WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A study on E banking and their Risk

Nitya Raj Srivastava[1], Nidhi[2], Ritika Kumari[3]

Noida Institute of Engineering and Technology

ABSTRACT :

In recent years, electronic banking (e-banking) has revolutionized the financial services industry by offering greater convenience, speed, and efficiency to customers worldwide. However, alongside its numerous benefits, e-banking also introduces a range of significant risks, including cyber threats, data breaches, fraud, and operational vulnerabilities. This study aims to explore the evolution of e-banking, identify the types of risks associated with its adoption, and examine the measures taken by financial institutions to mitigate these risks. Through a combination of secondary data analysis and a review of recent case studies, this research highlights the critical challenges faced by banks and customers in the digital environment. It also discusses the role of regulatory frameworks, technological innovations, and risk management practices in enhancing the security and resilience of e-banking systems. The findings contribute to a deeper understanding of the importance of balancing technological advancements with comprehensive risk management strategies to ensure customer trust and sustainable growth in the banking sector.

Keywords:
E-Banking, Financial Technology, Cybersecurity, Banking Risks, Digital Fraud, Risk Management, Online Banking Security, Regulatory Compliance.

Introduction

The rapid advancement of information technology has transformed traditional banking practices, leading to the emergence of electronic banking (e-banking) as a core service offering. E-banking enables customers to conduct a variety of financial transactions remotely via the internet, mobile devices, and automated teller machines (ATMs), providing enhanced convenience, accessibility, and efficiency. As the banking sector continues to embrace digitalization, the adoption of e-banking has expanded globally, reshaping the way individuals and businesses interact with financial institutions.

Despite its numerous advantages, the rise of e-banking has introduced a new spectrum of risks and challenges. Cybersecurity threats, including hacking, phishing attacks, identity theft, and data breaches, have become increasingly sophisticated, posing significant risks to both banks and their customers. Operational risks, such as system failures, technological disruptions, and lack of user awareness, further compound the vulnerabilities associated with e-banking services. Moreover, the growing reliance on third-party service providers and evolving regulatory requirements have added additional layers of complexity to the risk landscape.

Understanding and addressing these risks is crucial for maintaining customer trust, ensuring financial stability, and promoting sustainable growth in the banking industry. This study seeks to explore the nature and types of risks associated with e-banking, examine the key factors contributing to these risks, and analyze how financial institutions implement strategies to mitigate them. By doing so, the research aims to provide valuable insights into building a secure, resilient, and customer-centric e-banking environment.

Objectives of the Study

The primary objective of this study is to investigate the various risks associated with the use of e-banking services and to understand customer perceptions, awareness, and experiences related to these risks through primary data collection. Specifically, the study aims to:

- To identify and categorize the major risks faced by users while using e-banking services.
- To assess customer awareness regarding security measures and risk factors in e-banking.
- To analyze the experiences of customers with cyber fraud, data breaches, or technical failures in e-banking platforms.

Literature Review

The growth of e-banking has significantly transformed the traditional banking landscape by offering enhanced convenience, speed, and accessibility to customers. However, it has also introduced various risks and challenges related to cybersecurity, data privacy, and system reliability. Several studies have addressed these critical issues, providing valuable insights into the evolution and vulnerabilities of e-banking services.

Chavan (2013) emphasized the dual aspects of e-banking — highlighting its benefits, such as faster transactions and broader financial inclusion, alongside challenges like cyber threats and user distrust. The study suggested that banks must continuously innovate and invest in security infrastructure to maintain customer confidence.

Malhotra and Singh (2007) examined the determinants that influence internet banking adoption among Indian banks. Their findings showed that technological competence, security assurance, and customer awareness are crucial factors driving the success of e-banking platforms.

Kaur and Kaur (2014) focused specifically on security issues associated with e-banking, suggesting biometric solutions as a possible answer to reducing fraud and enhancing authentication processes. Their research underlined that traditional security methods like passwords and PINs may no longer be sufficient in combating advanced cyber threats.

Uppal (2011) provided a comprehensive view on the delivery channels of banks, stating that with the proliferation of e-delivery methods such as mobile banking and ATMs, there is a greater need for robust risk management frameworks to address emerging vulnerabilities.

Khan (2010) conducted a comparative study on customer satisfaction and loyalty between private and public sector banks in the context of e-banking. The study concluded that customer trust, largely influenced by perceptions of security and responsiveness to fraud incidents, plays a vital role in ensuring loyalty toward online banking services.

In addition to academic research, reports from regulatory bodies like the Reserve Bank of India (RBI) and institutions such as the National Payments Corporation of India (NPCI) offer updated frameworks and guidelines to strengthen cybersecurity in the banking sector. The RBI Annual Reports and Cyber Security Frameworks emphasize the need for banks to adopt multilayered security protocols and to educate customers about safe e-banking practices.

Furthermore, various online sources such as Investopedia and Bankingsupport.com provide accessible information on best practices, current trends, and the latest threats in the field of e-banking, aiding in a broader understanding of the operational environment.

Research Methodology

1. Research Design

The present study is *descriptive* in nature. It aims to investigate and analyze the various risks associated with e-banking, assess customer awareness regarding security practices, and understand their experiences with cyber fraud, data breaches, or technical failures.

2. Research Approach

The study is based on a *primary research approach* through a structured questionnaire designed to collect first-hand information directly from users of e-banking services.

3. Data Collection Method

- *Primary Data*: Collected using a well-structured questionnaire distributed among e-banking users.
- *Secondary Data*: Gathered from journals, articles, reports from RBI and NPCI, websites, and research papers to supplement the study.

4. Sampling Technique

A *convenience sampling* technique was used to collect data from respondents who use e-banking services.

5. Sample Size

The sample size selected for the study was *100 respondents*.

6. Data Collection Tool

The main tool for data collection was a *questionnaire* which was divided into four sections:

- Basic Information
- Identification of Major Risks
- Customer Awareness about Security
- Experiences with Cyber Fraud, Data Breaches, or Technical Failures

7. Data Analysis Technique

The collected data was analyzed using *simple percentage analysis*. Tables were prepared showing the number of respondents and their percentage distribution to interpret the results effectively.

8. Scope of the Study

- To identify and categorize the major risks faced by e-banking users.
- To assess the level of customer awareness regarding security measures.
- To analyze customer experiences with technical failures, frauds, and data breaches in e-banking.

9. Limitations of the Study

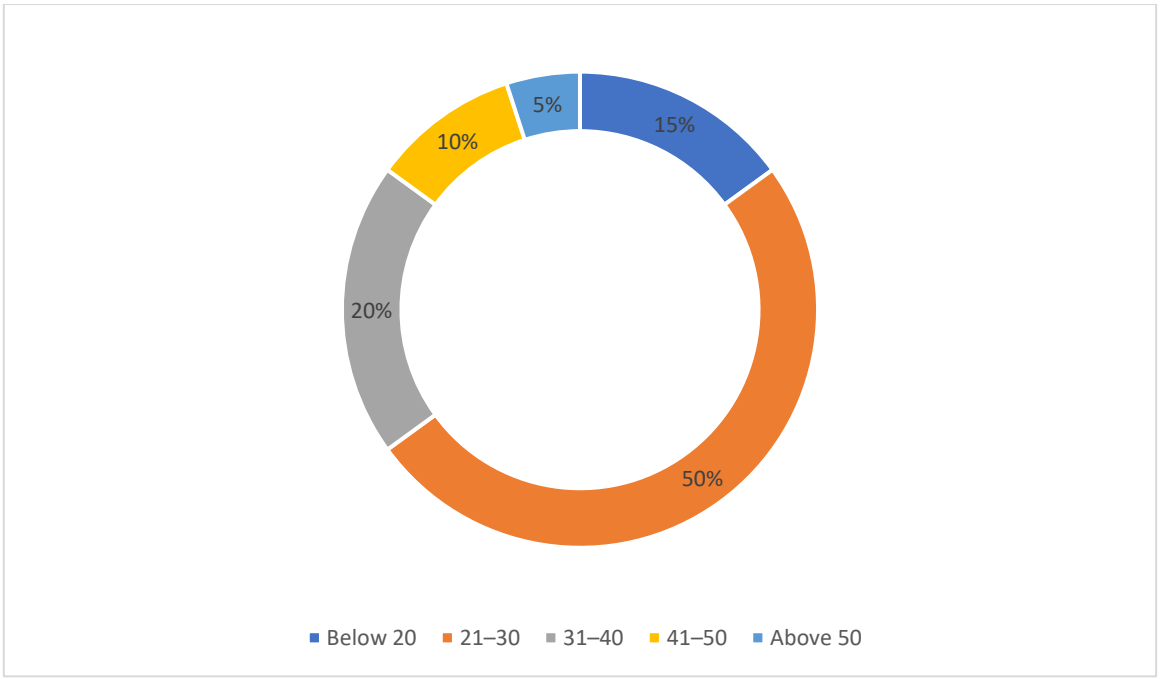
- The sample size is limited to 100 respondents, which may not fully represent the entire e-banking user population.
- The study relies on the honesty and accuracy of the respondents' answers.
- Geographical limitations as the survey participants were primarily urban-based users.

Data Analysis & Interpretation

Section A: Basic Information

Table 1: Age of Respondents

Particular	No. of Respondents	Percentage (%)
Below 20	15	15%
21–30	50	50%
31–40	20	20%
41–50	10	10%
Above 50	5	5%

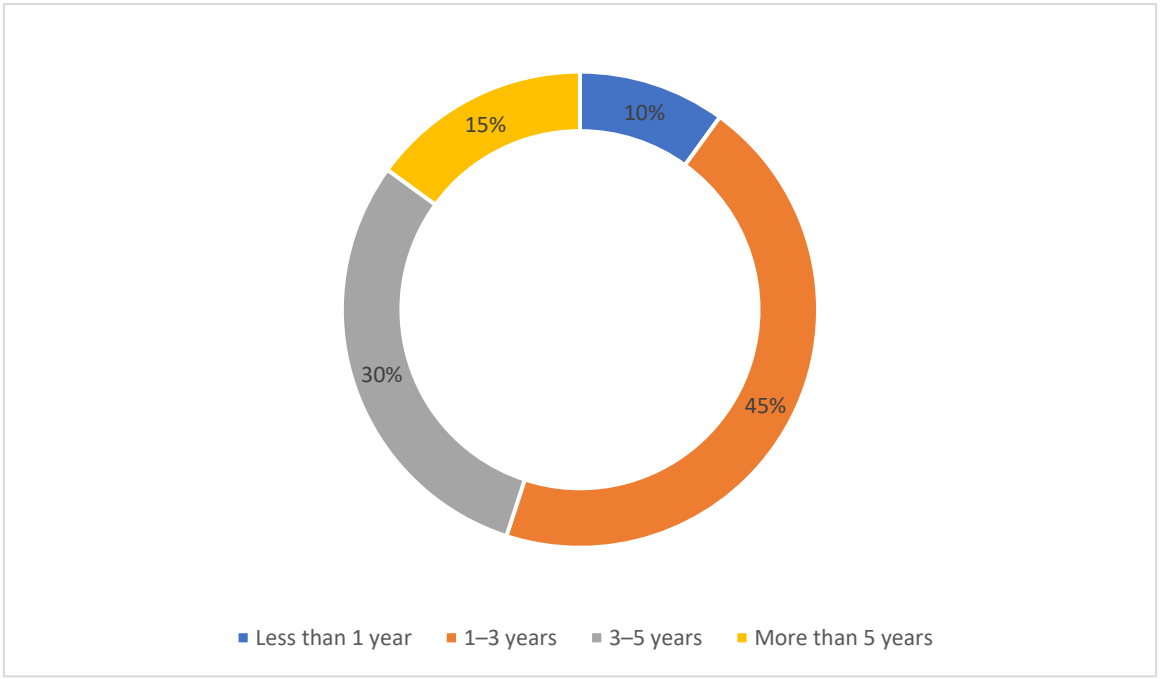


Interpretation:

The majority of respondents (50%) fall in the age group of 21–30 years, showing that younger individuals are the primary users of e-banking services. Very few users are above 50 years of age.

Table 2: Duration of Using E-Banking Services

Particular	No. of Respondents	Percentage (%)
Less than 1 year	10	10%
1–3 years	45	45%
3–5 years	30	30%
More than 5 years	15	15%



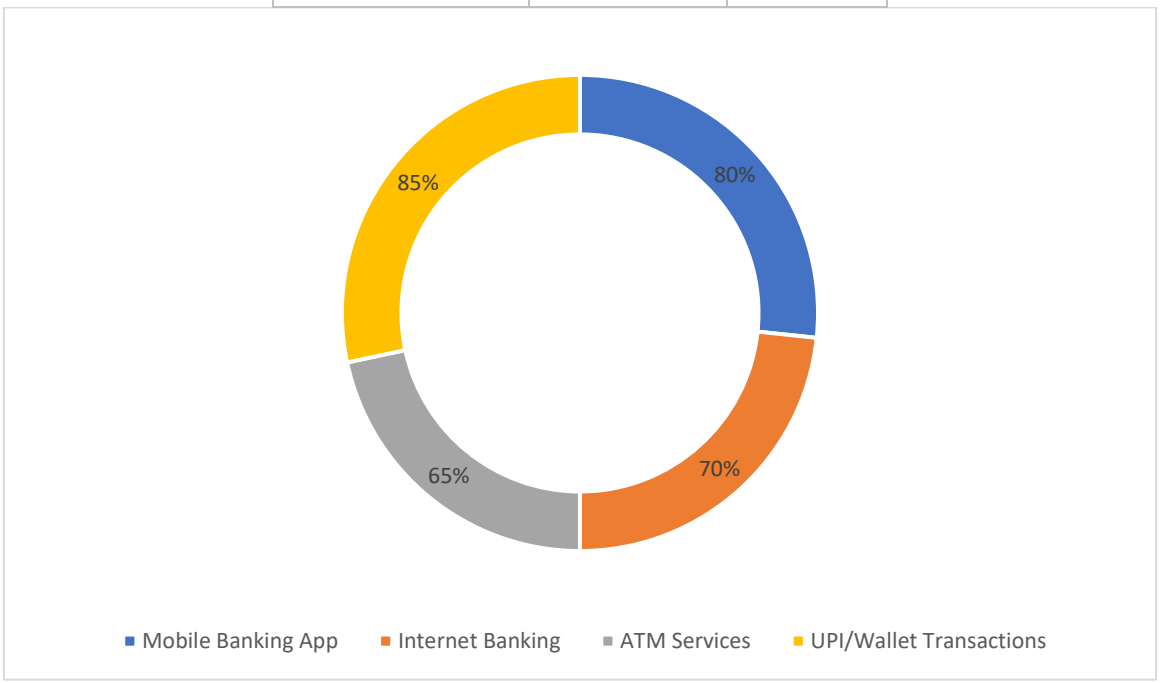
Interpretation:

Most respondents (45%) have been using e-banking services for 1–3 years, indicating a growing adoption of digital banking in recent years.

Section B: Identification of Major Risks

Table 3: Commonly Used E-Banking Services

Particular	No. of Respondents	Percentage (%)
Mobile Banking App	80	80%
Internet Banking	70	70%
ATM Services	65	65%
UPI/Wallet Transactions	85	85%

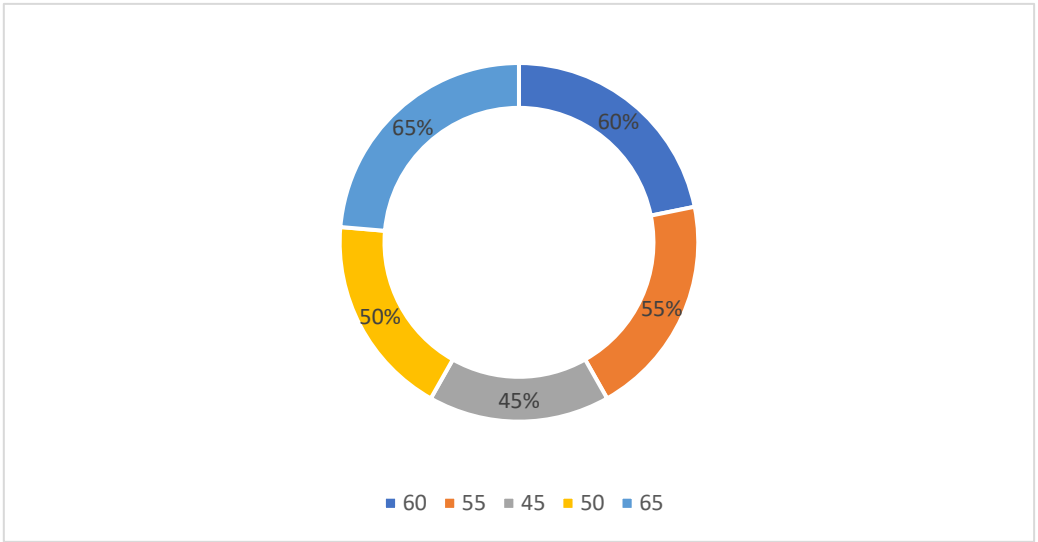


Interpretation:

UPI/Wallet Transactions (85%) and Mobile Banking Apps (80%) are the most commonly used services among respondents, showing the increasing popularity of mobile-based transactions.

Table 4: Most Common Risks in E-Banking

Particular	No. of Respondents	Percentage (%)
Unauthorized transactions	60	60%
Phishing attacks	55	55%
Technical errors/system failures	45	45%
Data breach/personal information leak	50	50%
Account hacking	65	65%

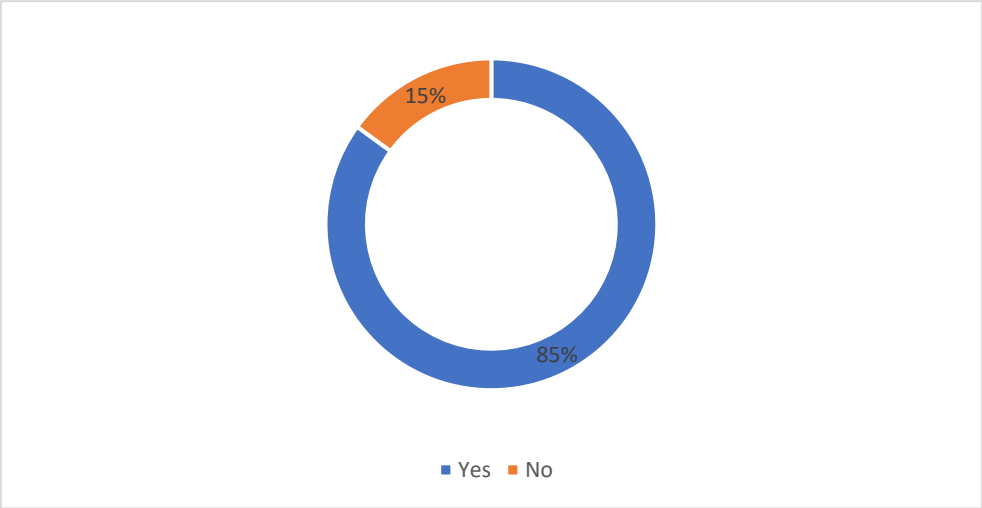


Interpretation:
Account hacking (65%) and unauthorized transactions (60%) are perceived as the major risks by users, reflecting growing concerns about the security of online banking platforms.

Section C: Customer Awareness about Security

Table 5: Awareness of Security Practices

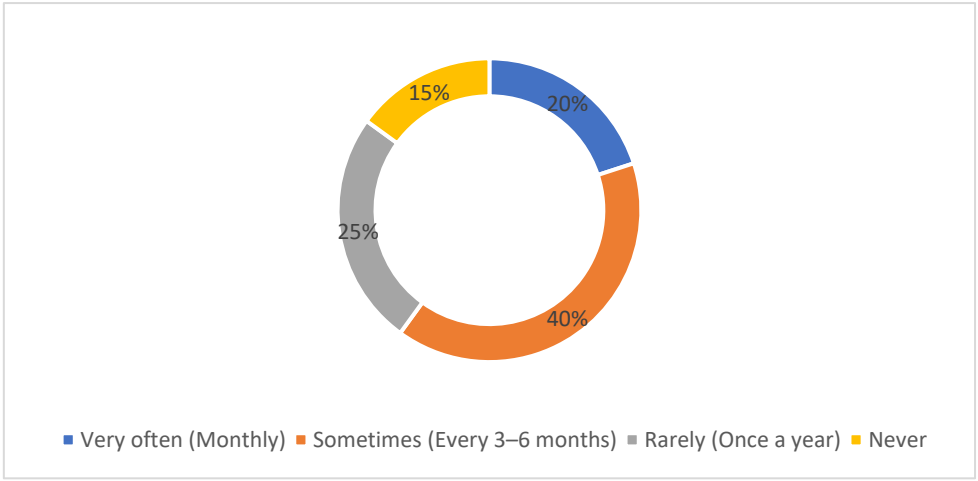
Particular	No. of Respondents	Percentage (%)
Yes	85	85%
No	15	15%



Interpretation:
A significant majority (85%) of respondents are aware of security practices like two-factor authentication and strong passwords, indicating a relatively high level of security awareness.

Table 6: Frequency of Updating Passwords or Security Settings

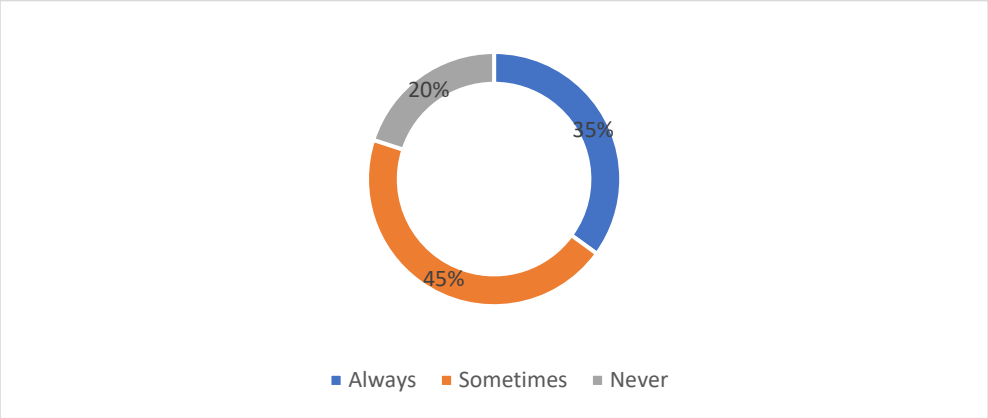
Particular	No. of Respondents	Percentage (%)
Very often (Monthly)	20	20%
Sometimes (Every 3–6 months)	40	40%
Rarely (Once a year)	25	25%
Never	15	15%



Interpretation:
40% of respondents update their e-banking passwords sometimes (every 3–6 months), but a concerning 15% never update their passwords, indicating a potential security risk.

Table 7: Following Bank's Safety Guidelines

Particular	No. of Respondents	Percentage (%)
Always	35	35%
Sometimes	45	45%
Never	20	20%

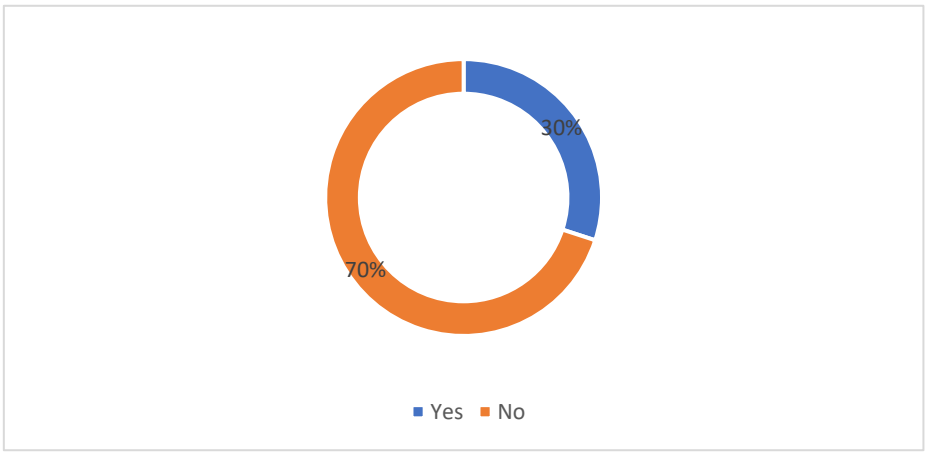


Interpretation:
Only 35% of respondents always follow the bank's safety guidelines, while 20% never do, highlighting the need for better customer education on e-banking safety.

Section D: Experiences with Cyber Fraud, Data Breaches, or Technical Failures

Table 8: Experience with Cyber Fraud or Data Breaches

Particular	No. of Respondents	Percentage (%)
Yes	30	30%
No	70	70%

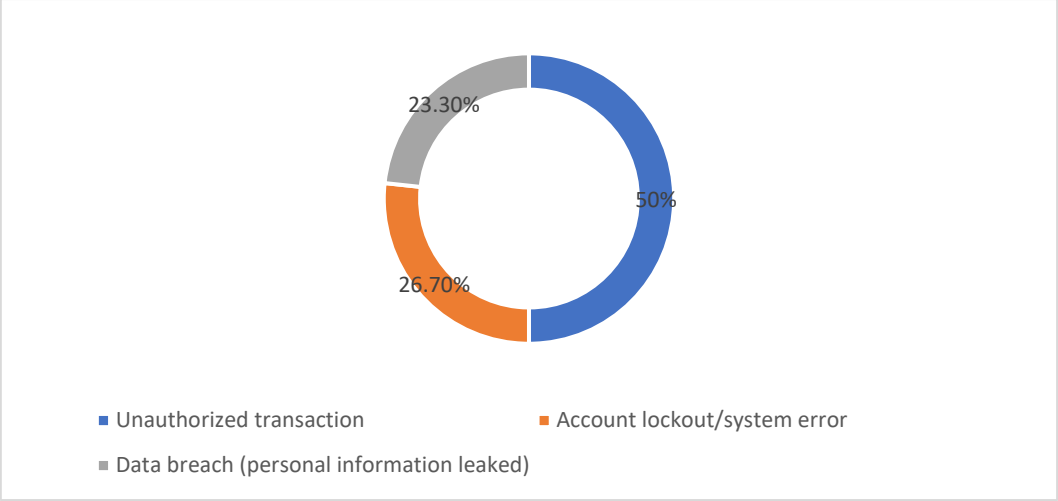


Interpretation:
30% of respondents have experienced some form of cyber fraud, technical glitch, or data breach, showing that while the majority have not faced issues, the risk remains significant.

(For those who answered "Yes" in Q8 only)

Table 9: Type of Issues Experienced

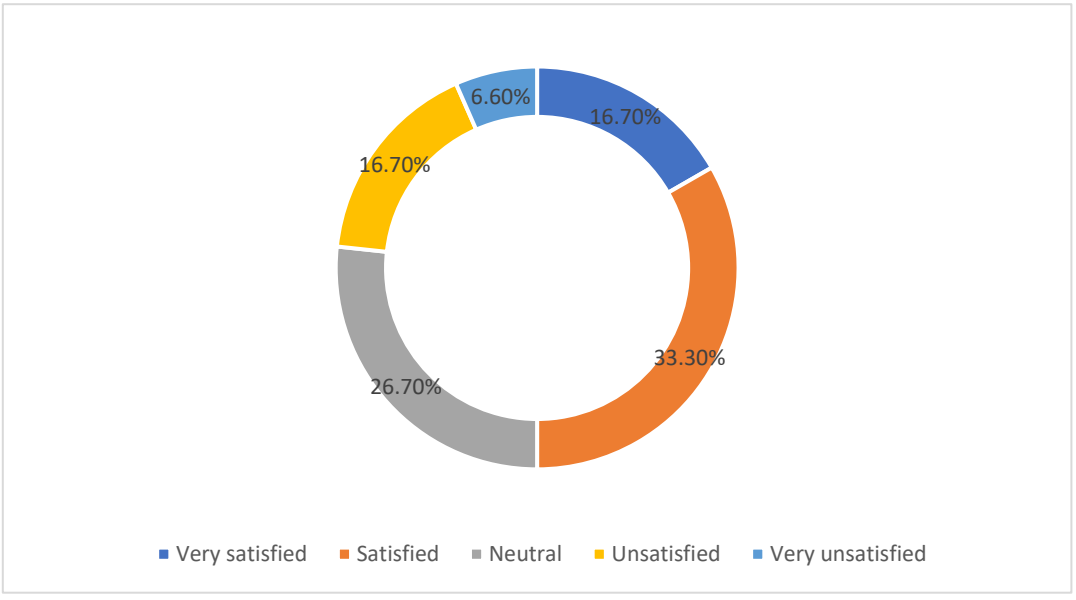
Particular	No. of Respondents	Percentage (%)
Unauthorized transaction	15	50%
Account lockout/system error	8	26.7%
Data breach (personal information leaked)	7	23.3%



Interpretation:
Among those who faced issues, unauthorized transactions were the most common (50%), followed by account lockouts and data breaches.

Table 10: Satisfaction with Bank's Handling of Issues

Particular	No. of Respondents	Percentage (%)
Very satisfied	5	16.7%
Satisfied	10	33.3%
Neutral	8	26.7%
Unsatisfied	5	16.7%
Very unsatisfied	2	6.6%



Interpretation:
Only 50% of affected customers (Very Satisfied + Satisfied) were happy with their bank's handling of the issue, indicating a need for better complaint resolution and customer support in e-banking.

Findings

This study was conducted on a sample of 100 respondents to investigate the risks associated with e-banking, customer awareness regarding security practices, and their experiences with cyber fraud, data breaches, or technical failures. Based on the analysis of primary data collected through a structured

questionnaire, the key findings are as follows:

- The majority of e-banking users (50%) belong to the 21–30 years age group, indicating that younger individuals are the most active users of digital banking services.
- Most respondents (45%) have been using e-banking services for a period of 1–3 years, showing recent growth in the adoption of online financial services.
- UPI/Wallet transactions (85%) and mobile banking apps (80%) are the most commonly used e-banking services among users, reflecting a preference for mobile and instant payment methods.
- In terms of perceived risks, account hacking (65%) and unauthorized transactions (60%) emerged as the two most common concerns among e-banking users.
- A large proportion of respondents (85%) are aware of essential security practices such as two-factor authentication, strong passwords, and using secure networks for online banking activities.
- Despite good awareness, only 20% of users update their passwords or security settings very often (monthly), and 15% never update them, indicating some negligence in maintaining account security.
- Regarding safety guidelines provided by banks, 35% of the respondents reported always following them, whereas 20% admitted they never follow such guidelines.
- Around 30% of the respondents have personally experienced cyber fraud, technical glitches, or data breaches while using e-banking services.
- Among those who faced issues, unauthorized transactions (50%) were the most frequently encountered problem, followed by account lockouts (26.7%) and data breaches (23.3%).
- In terms of customer satisfaction with the handling of cyber issues by banks, only 50% of the affected users were either satisfied or very satisfied, indicating a gap in effective resolution of cyber incidents by banks.

Conclusion

The study on "E-Banking and Their Risk" highlights the growing importance and challenges of digital financial services in today's technologically advanced environment. With the increasing reliance on e-banking platforms such as mobile banking apps, internet banking, ATMs, and UPI/wallet transactions, customers are enjoying greater convenience and accessibility. However, this convenience also brings significant risks related to cybersecurity, unauthorized transactions, phishing attacks, technical failures, and data breaches.

The primary research findings reveal that while a majority of users are aware of basic security practices, a gap still exists in the actual implementation of protective measures, such as regularly updating passwords or consistently following banking safety guidelines. Furthermore, a significant number of respondents have experienced cyber fraud or technical glitches, with many expressing dissatisfaction or only moderate satisfaction with the banks' response to these incidents.

Overall, the study concludes that while e-banking is rapidly becoming a preferred mode of financial transaction, ensuring security remains a major concern for both customers and banking institutions. Strengthening customer education, enhancing technical safeguards, and improving the handling of cyber incidents are essential to building a safer and more trustworthy e-banking environment.

BIBLIOGRAPHY

1. Chavan, J. (2013). *Internet Banking - Benefits and Challenges in an Emerging Economy.* International Journal of Research in Business Management (IJRBM), Vol. 1, Issue 1.
2. Malhotra, P., & Singh, B. (2007). *Determinants of Internet Banking Adoption by Banks in India.* Internet Research, Vol. 17, Issue 3.
3. Kaur, R., & Kaur, P. (2014). *E-Banking Security Issues – Is There A Solution in Biometrics?* Journal of Internet Banking and Commerce, Vol. 19, No. 1.
4. Uppal, R. K. (2011). *E-Delivery Channels in Banks - A Fresh Outlook.* Journal of Arts Science & Commerce, Vol. II, Issue 1.
5. Khan, S. (2010). *Impact of E-Banking on Customer Satisfaction and Loyalty: A Comparative Study of Private and Public Sector Banks in India.* International Journal of Business and Management.

Websites:

1. www.rbi.org.in (Reserve Bank of India official website)
2. www.npci.org.in (National Payments Corporation of India)
3. www.bankingsupport.com
4. www.investopedia.com (for general definitions and concepts)

Reports:

1. RBI Annual Reports on Trends and Progress of Banking in India
2. Cyber Security Frameworks in Indian Banking Sector, 2023

Research Articles:

1. Various research papers and articles on Google Scholar related to E-Banking risks and security measures.