
Journal of Informatics and Web Engineering

Vol. 4 No. 2 (June 2025)

eISSN: 2821-370X

Exploring User Perceptions of Security in Mobile Banking: A Study in Malaysia

Kai En Lim¹, Ying Han Pang^{2*}, Shih Yin Ooi³, Wan Xuan Kow⁴, Tang Xing Cheang⁵,
Mao Wei Tan⁶

^{1,2,3,4,5,6} Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Bukit Beruang,
Melaka, Malaysia

**corresponding author: (yhpang@mmu.edu.my; ORCID: 0000-0002-3781-6623)*

Abstract - Mobile banking has become increasingly popular in Malaysia due to its convenience and efficiency. However, persistent security concerns such as vulnerabilities to cyber attacks, malware and phishing affect user trust and impede adoption. This study aims to explore how users perceive and experience the security features of mobile banking applications. In spite of the implementation of security controls, understanding user perceptions and experiences remains essential, as these are core factors which influence mobile adoption. Thus, this study investigates the user experience of mobile banking security features in Malaysia. Specifically, we focus on the users' perceptions, satisfaction levels and concerns. We employed a hybrid approach consisting of online surveys in-person interviews, and online interview sessions for data collection. This study comprises a detailed assessment of user awareness and behavior regarding mobile banking security, insights into the impact of security features on the users' trust and recommendations for enhancing the security and usability of mobile banking applications. Our findings revealed that there were significant variations in user experiences across diverse demographic groups, with younger users exhibiting higher security concerns. Furthermore, usability issues associated with confusing navigation and slow response times were reported, negatively affecting the overall user experience. From the analysis, we noticed that while users generally rated the overall Malaysian mobile banking security applications positively, they identified key areas for improvement. These include the need for enhanced access control authentication mechanisms for secured transactions and more intuitive security interfaces for user-friendly navigation and use. In summary, this study highlights that user perceptions and experiences are central to understanding mobile banking security concerns in Malaysia. Hence, user-centric security designs are desired for balanced protection with ease of use.

Keywords— Mobile Banking, Security Features, User Experience, Cybersecurity Threats, Trust and Usability

Received: 10 February 2025; Accepted: 01 May 2025; Published: 16 June 2025

This is an open access article under the [CC BY-NC-ND 4.0](#) license.



1. INTRODUCTION

User experience (UX) refers to the overall experience that a customer has while interacting with a system through its digital products, in this case, mobile banking applications. It embraces how easy, efficient and satisfactory the system is to use from the user's perspective. To be specific, in the context of mobile banking, UX includes several aspects which include easy navigation, reducing user actions and inputs, keeping the app up to date, ensuring security,

providing an intuitive UI, optimizing the mobile application performance, and supporting a user-friendly layout and design [1].

In the past decade, the number of mobile banking users in Malaysia has increased significantly [2], [3], [4]. The main factor is that mobile banking offers users convenient access to remote financial services. Nevertheless, security concerns remain a major obstacle to adoption [5], [6], [7]. Mobile banking applications are frequent targets of cyber-attacks, malware, phishing scams, etc. While banks have implemented various security controls, users' perceptions of security and usability continue to impact their trust and adoption of mobile banking services. This study aims to investigate the user experience of mobile banking security features in Malaysia. To gain comprehensive insights into Malaysia's mobile banking experiences, we employed a hybrid data collection approach, which includes online surveys, in-person interviews and online interview sessions. The surveys mainly focus on user perceptions, satisfaction levels and security concerns of their adopted mobile banking services. By gaining insights into these aspects, relevant financial institutions can design and develop user-centric security solutions for balanced security protection and usability.

The contributions of this study are listed as follows:

- Provide a detailed assessment of user experiences with mobile banking security features in Malaysia. Security concerns, usability challenges and trust factors are examined.
- Examine security features and their impact on trust. The effectiveness of security measures such as biometric access control authentication, tokenization, One-Time Password (OTP) and traditional password-based authentication is analyzed.
- Propose recommendations to improve mobile banking security and usability, facilitating a balance between reliable security protection and seamless user experience.

2. LITERATURE REVIEW

According to a study by [8], technological advancements enable banks to successfully implement mobile banking applications. The study claims that mobile banking aims to facilitate customer transactions via mobile devices using SMS media and internet connectivity. Additionally, [9] highlighted that there is a positive correlation between mobile banking and inclusive development of mobile banking in 93 developing countries, particularly when a certain threshold of the human development index is met. The authors suggested that improving mobile banking mechanisms can contribute to economic growth and minimal inequality, especially at higher levels of inclusive development distribution. This study encourages the use of mobile banking applications to address the challenges of exclusive growth, inequality, and poverty in developing countries. Furthermore, [10] argued that regulators and governments should encourage and adapt mobile banking for widespread accessibility. They analyzed the influences of perceived convenience, subjective norms and perceived usefulness on customer loyalty in mobile banking. The findings reveal that customer loyalty is closely correlated to mobile banking usage. Thus, banks should optimize UI design to enhance user usability, eradicate software bugs, and implement user-friendly mobile banking interfaces.

In recent years, Malaysia has experienced a substantial surge in digital payments and online banking, particularly during the Covid-19 pandemic [11]. However, the rate of cybercrime related to online banking is also increasing directly proportionally. According to Commercial Crime Investigation Department (CCID) Director, Datuk Seri Ramli Mohamed Yoosuf, Malaysia lost about RM11.23 billion to online financial fraud over the past five years [12]. To tackle this threat, Bank Negara Malaysia instructed financial institutions to discontinue the use of SMS OTPs as a form of authentication for online transactions [13]. The rationale behind this decision is this kind of authentication can be easily stolen or leaked by human mistake. Hiyam Nadhim Khalid, a researcher from Universiti Kebangsaan Malaysia, highlighted that one of the challenges in deploying cybersecurity for online banking is the swift evolution of cyber threats [14]. Hackers continuously develop diverse techniques, making it difficult to keep security controls up to date. Additionally, Hiyam Nadhim Khalid also pointed out that humans are the weakest link in cybersecurity. Despite how strong the online banking firewall is or how perfect the banking security system is, a user's lack of awareness or negligence may cause password or OTP leakage.

Undoubtedly, mobile banking has revolutionized financial management by providing convenience and accessibility. However, this convenience comes with considerable security challenges. Ernest Aryee claimed that one of the major threats to mobile banking security is malware [15]. Mobile Malware, such as trojans and spyware, can masquerade as

legitimate banking applications, stealing user credentials and sensitive information. The authors also indicated that poor coding practices and inadequate security testing introduce security vulnerabilities in mobile banking applications. Common issues include weak encryption, improper session handling, and insecure data storage; all these can be exploited. Jailbroken or rooted devices, which bypass built-in security features, expose mobile banking applications to attack. Besides that, frequent neglect of system updates leaves the devices vulnerable to exploits [16]. As a consequence of these vulnerabilities, man-in-the-middle attacks can result in financial loss, identity theft and bank-client distrust.

To combat these risks, various security measures are applied, [17] highlighted that encryption, multi-factor authentication, secure software development methods, and good practices of software development are strategies adopted to mitigate vulnerabilities. [18] suggested that Multi-Factor Authentication (MFA) can efficiently enhance security. An additional layer of security is added by requiring multiple pieces of identity such as passwords, biometrics and OTPs which help lower the risk of unauthorized access. In addition, developers should regularly conduct security testing throughout development, code reviews, and vulnerability assessments. [19] emphasized that human factors are significant aspects of the security of mobile banking. Educating users about the importance of device security, recognizing phishing attempts and avoiding unsecured networks can reduce risks. Besides, a clear guideline on security should be provided as a best practice that can empower users to protect their data. Furthermore, implementing strong encryption for data storage and transmission is essential. Protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are used to encrypt data transmitted between a user's mobile device and the bank's server. With this, it becomes difficult for attackers to intercept and decipher the information.

In view of this, more secure and user-friendly authentication methods are needed. [20] proposed a multi-factor authentication, incorporating face recognition and biometric fingerprint authentication to provide accurate authentication. The uniqueness of fingerprints and facial features makes unauthorized transactions almost impossible. This authentication method increases users' satisfaction and confidence in online banking. In addition, this approach is user-friendly, and it provides mobile operability which allows users to verify transactions anytime, anywhere. [21] emphasized the significance of the Confidentiality, Integrity, and Availability (CIA) triad in the cybersecurity framework. By integrating reliable authentication mechanisms with the CIA triad principles, they could create a more secure and resilient online banking environment.

3. RESEARCH METHODOLOGY

In today's digital era, the widespread of mobile banking facilitates easy access to financial services. However, ensuring this service is both secure and user-friendly is a significant challenge for banks. Understanding what users expect from security measures is crucial for building trust and maintaining the reliability of mobile banking. To achieve our goal, we surveyed to study user experiences with security elements in mobile banking. The methodology employed includes:

- *Online Survey:* An online survey was designed to gather opinions from diverse participants based on age, occupation and background to ensure data quality and diversity. Instead of posting the survey on social media or other public platforms, we reached out personally to friends, family members, colleagues and their acquaintances for reliable and accurate responses. This approach helped maintain the integrity and reliability of our data.
- *In-Person Interviews:* One major challenge we faced was reaching users aged 65 and above. To address this, we conducted in-person interviews to collect data from diverse age groups, particularly the elderly as well as retail workers and business owners. These interviews revealed that many elderly people rarely use mobile banking.
- *Online Interview Session:* We also conducted online interviews. This session provided valuable perspectives on mobile banking adoption among educators. The participants expressed concerns about scams and cybersecurity threats, reflecting a key barrier to adoption within this demographic.

To ensure the quality and reliability of the data collected, a purposive sampling method was employed. For online surveys, the respondents were not selected randomly from public social media. Instead, we distributed the survey through personal networks, including family, friends, colleagues, and their acquaintances. This approach was selected to obtain more thoughtful and sincere responses since these individuals were more likely to engage meaningfully with the survey content. In the case of in-person interviews, we specifically targeted small business owners and elderly street vendors such as hawkers and stall owners as these groups frequently use mobile banking for daily financial

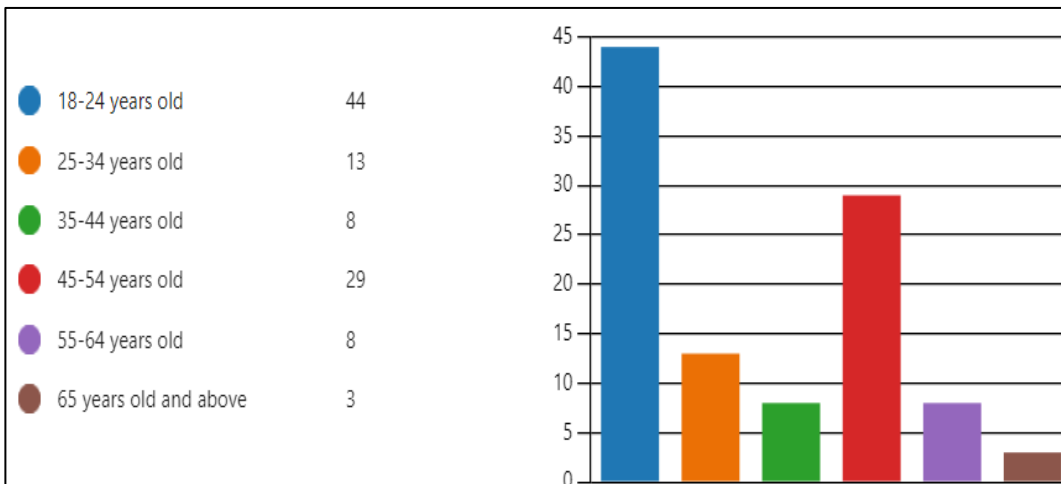
activities. Their experiences offered practical insight into real-life usage, challenges, and confidence in the security measures of mobile banking. All participants were required to use any mobile banking application within the past six months. This assisted in ensuring that the responses reflected current and relevant user experiences across various demographics.

By employing these diverse methods, we collected comprehensive data to understand the user experience and security concerns in mobile banking. This multi-faceted approach enabled us to ensure the survey's robustness, validity, and relevance, providing a thorough understanding of user perspectives on mobile banking security. To ensure ethical research practices, we obtained consent from all participants and assured them of their anonymity. This compliance with the Personal Data Protection Act (PDPA) protects the users' information.

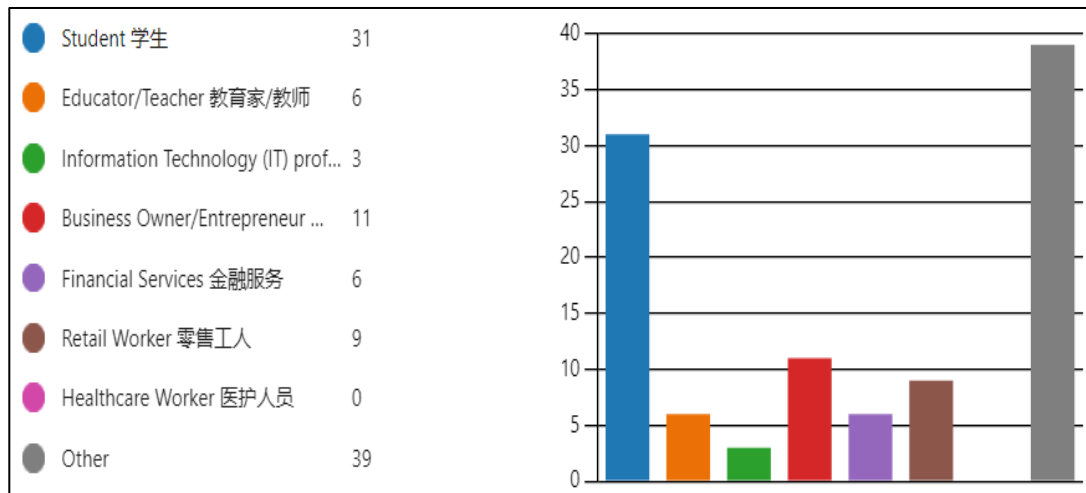
4. RESULTS AND DISCUSSIONS

In this study, we gathered 123 responses using a hybrid method. This included 105 respondents via online surveys, 17 participants through in-person interviews, and 1 participant through an online interview session. This combination allowed us to gain valuable insights into user experiences and perceptions regarding security elements in mobile banking. The dataset encompasses various demographics, including age, occupation, and educational background, as illustrated in Figure 1.

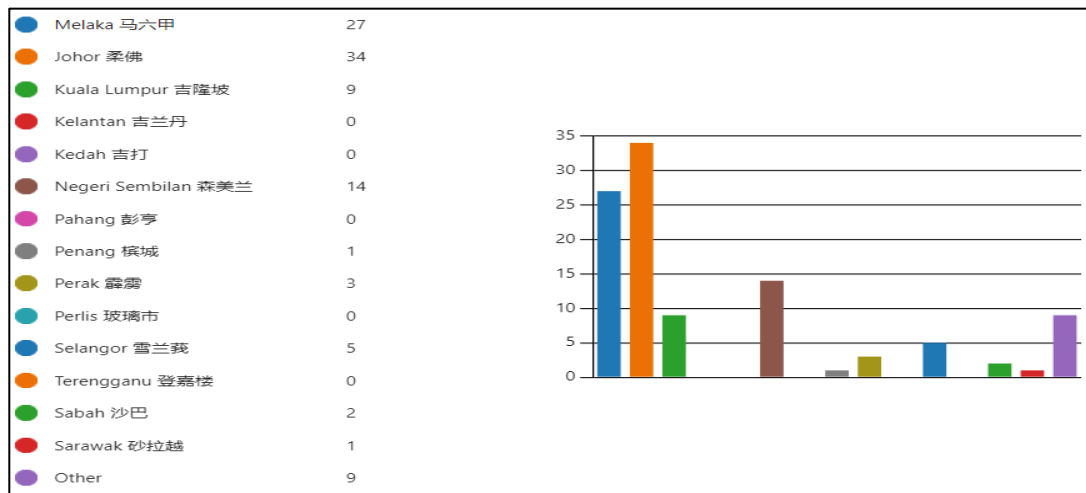
Figure 1(a) depicts the age distribution of participants in the survey; Figure 1(b) illustrates the occupation distribution of the participants; and Figure 1(c) illustrates the location graph of the respondents in Malaysia, showing the geographical distribution of participants across different regions. Through analysis, several key trends emerged, providing an understanding of user adoption, security concerns, behavioral patterns and user preferences.



(a)



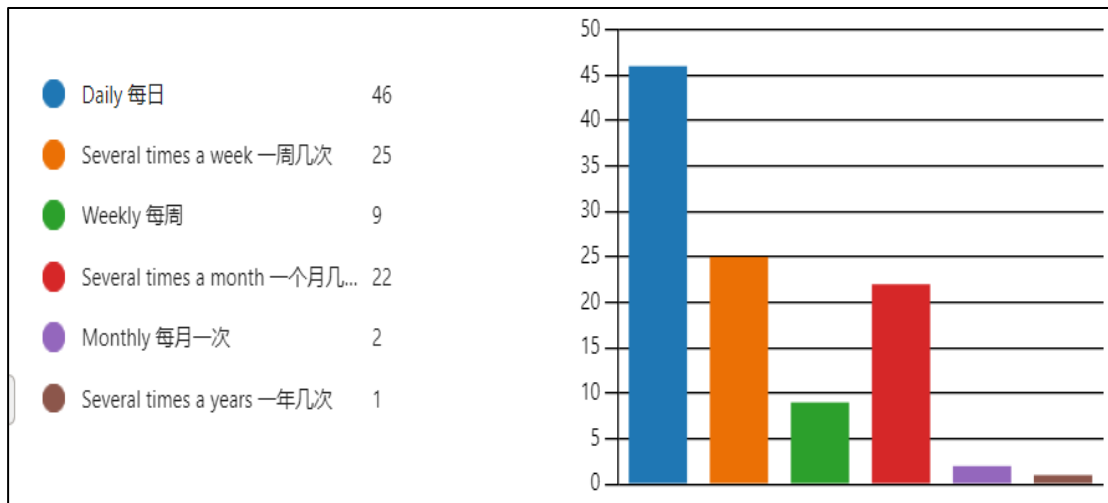
(b)



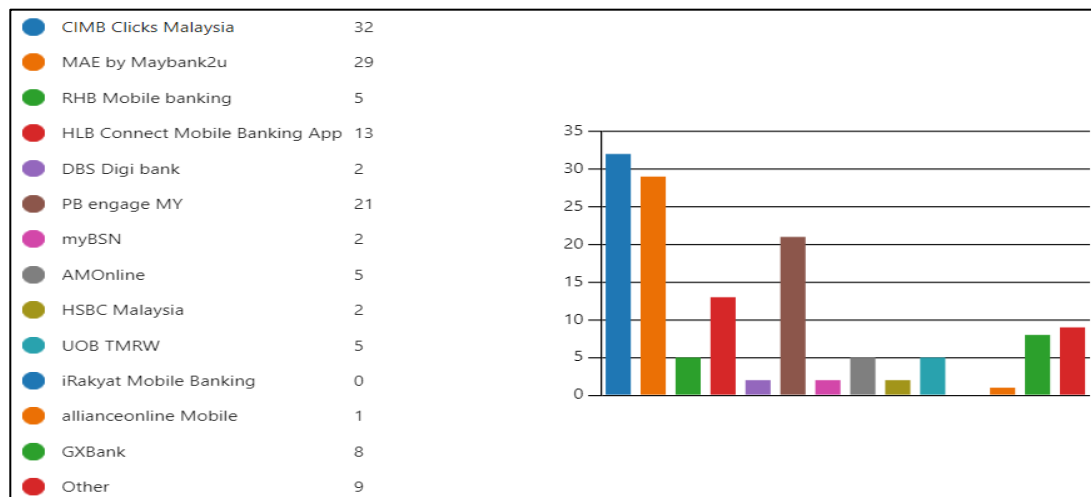
(c)

Figure 1 (a) Age Distribution, (b) Occupation Distribution and (c) Location

Figure 2(a) illustrates the frequency of mobile banking usage. From the data, we can observe that the majority use mobile banking daily. This indicates that mobile banking has emerged as an essential element of financial transactions, gradually replacing traditional banking approaches. This could be due to the easy accessibility and convenience of mobile banking applications. However, the respondents also highlighted their concern about the system's reliability, particularly system security. Figure 2(b) depicts the preference for mobile banking platforms. From the obtained data, it is noticed that CIMB Clicks Malaysia and MAE by Maybank2u are the two most widely used mobile banking applications. This may be because these two banks are among the largest financial institutions in Malaysia. CIMB Group serves a customer base of over 24 million across the ASEAN [22], with 80% of its customers being digitally active, revealing strong engagement with its digital services [23]. Similarly, Maybank serves approximately 22 million customers [24]. With this extensive customer base, a high frequency of mobile usage is expected as a large number of customers engage with their mobile banking application for financial services.



(a)



(b)

Figure 2. (a) Frequency of Mobile Banking Usage and (b) Mobile Banking Use

Table 1 records the findings of the user-friendliness survey. From the table, we can notice that respondents are generally satisfied with the appearance of Malaysian mobile banking applications, with an average rate of 4 out of 5. Compared to five years ago, Malaysian banking applications have significantly improved their interface layouts and designs [25]. However, a relatively low score, i.e. 2.64, was obtained regarding the difficulty of performing usual banking tasks such as checking balances, transferring funds, and paying bills. This suggests that while users can navigate the application easily, the execution of specific tasks may be cumbersome due to multiple steps required for processes or security measures. On the other hand, users reported positive experiences with the ease of application navigation and finding functions. Most Malaysian banks provide detailed guidelines to help users familiarize themselves with the applications. Furthermore, essential functions and features are usually displayed on the main dashboard for fast accessibility.

However, service availability and API integration/compatibility received low ratings. Many respondents experienced temporary inaccessibility due to scheduled system maintenance. Although system maintenance is usually conducted at midnight to minimize disruption, it still results in inconveniences to users who prefer to perform online transactions before sleeping. Moreover, some users expressed their difficulties in integrating banking applications with external services such as e-commerce or mobile wallet platforms. Despite the availability of APS for direct integration, certain

users still manually top up their mobile wallets as more convenient. Hence, the enhancement of third-party compatibility could improve the overall banking experience. Anyhow, the overall user-friendliness satisfaction remains high with a score of 4.04 out of 5. Users can generally complete their banking tasks efficiently.

Table 1. User-friendliness Finding Summary

Question			Average Rating
Did you find the layout and design of the application intuitive?			4.00
Did you encounter any difficulties while performing common tasks such as checking your balance, transferring funds, or paying bills?			2.64
How easy was it to navigate through different sections of the application?			3.95
Were you able to easily find the functions or features you were looking for?			3.90
Do you receive timely notifications for accounting activity?			3.91
Have you experienced any instances of service downtime or unavailability when trying to access your banking application?			2.91
Have you experienced any issues with compatibility or integration while using your banking application with other systems, services, or third-party APIs?			2.64
Do you receive immediate feedback from your banking application when you encounter issues or detect any unexpected event?			3.47
How satisfied are you with the user-friendliness of your mobile banking app?			4.04
Question			Percentage
Which features of the application do you find most useful?		Checking account balance	28%
		Online Transfer (DuitNow)	30%
		QR Payment	20%
		Auto Debit	6%
		Checking recent transaction/ Obtain Statement	16%
Question		Yes	No
Any features you would like to see added to the application	Chatbot and voice assistants	44.8%	55.2%
	Expense tracker	62.9%	37.1%
	Cashback services	78.1%	21.9%
	Personalized offers	61.0%	39.0%
	Bill-splitting	56.2%	43.8%
Issues or problems that you encountered with the mobile banking app.	Slow response time	46.7%	53.3%
	Confusing navigation	34.3%	65.7%
	Transaction failure	56.2%	43.8%
	App crashed	38.1%	61.9%
	Security Concern	36.2%	63.8%

The most used feature in mobile banking applications is online transfers. This reflects Malaysia's shift towards digital payments for their efficiency and convenience. Conversely, the auto-debit function was the least used feature. Users are hesitant to enable auto debit, but opt for manual payments. This is because the auto debit feature reduces the users' control over payments, while manual payments allow them to review the bills before making a transaction. The most reported issue encountered by the respondents with mobile banking applications is transaction failure (56.2%). The possible reasons can be insufficient balances or temporary service disruptions.

Table 2 summarizes the survey findings regarding the security concerns of Malaysian mobile banking applications. Password authentication is significant in security mobile banking applications. 83% of respondents agreed that an additional password is important to verify certain transactions. A good practice for password usage is to change passwords regularly and use different passwords for different applications/ platforms. However, users admitted that they do not frequently change their passwords due to the difficulty of memorization. Furthermore, 41% of respondents use the same password across multiple applications/ platforms, which may make their accounts vulnerable to potential breaches. The security control of OTPs received a high rating of 3.9. This signifies their requisite to provide secure transactions.

Table 2. Security Concern Summary

Question		Percentage		
Which authentication method do you find most secure?	Password	43%		
	Fingerprint	29%		
	Facial Recognition	27%		
	Other	2%		
Which additional security measures would you like to add to mobile banking applications?	Transaction monitoring and alert	32%		
	Geolocation tracking	18%		
	Secure Vault for Sensitive Documents	20%		
	Threat Intelligence Integration	13%		
	Behavioral Biometrics	17%		
Question		Yes		No
Do you think that additional passwords, requested during use of the Internet or mobile banking, while verifying certain transactions, are needed?		83.0%		17.0%
Changing the password periodically (for example every month)		34.0%		66.0%
I am using the same password for several applications: (Internet/mobile bank, Facebook, Twitter, etc.).		41.0%		59.0%
Have you ever encountered any security incidents, such as unauthorized access or suspicious activities, while using your banking application?		28.0%		72.0%
Have you ever avoided using certain security features because if too complicated is inconvenient to you?		66.0%		34.0%
Do you feel that the security feature on banking application in Malaysia has sufficient security control to protect your sensitive information?		Yes	No	Not Sure
		30.0%	20.0	50.0%
Question				Average Rating
How satisfied are you with the authentication methods provided by your banking application (e.g., password, PIN, biometric authentication)?				4.02
Do you find the process of receiving and entering OTPs during transactions convenient and user-friendly?				3.90
How concerned are you about the privacy of your data (e.g., transaction history, personal details) stored and processed by your banking application?				4.04
How important are regular security updates and maintenance activities to ensure the integrity of your banking application?				4.18
How would you rate the overall security of your banking application?				3.73

Users are concerned about the confidentiality and privacy of their transactional records, personal information, and biometric data. To enhance security features, 32% of respondents preferred transaction monitoring and alerts as an additional security measure. Banks should promptly notify users of any online transactions, allowing the users to

detect and respond to those unauthorized activities immediately. The overall security rating of Malaysian mobile banking applications was rated 3.73 out of 5. There is still room for improvement to harden security controls and address user concerns, particularly from a security perspective.

5. CONCLUSION

Users appreciate the enhanced interface layouts and designs in the current mobile banking applications. Thus, the user-friendliness of Malaysian mobile banking applications is considered satisfactory. However, service availability and API integration received low ratings. These issues can negatively impact the overall user experience, potentially deterring users from fully engaging with mobile banking services. Furthermore, the auto-debit function is unpopular because of the concern that this function reduces the users' control over payments. From the perspective of security, the overall security rating of Malaysian mobile banking applications was 3.73 out of 5. The respondents suggested the introduction of new security features, such as advanced fraud detection and real-time security alerts to enhance protection and trust. In order to balance between security and ease of use, mobile banking applications can adopt mechanisms such as MFA, biometric authentication or adaptive authentication. These countermeasures maintain robust protection while streamlining the user experience.

However, there are certain restrictions on this study. Firstly, age coverage was limited, particularly among the users who are 65 and above, whose generation provides more perspectives on issues related to usability and trust. Additionally, geographic coverage was not comprehensive since there were no responses from several states like Kedah, Kelantan, Pahang, Perlis, and Terengganu. These important gaps may compromise the representativeness of the findings to the entire Malaysian population. Future efforts should focus on obtaining more diverse geographic regions and a broader age range, especially elderly users to gain a more comprehensive understanding of mobile banking security perception. On top of that, further exploration into the impact of specific security frameworks on user satisfaction and trust would be valuable in guiding the design of a user-centric mobile banking system.

ACKNOWLEDGEMENT

We thank the anonymous reviewers for the careful review of our manuscript.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Lim Kai En: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation;
Pang Ying Han: Project Administration, Supervision, Writing – Review & Editing;
Ooi Shih Yin: Project Administration, Supervision – Review & Editing.
Kow Wan Xuan: Methodology, Writing – Original Draft Preparation;
Cheang Tang Xing: Result and Discussion, Writing – Original Draft Preparation;
Tan Mao Wei: Result and Discussion, Writing – Original Draft Preparation;

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS


Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. <https://publicationethics.org/>

REFERENCES

- [1] P. Modh and P. Modh, "User Experience focused Banking Apps: A journey to Excellence," Prismetric, Aug. 21, 2024. [Online]. Available: <https://www.prismetric.com/user-experience-in-mobile-banking-apps/>
- [2] H.-B. Ong, and L.-L. Chong, "The effect of cashless payments on the internet and mobile banking," *Journal of Financial Services Marketing*, vol. 28, no. 1, pp. 178–188, Mar. 2022. doi: 10.1057/s41264-022-00145-0.
- [3] A. A. Alsmadi, A. Moh'd Al_hazimeh, M. A. Al-Afeef, A. W. Al-Smadi, F. Rifai, and M. Al-Okaily, "Banking Services transformation and Financial Technology role," *Information Sciences Letters*, vol. 12, no. 1, pp. 315–324, 2023. doi: 10.18576/isl/120126.
- [4] B. Eneizan, T. Obaid, M. S. Abumandil, A. Y. Mahmoud, S. S. Abu-Naser, K. Arif, and A. F. Abulehia, "Acceptance of mobile banking in the era of COVID-19," in *Lecture notes in networks and systems*, pp. 29–42, 2022. doi: 10.1007/978-3-031-16865-9_3.
- [5] N. H. Al-Fahim, A. A. Ateeq, Z. Abro, M. Milhem, M. Alzoraiki, T. M. Alkadash, and M. Nagi, "Factors influencing the mobile banking usage: Mediating role of perceived usefulness," in *Digital technology and changing roles in managerial and financial accounting: theoretical knowledge and practical application*, pp. 115–128, 2024. doi: 10.1108/s1479-351220240000036011.
- [6] Y. K. Oh and J.-M. Kim, "What improves customer satisfaction in mobile banking apps? an application of text mining analysis," *Asia Marketing Journal*, vol. 23, no. 4, Feb. 2022. doi: 10.53728/2765-6500.1581.
- [7] P. Verma, T. Newe, G. D. O'Mahony, D. Brennan, and D. O'Shea, "Towards a unified understanding of cyber resilience: a comprehensive review of concepts, strategies, and future directions," *IEEE Access*, pp. 1, Jan. 2025. doi: 10.1109/access.2025.3551887.
- [8] I. K. Rachmawati, M. Bukhori, Y. Majidah, S. Hidayatullah, and A. Waris, "Analysis of Use of Mobile Banking with Acceptance and Use of Technology (UTAUT)," *International Journal of Scientific and Technology Research*, vol. 9, no. 8, pp. 534–540, Aug. 2020.
- [9] S. A. Asongu, and N. M. Odhiambo, "Mobile banking usage, quality of growth, inequality and poverty in developing countries," *Information Development*, vol. 35, no. 2, pp. 303–318, Nov. 2017. doi: 10.1177/0266666917744006.
- [10] J. Putrevu, and C. Mertzanis, "The adoption of digital payments in emerging economies: challenges and policy responses," *Digital Policy Regulation and Governance*, vol. 26, no. 5, pp. 476–500, Sep. 2023. doi: 10.1108/dprg-06-2023-0077.
- [11] T. S. Sin, C. Z. Han, C. S. Fai, L. Z. Xuan, N. H. Ning, and T. K. Xi, "Exploring the factors influencing the intention to adopt the contactless payments in Post-COVID 19 in Malaysia," in *Advances in economics, business and management research/Advances in Economics, Business and Management Research*, 2025, pp. 112–133. doi: 10.2991/978-94-6463-666-6_7.
- [12] F. Fong, "Malaysians lost a Mind-Boggling RM11.2 billion to scammers in just 5 years," TRP, Jan. 10, 2025. [Online]. Available: <https://www.therakyatpost.com/news/malaysia/2025/01/10/malaysians-lost-a-mind-boggling-rm11-2-billion-to-scammers-in-just-5-years/>
- [13] "BNM orders banks to switch from OTPs to more secure authentication," The Vibes, Sep. 26, 2022. [Online]. Available: <https://www.thevibes.com/articles/business/72487/bnm-orders-banks-to-switch-from-otps-to-more-secure-authentication>
- [14] C. S. Teoh, A. K. Mahmood, and S. Dzazali, "Cyber security challenges in organisations: A case study in Malaysia," In *2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, IEEE, pp. 1-6. 2018.
- [15] E. Aryee, "Enhancing Mobile Banking Security through Blockchain Technology: Mitigating Unauthorized Access and Protecting Financial Assets," *International Journal of Finance and Banking Research*, Jun. 2023. doi: 10.11648/j.ijfbr.20230902.12.

- [16] F.N.U. Jimmy, “Cyber security Vulnerabilities and Remediation Through Cloud Security Tools,” *Journal of Artificial Intelligence General science (JAIGS)*, vol. 2, no. 1, pp. 129–171, Apr. 2024. doi: 10.60087/jaigs.v2i1.102.
- [17] G. Wainaina, D. Kiyeng, and N. Masese, “Enhancing Security Measures for Mobile Banking Applications: A Comprehensive Analysis of Threats, Vulnerabilities, and Countermeasures in Kenya Banking Industry,” *International Journal of Computer Applications Technology and Research*, Aug. 2023. doi: 10.7753/IJCATR1208.1014.
- [18] A. H. Sarower, T. Bhuiyan, M. M. Hasan, M. S. Arefin, and G. Hossain, “SMFA: Strengthening Multi-Factor Authentication with Steganography for Enhanced Security,” *IEEE Access*, pp.1, Jan.2025. doi: 10.1109/access.2025.3545769.
- [19] I. Riasat, M. Shah, and M. S. Gonul, “Strengthening Cybersecurity resilience: An investigation of customers’ adoption of emerging security tools in mobile banking apps,” *Computers*, vol. 14, no. 4, p. 129, Apr. 2025. doi: 10.3390/computers14040129.
- [20] A. Dhoot, A. N. Nazarov, and A. N. A. Koupaei, “A security risk model for online banking system,” *Systems of Signals Generating and Processing in the Field of on Board Communications*, pp. 1–4, Mar. 2020. doi: 10.1109/ieeeeconf48371.2020.9078655.
- [21] D. Arora, M. Garg, and S. Mongia, “Global Case Studies, Domains and Used Methodologies Concerning Cyber Security in Online banking: A Review,” *10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1–7, Oct. 2022. doi: 10.1109/icrito56286.2022.9965094.
- [22] Cimb, “Customer experience,” CIMB, Nov. 22, 2024. <https://www.cimb.com/en/sustainability/our-priorities/customer-experience.html>
- [23] “CIMB named Best Bank in Malaysia by Euromoney,” CIMB, Aug. 15, 2023. [Online]. Available: <https://www.cimb.com/en/newsroom/2023/cimb-named-best-bank-in-malaysia-by-euromoney.html>.
- [24] C. Smith and C. Smith, “Maybank,” DMR, Dec. 15, 2024. [Online]. Available: <https://expandedramblings.com/index.php/maybank-statistics-facts/>
- [25] S. Laurens, M. Kartikasary, A. Sujarminto, A. Tihar, T. Hapsari, and R. P. Situmorang, “The importance of interface design and security awareness in improving service quality and its impact on digital customer loyalty of smart mobile banking,” *2024 7th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 271–276, Dec. 2024. doi: 10.1109/isriti64779.2024.10963502.

BIOGRAPHIES OF AUTHORS

	<p>Lim Kai En is a student studying at Multimedia University, majoring in Bachelor of Information Technology (Hons) degree in Security Technology. Her research focuses on machine learning, deep learning, and fraud detection. She can be contacted at email: limkaien0909@gmail.com.</p>
---	--

	<p>Pang Ying Han received her B.E. (Hons) degree in Electronic Engineering in 2002, Master of Science degree in 2005 and PhD degree in 2013 from Multimedia University. She is an Associate Professor in the Faculty of Information Science and Technology at Multimedia University, Malaysia. Her research interests include human activity recognition, machine learning, deep learning and pattern recognition. She can be contacted at email: yhpang@mmu.edu.my.</p>
	<p>Ooi Shih Yin received her Bachelor of Information Technology (Hons), Master of Science and PhD from the Multimedia University, Malaysia. She was a research fellow at Yonsei University, South Korea, 2018-2019. She is an Associate Professor in the Faculty of Information Science and Technology at Multimedia University, Malaysia. Her research interests include image processing, computer vision, and machine learning. She can be contacted at email: syooi@mmu.edu.my.</p>
	<p>Kow Wan Xuan is a student studying at Multimedia University, majoring in Bachelor of Information Technology (Hons) degree in Security Technology. Her research focuses on machine learning, deep learning, and fraud detection. She can be contacted at email: kwx031120@gmail.com.</p>
	<p>Cheang Tang Xing is a student studying at Multimedia University, majoring in Bachelor of Information Technology (Hons) degree in Security Technology. His research focuses on cryptography and information security. He can be contacted at email: cheangtangxing@gmail.com.</p>
	<p>Tan Mao Wei is a student studying at Multimedia University, majoring in Bachelor of Information Technology (Hons) Security Technology. His research focuses on machine learning, and phishing detection. He can be contacted at email: tmw5034@gmail.com.</p>