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 : 1604-1608

e-ISSN : 2583-1062
Impact Factor : 7.001

EVALUATION OF E-BANKING RISK

E. Sudharsan[1], Dr. Nagalakshmi M[2]

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

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

DOI: https://www.doi.org/10.58257/IJPREMS40070

ABSTRACT

As a fundamental component of contemporary financial services, e-banking provides accessibility and convenience but also presents a number of hazards that need to be properly addressed. However, there are a number of serious hazards associated with this move to digital platforms, such as fraud, identity theft, Dara breaches, cybersecurity threats, operational failures, and problems with regulatory compliance. These hazards are thoroughly examined in this study, which divides them into operational, technological, and human elements. In order to guarantee safe and dependable e-banking systems, the report also examines mitigation techniques such sophisticated cybersecurity frameworks, client education, and regulatory compliance measures. The results highlight how crucial proactive risk management is to maintaining operational stability and trust in e-banking systems.

Key Words: electronic banking, risk, difficulties, and risk control

1. INTRODUCTION

Customers can now perform financial transactions at any time and from any location thanks to e-banking, commonly referred to as online or electronic banking, which has completely transformed the financial services sector. For financial institutions, this paradigm change has greatly improved operational efficiency and client convenience. But as the use of digital platforms increases, so do the risks and weaknesses that come with them.

Cyberattacks, fraud, illegal access, and system failures are the main hazards associated with online banking. These can lead to monetary losses, harm to one's reputation, and legal repercussions. Furthermore, these difficulties are made worse by the human element, which includes low user knowledge and internal fraud.

2. OBJECTIVES OF THE STUDY

1. to research the effects and raise awareness of online banking services.
2. The study discusses the benefits and drawbacks of utilizing online banking services.
3. to research and assess how well e-banking activities are performing.
4. to research the most recent technological developments and how they affect e-banking operations.

3. REVIEWS OF LITERATURE

The risks facing the dynamic and expanding e-banking industry are becoming more complicated. Many studies have examined the different aspects of e-banking hazards during the last ten years, with an emphasis on how to identify, categorize, and mitigate them. The seamless operation of e-banking platforms depends on these risks, which are divided into four categories: cybersecurity risks, operational risks, financial and fraud-related risks, and regulatory compliance risks.

Risk to Cybersecurity

Since cybersecurity is the biggest danger associated with online banking, a large amount of the literature has focused on this topic. The widespread use of online banking platforms has drawn cybercriminals, leaving e-banking open to a variety of threats like ransomware, phishing, and data breaches.The authors of a study by Jain et Ai (2021) highlight the growing sophistication of cyberattacks that target e-banking platforms, particularly as cloud computing and mobile banking technologies become more widely used. A number of studies, like as Singh and Gupta (2020), underline the growing concern over Dara privacy and security. They emphasize the necessity of multi-factor authentication, greater encryption, and machine learning-based threat detection in order to safeguard sensitive financial data. In light of prospective cyberattacks, these studies emphasize the significance of regular system upgrades and the deployment of thorough cybersecurity frameworks.

Risks to Operations

System malfunctions, service interruptions, and human mistake are examples of operational hazards in online banking. System outages, transaction mistakes, and inefficient processes can seriously erode consumer confidence and interfere with banking services, claim Bun and Imtiaz (2022).

Additionally, the launch of AI-powered banking services raises the possibility of computational errors or system failures even though it also offers innovation. Thakur and Sharma's research from 2021 looks at how disaster recovery

plans and real-time monitoring tools might improve operational resilience in e-banking. Their results highlight the value of operational risk management systems that guard against technical disruptions and guarantee continuous services.

Risks Associated with Finance and Fraud

Recent research has focused a lot of emphasis on fraud and financial crimes in e-banking, particularly as cybercriminals come up with novel ways to take advantage of the digital financial environment. In a study published in 2022, Kumar and Narula examined a number of fraud concerns, including as internal fraud, fraudulent transactions, and identity theft. According to the authors, while conventional fraud detection systems are crucial, integrating AI-based systems can improve fraud prevention by identifying suspicious activity in real time and analyzing behavioral patterns.

Risk of Regulatory Compliance

The regulatory structures that oversee the financial industry change along with digital banking. According to Narayan and Sharma (2023), the literature frequently discusses the compliance concerns connected to online banking. Regulatory bodies worldwide struggle to keep up with technological developments, which leads to legal framework gaps. These holes give hackers the chance to take advantage of weaknesses in e-banking systems.

Technological Solutions and Mitigation Techniques

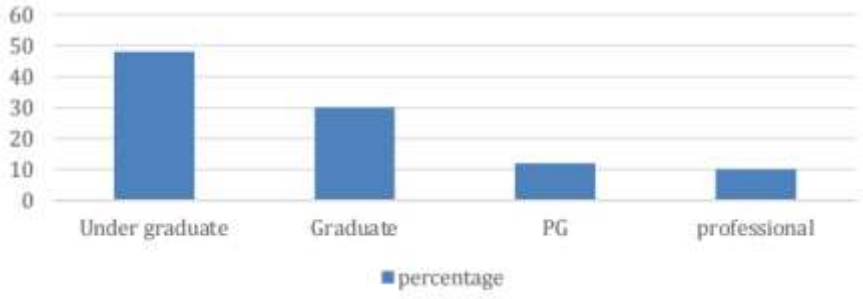
The efficiency of different risk-reduction techniques and technical advancements has been the subject of numerous studies. The potential of artificial intelligence to enhance the effectiveness and security of e-banking systems was investigated by Ali and Singh (2022). They contend that creating predictive models for fraud detection analysis requires the use of AI and machine learning. In a similar vein, Amin and Tiwari (2021) emphasize the growing significance of blockchain technology in improving transaction security by guaranteeing that all digital transactions are transparent, unchangeable, and impenetrable, hence lowering operational and fraud risks.

4. DATA ANALYSIS AND INTERPRETATION

To gather respondents' opinions, a systematic questionnaire on e-banking risk analysis is created. Respondents in twin cities are sent a Google Form to complete the survey. We receive and analyze one hundred responses.

Showing education :

Education	Percentage	Total
Under Graduate	48	15
Graduate	30	24
PG	12	5
Professional	10	6



According to the data, 48% of respondents are undergrads, 30% are graduates, 12% are postgraduate students, and 10% are professionals.

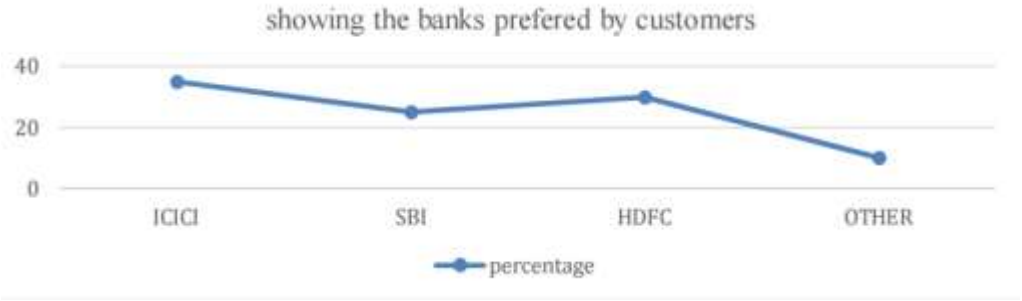
Displaying the banks that clients use :

Banks	Percentages	Total
ICICI	35	15
SBI	25	5
HDFC	30	20
Other	10	15

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 : 1604-1608

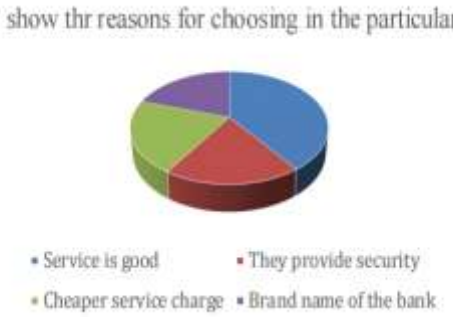
e-ISSN : 2583-1062
Impact Factor : 7.001



According to the statistic, 35% of people are ICICI Bank clients, 25% are SBI customers, 30% are HDFC customers, and 10% are customers of other banks.

showing the reasons for choosing the particular bank :

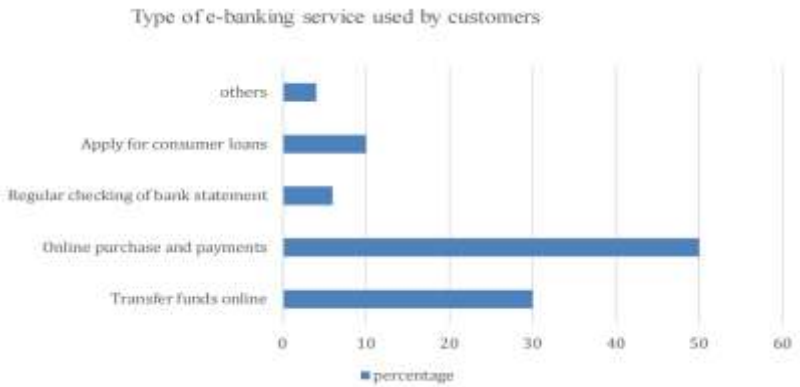
Options	Percentage	Total
Service is good	40	20
they provide security	19	9
15Cheap service charge	21	15
Brand name of the bank	20	10



The figure illustrates the respondents' reasons for selecting the specific banks: 40% chose the bank's brand name, 19% chose greater security, 21% chose lower service fees, and 20% chose better service.

The kind of online banking service that clients use :

Options	Percentage	Total
Transfer fund online	30	18
Online purchase and payments	50	28
Regular checking of bank statement	6	8
Apply for customer loans	10	10
Other	4	2

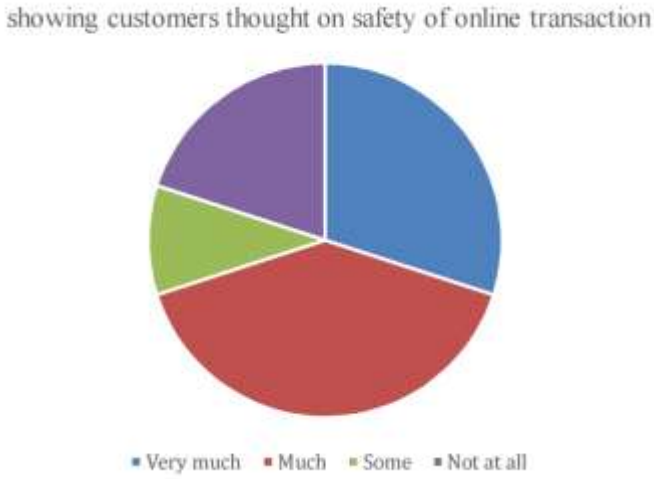


According to the graph, 30% of consumers use the web service for online money transfers. 50% use it to make purchases online, 6% to check their statements, 10% to apply for consumer loans, and 4% for other purposes.

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 : 1604-1608
e-ISSN : 2583-1062
Impact Factor : 7.001

displaying consumers' opinions about the security of online transactions :

Options	Percentaage	Total
Very much	30	10
Much	40	30
Some	10	12
Not at all	20	6



Customers' opinions on the safety of online banking are depicted in the image; the majority voted for much, 30% for very much, 10% for some, and 20% for not at all.

5. FINDINGS

1. Technology is a valuable resource and instrument for risk management.
2. It is evident that security risks are the most significant.
3. Strategic risks: rivals providing better or safer services. Not implementing cutting-edge technologies like blockchain or artificial intelligence
4. Financial risk: losses resulting from identity theft or fraudulent transactions. harm to one's reputation as a result of violations that undermine consumer confidence.
5. Phishing attacks that target employees and customers pose a cybersecurity risk. Services are being disrupted by distributed denial of service (DDOS) attacks.
6. Risk of noncompliance with data production regulations

6. SUGGESTIONS

1) Have appropriate access control and implement the appropriate systems and technology.
2) Make sure there is enough internal communication, and train and improve management and employee abilities.
3) Examine the capabilities of the current software and hardware on a regular basis.
4) Customers of the bank should be encouraged to use online banking more.
5) Establish a sense of trust with consumers regarding security concerns.

7. CONCLUSION

The delivery of financial services has been completely transformed by e-banking, which provides users all over the world with unmatched accessibility, efficiency, and convenience. But the development of digital banking also brings with it a number of hazards that need to be properly controlled.

These hazards include phishing attacks, data breaches, cybersecurity threats, operational disruptions, non-compliance with regulations, and harm to one's reputation.

Banks must implement a multi-layered strategy to risk management in order to lessen these difficulties. This entails implementing cutting-edge cybersecurity solutions, encouraging a culture of awareness among clients and employees, and guaranteeing strict adherence to regulations.

The security architecture can be further strengthened through collaborations with technology suppliers, efficient incident response strategies, and routine audits.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1604-1608

e-ISSN : 2583-1062
Impact Factor : 7.001

8. REFERENCES

[1] J.M. Gomez and J.M. del Pozo's "E-banking and risk management" (Springer, 2017)

[2] S.K. Goyal and R.K. Singh's "Risk management in e-banking" (CRC press, 2018)

[3] Review of the literature on e-banking risk management by S. K. Goyal and R. K. Singh (Journal of Internet Banking and Commerce, 2017)

[4] A. K. Singh and R. K. Singh's paper "Risk analysis of e-banking systems using fuzzy logic" was published in the Journal of Intelligent Information Systems in 2018.

[5] R. K. Singh and S. K. Goyal's article "E-banking security risks and mitigation strategies" appeared in the Journal of Information Security and Applications in 2019.