Indonesian Banking Review
Volume 1, Number 2, 2022

Mobile Banking Data Security in Indonesia: Challenges, Solutions, and Policy Implications

Muhammad Kafal Faa'Id[1*]

[1] Universitas Sarjanawiyata Tamansiswa, Yogyakarta, Indonesia

Abstract

Article history:
Received: July 19, 2022
Revised: August 10, 2022
Accepted: September 25, 2022
Published: December 30, 2022

Keywords:
Banking Regulation,
Data Security,
Digital Literacy,
Financial Inclusion,
Mobile Banking.

Identifier:
Zera Open
Page: 166-183
https://zeraopen.com/journal/ibr

The advancement of mobile banking in the era of the Fourth Industrial Revolution has become a major driver of digital transformation in Indonesia's financial sector. This service not only improves transactional efficiency but also plays a vital role in promoting financial inclusion by reaching communities previously excluded from conventional banking. However, rapid growth has also introduced critical challenges regarding data security. This study employs a qualitative approach through literature review to examine global trends, national conditions, key threats, and available solutions. The findings reveal that phishing, malware, hacking, and data breaches remain dominant threats in mobile banking ecosystems. Meanwhile, technical solutions such as encryption, multi-factor authentication, biometrics, as well as artificial intelligence and blockchain technologies have proven effective, yet their success highly depends on users' digital literacy. Furthermore, national regulations lag behind international standards, requiring more proactive policymaking and continuous education. This research emphasizes that a holistic approach integrating technology, digital literacy, and adaptive regulation is essential to safeguard public trust in mobile banking.

*Corresponding author:
(Muhammad Kafal Faa'Id)

1. Introduction

The Industrial Revolution 4.0 has brought major changes in the global order of life, especially through the acceleration of digitalization in various sectors, including banking. One of the tangible manifestations of digitalization is the rapid growth of mobile banking as the main medium of financial transactions. Recent reports show that the number of mobile banking users globally continues to increase, with high penetration in both developing and developed countries. In Indonesia, the number of digital banking transactions through mobile banking reached more than IDR 50,000 trillion, experiencing significant growth from the previous year. This trend underscores the vital role of mobile banking in driving financial service efficiency, expanding financial inclusion, and providing more equitable access to banking products.

However, behind this growth, there are major challenges related to data security. Users' trust in mobile banking services is greatly influenced by the information security guarantees they have. Cases of cyber attacks such as phishing, malware, and data breaches are increasingly found in the digital banking ecosystem (Wazid et al., 2019). In Indonesia itself, the Financial Services Authority (*Otoritas Jasa Keuangan* /OJK) recorded an increase in cases of banking digital crimes, especially due to weak user awareness and bank security systems that still need to be strengthened. This phenomenon emphasizes the urgency of discussing the data security aspect in mobile banking, not only from a technical but also non-technical perspective such as regulation and user education.

The concept of data security in mobile banking involves various key aspects, ranging from encryption, authentication, to authorization. In addition, the protection of data integrity and availability is an absolute requirement in maintaining user trust (Sharma et al., 2021). Furthermore, security practices cannot be separated from the user's awareness. Studies show that even though banks have implemented cutting-edge security systems such as multi-factor authentication (MFA) and biometrics, there is still a high risk if users do not understand the importance of strong passwords or are wary of phishing (Baabdullah et al., 2019).

Correspondingly, the best practices implemented by the modern banking industry include the integration of new technologies such as artificial intelligence (AI), machine learning (ML), and blockchain to improve security systems. However, previous research shows that there is a research gap related to non-technical aspects such as customer digital literacy and security regulations in developing countries, including Indonesia. The majority of research tends to emphasize technical aspects, whereas user education and the capacity of banking staff are equally important in reducing the risk of cyberattacks (Rana et al., 2020).

Based on this background, this study aims to identify the main challenges in mobile banking data security in Indonesia, evaluate the effectiveness of technical solutions such as encryption and biometrics, and emphasize the importance of user education. The results of this study are expected to be able to provide relevant strategic recommendations for banks and regulators, so as to increase public confidence in mobile banking services and strengthen the resilience of the national financial system.

2. Literature Review

2.1. Global and National Trends in Mobile Banking

The growth of mobile banking globally has shown a significant increase in the last decade. The main driving factors include smartphone penetration, internet connectivity, and changes in consumer behavior towards fast and efficient digital services. A global study shows that more than 70% of banking service users in Southeast Asia have switched to mobile banking applications as the primary channel of their financial transactions (Abidin et al., 2019). In Indonesia, the digital transformation of banking has been accelerated by the COVID-19 pandemic which has encouraged people to minimize physical contact in financial activities. Value of digital banking transactions grew by more than 25% compared to the previous year, indicating the acceleration of mobile banking adoption in the community. This growth has had a major impact on financial inclusion.

Mobile banking provides access to banking services to people in remote areas that were previously difficult to reach by the bank's network of physical offices. This supports the Sustainable Development Goals (SDGs), especially in expanding access to formal finance. However, the surge in mobile banking usage is also accompanied by increased vulnerability to cybercrime risks. Ordinary users who are accessing digital banking services for the first time often lack data security literacy, making them easy targets for criminals (Ramadhan, 2021). Therefore, the positive trend of mobile banking adoption needs to be balanced with strengthening security systems and user education so that this growth is not accompanied by adverse risks.

2.2. Security Challenges in Mobile Banking

Data security is a central issue in the development of mobile banking. The most common threats are phishing, malware, hacking, and data breaches. These attacks not only harm individual users but also degrade the public's reputation and trust in banks. Recent studies show that phishing attacks through messaging apps and social media have increased significantly since 2020, with the mode of pretending to be the bank's side to steal user credentials (Goel & Jain, 2018). On the other hand, mobile banking malware is getting more sophisticated because it takes advantage of loopholes in smartphone operating systems that are not updated by users. In addition to external threats, there are also internal challenges from the bank itself. Some banks in developing countries still use legacy security systems that are vulnerable to exploitation.

National security regulations and standards often lag behind compared to the ever-evolving complexity of cyber threats. In Indonesia, although OJK and Bank Indonesia have issued cybersecurity policies, implementation at the operational level of banks often faces limited resources and technology. The study by Mendhurwar and Mishra (2021) emphasized that internal weakness factors, including the lack of training of bank staff in dealing with cyber incidents, magnify the potential for losses. Thus, mobile banking security cannot only rely on technology, but must also be supported by internal policies, effective regulations, and adequate digital literacy among users.

2.3. Solutions and Best Practices in Mobile Banking Security

To meet these challenges, global banks and regulators have adopted various technical and non-technical solutions. From a technical perspective, the use of end-to-end encryption, multi-factor authentication (MFA), and biometrics has become standard in modern mobile banking applications. This solution has proven to be effective in reducing the potential for digital identity theft. For example, the implementation of biometric authentication such as fingerprinting and facial recognition increases the layer of security because it is difficult to counterfeit (Gupta et al., 2019). In addition, the application of artificial intelligence (AI) and machine learning allows bank systems to detect suspicious transaction patterns in real-time and prevent fraud. On the non-technical side, user education is a key element. Banks that are successful in maintaining customer trust are usually actively conducting digital literacy campaigns to increase awareness of phishing risks, the importance of using strong passwords, and being aware of unofficial applications.

Governments and regulators also have a strategic role in setting security standards and ensuring banking compliance. In Indonesia, the implementation of the banking information technology risk management policy issued by the OJK is one of the important steps to strengthen the mobile banking ecosystem. According to Rana et al. (2020), the combination of advanced technical solutions and comprehensive non-technical strategies is the most effective approach in dealing with mobile banking security threats. Therefore, long-term success depends not only on technological innovation, but also on the active involvement of users, regulators, and banking institutions.

3. Methods

This study uses a qualitative approach with literature study methods or literature review as the main strategy in data collection. This approach was chosen because it is to understand in depth the phenomenon of data security in the context of mobile banking, especially in Indonesia. The literature review allows researchers to examine various results of previous research, relevant government regulations, in order to compile a comprehensive analysis related to existing research challenges, solutions, and gaps. Thus, this method serves as a basis for building strong arguments and compiling strategic recommendations for banks and regulators. The main data source in this study comes from international and national journal articles published available. This time frame was chosen to keep the literature review up-to-date and relevant to the current dynamics in mobile banking security. In addition to scientific articles, the reports of institutions such as Bank Indonesia, and the OJK were analyzed to enrich the research perspective.

The criteria for selecting sources include relevance to data security topics, contributions to the literature on mobile banking, and the quality of publications that have gone through a peer review process or are published by trusted institutions. This is done to ensure the validity and reliability of the information used in the analysis. The literature collection process is carried out systematically using academic databases such as Google Scholar or Elsevier. Keywords used in searches include "mobile banking security", "cybersecurity in digital banking", "user awareness mobile banking", and "financial inclusion digital banking". The search results are then filtered by relevance, year of publication, and availability of the full text for

further analysis. From the results of the selection, between some core articles were selected which became the basis of the main analysis.

Data analysis was carried out using thematic analysis techniques. This process begins with organizing the selected literature, then coding the main themes that emerge, such as mobile banking security threats, technical solutions, non-technical strategies, regulation, and user literacy. After that, the themes are categorized in a larger framework according to the structure of the research: general context, problems and challenges, basic concepts of data security, existing solutions, research gaps, and research objectives. In this way, the analysis is not only descriptive, but also interpretive to uncover the interplay between technical, regulatory and user behavioral factors. To ensure the credibility of the research results, a triangulation process is carried out, which is comparing information from various types of literature, ranging from academic articles to official reports of financial institutions. This aims to avoid the interpretation bias that may arise if the research relies on only one type of source.

With this qualitative approach based on literature studies, the research is expected to provide a comprehensive picture of the state of data security in mobile banking in Indonesia. Furthermore, this method also allows researchers to identify gaps that have not been widely studied in the literature, such as the relationship between user awareness and the effectiveness of implementing technical solutions. The results of this analysis will then serve as the basis for formulating relevant strategic recommendations for the banking industry and regulators, in order to

strengthen the resilience of mobile banking systems and increase public trust in digital banking services.

4. Results

This study found that the development of mobile banking in Indonesia has two contrasting faces. On the one hand, mobile banking has made a major contribution to financial inclusion by expanding access to banking services to segments of society that were previously unreachable by conventional banks. In addition, the latest literature shows that mobile banking also plays a strategic role in strengthening people's economic resilience during the COVID-19 pandemic, particularly through integration with digital wallets that are able to reach community groups without traditional bank access (Alwi et al., 2021). On the other hand, the increase in the use of mobile banking applications is also accompanied by an increased risk of cyberattacks. Digital banking transactions in Indonesia have increased significantly to more than IDR 50,000 trillion, reflecting the acceleration of the digitalization of the financial sector. However, these enhancements simultaneously open up new attack loopholes that target the technical weaknesses of the system as well as the low digital literacy of users (Abidin et al., 2019). Thus, the positive growth of mobile banking actually presents a serious challenge in maintaining public trust.

The next key finding shows that phishing attacks are the most dominant threat in Indonesia. The attack pattern generally uses short messages, social media, or chat applications by disguising themselves as banks to steal user login data. The

stude Goel and Jain (2018) study confirms that phishing is still the most effective technique used by cybercriminals because it takes advantage of human psychological weaknesses. Seputra and Sandiasa (2020) also explained that the main challenges in maintaining data security in mobile banking applications in Indonesia, including cyber attacks such as phishing and malware, low user awareness of good security practices, and the use of outdated security technology by several banks. Many users are still easily deceived by fake links or offer of prizes, despite the bank warning many times through educational campaigns.

This phenomenon reinforces the evidence that non-technical aspects, particularly user awareness, have an equally important role as technical solutions in reducing vulnerability. In addition to phishing, mobile banking malware is also a significant threat. Malicious apps disguised as legitimate apps are often downloaded by users without realizing it, giving perpetrators direct access to steal credentials and financial data. Wazid et al. (2019) reported an increase in banking malware variants that are able to evade traditional antivirus detection and target popular mobile banking applications. In Indonesia, this kind of case is increasingly reported, especially among new users who are not used to checking the authenticity of apps before downloading them. This shows that even though banks have developed advanced security systems, users remain vulnerable if they are not equipped with adequate digital literacy.

From the internal banking side, the study found that there are still a number of banks in Indonesia that use old security systems that are vulnerable to exploitation. The study by Mendhurwar and Mishra (2021) highlights that many

banks in developing countries face limited resources to adopt the latest security technologies. In Indonesia, this limitation can be seen from the slow implementation of multi-factor authentication (MFA) across all mobile banking services, as well as the lack of use of AI and machine learning technology for fraud detection. This contrasts with practices in developed countries, where major banks have integrated AI-based detection systems capable of identifying transaction anomalies in real time.

However, the research also shows positive developments in Indonesia's banking sector. Some major banks are starting to adopt biometric technologies such as fingerprints and facial recognition as an additional layer of authentication. According to Gupta et al. (2019), biometric authentication has proven to be more secure than traditional passwords because they are difficult to forge. This technology, when combined with effective education campaigns, helps to significantly reduce the risk of cyberattacks (Seputra & Sandiasa, 2020). The implementation of this technology in Indonesia has increased user confidence in mobile banking, although its application is still limited to large banks. In addition, some banks have also worked with regulators to strengthen security standards, for example through regular IT system audit obligations.

The results of the literature review also show that user education is one of the weakest aspects of the mobile banking ecosystem in Indonesia. Research by Baabdullah et al. (2019) emphasizes that customer digital literacy greatly determines the effectiveness of technical solutions. For example, even though MFA has been implemented, many users still opt for the most straightforward option such as SMS OTP, which is more vulnerable than token-based authentication applications. In

addition, the low awareness of the importance of app updates makes most users stick with older versions that are vulnerable to exploitation. In other words, without continuous education, security technology will not achieve optimal effectiveness.

In the context of regulation, this study found that Indonesia still faces gaps compared to international standards. OJK has issued a policy on information technology risk management, but implementation in the field still faces obstacles. According to Rana et al. (2020), developing countries often lag behind in terms of digital security regulation due to limited resources, lack of coordination between institutions, and the speed of evolution of cyber threats. This is also true in Indonesia, where regulations are often reactive, i.e. only updated after a major attack, rather than proactive in anticipating threats.

In addition to regulatory factors and user literacy, the research also highlights the important role of international cooperation in strengthening the security of mobile banking. Cyber threats are cross-border, so solutions cannot rely solely on national efforts. The Sharma et al. (2021) study emphasizes that global collaboration in sharing information about cyberattack patterns can accelerate responses to new threats. For Indonesia, this cooperation is important considering that most malware and phishing attacks come from complex international networks.

The results of this study confirm that mobile banking security in Indonesia is influenced by a combination of technical, regulatory, and user behavior factors. Technical solutions such as encryption, MFA, and biometrics have proven to be effective, but their effectiveness relies heavily on user awareness and strong regulatory support. The main gap that still exists is the low digital literacy of users

and regulatory delays compared to the complexity of cyber threats. Therefore, the future strategy must be holistic, by combining technological innovations, strengthening regulations, and sustainable user education programs to ensure the security and sustainability of the mobile banking ecosystem in Indonesia.

5. Discussion

The results show that the development of mobile banking in Indonesia presents great potential for financial inclusion while posing serious challenges related to data security. This discussion focused on three main aspects: the effectiveness of technical solutions, the role of digital literacy users, and the relevance of national regulations to global standards. These three aspects are interrelated and determine the success of efforts to maintain public trust in mobile banking services. First, from the technical side, various innovations such as encryption, multi-factor authentication (MFA), and biometrics have been proven to improve the security of mobile banking applications. However, the application of this technology has not been even across all Indonesian banking institutions. Some large banks are already implementing biometric authentication and AI-based detection systems, but many medium and small banks are still limited to the use of traditional passwords and SMS-based OTPs that are vulnerable to exploitation. According to Gupta et al. (2019), technical solutions such as biometrics can provide stronger protection, but their adoption requires a large investment in infrastructure and supporting devices. Thus, the gap between banks in the application of security technology has the potential to create an unequal protection for customers.

Second, user digital literacy has emerged as a critical factor in determining the effectiveness of technical solutions. The findings show that despite the availability of advanced security systems, low user awareness is often a weak point that cybercriminals exploit. For example, phishing is still a major threat because many users are easily deceived by fake messages or links. Research by Baabdullah et al. (2019) confirms that low digital security awareness causes users not to make optimal use of security features. This shows that technology cannot completely replace the role of users in maintaining data security. In other words, the success of a mobile banking security system requires synergy between technology and user behavior. Therefore, digital literacy education programs must be designed massively and sustainably, not just short campaigns.

Third, national regulations play an important role in creating a strong digital security ecosystem. In Indonesia, the policies of OJK and Bank Indonesia related to information technology risk management have been a good first step, but implementation on the ground often faces obstacles. Existing regulations tend to be reactive, updating the rules after a major attack, rather than proactively anticipating threats. The study by Rana et al. (2020) emphasizes that developing countries need to accelerate regulatory updates to keep pace with global threat dynamics. For Indonesia, this means that regulators need to encourage closer collaboration with the banking sector, cybersecurity agencies, and international partners to strengthen the response to cross-border attacks.

In addition, this discussion also revealed the importance of a combination of technical and non-technical approaches. Technical solutions such as AI and

blockchain do promise increased detection and protection, but without strict regulatory support and good user literacy, their effectiveness will be limited. On the other hand, user education without the help of technology is also not enough, as the pattern of cyberattacks continues to evolve to become increasingly complex. Therefore, a mobile banking security strategy should be viewed as an ecosystem that involves all stakeholders: banks, regulators, governments, and society. The integration of policy, technology, and public awareness will create a system that is more resilient to cyber threats. This discussion emphasized that the security challenges of mobile banking in Indonesia cannot be overcome with a single approach. Success requires a combination of advanced technical solutions, strong user literacy, and proactive and adaptive regulation. With this synergy, mobile banking can continue to develop as a motor of financial inclusion without sacrificing the data security aspect that is the main foundation of public trust.

6. Conclusion

This research confirms that the development of mobile banking in Indonesia has made a significant contribution to the growth of the digital economy and the expansion of financial inclusion. Mobile banking allows people to access financial services more easily, quickly, and efficiently, including those previously unreached by the conventional banking system. However, behind these positive impacts, serious challenges arise in the form of data security threats that can disrupt public trust in digital banking services. This threat comes from external factors such as phishing and malware attacks, as well as internal factors such as the limited security

infrastructure of banks and regulations that are still lagging behind the dynamics of cyber threats. The results of the literature review show that technical solutions such as encryption, multi-factor authentication, biometrics, as well as artificial intelligence and blockchain-based technologies have great potential to strengthen mobile banking security systems.

However, the effectiveness of this technology is highly dependent on the level of awareness and digital literacy of users. Without adequate understanding, users remain vulnerable points that can be exploited by criminals. In addition, national regulations also play an important role in creating a secure digital banking ecosystem. Proactive, adaptive, and aligned regulations with international standards are needed to support security and increase public trust. Based on the findings of the research, it can be concluded that efforts to maintain mobile banking security in Indonesia must be carried out holistically. An approach that combines technological innovation, improving users' digital literacy, and strengthening banking regulations and policies will create a more resilient system in the face of cyber threats. Collaboration between banks, regulators, governments, and the public is the main key to success. With the right strategy, mobile banking in Indonesia is not only able to improve the efficiency of financial services, but also provide optimal protection for user data, thereby boosting public trust and strengthening the foundation of the national digital financial ecosystem.

References

Abidin, W. Z., Rivera, O., Maarop, N., & Hassan, N. H. (2017, July). Mobile payment framework for the unbanked Filipinos. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.

Alwi, S., Salleh, M. N. M., Alpandi, R. M., Ya'acob, F. F., & Abdullah, S. M. M. (2021). Fintech as financial inclusion: Factors affecting behavioral intention to accept mobile e-wallet during Covid-19 outbreak. *Turkish Journal of Computer and Mathematics Education*, *12*(7), 2130-2141.

Baabdullah, A. M., Rana, N. P., Alalwan, A. A., Islam, R., Patil, P., & Dwivedi, Y. K. (2019). Consumer adoption of self-service technologies in the context of the Jordanian banking industry: Examining the moderating role of channel types. *Information Systems Management*, *36*(4), 286-305.

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *computers & security*, *73*, 519-544.

Gupta, S., Buriro, A., & Crispo, B. (2019). DriverAuth: A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms. *Computers & Security*, *83*, 122-139.

Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*, *15*(4), 565-584.

Otoritas Jasa Keuangan (OJK). Laporan Perkembangan Teknologi Informasi di Sektor Jasa Keuangan. *Otoritas Jasa Keuangan*.

Ramadhan, F. (2021). Peran Fintech Dalam Meningkatkan Inklusi Keuangan Syariah Pada UMKM Di Kota Makassar:(Studi Kasus Pada Aplikasi Paytren). *Madinah: Jurnal Studi Islam*, *8*(2), 247-259.

Rana, N. P., Luthra, S., & Rao, H. R. (2020). Key challenges to digital financial services in emerging economies: the Indian context. *Information Technology & People*, *33*(1), 198-229.

Seputra, K. A., & Sandiasa, G. (2020). Rancang Bangun Sistem Informasi Satgas Gotong Royong (Si Garong) Desa Adat Berbasis Mobile. *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, *9*(3), 338-350.

Sharma, A., Singh, S. K., Kumar, S., Chhabra, A., & Gupta, S. (2021). Security of android banking mobile apps: Challenges and opportunities. In *International conference on cyber security, privacy and networking*. Cham: Springer International Publishing, 406-416.