Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Digital Banking Under Siege: Trends and Challenges in Emerging Security Threats

Neeraj Kumar[1)], Suprina Sharma[2)], Palki Sharma[3)], Dr. Prakash Mishra [4)], Bhavna Sharma[5)], Ankita Sharma[6)]

[1] *Associate Professor, Department of Business Administration, Swami Vivekanand Institute of Engineering and Technology, Banur-140601, Punjab, India*

[2] *Department of Management, Chandigarh Group of Colleges Jhanjeri, Mohali-140307, Punjab, India, Department of Management, Chandigarh School of Business*

[3] *Department of Management, Chandigarh Group of Colleges Jhanjeri, Mohali-140307, Punjab, India, Department of Management, Chandigarh School of Business*

[4] *Associate Professor, Department of Management and Commerce, Mangalayatan University Jabalpur (M.P)*

[5] *Assistant Professor, Department of Management and Commerce, Mangalayatan University Jabalpur (M.P)*

[6] *Department of Management, Chandigarh Group of Colleges Jhanjeri, Mohali-140307, Punjab, India, Department of Management, Chandigarh School of Business*

[a)] ***Corresponding author:*** ***neeraj_kumar@sviet.ac.in***

ARTICLE INFO

Received: 10 Jan 2025

Revised: 12 Feb 2025

Accepted: 31 March 2025

ABSTRACT

Financial services have changed as a result of the growing reliance on digital banking technologies, yet there are also serious security and privacy issues. Based on existing literature, this research aims to examine the literature in order to identify the vulnerabilities affecting the integrity of the digital banking systems such as malware, phishing and data breach attacks. It also looks at the effectiveness of employing various risk mitigation methods such as multi-factor authentication, encryption, and biometric verification. Other areas of focus include the impact of user awareness campaigns and the effects of legislative measures on security enhancements. The findings stress the importance of developing effective strategies and remaining up to date with technological changes to address evolving threats. This article provides an extensive analysis of new technologies and effective methods in order to ensure a safer comprehensive environment for digital banking.

Keywords: Digital Banking, Security, Privacy, Multi-factor Authentication, Encryption, Biometric Verification, Regulatory Frameworks, Financial Data Protection.

Introduction

Digital banking entails the delivery of banking services over the Internet, allowing customers to open accounts, transfer funds, and use other services with electronic devices like mobile phones, tablets, laptops or desktops, and ATMs. The pandemic period demonstrated the usefulness of online banking as there were few visits to the physical branches. Use of digital wallets, mobile bank apps, bank cards and contactless payments changed the way of banking for consumers as they become more popular.

In spite of the transformative impact, investing in digital economies has its competitive practitioners but banks are struggling with the increasing expectations from the customers. This paper reviews the existing literature on the major challenges confronting the expansion of digital banking, which are the technological, security, and operational ones, and suggests how best to overcome these challenges.

Key Challenges in Digital Banking

1. Volatile Banking Patterns and Product Enhancements: As consumers grow accustomed to fast and effective interaction with the bank, the pressure on the banks to change their processes and provide tailored financial products increases. Increase in cashless payments makes it necessary to create products meeting consumer needs in different markets, especially in regions that are not well developed. Additionally, Financial products

must be effectively localized to enhance their uptake in foreign countries. Additionally, banks require strong mechanisms.

2. Security Threats: As more people embrace digital banking, the chances of finding fraudsters have also increased significantly, thus making customers and the banks likely to suffer losses. Some of the common fraudulent techniques include:

Vishing: Phone calls deceiving people that they need to provide sensitive information during KYC updates or while activating the card.

Phishing: Emails or SMS pretending to come from the banking institution.

Remote Access Attacks: Users unknowingly download malicious software applications that allow hackers to breach the customers database.

Fake UPI Requests: Fake UPI payments with the intent of stealing money.

Social Engineering Scams: Use of fake bank numbers or posing as a bank staff through search engines and social media.

To counter these threats, it is no doubt that stronger restrictions on security like multifactor authentication should be effective, as well as restricting the amount of knowledge customers should be aware of when performing any banking activities online.

3. Technical Challenges

As more and more consumers demand a high level of reliability and was to perform their transactions swiftly, it has put a lot of stress to the current communication and transaction structure in place, including blackouts and obsolete core banking establishments. It is essential to develop the technological success aspects of the business which will include rolling out futuristic cloud compatible systems that are robust to be able to meet the service demand without and bottlenecks. Initiatives geared at reducing the downtimes of UPI and enhancing communications to users in the event of service extravagances should be handled aggressively.

5. Change in the Foreseeing of the Customer

As the world continues to digitise, customers' demands for better products and services are on the rise. The rapid growth of UPI transactions, amounting to INR 10.4 lakh crore in August 2022, only highlights the pressing demand for robust technological development. It is important for banks to have a modern and flexible workforce that can address these areas while still adhering to risk and control standards.

Review of Literature

Hutchinson, D., & Warren, M. (2003) presented the recommendations to improve the security technology in the internet banking services. It looks towards assessing risks and implementing strategies to counter phishing, malware, and illegal access. The authors highlight the trends in the studies that reveal multilevel security comprising encryption of data, firewalls, and authentication is needed.

Kumar, M. (2023) discussed issues, such as, ransomware, identity theft, and transaction frauds, and argues the necessity of implementing effective cybersecurity policies. Suggested measures included system updates, user training, and deployment of AI based abnormality detection systems.

Revathi, P. (2019) examined the reasons for rural non-use and urges incorporation of appropriate regulations for enhanced security solutions that are contextual.

M. F. Mridha, K. Nur, A. K. Saha & M. A. Adnan (2017) Proposed a new Security Mechanism to Mitigate Internet Banking Vulnerabilities Utilizing multifactor authentication, biometric verification and tokenization, the research proposes a framework that enhances the security of digital transactions by orders of magnitude.

Wodo, W., & Stygar, D. (2020) emphasized on User-Centered Research: Digital Banking Security Perception by End-Users in Poland It notes the lack of user knowledge and awareness as a specific weak link, stressing that customers must be educated in safe banking conduct.

Dhoot, A., Nazarov, A. N., & Koupaei, A. N. A. (2020) proposed a novel holistic risk model for online banking systems considering threats, vulnerabilities and consequences The model allows users to proactively manage risk by identifying which areas are deemed high-risk and managing countermeasures—such as near real-time monitoring and strong encryption mechanisms-at the beginning of key activities throughout OI and applying appropriate action before risks manifest.

Puente, F., Sandoval, J. D., Hernandez, P., & Molina, C. J. (2005) proposed online Financial Service Security in enhancing such security, using a separate hardware device developed for special purpose use like a security token and USB key to do identification. They provide two-factor authentication through one-time passwords, resulting in a more secure login process.

Dagada, R. (2013) highlighted the challenges such as ATM fraud, data breach and weak user authentication systems adding that regulatory compliance by organizations and better awareness among end-users can improve security.

Chaimaa, B., Najib, E., & Rachid, H. (2021) introduced the fundamentals of e-banking and enumerates challenges such as crimes related to hacking, phishing, and transaction fraud. Solutions that you can speak about include defining encryption protocols, secure socket layers (SSL), two-factor authentication to counteract security issues.

Indriasari, E., Prabowo, H., Gaol, F. L., & Purwandari, B. (2022) studied the emerging technologies for the security of digital banking: A review banks are emerging businesses to the era of Industry with rapidly developing technology and infrastructure in the financial sector they completely have to be aware of their business processes that must securely run. The report highlights data breaches, malware, and identity theft as the most serious issues confronting the nation while recommending a research agenda that advances RFID technologies in order to be more secure.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024) dealt with the twin issues of customer data security and cybersecurity management during the rapid digitalization of the banking sector. It puts a premium on data privacy regulations (GDP, for example) and advanced threat management for the protection of private data.

Ali, M., Khan, M. A., & Kalwar, M. A. (2021) examined customer concerns regarding online banking, focusing particularly on security. They identified issues such as inadequate user authentication methods and a general lack of awareness around cyber hygiene, proposing that enhanced customer education and improved interface security could address these challenges.

Research Gaps

Limited User-Centric Security Measures and Awareness Strategies

While multiple studies (Wodo & Stygar, 2020; Ali et al., 2021) stress the significance of user awareness in reducing cybersecurity risks, there is a noticeable absence of comprehensive frameworks that combine technological solutions with user-centered strategies. Existing literature often overlooks the interplay between user behavior, education, and technological advancements, leaving a gap in strategies to simultaneously enhance system security and user trust.

Inadequate Focus on Regulatory Compliance and Cross-Border Security Challenges

Studies like *Wang et al. (2024)* and *Dagada (2013)* discuss data privacy and regulatory frameworks in specific regions but fail to address the challenges of cross-border digital banking operations. The global nature of digital transactions necessitates research on harmonizing international regulatory standards and addressing security risks arising from cross-border data flows, which remains a critical yet underexplored area in the existing literature.

Objectives of the study

1. To identify the security issues and challenges faced by customers in digital banking technology.
2. To suggest solutions to the customers regarding digital transactions issues and challenges to create awareness among customers.

Research Methodology

The secondary data was collected for the research purpose from various literatures and websites. The research was descriptive in nature as behaviour of customers towards security, issues and challenges has been observed in this study. The study relied on existing data to explore and analyze the behaviour of customers regarding security, issues and challenges in digital banking. Being descriptive in nature, the research focused on observing patterns, trends, and concerns reflected in secondary data with the help oh thematic analysis, rather than primary data collection. This approach provided insights into customers perceptions and responses, supported by existing evidence and documented findings, offering a broader perspective on the challenges faced in digital banking technologies.

Limitations of the study

The study relies solely on secondary data from existing literature and reports. This limits the ability to verify findings through primary data collection, such as customer surveys or interviews, which could provide real-time insights.

Analysis & Interpretation

Security Challenges of Digital Banking

The research describes the critical security threats such as malware, phishing, data breaches and identity theft that erode trust in digital banking. These tactics are referred to as phishing and vishing respectively. Data is compromised with remote access and malware attacks with hackers asking for unauthorized access. Similarly, with the growing adoption of digital payments, we have seen the emergence of fake requests for UPI and social engineering scams.

The most significant problem is about vulnerabilities in digital banking solutions, fueled by cyber threats and bad user habits.

Security Vulnerabilities in Digital Banking

The research suggests multi-factor authentication (MFA), encryption and biometric verification to protect sensitive banking information. Encryption makes secure transfer of data possible, and MFA provides an additional layer of security. Student biometric verification is an advanced method of identifying students through their physical attributes. Such technological solutions play an integral role in securing digital banking systems against emerging cyber threats.

User Awareness and Education Approach

Awareness campaigns may help consumers recognize phishing attacks and actually implement secure online banking methods. The paper also proposes to include easy interfaces to direct customers, especially those with limited experience on digital platforms. This approach aims to provide customer education while enhancing user habits to mitigate potential vulnerabilities.

Regulatory and compliance challenges

It is not enough to say that the regulatory framework exists for banks to meet security standards. But it sees a hole in cross-border security because of conflicting national regulations. This adds to the discussions surrounding the need for global cyber security regulations, particularly as digital banking is closely tied to international data transactions and flow.

Technological Innovations and Obstacles

The phenomena of digital banking evolving quickly but the transitional problems of aging core banking solutions and low adoption of new technologies. SHARE ON SOCIAL MEDIA You can share this story on social media: With the increasing use of UPI transactions, this also puts a strain on banks to scale their infrastructure to ensure demand. However, the theme is on technicalities and upgrading infrastructure to support higher transaction volumes.

Consumer Demand and Behavior

Consumers expect faster, more efficient services, pushing banks to provide customized products for various needs. As digital wallets and cashless payments become more prevalent, banks must guarantee their platforms are secure. It suggests that product localization in different markets is a growing requirement as customer needs and expectations evolve, and that companies increasingly need to meet them.

Difficulties in Rural and Semi-Urban Areas

There is a divide between availability of digital banking in urban and rural regions as the latter is still facing challenges of access to digital means of exchange. High street banks are encouraged to put their time and emphasis on producing localized solutions to meet the needs of its Digital banking offerings in neglected regions. The attention is on digital inclusivity and closing the gap for rural and semi-urban areas.

Impact of the Pandemic

This trend continued further post COVID-19 pandemic, which played an important role in adoption of digital banking services, where need of security measures acts as a driver. Answering the specific issues alluded to by the character of the pandemic (the increase in digital transactions and the accompanying vulnerabilities) were essential and helped highlight the need to adapt security measures to improve and isolate the vulnerabilities introduced by the changes to technology, as needed.

Suggestions and Future directions

Previously, banks required different systems to provide security and accessibility for digital banking. It is very important to have security measures in place to detect and prevent fraud such as multi-factor authentication, end-to-end encryption and real time monitoring. Just as important is educating customers on phishing and spear-phishing and other threats from cyberspace through seminars, webinars and social media campaigns. Train your users to secure their digital banking accounts step by step, beginning from creating a new password and avoiding social networks. Banks must coordinate with regulators to establish cross border cybersecurity policy that maintains consistency and trust of operations globally. With firm understanding of customer need, sustain the human touch by using electronic system to solve specific customer problems. Local dialogues and efficient customer experiences that can span the digital divide can help digital marketing agencies to be more inclusive and personalized for different demographics, for different demographics like rural and semi-urban people. Moreover, with the creation of products and services based on the unique needs of the underserved areas, both the economic impact will rise up along with the economic growth. It proposes, for example, to reduce digital (online) fraud, with customer-oriented solutions, like clear and concise instructions on how to safely bank online, but also to improve support via human interfaces. Discussion of mutual collaboration between countries in the area of cyber security and the production of cyber security products by global companies for underserved areas. They provide customers with better security and convenient access, especially for rural and semi-urban communities.

Conclusion

The rapid growth of digital banking has transformed the financial landscape, offering consumers unparalleled convenience and efficiency. However, this transformation has also introduced significant security and privacy challenges. The paper emphasizes the importance of adopting a multi-pronged approach to address these challenges, which includes technological advancements such as multi-factor authentication (MFA), encryption, and biometric verification. Additionally, raising user awareness through educational campaigns and improving regulatory frameworks are crucial to enhancing security. Banks must continuously adapt their systems to meet evolving consumer expectations, while also addressing the digital divide and ensuring inclusive access for underserved populations. The COVID-19 pandemic has accelerated the need for these changes, making it imperative for banks to stay ahead of technological and security risks. Ultimately, the study stresses that a balanced approach combining innovative technology, comprehensive education, robust regulatory compliance, and improved infrastructure will enable digital banking to remain a secure, trusted, and effective service for all users.

References

[1] Ali, M., Khan, M. A., & Kalwar, M. A. (2021). Challenges for online banking in customers perspective: a review. *International Journal of Business Education and Management Studies*, *5*(1), 37-56.

[2] Chaimaa, B., Najib, E., & Rachid, H. (2021). E-banking overview: concepts, challenges and solutions. *Wireless Personal Communications*, *117*, 1059-1078.

[3] Dagada, R. (2013, March). Digital banking security, risk and credibility concerns in South Africa. In *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013). Kuala Lumpur, Malaysia* (pp. 4-6).

[4] Dhoot, A., Nazarov, A. N., & Koupaei, A. N. A. (2020). A Security Risk Model for Online Banking System. 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, 1–4. *IEEE. https://doi. org/10.1109/IEEECONF48371*.

[5] Hutchinson, D., & Warren, M. (2003). Security for internet banking: a framework. *Logistics information management*, *16*(1), 64-73.

[6] Indriasari, E., Prabowo, H., Gaol, F. L., & Purwandari, B. (2022). Digital banking: challenges, emerging technology trends, and future research agenda. *International Journal of E-Business Research (IJEBR)*, *18*(1), 1-20.

[7] Kumar, M. (2023). An overview of cyber security in digital banking Sector. *East Asian Journal of Multidisciplinary Research*, *2*(1), 43-52.

[8] Mridha, M. F., Nur, K., Saha, A. K., & Adnan, M. A. (2017). A new approach to enhance internet banking security. *International Journal of Computer Applications*, *160*(8).

[9] Puente, F., Sandoval, J. D., Hernandez, P., & Molina, C. J. (2005, October). Improving online banking security with hardware devices. In *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology* (pp. 174-177). IEEE.

[10] Revathi, P. (2019). Digital banking challenges and opportunities in India. *EPRA International Journal of Economic and Business Review*, *7*(12), 20-23.

[11] Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, *147*, 104051.

[12] Wodo, W., & Stygar, D. (2020, February). Security of Digital Banking Systems in Poland: Users Study 2019. In *ICISSP* (pp. 221-231).