

Benefits Challenges and Security of Mobile Banking: A Study on Customer Perspective

Pradeep Joshi

Associate Professor, School of Management, Graphic Era Hill University,
Dehradun Uttarakhand India

Abstract

Mobile banking offers numerous benefits that have transformed the way people manage their finances. One of the key advantages is the convenience it provides. Users can access their accounts anytime and anywhere, enabling them to make transactions, check balances, and pay bills without the need for physical visits to a bank. This accessibility allows for greater financial control and flexibility, especially for those with busy lifestyles. However, mobile banking also presents certain challenges. One major hurdle is the issue of security. As financial transactions are conducted over mobile devices, there is a heightened risk of fraud and unauthorized access. Malicious actors may try to get sensitive data by using social engineering methods or exploiting flaws in mobile banking applications. Ensuring robust security measures, such as two-factor authentication and encryption, is crucial to protect users' financial data. A group of 217 people (mobile banking customers) were surveyed to find out about the Customer Perspective regarding Benefits, Challenges and Security of Mobile Banking and found that mobile banking allows users to access their accounts anytime and anywhere but there is a risk of fraud and unauthorized access while financial transactions and authentication and encryption, is crucial to protect users' financial data.

Keywords: *Mobile Banking, Convenience, Accessibility, Transactions, Security*

Introduction

Mobile banking has revolutionized how individuals manage their finances, providing benefits that enhance convenience and accessibility. One of the key advantages of mobile banking is the ability to conduct transactions anytime and anywhere. Gone are the days of standing in long queues at banks or rushing to meet payment deadlines. With mobile banking, users can effortlessly transfer funds, pay bills, and check balances with just a few taps on their smartphones. This convenience is particularly beneficial for individuals with busy lifestyles or those residing in remote areas where physical access to banking services may be limited. Mobile banking has truly empowered users by giving them greater control over their financial affairs. Despite the challenges, mobile banking has made significant strides in enhancing security. Banks and financial institutions have implemented advanced security protocols to protect user information. Biometric authentication, such as fingerprint or facial recognition, has become a standard security feature, adding an extra layer of protection. Additionally, banks often provide real-time transaction alerts and monitoring systems, enabling users to detect and report any suspicious activity promptly.

Nevertheless, the rise of mobile banking has also brought forth a set of challenges, with security being the foremost concern. As financial transactions are conducted through mobile devices, there is an increased risk of fraud and unauthorized access. Cybercriminals constantly devise new methods to exploit vulnerabilities in mobile banking applications or trick users into revealing sensitive information. To address these challenges, financial institutions have implemented stringent security measures. Biometric authentication, such as fingerprint or facial recognition, has become a standard security feature in mobile banking apps. This ensures that only authorized users can access their accounts. Moreover, encryption technology is utilized to protect data transmitted between the user's device and the banking server. While

these security measures are effective, it is imperative for users to remain vigilant and adopt safe practices such as avoiding suspicious links or sharing personal information.

Despite the challenges, mobile banking continues to evolve, with advancements in security and user experience. Real-time transaction alerts and monitoring systems have become standard features in mobile banking apps. These mechanisms enable users to promptly detect any unauthorized activity and take appropriate action. Banks also provide customer support services specifically tailored for mobile banking, ensuring that users receive timely assistance for any concerns or issues. Furthermore, financial institutions actively educate their customers about safe mobile banking practices, emphasizing the importance of regularly updating their mobile devices and using strong, unique passwords. Individuals can confidently enjoy the convenience and efficiency offered by mobile banking by staying informed and practicing caution.

Literature Review

An article suggests a brand-new secure mobile banking protocol that offers robust authentication procedures. While minimizing computational processes and communication passes between them, it manages to entirely secure and protect the concerned parties and their money transactions. The suggested protocol's security features will be examined and proven. (Ngo et. al., 2011). Another article investigates the factors that determine service quality and how they affect a user's intention to continue using mobile banking. It revealed a strong correlation between all research constructs using a sample size of 258 North Indian respondents. Results showed that satisfaction somewhat mediated the connection between service quality and impact; trust did not function as a moderator. According to research, banks should prioritize user-friendly user interfaces and prioritize mobile security as a critical problem to safeguard clients from fraud. Only the northern region of India was the source of the data. (Srivastava & Vishnani, 2021).

Research examined Slovenian users' perspectives on mobile and Internet banking. An online poll of 15 Slovenian banks' customers generated data for statistical analysis. Security and reliability are the most critical factors in mobile and internet banking in Slovenia, where mobile banking utilization is limited. 69% selected the correct authentication technique, while 88% said that when they use mobile and Internet banking, authentication procedures do not impede them. Experts disagreed on the security-usability balance. The results show that Internet and mobile banking consumers prioritize security over user experience but still desire easy-to-use products (Svila & Zupancic, 2016). Another research was done to look at how trust and satisfaction are impacted by security and privacy concerns. It gathered 365 useful responses from Malaysian users of mobile banking using a survey research approach and a questionnaire. The findings indicated that security and privacy, operationalized as perceived credibility, are important predictors of trust and satisfaction. Furthermore, trust and satisfaction are strongly correlated with perceived quality. This emphasizes how crucial privacy and security are to the achievement of mobile banking services. (Masrek et. al., 2018).

According to the findings of an article, subjective norm, perceived risk, and perceived financial cost are the three factors most likely to influence people's behavioural intention to use mobile banking. This study is more important for Bangladeshi policymakers and mobile banking service providers since it will help them build services that will boost users' access to and use of the service, which will benefit the nation's effort to promote financial inclusion. (Siddik et. al., 2014). In another paper, it is stated that consumers now frequently use mobile banking to complete financial transactions. A brand-new system named S-Mbank is suggested to address this problem. To prevent attackers from using the unencrypted message provided to the user's mobile phone, it swaps the one-time password for a contactless smart card. Additionally, pair-based text authentication is suggested for the login process as a defense against shoulder-surfing attacks, along with a public-private key pair and PIN for two-factor and mutual authentication, an encryption method for computation efficiency, and public-private key pair for the PIN. To increase the security protection for mobile banking services, the Scyther tool is used to analyse the authentication protocol's security in the S-Mbank scheme. (Putra et. al., 2017).

A survey was done to determine the most recent authentication and communication security implementations for online banking. Global regions use different SSL/TLS implementations and single- or multifactor authentication techniques. It is anticipated that mobile banking will move into a third phase that would emphasize the use of standard web technology. Due to this, mobile banking may become a target for assaults. (Kiljan et. al., 2016). Another research examines the determinants and barriers to banks implementing mobile banking globally. Blogging was used to gather information for a two-round modified Delphi research. Results show that DOI theory is still useful in mobile environments for understanding the spread of mobile banking. Global mobile phone penetration, competitive advantage, consumer convenience, strategic importance, customer demand, low perceived risk/security concerns, and stakeholder alliances were important factors in the adoption of banks. According to research, banks face major obstacles from poor client demand and a lack of return on investment (ROI). Regarding multi-channel banking and the drivers and obstacles driving its adoption, this study has significance for banks. (Mullan et. al., 2017).

An article investigates why a person chooses to utilize mobile banking, both for social and professional reasons. It links technical innovation research with studies on entrepreneurship and learning and underlines the significance of financial risk in deciding someone's intent to use mobile banking. It also highlights how crucial it is for financial institutions to promote mobile banking innovation while addressing security issues. The paper combines research on mobile banking with contemporary ideas about how learning and entrepreneurship affect how people accept technical innovations. (Ratten, 2011). Another paper states that mobile banking services can increase access to financial services for the underprivileged while also offering a practical and affordable method of accessing bank accounts. This study examines the factors that affect mobile banking use with a focus on the regulatory environment. According to the findings, both the public and the unbanked use mobile banking more frequently when there is a supportive regulatory environment. (Gutierrez & Singh, 2013). A paper covers the security of SMS and USSD, two widely used mobile payment methods in poor nations. It assesses their security in relation to mobile banking systems and suggests a safer approach. To enhance data confidentiality, message integrity, and user authenticity, it advises integrating security elements into the system architecture. The recommendations are based on the technology's capacity to support these extra measures for data protection. (Nyamtiga et. al., 2013). Another research focuses on the obstacles to mobile banking adoption as well as client preferences and the impact of demographic factors on service uptake. According to the findings, the main obstacle is consumers' security concerns, and they favour information-based services over financial services offered by the bank. (Bamoriya & Singh, 2013).

Objective: To measure the Customer Perspective regarding Benefits, Challenges and Security of Mobile Banking.

Methodology: A group of 217 people (Mobile Banking Customer) were surveyed to know the Customer Perspective regarding Benefits, Challenges and Security of Mobile Banking. A checklist question was used to analyze and interpret the data. In a checklist question respondents choose “Yes” or “No” for all the questions.

Dataanalysis and interpretation

Table 1 Benefits, Challenges and Security of Mobile Banking

S. No.	Benefits, Challenges and Security of Mobile Banking	Yes	% Yes	No	% No	Total
1	Mobile banking allows users to access their accounts anytime and anywhere	150	69.1	67	30.9	217
2	Allows greater financial control and flexibility, especially for those with busy lifestyles	169	77.9	48	22.1	217

3	There is a risk of fraud and unauthorized access while financial transactions	157	72.3	60	27.7	217
4	Sensitive data can be used by social engineering methods or exploiting flaws in mobile banking applications	162	74.6	55	25.4	217
5	Authentication and encryption, is crucial to protect users' financial data	155	71.4	62	28.6	217
6	Banks provide real-time transaction alerts and monitoring systems, enabling users to detect and report any suspicious activity	164	75.6	53	24.4	217

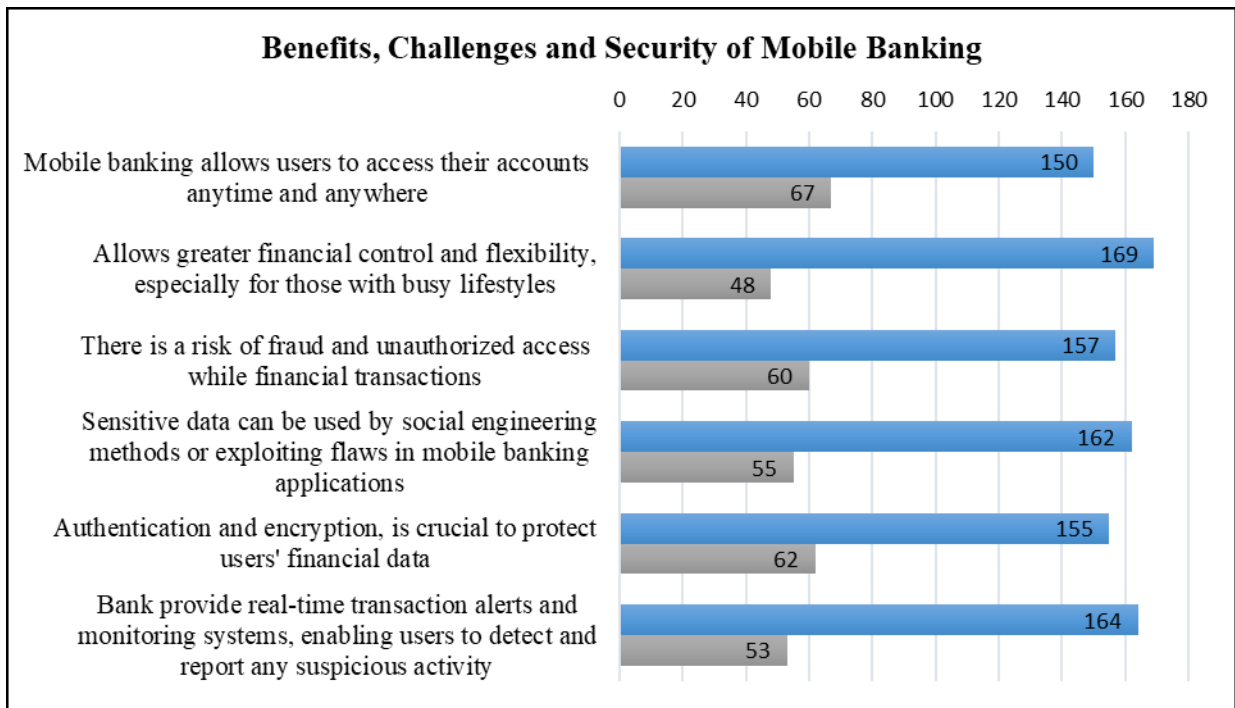


Figure 1 Benefits, Challenges and Security of Mobile Banking

Table and figure above are showing Benefits. Challenges and Security of Mobile Banking. It is found that around 69.1% of the respondent accept that Mobile banking allows users to access their accounts anytime and anywhere followed by mobile banking allows greater financial control and flexibility, especially for those with busy lifestyles (77.9%), there is a risk of fraud and unauthorized access while financial transactions (72.3%), Sensitive data can be used by social engineering methods or exploiting flaws in mobile banking applications (74.6%), Authentication and encryption, is crucial to protect users' financial data (71.4%) and Bank provide real-time transaction alerts and monitoring systems, enabling users to detect and report any suspicious activity (75.6%).

Conclusion

In conclusion, mobile banking has transformed the way individuals manage their finances, providing unprecedented convenience and accessibility. While security challenges exist, the industry has made significant strides in implementing robust measures to protect user information. By staying informed, adopting secure practices, and leveraging the built-in security features offered by mobile banking apps, users can confidently embrace this modern and efficient way of conducting financial transactions. The

future of mobile banking looks promising, with continuous advancements aimed at enhancing security, user experience, and financial empowerment. The study was conducted to know the Customer Perspective regarding Benefits, Challenges and Security of Mobile Banking and found that maximum people says that mobile banking allows greater financial control and flexibility, especially for those with busy lifestyles, Bank provide real-time transaction alerts and monitoring systems, enabling users to detect and report any suspicious activity but at the same time sensitive data can be used by social engineering methods or exploiting flaws in mobile banking applications.

References

- Bamoriya, D., & Singh, P. (2013). Mobile Banking in India: Barriers in Adoption and Service Preferences. *Banking & Insurance eJournal*.
- Gutierrez, E., & Singh, S. (2013). What Regulatory Frameworks are More Conducive to Mobile Banking? Empirical Evidence from Findex Data. *IO: Regulation*.
- Kiljan, S., Simoens, K., Cock, D. D., Eekelen, M. V., & Vranken, H. (2016). A survey of authentication and communications security in online banking. *ACM Computing Surveys (CSUR)*, 49(4), 1-35.
- Masrek, M. N., Halim, M. S. A., Khan, A., & Ramli, I. (2018). The impact of perceived credibility and perceived quality on trust and satisfaction in mobile banking context. *Asian Economic and Financial Review*, 8(7), 1013-1025.
- Mullan, J., Bradley, L., & Loane, S. (2017). Bank adoption of mobile banking: stakeholder perspective. *International Journal of Bank Marketing*.
- Ngo, H. H., Dandash, O., Le, P. D., Srinivasan, B., & Wilson, C. (2011). Formal verification of a secure mobile banking protocol. In *Advances in Networks and Communications: First International Conference on Computer Science and Information Technology, CCSIT 2011, Bangalore, India, January 2-4, 2011. Proceedings, Part II 1* (pp. 410-421). Springer Berlin Heidelberg.
- Nyamtiga, B. W., Sam, A., & Laizer, L. S. (2013). Security Perspectives for USSD versus SMS in conducting mobile transactions: A case study of Tanzania. *international journal of technology enhancements and emerging engineering research*, 1(3), 38-43.
- Putra, D., Sadikin, M., & Windarta, S. (2017). S-Mbank: Secure mobile banking authentication scheme using signcryption, pair-based text authentication, and contactless smart card. *2017 15th International Conference on Quality in Research (QiR): International Symposium on Electrical and Computer Engineering*.
- Ratten, V. (2011). Mobile banking innovations and entrepreneurial adoption decisions. *International Journal of E-Entrepreneurship and Innovation (IJEEI)*, 2(2), 27-38.
- Siddik, M. N. A., Sun, G., Yanjuan, C. U. I., & Kabiraj, S. (2014). Financial inclusion through mobile banking: a case of Bangladesh. *Journal of Applied finance and Banking*, 4(6), 109.
- Srivastava, S., & Vishnani, S. (2021). Determinants of mobile bank usage among the bank users in North India. *Journal of Financial Services Marketing*, 26(1), 34-51.
- Svilar, A., & Zupančič, J. (2016). User experience with security elements in internet and mobile banking. *Organizacija*, 49(4), 251-260.