الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
Garden of Knowledge and Virtue
LEADING THE WAY
KHALĪFAH • AMĀNAH • IQRA' • RAHMATAN LIL 'ĀLAMĪN
LEADING THE WORLD
INTERNATIONAL MULTI-AWARD WINNING INSTITUTION FOR SUSTAINABILITY
KICT
KULLIYYAH OF INFORMATION AND COMMUNICATION TECHNOLOGY

Advancement in ICT: Exploring Innovative Solutions (AdICT)

Series 1/2024

KICT Publishing

ADVANCEMENT IN ICT: EXPLORING INNOVATIVE SOLUTIONS (AdICT) SERIES 1/2024

Editors
Noor Azura Zakaria
Dini Oktarina Dwi Handayani
Elin Eliana Abdul Rahim
Ahmad Fatzilah Misman

KICT Publishing

ADVANCEMENT IN ICT: EXPLORING INNOVATIVE SOLUTIONS (AdICT) SERIES 1/2024

First Publication 2024

Published by

KICT Publishing
International Islamic University Malaysia
53100 Kuala Lumpur, Selangor, Malaysia

e ISBN 978-629-99388-0-4

9 786299 938804

Cataloguing-in-Publication Data

Perpustakaan Negara Malaysia

A catalogue record for this book is available from the National Library of Malaysia

eISBN 978-629-99388-0-4

KICT Publishing

(Online)

Preface

Advancement in ICT: Exploring Innovative Solutions (AdICT) Series 1/2024 is an e-book showcases the collective achievements of Final Year Project (FYP) in Kulliyyah of Information and Communication Technology (KICT). This compilation represents evidence to the technical passion and academic skills of our students before they venture into the professional realm.

FYP is a journey that demands creativity, critical thinking, and perseverance. This book encapsulates the diverse range of projects undertaken by our students, each a unique exploration into the vast landscape of Information and Communication Technology (ICT). From cutting-edge software applications to groundbreaking research, these projects not only demonstrate technical proficiency but also the ability to address real-world challenges.

In this comprehensive collection, the topics covered span a spectrum from cutting-edge software development, cybersecurity, artificial intelligence and multimedia technologies reflecting the breadth and depth of our academic program. This offers a curated journey through the diverse landscape of final year ICT projects toS the readers while appreciating the impact these projects can have on the wider community.

This e-book carries significant benefits and impact whereby it serves as a valuable knowledge repository, offering a diverse audience—from students and educators to industry professionals—a comprehensive view of the latest innovations and technological solutions in ICT. Moreover, the book fosters a culture of knowledge sharing and collaboration, as each project represents a unique contribution to the broader technological landscape.

"When the human being dies, his deeds end except for three: ongoing charity, beneficial knowledge, or a righteous child who prays for him" *– Sahih Muslim*

Editors

Noor Azura Zakaria
Dini Oktarina Dwi Handayani
Elin Eliana Abdul Rahim
Ahmad Fatzilah Misman

TABLE OF CONTENTS

Security and Privacy in Next-Generation Mobile Payment Systems

Ani Afiqah
Kulliyyah of ICT
International Islamic University Malaysia
Selangor, Malaysia
aniafiqah00@gmail.com

Hafizah Mansor
Kulliyyah of ICT
International Islamic University Malaysia
Selangor, Malaysia
hafizahmansor@iium.edu.my

***Abstract*— As the number of mobile payment transactions increases, there is also an increase in crimes related to mobile payment systems. Fraud, scams, data theft, and stealing are among some crimes affecting mobile payment application users. This paper compares the features of five existing mobile payment applications in Malaysia, Boost, Grab Pay, Touch 'n Go, MAE, and ShopeePay, to gain insights into how Malaysia's mobile payment applications work. Besides that, this paper identifies the major security and privacy issues in mobile payment systems by assessing threats, vulnerabilities, and risks. Moreover, this paper identifies the security mechanisms of mobile payment systems. In addition, this paper discovers some methods to improve the security of mobile payment systems by conducting a literature review on the existing security properties of mobile payment systems. Hence, it is believed that a better secure mobile payment system can be developed. It would increase the trustworthiness of the users and encourage them to keep using mobile payment applications.**

Keywords— mobile payment, e-wallet, financial technology, security and privacy

I. INTRODUCTION

Recently, the number of mobile payment transactions has skyrocketed. Several types of mobile payment applications for trading activities exist in the market. Mobile payment refers to payment services that can perform financial transactions from or via mobile devices and smartwatches [1]. Mobile payment technology enables users to make instantly and simply in-store and online purchases, which offers them more flexibility and convenience in their payment options.

Using the quick-response (QR) code that the seller generates facilitates collecting money from customers. Other than QR codes, Near Field Communication (NFC) is one of the new technologies being used to make the payment experience better than ever before. NFC is a technology that allows users to securely transmit and receive information over a short distance via phone [2] [3]. NFC is an evolution of existing radio-frequency identification (RFID) technology that combines both the reader and the smart card interface in a single device.

Moreover, mobile payment systems can be broadly divided into two types: closed loop and open loop [4]. Both closed, and modern companies often accept open-loop payment methods to provide more convenience to customers. Open loop mobile payments are typically prepaid, meaning that instead of connecting directly to a bank account or credit card, the account balance must be topped up first, and the balance is used from there. Users can use this type of mobile payment to purchase at selected merchants partnered with the application provider. Closed-loop mobile payments are prepaid as well. However, the function is very different. With this type, users can only use the funds to make purchases at a specific retailer, such as loyalty cards.

In addition, some mobile payment systems allow for bank transfers, which means the users can withdraw the money from the mobile payment account to their bank account. Examples of mobile payment systems implemented and widely used in Malaysia are GrabPay, Boost, Touch 'n Go E-wallet, MAE, ShopeePay, and many more.

However, as the number of mobile payment transactions increases, there is also an increase in crime related to mobile payment systems. People have become more concerned about the security of mobile payment systems, such as authentication issues. Some crime cases are related to a mobile payment system, which happened in Malaysia. On 12th February 2022, Sinar Harian's news reported that nearly 50 teachers in eight schools around the Klang Valley claimed to be victims of the Touch 'n Go wallet fraud syndicate [5]. To make matters worse, some of them had activated auto-reload linked to their bank accounts. One of the victims only realized his mobile payment account had been hacked after finding that his balance in the bank had been reduced. After realizing the incident, he no longer connects his mobile payment account with his debit card and has changed his PIN. Another victim claimed that the transactions happened using their PIN number because he found that the scammers were still trying to make transactions at that time until his mobile payment account was blocked. After all, the wrong PIN was entered more than three times. Another reported case of fraud involves a phishing scam. The scammer will send an email or short messaging service (SMS) to the victim together with a suspicious link, which is disguised as a mobile payment application. This is a tactic used by scammers to obtain information such as the phone number and PIN of a mobile payment account through a fake website. On 2 August 2022, Malay Mail reported that Tenaga Nasional Berhad (TNB) warned of a new scam that purports to compensate affected users of power outages via Touch 'n Go wallet [6]. The message was sent using the shortcode (15454) and announced that Malaysians affected by the power disruption would receive compensation of RM100 through the Touch 'n Go wallet. To claim the money, users must click on a link that goes to a fake website. This appears to be the same phishing

tactic used for the RM800 Covid-19 financial aid scam, which the same news company reported in July 2022 [7]. The given link leads to a website designed to trick users into entering their registered mobile number, the 6-digit PIN, and the one-time password (OTP) for the Touch 'n Go wallet.

Thus, the payment gateway is vital in the mobile payment systems' transactions. A payment gateway acts as an intermediary to safely transfer payment money from a user's bank account to a merchant's bank account. The payment gateway is a security layer that helps authenticate and authorize online transactions. Users of mobile payment systems often need a PIN or fingerprint to be authenticated before proceeding with the transaction.

This paper aims to examine the properties of a few existing mobile payment systems and analyze the authentication methods t used in those mobile payment systems. Moreover, this paper aims to evaluate potential improvements that could sufficiently guarantee user protection. Therefore, the existing authentication mechanism needs to be analyzed to see how effective it is in securing and protecting customers.

II. Literature Review

Various relevant literature focused a significant interest on studies regarding the security of mobile payment systems. Due to the growing popularity of online banking and shopping throughout the past years, the usage of mobile payment systems has kept on developing at an increasing rate. [1] However, the usage of mobile payment systems has been in question. A survey was conducted to evaluate the positive and negative impacts of mobile payment systems on users [2]. Based on the survey conducted, 38.9% of respondents are using mobile payment systems as their main payment method. Furthermore, most of the respondents agreed that mobile payment systems have security risks. The authors concluded that even though a mobile payment system might increase productivity, sometimes it might cause trouble for users. Security problems are believed to occur in mobile payment systems because of the rising trend.

According to [3], there are four categories of electronic payment: an online electronic cash system, an electronic cheque system, an online credit card payment system, and a smart card-based electronic payment system. The authors stated that each payment system has its advantages and disadvantages for customers and merchants. They highlighted the importance of analyzing the level of security concerning fraud vulnerability and established whether the relationships enhance user confidence. The authors demonstrated the categories of electronic payment systems with their number of authentication factors and authentication types. For future work, the authors suggest combining the discussed authentication technique with the three-factor authentication model to produce a better algorithm for electronic payment systems whose authentication capability would outperform the present online payment applications.

Authentication is one of the essential protections against unauthorized access to mobile payment applications [4]. The most popular authentication method now, particularly when utilizing mobile payment systems, is PINs, although this method has well-known drawbacks. Three authentication factors can be used, which are something you know (password and PIN), something you have (one-time-use-token and smartcard), and something you are (fingerprint, iris, and speech recognition) [5] The level of security must be considered during the creation of mobile payment authentication on mobile devices. Based on the study [4], a design of mobile payment applications with an additional layer of security that focuses on the inside of the current user authentication system was proposed. The proposed authentication design consists of a registration that is developed and executed using Android Studio Firebase real-time databases and PayPal. The functional testing demonstrates that the suggested technique's features fulfil the criteria, and since it is impossible to use the same account on two different devices, it is safe from attacks. Thus, no errors occur. They concluded that their proposed solution outperforms existing solutions regarding security criteria.

[6] claimed that using a mobile payment system always comes with risks. They included results from a 2015 survey that was conducted among mobile payment users in the US. The results show that 20% of people are concerned if someone is possibly intercepting their payment data or personal information, and 13% of them are concerned about their phones being hacked. The authors proposed defining minimum measures that should be followed by mobile payment providers and providing security recommendations for organizations wishing to provide mobile payment services. To have a thorough grasp of the numerous risks that might influence mobile payment applications and their potential security solutions, the study [7] has discovered and analyzed the various threats and vulnerabilities of a mobile payment application. The author used a few mobile payment applications such as Apple Pay, Google Pay, Paytm, Freecharge, Mobikwik, SBI's Buddy, ICICI Pay, Airtel Money, Jio Money, PayU Money, and HDFC Zap Pay to make a comparison. In addition, a mobile payment system, a mobile payment, and a mobile payment threat model, as well as the threats and vulnerabilities of mobile payment security measures, were defined by the author in the study. The author stated that the identified threats have not yet reached the expected level of maturity. Thus, new solutions to reduce threats or vulnerability must be implemented since the overall field continues to be an area of active study.

A literature review on the security limitations of mobile payment applications was also conducted. [8] performed research on the security limitations of several mobile payment applications in India. The authors listed the security objectives that must be followed to satisfy cybersecurity: availability, confidentiality, integrity, authentication, and accountability. Moreover, the authors include the vulnerability and threats of mobile payments in their investigation. To conclude the research, the authors made a comparative analysis of mobile payments, which lists the different features of the applications in the context of given security objectives.

[9] assessed the present and development of mobile payments besides considering the industry's future. Different systems of electronic payment services, mobile payment security problems, and its potential future use. The study's findings claim that many mobile phone users are promoting the growing popularity of using mobile devices to make online payments. Moreover, the authors argue that the mobile payment industry must overcome certain security and authentication challenges to make steady progress in the future. For future work, the authors wish to validate the factors

that can contribute to the widespread use of mobile payment systems.

III. METHODOLOGY

A literature review and analysis of Malaysia's existing mobile payment applications has been conducted to compare their features. The mobile payment applications were chosen based on the recent trends in the applications [10]. These include Boost, GrabPay, Touch 'n Go e-wallet, MAE, and ShopeePay. The main features that have been analyzed are how mobile payments support in-store proximity payment technologies and their type of security authentication. The purpose of this comparison is to analyze how secure the current mobile payment applications are. Table 1 below shows the comparison of different mobile payment applications.

TABLE 1 COMPARISON OF DIFFERENT MOBILE PAYMENT APPLICATIONS

Features	**Boost**	**GrabPay**	**Touch 'n Go**	**MAE**	**Shopee Pay**
Year of launch	2017	2017	2017	2019	2019
Payment type of wallet	Open loop	Open loop	Open loop	Open loop	Open loop
Supports in-store proximity payment technologies	Yes (QR code)	Yes (QR code)	Yes (QR code and NFC)	Yes (QR code and NFC)	Yes (QR code)
Bank transfer	Not allow-ed	Only premium accounts are allowed	Only premium account allowed	Allowed	Allow-ed
Security	Need to enter a 6-digit PIN	Need to enter 6-digit PIN	Need to enter a 6-digit PIN	Does not require any authentic-cation phase	Need to enter 6-digit PIN or biometric authentication
Application provider	Axiata	Grab	Alipay and Touch 'n Go	Maybank	Shopee

A. Threats, Vulnerabilities and Risk Assessment in Mobile Payment Systems

Threats could destroy or steal data, interrupt operations, and generally cause harm. Vulnerability is a weakness in a system's hardware, software, or operating processes. It is the gap that malicious people can use to access assets. In other words, threats exploit vulnerabilities. Risk is the intersection of assets, threats, and vulnerabilities. When a threat exploits a vulnerability, there is a risk that an asset may be lost, harmed, or destroyed. A threat, vulnerability, and risk assessment provides an investigation and interpretation of the risk existing in an organizational and technical environment [11]. Thus, we conducted threat, vulnerability, and risk assessments to ensure the necessary measures are in place to secure the availability, confidentiality, and integrity of information, to identify risks by determining potential security vulnerabilities, and to take appropriate measures for adequate risk management. Threat, vulnerability, and risk assessment is conducted to identify the significant security and privacy issues in mobile payment systems.

B. Threats

One of the threats is tampering with mobile payment applications. An attacker may decide to use a mobile payment system's backdoor to intercept login information and deliver the details to a server under their control. The attacker can use the details to cheat the users. The attacker can also easily download the sensitive data of mobile payment applications. The second threat is the exploitation of mobile payment application vulnerabilities. Attackers could utilize this to steal any sensitive and personal information stored by the application. The vulnerability of mobile payment Application Programming Interfaces (APIs) used for in-app purchases might lead to unauthorized access to mobile payment systems, enabling an attacker to carry out fraudulent transactions. With stolen bank card accounts connected to mobile payment applications, fraud is also a possibility. During the registration process, the attacker might add a different mobile device to the user profile and make false payments. This leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity you use in an equation.

C. Vulnerabilities

Weak user authentication could be one of the vulnerabilities of mobile payment systems. Usually, providers employ fingerprint biometric authentication. Research has demonstrated that fingerprint authentication can be defeated and is breakable [12]. It is possible to create a duplicate biometric identity using 3D printers, such as biometric stamps made from thumb impressions. Additionally, if the user's phone were stolen, it would be simple to resist biometric authentication, which unlocks the whole phone and the financial transaction procedure. Next, accountability for payment transactions is also a vulnerability. Mobile payment systems require fingerprint authentication before processing a transaction. Some mobile payment applications, such as ShopeePay, linked the fingerprint with the phone's database. However, many people could have registered in the fingerprint phone's database, making it possible for anyone who is registered to make a payment if they can authenticate to the phone. When several users have access to the device, there is a failure in accountability since it is impossible to identify the individual who performed the payment.

D. Risks

The first risk of mobile payment systems is reputational risk, which causes unfavourable impressions from customers and investors to harm the business and limit access to funding sources. In mobile payments, bad customer service, faulty technology, and agent misbehaviour can destroy customers' trust in the service provider and threaten their loyalty. The second risk of mobile payment systems is security risk. Security and fraud issues offer a major obstacle to consumer adoption. New fraud and security issues, including device and

mobile payment vulnerabilities, malware inside tags, data eavesdropping, and man-in-the-middle attacks, are particularly prominent with contactless technologies. Third, the operational risk results from the possibility of loss related to apparent problems in the integrity or dependability of the system. Due to the possibility of external or internal assaults on banks' systems or goods, security concerns are of the utmost importance. Customer exploitation and improperly planned or implemented electronic banking and electronic money systems are further sources of operational risk.

IV. Results and Analysis

A. Security Objectives of Mobile Payment Systems

The biggest issue with electronic payment methods is protection. No one will consider them secure to use without secure industrial information interchange and secure electronic money transfers over networks. Users require confidentiality, data integrity, availability, non-repudiation, and authentication as essential requirements for the secure processing of payments over the Internet [13]. Mobile payment systems must have all the above protective features because users will certainly not rely on mobile payment systems that are not secure. In addition, trust is crucial to ensure customer approval. This section presents the security features to prevent mobile payment fraud.

1) Confidentiality

In the world of e-commerce, confidentiality is crucial due to the chance that attackers could gain critical client data. A consumer should be allowed to use an electronic bank account for mobile payments after sufficient authentication. Other clients who use electronic banking do not immediately have access to the customer's information. Only people or entities will get information under the protection of confidentiality. The encrypted message should be protected so only the allowed recipients can decipher its contents.

2) Integrity

Integrity is associated with the credibility of information resources. It is used to ensure that the information is accurate for the need at hand. The information must be accurate and authentic to ensure that the information is not modified or corrupted throughout the transaction or transmission period. External parties have not altered or corrupted the information and devices. In most cases, valid user credentials are recognized.

3) Availability

In electronic payments, the service must be available which meets both the security needs of those involved in the purchase and the convenience of customers. It requires accessibility that allows the purchase to be completed at any time the user wishes. Availability defines access to information sources to ensure that a transaction that has been initiated can be completed in a timely and complete manner.

4) Authentication

Authentication is the process of authenticating and identifying a procedure or perhaps a device, which is usually required before releasing the utilization of materials on a product. The main issue of a mobile payment system is authentication, which identifies the customer and verifies that the person is who they claim to be. A variety of authentication techniques have been developed to ensure the protection of electronic purchases. The authentication procedure allows individuals to enter their credentials, and if they match the existing ones, then the individual is a verified user and can log into the system. Authentication methods such as individual IDs and passwords that identify people can assist in achieving the goal of confidentiality.

5) Non-repudiation

Non-repudiation is a property that assures the user is connecting to the legitimate server, ensuring that none of the communication parties may subsequently fraudulently deny that the transaction was performed. In terms of electronic security of monetary transactions, the application of non-repudiation requires a solution that proves the stability and origin of information and a verification tool that can be classified as genuine with a high guarantee. The system maintains records of purchases and is often updated by banks. It records a variety of information, including the type, time, and date of transactions in which consumers were involved. These records enable the verification of numerous completed transactions and provide the necessary evidence for any concerns that may arise.

B. Mitigation of Risks in Mobile Payment Systems

Mitigation refers to reducing the risk or the impact of a threat. Focusing on the mobile payment system and having a very secure system will prevent all the listed threats from happening. System security is about protecting information and property from theft, corruption, and other damage while ensuring that the information and property remain accessible and usable. It covers the conception and implementation of security measures. The basics of system security that are required in any mobile payment system include encryption and authentication.

1) Encryption

Encryption must be used when transmitting data over the Internet that others can view to avoid data leakage. Encryption involves scrambling for information so that it cannot be read in cleartext by normal means. Most mobile payment applications ask for the user's personal data, such as credit or debit card data, identification card information, and more. Therefore, encryption is required to protect this data, and the encryption changes the data to make it difficult to read and time-consuming to decrypt the result of encryption without any specific techniques. Public Key Infrastructure (PKI), combined with symmetric encryption, is one of the most widely used encryption methods. PKI is important for mobile payment applications because it provides a reliable foundation for protecting electronic transactions within financial applications. It also functions as an encryption and authentication technique, creating a win-win situation for the creation of secure applications for financial technology (FinTech). PKI encryption systems are comprised of a key pair containing a private key and a public key. In other words, the sender encrypts the data using a public key, and only the receiver may decrypt the data using a private key. The purpose is to provide secure electronic information transmission better for various network activities, particularly those that need validation of the identity of the persons involved in communication validation of the data being transmitted.

2) Authentication

To utilize all mobile payment services, users should first create an account. Users must validate and confirm their

identity as part of the sign-up procedure. This allows the merchant to verify the authenticity of users, reducing the chance of fraud or identity theft. A digital signature (DS) is used to verify the origin of the identity received and prove whether the identity received is unchanged, which assists in reducing the chance of fraud and enables secure online transactions. Each digitally signed digital document is validated by a verified digital identity. DS is a string value calculated from text values to a hash value. When someone accesses a DS, a unique hash value of a message or document is displayed. The hash concatenation is always unique and cannot be reversed. In addition, the hash that emerges from the digitally signed file is encrypted using cryptographic methods. PKI is commonly used to certify the availability of DS. It offers a complete package of security guarantees and follows different PKI standards for different areas.

C. Security Mechanisms in Mobile Payment Systems in Malaysia

This study furthers the security mechanisms in mobile payment systems. Table 2 shows the security mechanisms in mobile payment applications.

TABLE II SECURITY MECHANISMS

Feature	Boost	GrabPay	Touch 'n Go	MAE	ShopeePay
Login	Alpha-numeric pass-word	6-digit SMS code AND 6-digit PIN	6-digit PIN OR Face verification	Alpha-numeric password OR biometric verifica-tion	Alpha-numeric passwor d
Pay (Self-scan)	Fingerprint verificati on OR 6-digit PIN	Fingerprint verificati on OR 6- 6-digit PIN	6-digit PIN OR Face ID verificati on	No need any authentic-cation phase	Fingerprint verificati on OR 6-digit PIN
Pay (merchan t- scan)	Fingerprint verificati on OR 6-digit PIN	Fingerprint verificati on OR 6- digit PIN	6-digit PIN OR Face ID verificati on	No need for any authentic-cation phase	Fingerprint verificati on OR 6-digit PIN

D. Security Settings and Privacy Policy in Mobile Payment Systems in Malaysia

This study continues by analyzing security configuration settings and privacy policies offered by mobile payment systems in Malaysia. This aims to gain more insights into how every mobile payment system secures the application and user's personal information.

TABLE III SECURITY SETTINGS AND PRIVACY POLICY

Wallet	Security	Privacy
Boost	• Allows users to enable fingerprint payment. • Allow the user to reset the 6-digit PIN and password.	• Collects data when users provide. • Personal data will be disclosed to the Axiata corporate group of companies, third-party service providers, affiliated companies, and professional advisors.
GrabPay	• Allows users to update their PIN. • Provides password recovery methods by using email, Facebook, and Google authentication. • Provides fingerprint authentication setting.	• Collects and combines personal data when users provide it to them. • The personal data will be used to provide services and features for safety and security, legal purposes, and marketing and promotions. • Personal data will be disclosed to the subsidiary companies, G r a b ' s • service providers, and governmental authorities.
Touch 'n Go	• Provides payment order. • Allows the user to change a 6-digit PIN. • Allows users to reset the security question. • Allows users to change mobile numbers. • Allows users to choose if they want to use the face verification method.	• Personal data requested by Touch 'n Go are mandatory, which the users must provide and agree to in order to proceed with the provided services. • Personal data provided may be held in a database and may be used to provide the users with Touch 'n Go services, enable communication for administrative purposes and send advertising. • Personal data will be disclosed to the affiliated companies with Touch 'n Go, government agencies, and Touch 'n Go's contractors.
MAE	• Allows users to choose if they want to use a biometric login. • Allows users to change PIN.	• Collects personal data that users voluntarily provide. • Personal data will be used to provide the requested services for promotions and marketing purposes.

Wallet	Security	Privacy
ShoppeePay	• Allow users to change their PIN. • Allows users to activate biometric authentication.	*(Cannot check for the privacy policy because it states that the document is not available)*

E. Methods to Improve Security

1) Using a stronger password for login and payment authentication

GrabPay and Touch ‘n Go rely on a 6-digit PIN to secure the mobile payment login. However, GrabPay also requires the user to log in via an OTP to verify the user before entering the 6-digit PIN. Meanwhile, Boost, MAE, and ShopeePay use an alphanumeric password to log into the mobile payment. GrabPay and Touch ‘n Go EWallet use the same 6-digit number PIN for both logging in and authorizing payments. Boost and ShopeePay ask for verification by fingerprint or the 6-digit number PIN, while there is no payment authentication for MAE. Using the same 6-digit PIN for both enrollment and payment authorization could pose a potential risk if someone observes the user entering the 6-digit PIN while making a payment at the counter. A mobile payment system could use a different password for payment authorization. This could be an alphanumeric password that is more complicated. If the 6-digit number PIN is compromised, it will be more difficult for another person to access the account as a more complicated password will be required to process the transactions.

2) Biometric unlock for payment systems

Boost, GrabPay, and ShopeePay currently support fingerprint verification, while Touch ‘n Go supports face verification ID for payment. However, MAE does not require the user to enter the 6-digit number PIN, password, fingerprint, or face ID verification to proceed with the transaction. It is quite difficult to protect the 6-digit number PIN or password from prying eyes when the user must enter the code while paying in public. To make it more convenient and secure, all mobile payment systems should allow biometric verification such as fingerprint, face ID, and iris verification. This will reduce the disclosure of PIN and the user's password and make payment easier.

V. CONCLUSION

This study compares Malaysia's existing mobile payment applications, focusing on their security and privacy properties. The security and privacy issues in mobile payment applications are presented in threats, vulnerabilities, and risks assessment. Furthermore, this paper also discussed the security mechanisms implemented in each of the chosen mobile payment systems. Additionally, this paper suggested a few techniques to improve the security of mobile payment systems. The main objective of this paper is to assure users about the security of mobile payment systems, thereby ensuring users feel safe and confident to continue using them. Future works will include expanding the scope of research by going through all the layers in the OSI model and comparing mobile payment applications between Malaysia and other countries.

REFERENCES

[1] M. A. Hassan, Z. Shukur, M. K. Hasan and A. S. Al-Khaleefa, " A review on electronic payments security," Symmetry, vol. 12, no. 8, p. 1344, 2020.

[2] K. Subaramaniam, R. Kolandaisamy, A. B. Jalil and I. Kolandaisamy, "The impact of E-Wallets for current generation," Journal of Adv. Research in Dynamical & Control Systems, vol. 12, no. 1, pp. 751-759, 2020.

[3] P. Aigbe and J. Akpojaro, "Analysis of security issues in electronic payment systems," International journal of computer applications, vol. 108, no. 10, pp. 10-14, 2014.

[4] M. A. Hassan and Z. Shukur, "A secure multi factor user authentication framework for electronic payment system," in 2021 3rd International Cyber Resilience Conference (CRC), 2021.

[5] J. M. Stewart, "The Three Types of Multifactor Authentication," Global Knowledge, 26th June 2018. [Online]. Available: https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/#gref.

[6] European Union Agency for Network and Information Security, "Security of mobile payments and digital wallets," 19th December 016. [Online]. Available: https://www.enisa.europa.eu/publications/mobile-payments-security.

[7] M. P. Bosamia, "Mobile wallet payments recent potential threats and vulnerabilities with its possible security measures," in 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp-20, 2017 .

[8] R. S. Rajput and P. Singh, "Cybersecurity Analysis in the context of Digital Wallets," June 2019. [Online]. Available: https://www.researchgate.net/publication/333555238_Cybersecurity_Analysis_in_the_context_of_Digital_Wallets.

[9] Z. Bezovski, "The future of the mobile payment as electronic payment system," European Journal of Business and Management, vol. 8, no. 8, pp. 127-132, 2016.

[10] F. Gazi, "What is an e-wallet and how is it different from a credit card," iMoney, 2020. [Online].

[11] N. A. Renfroe and J. L. Smith, "Th reat/Vulnerability Assessments and Risk Analysis," WBDG Whole Building Design Guide, 2016. [Online].

[12] L. O'Donnell, "‘Fake Fingerprints’ Bypass Scanners with 3D Printing," treatpost, 8th April 2020. [Online]. Available: https://threatpost.com/fake-fingerprints-bypass-scanners-3d-printing/154535/.

[13] "Security requirements for safe e-payment systems," indiafreenotes, 12th June 2020. [Online]. Available: https://indiafreenotes.com/security-requirements-for-safe-e-payment-systems/.