two-factor authentication.
8. Thompson, The Human Aspect of Cybersecurity (2019)
   In his study on insider threats, Thompson emphasized the value of background checks, ongoing oversight, and a robust corporate culture in preventing employee-caused breaches.
9. Ravindra Kumar (2019): Indian Banking's Cybersecurity Challenges
   The quick digitization of Indian banks and the corresponding increase in cyberattacks were both noted in Kumar's paper. According to the study, malware and phishing attacks are the most frequent dangers in India, impacting more than 25% of banks each year. The report underlined the necessity of strict security regulations and cutting-edge monitoring technologies designed specifically for Indian banking operations.
10. Pooja Mehta (2020): How Digital Payments Affect India's Cybersecurity Risks
    Mehta's study examined the rise in digital payment systems in India following demonetization and the related cybersecurity issues. She discovered a 40% rise in frauds involving UPI and mobile wallet fraud. In order to lower these risks, the study emphasized the necessity of customer education initiatives.

4. RESEARCH METHODOLOGY

In order to comprehend cybersecurity issues in contemporary banking, assess the efficacy of new technologies, and suggest workable solutions, the study employs a descriptive research design. To collect numerical data for analysis, the study uses quantitative data surveys and questionnaires that are given to clients, staff members, and financial institutions. Secondary data from numerous websites, journals, and reference books was used in the research study. A sample size of 20 respondents is also used to gather primary data in order to assess the general public's understanding of the difficulties associated with cyber security.

5. DATA ANALYSIS AND INTERPRTATION

An analysis on Cybersecurity Challenges in Modern Banking

1) Levels of Customer Awareness

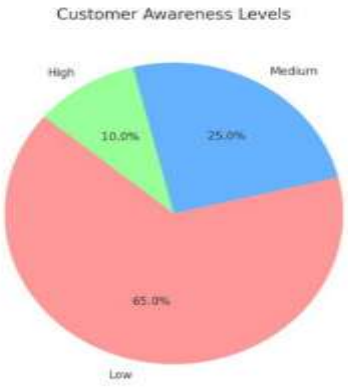
Survey Question: How well-informed are you about the hazards associated with internet banking cybersecurity?

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 344-349

e-ISSN : 2583-1062
Impact Factor : 7.001

Awarness level	Percentage
Low	65
high	10
Medium	25

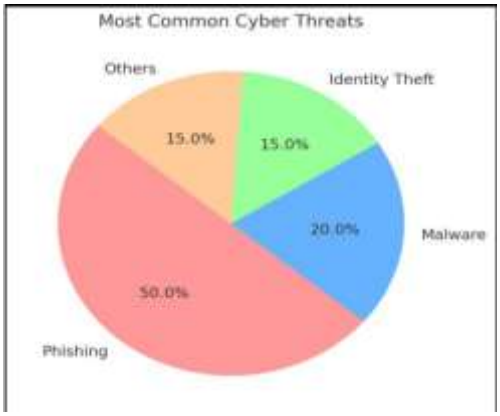


With 65% of consumers rating their awareness as "low," there is a clear knowledge gap about cybersecurity threats. 10% think they are highly aware. Campaigns to inform consumers about safe online conduct should be a top priority for banks.

2) Cyber Threats Most Often (Pie Chart)

Survey Question: Which kind of cyberthreats do you think affects banks the most?

Cyber threat	Percentage
phishing	50
malware	20
identity	15
others	15



Interpretation: Of the threats, phishing is the most common, impacting 50% of respondents. Malware comes in second at 20%. Thirty percent are affected by identity theft and other dangers combined. Strengthen anti-phishing protocols and encourage user education, it is suggested.

3) Banks Using Emerging Technologies (Bar Graph)

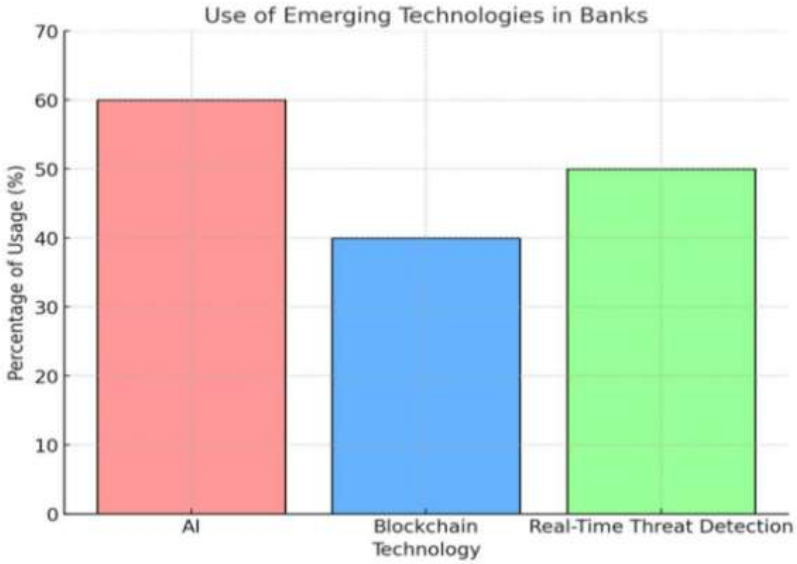
Survey Question: Which emerging technologies are used in your bank's cybersecurity measures?

Technology	Percentage
AI	60
Blockchain	40
Real- time threat detection	50

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 344-349

e-ISSN : 2583-1062
Impact Factor : 7.001

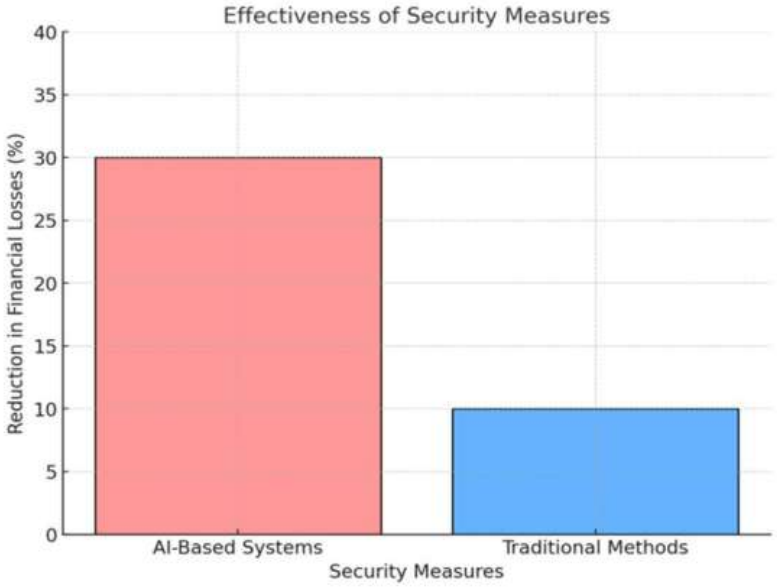


Interpretation: Blockchain adoption is at 40%, real-time threat detection is at 50%, and AI is at 60%. Increase the usage of blockchain technology for safe transactions and improve AI-powered solutions.

4) Security Measures' Effectiveness (Bar Graph)

Data of a Case Study: Lower Financial Losses Following AI Implementation.

Security measure	Reduction in losses
AI based system	30
Traditional methods	10



Interpretation: Compared to traditional methods, which only reduced financial losses by 10%, AI-based systems decreased losses by 30%. To improve their capacity for danger identification and prevention, banks ought to make greater investments in AI-driven solutions.

5) Cybersecurity Training for Employees (Bar Graph)

Survey Question: Does your bank regularly train its staff in cybersecurity?

response	Percentage
Yes	30
No	70

www.ijprems.com
editor@ijprems.com

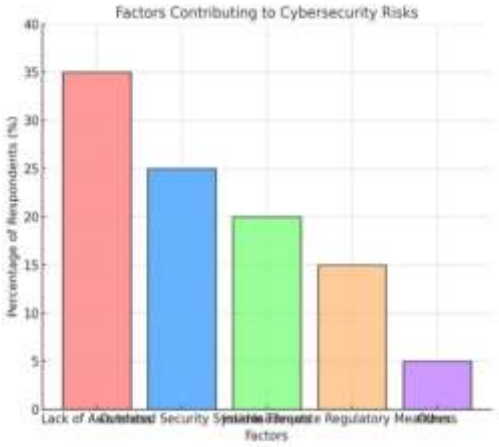
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 344-349

e-ISSN : 2583-1062
Impact Factor : 7.001

Interpretation: Just 30% of workers said they regularly received cybersecurity training. 70% of respondents said they lacked training, which is dangerous. Create required training courses for staff members to guarantee they are prepared for online attacks.

6) Factors Associated with Cybersecurity Issues

Factors	Frequency
Lack of customer awareness	65
Phishing attacks	50
Phishing attacks	70
Outdated security infrastructure	40
Lack of regulatory compliance	30



Interpretation: Insider threats (20%), out-of-date security systems (25%), and ignorance (35%), are the main causes of cybersecurity concerns. Although they contribute less, other variables (5%) and inadequate regulatory actions (15%) are still significant issues. To effectively reduce risks, banks should prioritize raising awareness and modernizing security systems.

6. FINDINGS

1. Customer Awareness: There is a knowledge gap as evidenced by the fact that 65% of customers are unaware of cybersecurity threats.
2. Cyberthreats: According to 50% of respondents, phishing is the most common cyberthreats.
3. Emerging Technologies: Real-time threat detection comes in at 50%, blockchain at 40%, and artificial intelligence at 60%.
4. Employee Training: There is a notable training gap, since 70% of staff do not receive regular cybersecurity training.
5. Effectiveness of Security Measures: When compared to conventional techniques, AI-based solutions are three times more effective at minimizing monetary losses.

7. SUGGESTIONS

1. Create thorough education efforts aimed at consumers to increase their knowledge of cybersecurity threats, including phishing.
2. Provide interactive online resources (simulations and tests) so that clients can practice identifying cyberthreats in a secure setting.
3. Make cybersecurity education mandatory for all staff members, covering threat identification and safe online conduct.
4. Establish continuing education initiatives that are updated frequently to cover emerging risks and cybersecurity best practices.
5. Increase the usage of AI-based threat detection and response systems, emphasizing real-time analysis and notifications of questionable activity.
6. To improve proactive reactions to possible threats, give real-time threat detection systems top priority when making investments.
7. Encourage open dialogue about risks and best practices between staff and clients to cultivate a cybersecurity culture.
8. To evaluate the efficacy of security protocols and training initiatives, conduct routine security audits.
9. Use simulated phishing assaults to gauge staff awareness, then tailor training according to the findings.
10. Collaborate with cybersecurity companies and specialists to offer training sessions and workshops to staff members and clients.
11. Provide feedback channels so that clients can express their cybersecurity-related experiences and worries.

8. CONCLUSION

Unquestionably, the quick digital transformation of banking has improved operational effectiveness and client convenience, but it has also created new opportunities for cyberattacks. Critical issues such a lack of understanding among stakeholders, reliance on conventional techniques, and insufficient cybersecurity measures are highlighted in the study. There is a lot of promise for risk mitigation with emerging technologies like blockchain, artificial intelligence, and real-time threat detection systems. Strong regulatory frameworks, led by organizations like the Reserve Bank of India and backed by international norms, continue to play a crucial role. The study does, however, also point out weaknesses in these frameworks, which call for revisions and adaptation to changing threat environments.

9. REFERENCES

[1] D. Abawe (2021). Issues with cybersecurity in contemporary financial systems. Taken from the Financial Cybersecurity Journal website.

[2] India's Reserve Bank (2021). Indian banks' use of technology and cyber risk management. taken from the website https://www.rbi.org.in

[3] Corporation for Federal Deposit Insurance (2022). Report on Financial System Resilience and Cybersecurity. From https://www.fdic.gov, taken

[4] Board of the Federal Reserve (2022). Risks to Banking Cybersecurity and Financial Stability. taken from the Federal Reserve's website.

[5] PwC India (2020). India's trends in cybersecurity and digital banking. taken from the website https://www.pwc.in

[6] N. Chadha (2019). Trends and Remedies for Cyberthreats in Indian Banking. taken from the Indian Banking Journal's website.

[7] India's EY (2021). Indian banks' readiness for cybersecurity. taken from the website https://www.ey.com

[8] India's National Cyber Security Center, 2020. Financial Cybersecurity Guidelines. taken from the website https://www.ncsc.gov.in