Navigating the Hazards: Assessing the Consumer Risks of Fintech in Malaysia: A Conceptual Study

Mohd Fairuz Adnan*, Nurhazrina Mat Rahim, Fatin Shahirah Binti Shaharuddin, Nur Laili Aqilah Binti Ramli

Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam, Selangor, Malaysia.

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2024.8100116

Received: 03 October 2024; Revised: 08 October 2024; Accepted: 11 October 2024; Published: 08 November 2024

ABSTRACT

Fintech has come to be known as there is an increasing rate of users in Malaysia. The Covid-19 pandemic hastened the uptake of fintech and digital services in Malaysia, reflecting global patterns. According to the Fintech News Malaysia 2023, Malaysia remains the top-ranked country on the Global Islamic Fintech (GIFT) Index, reflecting its robust environment for Islamic fintech growth. Moreover, online and mobile banking maintained strong growth in 2022 and 2023, with electronic transactions via connected mobile devices and DuitNow QR codes becoming more widely adopted. This significant increase in fintech usage could expose consumers to potential risks. Users, particularly customers and bank employees, may have their rights violated because of cyber security issues such as identity theft and data breaches. This conceptual study utilizes a simple Systematic Literature Review (SLR) approach to explore and assess consumer risks within the Malaysian fintech industry. The main potential risks were identified as: (1) cybersecurity threats, (2) confidentiality, and (3) data protection.

Moreover, this study addresses the awareness and acceptance of fintech goods and services by Malaysian consumers. Given the potential risks posed by fintech, it is essential for users to be aware and take protective measures. The government should work towards establishing clear guidelines that mandate fintech companies to implement robust security protocols, ensuring that consumer data is adequately protected against breaches and misuse. Additionally, the government could enhance collaboration with industry stakeholders to create a more unified approach to risk management in the fintech sector

Keywords: Fintech, Risks, Cybersecurity, Confidentiality, Data Protections.

INTRODUCTION

Fintech, an abbreviation for financial technology, is a promising sector that incorporates technology into the services provided by financial companies, enhancing the utilization of financial services. This term covers a broad spectrum of applications, such as mobile banking, peer-to-peer lending, cryptocurrency platforms and others. In Malaysia, the fintech industry has experienced significant growth, reaching several phases of development over the past few years. The adoption of digital financial products and services has become essential in the post-COVID-19 era (Adnan et al., 2023). Online and mobile banking have continued to grow steadily, with electronic transactions via mobile devices and QR code payments becoming increasingly popular. E-payment transactions saw significant growth, reflecting a notable rise in usage over the past few years. This growth indicates that we are now better prepared to take advantage of the potential that fintech offers, and it has become an essential part of life for Malaysians in conducting transactions.

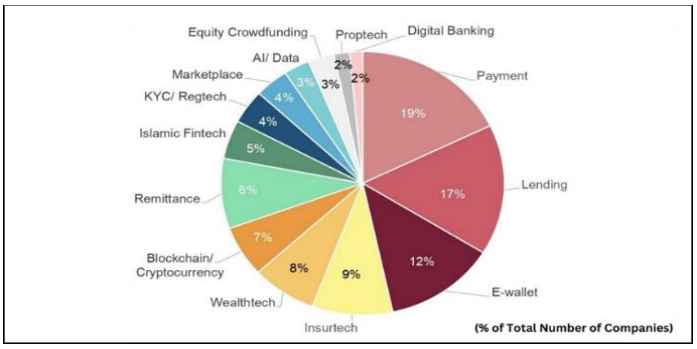
Despite the fintech revolution in Malaysia, it faces several challenges. Data privacy and cybersecurity are significant concerns as users share sensitive financial information on digital platforms (MyPF, 2024). A 2016

report by the Asian Institute of Chartered Bankers (AICB) and PricewaterhouseCoopers Risk Services Sdn Bhd (PwC) revealed that 82% of financial institutions in Malaysia are worried about the risks posed by fintech. However, only 47% have made fintech a priority in their strategic decision-making processes. To address this, fintech companies in Malaysia must comply with stringent regulations to safeguard user data and foster trust within the industry. Financial technology does, however, come with some difficulties despite the potential and advantages it offers. As a result, it is crucial to monitor the development of financial technology, ensuring that it is regulated and safe, as it will play a significant part in commercial and economic development.

BACKGROUND OF STUDY

According to the Fintech News Malaysia (2022), Malaysia has 294 fintech companies functioning in a variety of sectors. The four largest fintech segment in Malaysia are payments, making up 19% with 60 companies, followed by lending at 17% with 55 companies, e-wallets at 12% with 43 companies, and Insurtech at 9% with 31 companies. Figure 1 below shows the digital payments and lending leading Malaysian fintech.

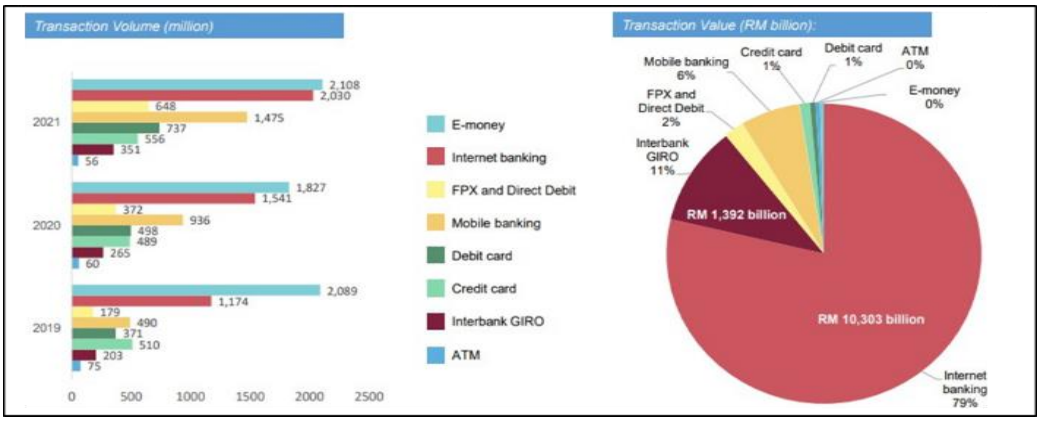
Figure 1: Malaysia fintech companies active in a range of sectors in 2022



(Source: Fintech News Malaysia in Malaysia Fintech Report 2022).

Furthermore, Malaysia's online banking capabilities have significantly increased. Based on Fintech News Malaysia (2022), the average number of e-wallet payment transactions per capita reaches pre-COVID levels at 64.5 in 2021. In Malaysia, e-payment channels were used in over 7.2 billion transactions last year alone, up 30% from the year before. Over the past ten years, digital payments have become more widely used and accepted in Malaysia. However, it was after the Covid-19 epidemic that the cashless revolution, a shift towards digital and card-based transactions, took hold. Figure 2 below shows the growth rate of transaction volume and value in Malaysia.

Figure 2: The Growth of Digital Payment in Malaysia



(Source: Fintech News Malaysia in Malaysia Fintech Report 2022).

Additionally, online and mobile banking experienced steady growth in 2022 and 2023, with electronic transactions via connected mobile devices and Duit Now QR codes becoming more widespread. E-payment transactions saw a 31.5% increase in 2022, rising to 9.5 billion from 7.2 billion in 2021 (Fintech News Malaysia,

2023).

As a result, fintech is a rapidly expanding industry and a relatively recent topic in the literature, yet it is often acknowledged as one of the most important breakthroughs in the financial sector. Rapid technological advancement has presented us with opportunities and difficulties, which we must constantly navigate. Consumers in this nation have the chance to participate in the adoption of the products and services provided by fintech. Therefore, assessing fintech risk in Malaysia is essential to ensure consumer protection and build trust in the financial system, fostering greater adoption of digital financial services to fully benefit from the advancement of technology.

Problem Statement

Fintech is a relatively fresh business in Malaysia that is fast growing and expanding because of the extraordinary and exponential growth in the usage of Information and Communications Technology (ICT). Consumers, investors, financial services firms, and financial market infrastructure are already benefiting from fintech, as are financial stability and inclusion. Despite the numerous benefits provided by fintech to consumers, there is also the possibility of customers needing help.

According to the KPMG report, consumers are unaware of the design and functionality of fintech. Consumers may not fully appreciate the nature and risks associated with the fintech-related products and services being offered to them. The other focus is on the increase in cost and the population of immigrants.

Adoption of innovative fintech solutions may mistakenly or purposely give new or different opportunities for a financial product and service producers and distributors to deceive customers or expose them to fraudulent activity. CTOS Data Systems Sdn Bhd (CTOS), through statistics from CTOS SecureID, has identified 335,000 pieces of personally identifiable information (PII) on the dark web, affecting 58,000 users over the past three years (Berita Harian, 2023). Malaysia has experienced yet another data breach, this time affecting a banking institution, a multimedia and broadcast agency, and a government electoral agency. Millions of personal records were reportedly sold online, raising serious concerns about data security (Loheswar, 2022). This highlights the growing concern over data security and the exposure of sensitive information, emphasizing the urgent need for more robust cybersecurity measures in Malaysia. Consequently, this research can contribute to the transformation of finance by providing insights for creating innovative financial solutions while also addressing the risks faced by users of financial technology.

Gap in Research

The growth of fintech has introduced both advantages and challenges for customers and financial service providers. On one hand, fintech can enhance the efficiency and accessibility of financial services, offering consumers more convenient and affordable choices. The rapid growth of fintech in Malaysia has transformed the landscape of financial services, offering innovative solutions to consumers. However, alongside these innovations come a range of consumer risks that demand thorough evaluation.

Although fintech adoption has rapidly increased in Malaysia, existing research primarily focuses on consumer acceptance, awareness, and the factors influencing adoption (Jin et al., 2019; Huei et al., 2018; Alkadi & Abedd, 2023). While there is a limited but expanding body of work addressing consumer risks (Boeddu et al., 2021), this conceptual paper aims to fill the research gap by systematically evaluating and identifying potential consumer risks in the Malaysian fintech landscape. It highlights the importance of fintech cybersecurity, confidentiality, and data protection while providing valuable insights for both regulators and industry stakeholders. Moreover, this study will look at the fintech industry to evaluate how regulators and industry actors have responded to the risk to financial technology users.

LITERATURE REVIEW

Consumer Risks of Fintech

This conceptual paper aims to explore the various risks associated with fintech services in Malaysia, focusing

on the interplay between cybersecurity threats, confidentiality issues, and data protection measures. By examining these key factors, the paper seeks to provide a comprehensive understanding of the challenges faced by consumers in the fintech landscape and highlight the need for enhanced protective measures to mitigate these risks. Through a thorough literature review, the paper will explore existing research and practices, ultimately offering recommendations for stakeholders in the fintech sector to improve consumer safety and trust.

Cybersecurity

Cybersecurity involves technologies, practices, and policies designed to protect systems, data, and people from cyberattacks like ransomware, malware, phishing, and data theft (Lindemulder & Kosinski, 2024). Cybersecurity can also be defined as a set of technologies, processes, practices, and mitigation strategies designed to protect networks, systems, programs, and data, ensuring their confidentiality, integrity, and availability by preventing attacks, damage, or unauthorized access (Kejwang, 2022). There are far too many ways to define cybersecurity, but they all boil down to the same thing: to guard against network attacks on our routine transactions and activities. Cybersecurity plays a crucial role in ensuring the smooth operation of the internet and its related activities and content while also safeguarding democratic institutions and protecting individual digital freedoms from being compromised (Roumpies & Kakarountas, 2023).

Cybersecurity threats can occur in various forms, starting with attacks targeting computers. These threats include any method that could harm computers, such as malware, viruses, or denial of service attacks. A hacker will use any information in the computer to perform all the classifications of computer crimes, such as phishing, spoofing, spam, cyberstalking, and identity theft. Cele & Kwenda (2024) found that identity theft, malware attacks, phishing and vishing are significant cybersecurity threats that hinder the adoption of digital banking.

Research from International Business Machines (IBM) in 2024, based on monitoring over 150 billion security events daily across more than 130 countries globally, revealed a 71% year-over-year rise in cyberattacks involving stolen or compromised credentials. Additionally, 32% of cyber incidents involved data theft and leaks, showing a shift toward data theft for resale over encryption for extortion. Furthermore, the A.I. sector, which now holds a 50% market share, is driving cybercriminals to develop affordable tools for targeting A.I. technologies. Moreover, Cyber Security Malaysia (CSM) reported a 1,192% increase in data thefts in 2023, with 646 cases compared to just 50 in 2022. In 2023, 5,917 cybersecurity incidents were reported, 3,705 of which were scams or fraud, and in the first three months of 2024, 142 data theft cases were recorded out of 1,555 incidents (Mok, 2024).

Fraud remains widespread, affecting people from students to professionals, as public awareness is still low, making citizens vulnerable. According to Malaysian Computer Emergency Responsive Team (MyCERT) report for second quarter 2024, the most common fraud cases reported to the Cyber999 Incident Response Centre included phishing, impersonation, spoofing, fraudulent websites, job scams, bogus emails, and business email compromise.

It can be said that companies in Malaysia have evolved and shifted their attention to online transactions like payments and money deposits as it is more convenient and faster to run their daily business. The conversion from traditional technology to modern technology has contributed to a competitive advantage for this sector. As a result, nations and other organizations must grasp how to implement cybersecurity measures to counter potential threats.

Adopting robust cybersecurity practices is crucial for both individuals and organizations of all sizes. A business can utilize a suite of tools referred to as network security to defend their computer networks. It involves the measures and policies implemented by a network administrator to prevent, detect, and control unauthorized access, alterations to the system, misuse, or denial of a computer network and its resources accessible via the network (Pawar & Anuradha, 2015). These fundamental "cyber hygiene" habits significantly enhance online security (America’s Cyber Defence Agency, 2024). Finally, the involvement of government and security agencies is also important to support the effectiveness of the adoption of methods to address cybersecurity threats.

Confidentiality

Generally, confidentiality refers to the nondisclosure of information beyond an authorized group of people. Hussain et al. (2019) explain that data confidentiality involves safeguarding information from being disclosed to unauthorized individuals, and it can be effectively maintained through encryption. The objective of confidentiality is to guarantee that only authorized persons or organizations have access to the information (Hammer & Schneider, 2007). Personal information should be kept private between the financial institution and the consumer and should not be shared with anyone else, including the client's close family members. In a nutshell, confidentiality means that any information gathered or acquired should be kept private and not disclosed to a third party.

Payment and wallets have been the most popular fintech solutions for facilitating daily transactions in Malaysia. In Malaysia, non-bank firms, mostly fintech startups and major technology corporations, have created a range of mobile wallets. According to a Financial Times Confidential Research survey, the most popular mobile wallets are GrabPay, Touch 'n Go, and WeChat Pay (Jin et. al, 2020). Privacy attacks are a common cause of breaches in data confidentiality (Hussain et al., 2019). Therefore, confidentiality is critical because personal identity information and card account information must be kept in the mobile application for mobile payment to work. As a result, it may be vulnerable to risks such as unauthorized users, intercepting, leaking, guessing, hijacking, or masquerading. To soothe consumer concerns about their privacy, merchants must assure customer data privacy and give the most significant degree of protection.

Fintech, such as mobile payment services, can only be called confidential if all transactions fulfil the demands and expectations of customers regarding security. Based on research by Mun et al. (2017), the findings show that the significant reason respondents did not use mobile payment services was because they were concerned that their personal information would not be kept confidential while using mobile payment services. According to Dhatshana et al. (2022), the most significant challenges are the lack of knowledge and awareness among people, the fear of loss of money by use of digital payment methods and the risk of hacking. Therefore, merchants' integrity and ethics are critical in preventing data leaks and misuse. They must handle consumer personal data with the highest level of care. This requires protecting the data from passive attacks and ensuring that only authorized individuals have access to view the information.

Data protection

Data protection and confidentiality are closely related, but data protection involves more than just keeping information private. For instance, personal data must be kept confidential, but it should also be accessible, accurate, and processed using reliable services that are protected against errors and failures. Data protection laws serve as the primary defense against violations of fundamental rights related to data. With more activities moving online, these laws have expanded their reach. As a result, data protection is often called "the law of everything" (Lynskey, 2023). The Personal Data Protection Department (PDPD), established by the Malaysian Ministry of Communications and Multimedia Commission (MCMC), is responsible for ensuring that the personal data of individuals involved in business transactions is not misused or mishandled by those participating in the transactions. The PDPA requires that users be safeguarded against any form of misuse in the storage or processing of personal data belonging to individuals, as well as in the public and commercial sectors in Malaysia for business transactions.

Malaysia's digital transformation has been underway for over a decade, but the Covid-19 pandemic significantly sped up the adoption of fintech. A significant contributor to this progress is Bank Negara Malaysia's (BNM) introduction of a regulatory sandbox framework designed to regulate and support the growth of fintech solutions since 2016. Similarly, another main regulator for Fintech in Malaysia which is the Securities Commission Malaysia plans to implement a regulatory sandbox and strengthen its regulatory framework to promote securities tokenization, aiming to stimulate innovation in the capital market. Additionally, BNM introduced its second Financial Inclusion Framework (2023–2026) to tackle ongoing challenges in financial inclusion, particularly in Digital Financial Services. One key issue is the low level of digital financial literacy, with 37% of Malaysians sharing their bank account passwords or PINs with close friends (Fintech News Malaysia, 2023).

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VIII Issue X October 2024

Issues with personal data will result in financial losses, crimes, and violations of personal information (Rohendi & Kharisma, 2024). Consumers are prone to data loss and may be unaware of how their information is being used (KPMG International, 2019). According to Murugiah (2018), the most challenging task for fintech is to emphasize information security and protection. Therefore, consumers need to be informed of the dangers and benefits of utilizing fintech services and take the required safeguards to protect their personal and financial information. Some fintech services may lack the same legal protections as traditional financial services, putting consumers at greater risk of fraud or financial loss.

There are several methods to reduce the risk of personal data breaches, with education being an effective approach to raising fintech users' awareness of personal data protection (Oliver et al., 2023). In addition, utilizing fintech services from trustworthy providers and consistently monitoring accounts for any unusual activity can be an effective approach. Another strategy that should be implemented to ensure personal data protection is the establishment of a Personal Data Protection Commission, along with enhancing consumers' financial literacy (Rohendi & Kharisma). Ultimately, safeguarding financial transactions and ensuring digital safety can be achieved by staying informed and adopting strong security practices (Hall, 2024).

METHODOLOGY

This study employs a simple Systematic Literature Review (SLR) research method to evaluate consumer risks within the fintech industry of Malaysia. SLR involves a comprehensive, methodical approach to synthesizing existing research on a specific topic and is valuable for informing primary research, serving as standalone academic work, and providing a broader understanding of a topic (Kabir et al., 2023). It relies on secondary data sources, including academic literature, industry reports, regulatory guidelines, and case studies from Malaysia and globally relevant contexts. The process includes:

Literature review: To uncover important consumer threats like cybersecurity threats, confidentiality and data protection issues, a thorough analysis of scholarly works and industry reports is conducted.

Case Study Analysis: To give practical instances of consumer hazards, a few case studies from Malaysia's fintech scene are analyzed.

Regulatory Review: To identify the existing legal framework governing the industry, relevant Malaysian regulations and guidelines related to fintech are examined (e.g., Bank Negara Malaysia and Securities Commission Malaysia regulations)

Research Design: To map out and categorize potential risks of fintech to consumers, a conceptual framework is developed.

Figure 3: The Proposed Conceptual Framework for Factors Influencing Risk of Fintech to Consumers.

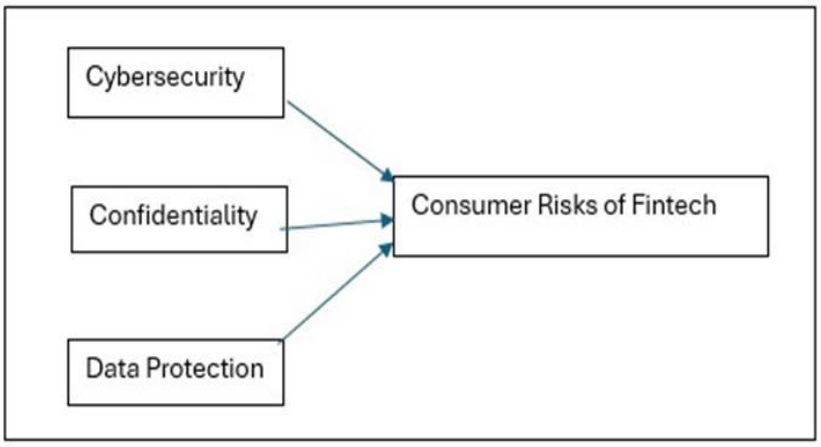


Figure 3 illustrates the relationships between three key variables: cybersecurity, confidentiality, and data protection, all of which are essential in addressing the risks fintech poses to consumers. Cybersecurity refers to

the measures and technologies that protect financial systems and data from cyber threats, such as hacking or malware. Strong cybersecurity helps ensure that consumer data remains safe from unauthorized access. Confidentiality focuses on keeping personal information private and secure from those who should not have access to it. Maintaining confidentiality is crucial for building consumer trust in fintech services. Data Protection encompasses the policies and practices that ensure personal data is collected, processed, and stored securely. Effective data protection measures prevent misuse of consumer information and ensure compliance with legal standards.

CONCLUSION

Malaysia's overall economic growth has been aided by the expansion of the fintech industry for the past few years. By leveraging cutting-edge technology and innovation to challenge conventional financial practices in the provision of financial services, fintech has significantly increased the effectiveness of the financial system and the financial outcomes for both businesses and consumers. Even though fintech has the potential to provide its users with many advantages but it also carries a risk that can give adverse effects on its consumers.

This study suggests that cyber security, confidentiality, and data protection are significant factors that influence the risk of fintech to consumers. These factors have an impact on financial transactions since all transactions now take place online which renders this industry particularly susceptible to breaches of security. It is important for fintech consumers to understand the risks and take the action to mitigate the risk accordingly.

As fintech continues to grow in Malaysia, the increasing prevalence of cybersecurity threats poses significant risks to consumers, making it essential for fintech providers to implement robust security measures. Adopting cybersecurity can prevent users from any cyber-attacks while utilizing fintech and providing innovative solutions. Additionally, ensuring confidentiality is equally important, as it safeguards personal information, and fosters trust between consumers and financial service providers. Moreover, effective data protection practices are crucial for managing and securing consumer information, ensuring compliance with regulations, and preventing misuse. By addressing these three major factors that influence the consumer's risk, fintech stakeholders can significantly reduce the risks and enhance *overall trust in the fintech landscape in Malaysia. This comprehensive approach will not only protect consumers but also promote sustainable growth and innovation within the fintech sector.*

RECOMMENDATION

To effectively mitigate consumer risks in the fintech sector, it is essential for fintech providers to strengthen their cybersecurity protocols. By adopting advanced technologies such as artificial intelligence and machine learning, companies can detect unusual activities and respond to potential breaches in real-time. Regular vulnerability assessments and penetration testing should also be conducted to identify and address weaknesses in their systems. This proactive approach not only helps safeguard consumer data but also fosters greater trust among users.

Additionally, fintech organizations should enhance their data protection policies to ensure compliance with local and international regulations. Developing comprehensive frameworks that outline clear data retention policies, secure storage solutions, and robust encryption methods for data both in transit and at rest will significantly reduce the risk of unauthorized access. By prioritizing data protection, fintech companies can safeguard consumer interests while also maintaining their reputations in a competitive marketplace.

Moreover, promoting consumer education and awareness such as digital financial literacy (DFL) is vital for minimizing risks associated with fintech services. The theory of planned behavior suggests that DFL is likely to affect a person's ability to practice good financial habits (Ali et al., 2024). Fintech providers can achieve this by offering educational resources such as webinars, articles, and interactive tools that inform consumers about best practices for protecting their personal information online. Regular updates on emerging threats and security measures will empower users to make informed decisions while using fintech services. By investing in consumer education, fintech companies can build trust and contribute to a more secure digital financial environment.

Finally, to further enhance understanding of consumer risks in the fintech sector, it is essential to conduct empirical studies that analyze the impacts of cybersecurity threats, confidentiality, and data protection on consumer behavior. Such research can provide valuable insights into how these factors influence consumer trust and adoption of fintech services.

ACKNOWLEDGMENT

The Authors would like to convey their appreciation to the Faculty of Accountancy, Universiti Teknologi MARA, Malaysia, for supporting and enabling this research project.

REFERENCES

1. Adnan, M. F., Rahim, N. M., & Ali, N. (2023). Determinants of Digital Financial Literacy from Students' Perspective. Corporate Governance and Organizational Behavior Review, 7(2), 168-177.
2. AICB & PWC (November 2016). Catching the FinTech Wave; A survey on FinTech in Malaysia. Available at: https://www.pwc.com/my/en/assets/publications/2016-pwc-aicb-catching-the-fintech-wave.pdf
3. Ali, N., Rahim, N. M., Adnan, M. F., Yanto, H., & Kiswanto, K. (2024). Determinants of Financial Behaviour: Does Digital Financial Literacy (DFL) Foster or Deter Sound Financial Behaviour? Accounting and Finance Research, 13(1), 1-6.
4. Alkadi, R.S., & Abed, S.S. (2023). Consumer Acceptance of Fintech App Payment Services: A Systematic Literature Review and Future Research Agenda. J. Theor. Appl. Electron. Commer. Res., 18, 1838-1860. https://doi.org/10.3390/jtaer18040093
5. America's Cyber Defence Agency (2024), Cybersecurity Best Practices, Cybersecurity and Infrastructure Security Agency (CISA). Available at: https://www.cisa.gov/topics/cybersecurity-best-practices
6. Bank Negara Malaysia (2016, October 18). Financial Technology Regulatory Sandbox Framework, Available at: https://www.bnm.gov.my/-/financial-technology-regulatory-sandbox-framework
7. Berita Harian (2023, December 21), CTOS kesan 335,000 kebocoran maklumat peribadi, Berita Harian, Available at: https://www.bharian.com.my/bisnes/lain-lain/2023/12/1191469/ctos-kesan-335000-kebocoran-maklumat-peribadi
8. Boeddu, G., Chien, J., Ivor, & Grady, R. (2021, April). Consumer Risks in Fintech New Manifestations of Consumer Risks and Emerging Regulatory Approaches. Available at: https://documents1.worldbank.org/curated/en/515771621921739154/pdf/Consumer-Risks-in-Fintech-New-Manifestations-of-Consumer-Risks-and-Emerging-Regulatory-Approaches-Policy-Research-Paper.pdf
9. Cele, N.N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime. https://doi.org/10.1108/jfc-10-2023-0263
10. Dhatshana, G., Sangeetha, D. D., & Selvarani, S. (2022). Mobile wallet - The next generation digital marketing. Journal of Management & Entrepreneurship, 16(1), 76-82.
11. Fintech News Malaysia (2022, July 18). Malaysia Charts a New Path for Fintech Growth, 2022 Malaysia Fintech Report: Available at: https://fintechnews.my/31945/malaysia/fintech-report-malaysia-2022/
12. Fintech News Malaysia (2023, June 26). BNM Lays Out Second Financial Inclusion Framework for the Next 4 Years, Available at: https://fintechnews.my/37202/financial-inclusion/bnm-lays-out-second-financial-inclusion-framework-for-the-next-4-years/
13. Fintech News Malaysia (2023, October 11). Landmark Year in Financial Innovation. 2023 Malaysia Fintech Report: Available at: https://fintechnews.my/40202/various/malaysia-fintech-report-2023-landmark-year-in-financial-innovation/
14. Hall, P. (2024, April 15). Securing Financial Transactions in the Digital Age, Available at: https://secarma.com/securing-financial-transactions-in-the-digital-age
15. Hammer, J. H., & Schneider, G. (2007, August). On the definition and policies of confidentiality. In Third International Symposium on Information Assurance and Security (pp. 337-342). IEEE.
16. Huei, C.T., Cheng, L.S., Seong, L.C., Khin, A.A., & Bin, R.L. (2018). Preliminary Study on Consumer Attitude towards FinTech Products and Services in Malaysia. International journal of engineering and

technology, 7, 166. https://doi.org/10.14419/IJET.V7I2.29.13310
17. Hussain, M., Mehmood, A., Khan, S., Khan, M. A., & Iqbal, Z. (2019). Authentication techniques and methodologies used in wireless body area networks. Journal of Systems Architecture, 101, 101655.
18. IBM (2024), IBM X-Force Threat Intelligence Index 2024, Know your threats, Available at: https://www.ibm.com/reports/threat-intelligence?utm content=SRCWW&p1= Search&p4= 43700079696819867&p5=p&p9=58700008682357289&gclid=Cj0KCQjwo8S3BhDeARIsAFRmkOMdSLMf4JIyyNAakGZGE0Idxu0h7GiXhp7hGuE_9fA1ow6kl8hyeEcaAswuEALw_wcB&gclsrc=aw.ds
19. Jin, C.C., Seong, L.C., & Khin, A.A. (2019). Factors Affecting the Consumer Acceptance towards Fintech Products and Services in Malaysia. International Journal of Asian Social Science. https://doi.org/10.18488/JOURNAL.1.2019.91.59.65
20. Kabir, R., Hayhoe, R., Bai, A. C., Vinnakota, D., Sivasubramanian, M., Afework, S., & Parsa, A. D. (2023). The systematic literature review process: a simple guide for public health and allied health students. https://dx.doi.org/10.18203/2320-6012.ijrms20232496
21. Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of the literature. International Journal of Research in Business and Social Science (2147–4478). https://doi.org/10.20525/ijrbs.v11i6.1947
22. KPMG International. (2019, Mac). Regulation and Supervision of Fintech. Available at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf
23. Lindemulder G., & Kosinski M. (2024, August 12). What is cybersecurity? IBM, Available at: https://www.ibm.com/topics/cybersecurity
24. Loheswar, R. (2022, December 31). Major data breaches in Malaysia in the past 24 months, Malaymail, Available at: https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722
25. Malaysian Computer Emergency Responsive Team (MyCERT) (2024, September 18). SR-027.092024: My CERT Report - Cyber Incident Quarterly Summary Report - Q2 2024, Cyber Security Malaysia, Available at: https://www.mycert.org.my/portal/advisory?id=SR-027.092024
26. Mok, O. (2024, April 13). Cyber Security Malaysia reports a steep jump in data thefts last year, Malaymail, Available at: https://www.malaymail.com/news/malaysia/2024/04/13/cybersecurity-malaysia-reports-a-steep-jump-in-data-thefts-last-year/128617
27. Murugiah, S. (April 12, 2018). Cybersecurity Biggest Barrier to Fintech, Banking Sector Partnerships, says Fortinet. The Edge Markets. Available at: https://theedgemalaysia.com/article/cybersecurity-biggest-barrier-fintech-banking-sector partnerships-says-fortinet
28. My P.F. (2024, April 28), The challenges and potential of Malaysia's fintech industry Available at: https://www.freemalaysiatoday.com/category/leisure/2024/04/28/the-challenges-and-potential-of-malaysias-fintech-industry/
29. Oliver, R., Magdalena, Y., & Deniswara, K. (2023). Analysis of Utilizing Mobile Application to Educate Fintech User's Data Protection: Mobile Learning Scale Approach. Proceedings of the 2023 7th International Conference on E-Commerce, E-Business and E-Government. https://doi.org/10.1145/3599609.3599625
30. Orla Lynskey, Complete and Effective Data Protection, Current Legal Problems, Volume 76, Issue 1, 2023, Pages 297–344, https://doi.org/10.1093/clp/cuad009
31. Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, 503-506. https://doi.org/10.1016/j.procs.2015.04.126
32. Rohendi, A., & Kharisma, D.B. (2024). Personal data protection in fintech: A case study from Indonesia. Journal of Infrastructure, Policy and Development. https://doi.org/10.24294/jipd.v8i7.4158
33. Roumpies, F., & Kakarountas, A. (2023). Cybersecurity and Democracy: A Review. 2023 8th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 1–8.
34. Schueffel, P. (2017). Taming the Beast: A scientific definition of fintech. Journal of Innovation Management, 4(4), 32-54. https://doi.org/10.24840/2183-0606_004.004_0004 Securities Commission Malaysia (SC) (2024, October 1). SC Unveils Three Initiatives to Spur Innovation. Measures announced at the SCxSC Fintech Summit 2024.Available at: https://www.sc.com.my/resources/media/media-release/sc-unveils-three-initiatives-to-spur-innovation