iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** Dec 2024

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Conference 'Technology and Knowledge Based Entrepreneur for Sustainable Industrial Development', held at Sridevi Women's Engineering College, Dec 2024

Risk Analysis of E-Banking

Boya Vijayalaxmi[1], Dr. U. Padmavathi[2]
[1]MBA II Year, [2]Professor HOD, Sridevi Women's Engineering College, Hyderabad

Abstract: ***E-Banking, as a cornerstone of modern financial services offers convenience and accessibility but also introduce a range of risks that must be effectively managed. However, this shift to digital platforms introduces significant risks, including cybersecurity threats, identity theft, Dara breaches, fraud, operational failures, and regulatory compliance issues. This study provides a detailed analysis of these risks, categorizing them into technological, operational, and human factors. The paper also explores mitigation strategies, such as advanced cybersecurity frameworks, customer education, and regulatory compliance measure, to ensure secure and reliable e-banking systems. The findings emphasize the importance of proactive risk management to sustain trust and operational stability in the e - banking systems. The findings emphasize the importance of proactive risk management to sustain trust and operational stability in the e-banking ecosystem.***
Keywords: E banking, risk, challenges, risk management, electronic banking.

I. INTRODUCTION

E-banking, also known as online or electronic banking, has revolutionized the financial services industry by enabling customers to conduct financial transactions anytime and anywhere. This paradigm shift has significantly increased customer convenience and operational efficiency for financial institutions. However, as reliance on digital platforms grows, so do the risks and vulnerabilities associated with them.

The primary risks in e-banking include cyber-attacks, fraud, unauthorized access, and system failures, which can result in financial losses, reputational damage, and regulatory penalties Moreover, the human factor, including inadequate user awareness and internal fraud, awareness and internal fraud, further exacerbate these challenges.

II. OBJECTIVES OF THE STUDY

1) To study impact and create awareness about E-Banking services.
2) The study address the profit and loss of using. E-Banking services.
3) To study evaluate performance of e-banking operations.
4) To study latest use of technology and its effects on e-banking operations.

III. REVIEW OF LITERATURE

E banking, a dynamic and growing sector, faces an increasingly complex landscape of risks. Over the past decade, numerous studies have explored the various dimensions of e-banking risks, focusing on their identification, classification, and mitigation strategies.

These risks are categorized into cybersecurity risks, operational risks, financial and fraud-related risks, and regulatory compliance risks, each of which is integral to the smooth functioning of e-banking platforms.

A. Cybersecurity Risk

A significant portion of the literature has concentrated on cybersecurity as the foremost risk in e-banking. The proliferation of online banking systems has attracted cyber-criminals, making e-banking vulnerable a wide array of attacks such as phishing, data breaches, and ransomware. In a study by Jain et Ai (2021), the authors emphasize the rising sophisticated of cyberattacks targeting e-banking platforms, especially with the adoption of cloud computing and mobile banking technologies. The growing concern over Dara privacy and security is echoed in several studies, including Singh and Gupta (2020), which highlight the need for stronger encryption, multi-factor authentication, and machine learning-based threat detection to protect sensitive financial data. These studies underline the importance of continual system upgrades and the implementation of comprehensive cybersecurity frameworks to the potential cyber-attacks.

B. Operational Risks

Operational risks in e-banking include system failures, service outages, and human errors. According to Bun and Imtiaz (2022), system downtime, transaction errors and process inefficiencies can severely damage customer trust and disrupt banking services.
Furthermore, the introduction of AI driven banking services, while providing innovation, also introduces potential risks from algorithmic errors or system malfunctions. Research by Thakur and Sharma (2021) examines how operational resilience in e-banking can be bolstered through real-time monitoring systems and disaster recovery strategies. Their findings stress the significance of operational risk management frameworks that ensure uninterrupted services and protect against technological disruptions.

C. Financial And Fraud -Related Risks

Fraud and financial crimes in e-banking have attracted significant attention in recent literature, especially as cybercriminals devise new methods to exploit the digital financial ecosystem. A study by Kumar and Narula (2022) analysed various types of fraud risks, including identity theft, fraudulent transactions and internal fraud. The authors suggest that while traditional fraud detection system are essential, incorporating AI based systems can enhanced fraud prevention by analysing behavioural patterns and flagging suspicious activities in real time.

D. Regulatory Compliance Risk

As digital banking evolves so too do the regulatory frameworks governing the financial sector. Compliance risks associated with e-banking are a recurring theme in the literature, according to Narayan and Sharma (2023), regulatory authorities across the world face the challenges of keeping pace with technological advancements, which creates gaps in the legal frameworks. These gaps provide opportunities for cybercriminals to exploit vulnerabilities in e-banking systems.

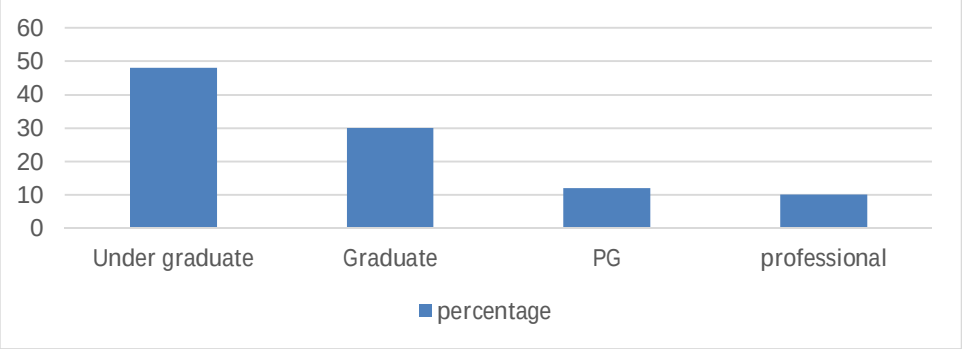
E. Mitigation Strategies And Technological Solutions

Several studies have focused on the effectiveness of various mitigation strategies and technological solutions in reducing risks. Ali and Singh (2022) explored the role of artificial intelligence in improving the security and efficiency of e-banking systems.AI and machine learning, they argue, are crucial in developing predictive models for fraud detection analysis. Similarly, Amin and Tiwari (2021) highlight the growing importance of block chain technology in enhancing transaction security, ensuring that every digital transactions in transparent, immutable, and tamper proof, thus reducing fraud and operational risks.

IV. DATA ANALYSIS AND INTERPRETATION

A structured questionnaire is prepared on risk analysis of e banking to get the view of respondents. The survey is conducted by sending the google form to the respondent in twin cities. 100 responses are received and analysed.
Showing education

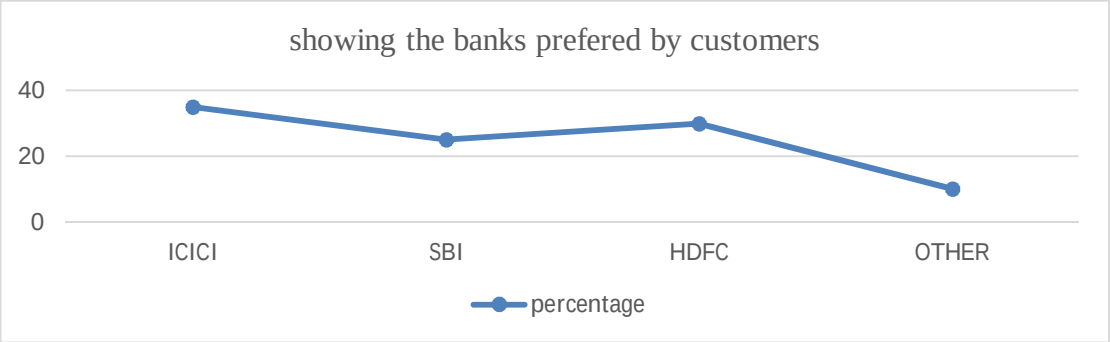
Education	percentage	count
Under graduate	48	15
Graduate	30	24
PG	12	5
professional	10	6



The figure shows 48%of the responders are under graduates,30%of them are graduate,12%of them are PG and 10%of them are professionals.

Showing the banks preferred by customers

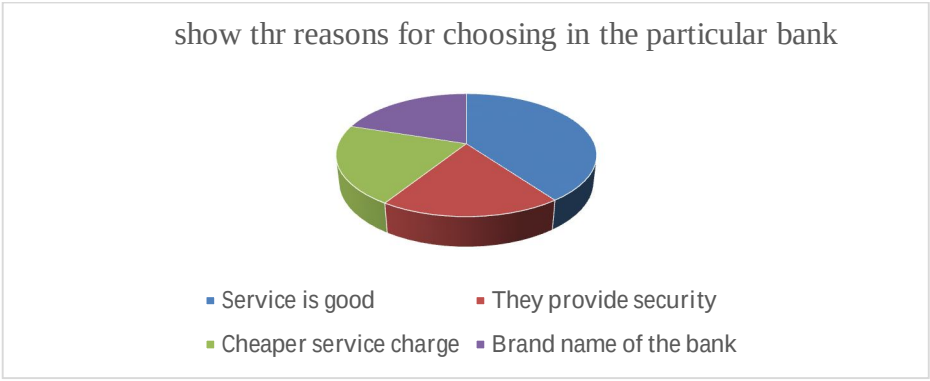
banks	percentage	Count
ICICI	35	15
SBI	25	5
HDFC	30	20
OTHER	10	15



The figure shows 35% of the population are customers to ICICI bank, 25% of SBI, 30% HDFC and 10% of other banks.

showing the reasons for choosing the particular bank

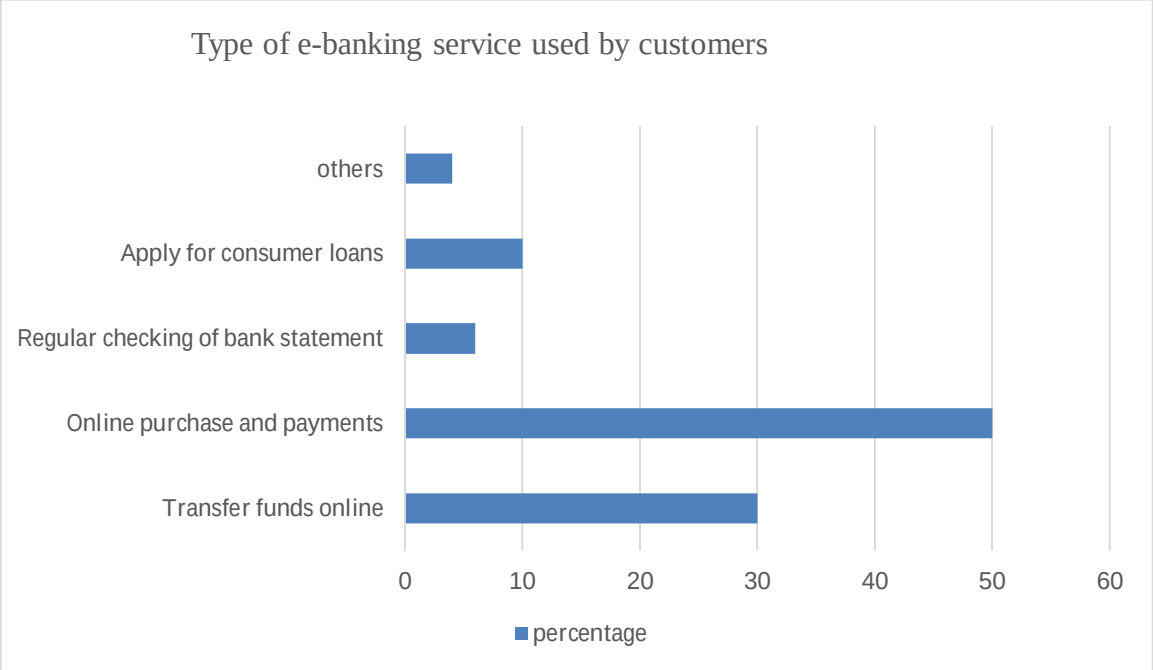
options	percentage	Count
Service is good	40	20
They provide security	19	9
Cheaper service charge	21	10
Brand name of the bank	20	15



The figure shows the reason for choosing the particular banks by respondents,40% have opted for better service,19%for the better security,21%for cheaper service charge and 20% for the brand name of the bank.

Type of e-banking service used by customers

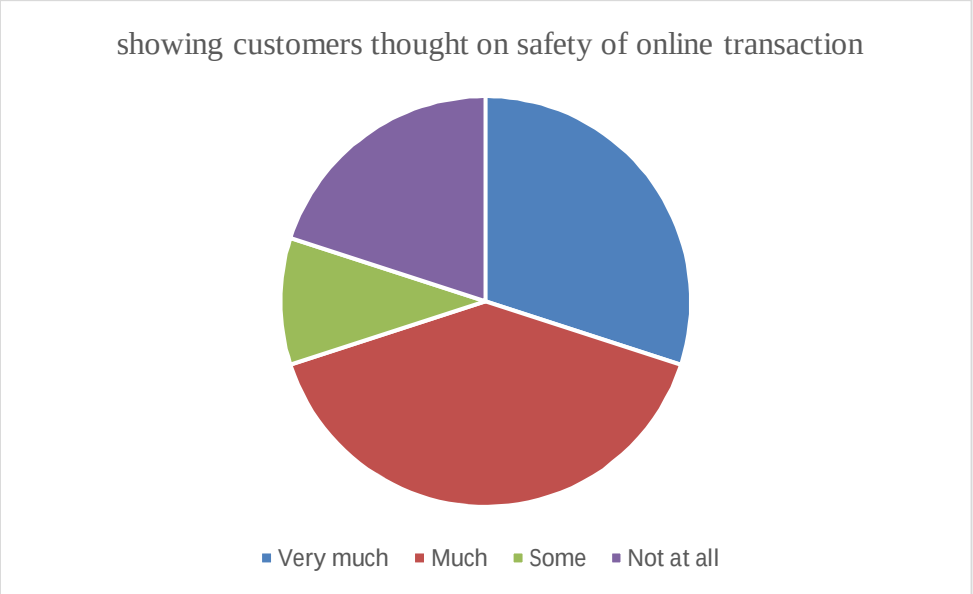
options	percentage	count
Transfer funds online	30	18
Online purchase and payments	50	28
Regular checking of bank statement	6	8
Apply for consumer loans	10	10
others	4	2



The graph shows type of online service used by customers,30%use it for online fund transfer.50%use it for online purchase,6%for statement check and 10% for applying consumer loans and 4%for others.

showing customers thought on safety of online transaction

Options	percentage	Count
Very much	30	10
Much	40	30
Some	10	12
Not at all	20	6



The figure shows the customers thought on safety of online banking, majority have voted for much,30%for very much,10%for some and 20%for not at all.

V. FINDINGS AND SUGGESTIONS

A. *Findings*

1) Technology plays as an important role as both a source and a tool for risk control.
2) Security risks are clearly identified as being most important.
3) Strategic risks- competition offering superior or more secure service. Failure to adopt emerging technologies like block chain or AI
4) Financial risk - losses from fraudulent transaction or identity theft. Reputational damage due to breaches affecting customer trust.
5) Cybersecurity risk-phishing attacks targeting customers and employees. distributed denial of service(DDOS)attacks disrupting services.
6) Compliance risk-failure to adhere to data production laws.

B. *Suggestions*

1) Adopt the right technology and systems and have proper access control.
2) Ensure adequate internal communication and educate and upgrades staff and management skills.
3) Regularly review the capabilities of existing hardware and software.
4) Bank should give awareness to their customers to use more of e banking services.
5) Create a trust in the minds of customers towards the security issues.

VI. CONCLUSION

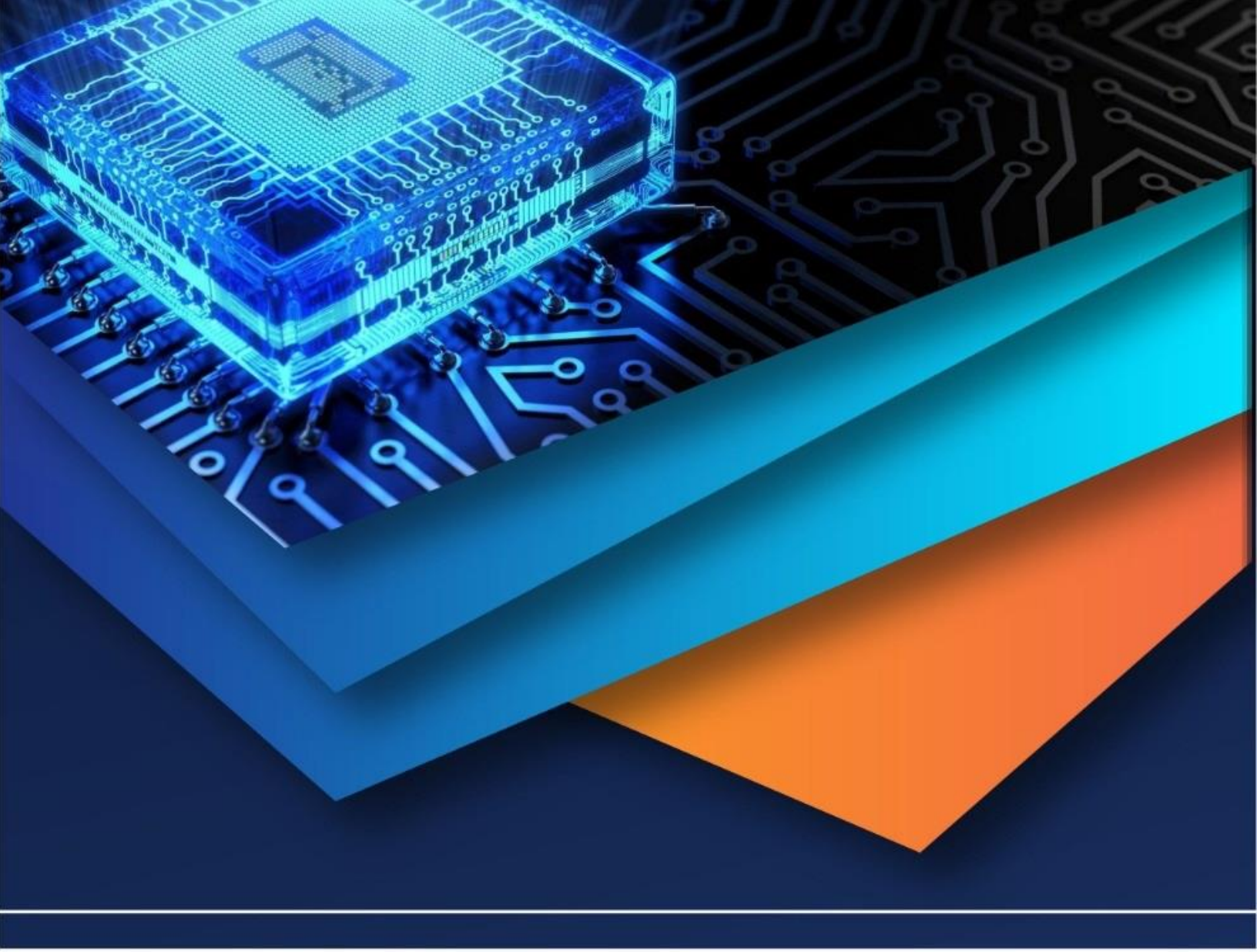
E-banking has revolutionized the way financial services are delivered, offering unparalleled convenience, efficiency and accessibility to user worldwide. However, the evolution of digital banking also introduce a range of risks that must be carefully managed.

These risks include cybersecurity threats, data breaches, phishing attacks, regulatory non-compliance, operational disruptions and reputational damage.

To mitigate these challenges, banks must adopt a multi-layered approach to risk management. This involves deploying advanced cybersecurity technologies, fostering a culture of awareness among customers and staff, and ensuring robust regulatory compliance. Regular audits, effective incident response plans, and partnerships with technology providers can further strengthen the security framework

REFERENCES

[1] E-banking and risk management" by J.M. Gomez and J.M. del Pozo(springer,2017)
[2] "Risk management in e-banking" by S.K. Goyal and R.K. Singh (CRC press,2018)
[3] E-banking risk management: A review of the literature" by S. K. Goyal and R. K. Singh (Journal of Internet Banking and Commerce, 2017)
[4] "Risk analysis of e-banking systems using fuzzy logic" by A. K. Singh and R. K. Singh (Journal of Intelligent Information Systems, 2018)
[5] "E-banking security risks and mitigation strategies" by R. K. Singh and S. K. Goyal (Journal of Information Security and Applications, 2019)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY