USE OF E-WALLET AND SECURITY OF DIGITAL TRANSACTIONS

AZRUL ENUAR BIN SAMSUDIN[1], MOHD KHAIRUDIN BIN KASIRAN[2]

[12]School of Computing, UUM-College of Arts and Sciences, Universiti Utara Malaysia, Sintok Kedah.

**Corresponding author: azrulenuar@gmail.com*

ABSTRACT: The expansion and capability of electronic transactions within the country's financial and economic system are influenced by the emergence of online financial services and the consumers' adoption of cashless transactions. It's evident that consumers are shifting to digital payment methods with the emergence of a number of digital payment technologies that use devices bearing the e-wallet brand. E-wallets are of great interest due to their ability to facilitate mobile electronic transactions. The information that is digitally recorded includes the user's biometric data and banking information, such as debit or credit cards, as well as a simulation of the user's pocketbook (Singh, G. 2019). Prior to beginning the payment process, users usually need to scan the Quick Response or QR code that has been issued by the merchant or service provider (Widayat et al., 2023). Prior to finalizing a transaction, it is necessary for the user to scan a Quick Response (QR) code and key a security personal identification number (PIN).There are now several e-wallet application vendors to choose from. The advantage that can be derived from this healthy competition is the opportunity to investigate capabilities based on the selection of a variety of applications that offer inevitably distinct facilities. Nonetheless, the selection priority is determined by the user's ability to obtain the finest criteria. Among them are the ease of use, the level of brand recognition, and the offered benefits and features. User preferences must include the most important factor, which is the level of control and security when using the application. The purpose of this summary is to examine the involved security features and how they are implemented. The study encompassed four electronic wallet service providers, specifically Touch 'n Go, Boost, GrabPay, and MAE.

KEY WORDS: *Smartphone, e-wallet, verification*

1. INTRODUCTION

The government has introduced a one-off digital stimulus through the presentation of Budget 2020 with the initiative of crediting RM30 into the e-wallets of all Malaysians aged 18 and above who have an annual income of less than RM100,000 (Mahomed, 2021). In the same year, an allocation amounting to RM750 under Pelan Pemulihan Ekonomi Jangka Pendek (PENJANA), the government also credited RM50 to users' e-wallet accounts (Mahomed, 2021). This government move indirectly benefits the increase in the number of users and merchants who use e-wallets. In the 2023 Budget, the government continues to support efforts towards the digital economy era with a combination of initiatives involving several national development components such as RMK-12, the Malaysia Digital Economy

Action Plan (MyDIGITAL), the 4IR National Policy and the implementation of 5G through Digital Nasional Berhad (DNB).

The e-wallet is a mobile-based digital payment application that enables cashless transactions and facilitates the process of conducting financial transactions (Shamsuddin et al., 2022). The e-wallet application is one of the electronic payment mobility facilities that is implemented under the user's control without involving the physical use of cash (Hatamleh et al., 2023). E-wallet apps are the preferred option for customers nowadays due to their easy and systematic money management and transaction processes. The e-wallet generally contains financial information such as user identifying details and banking information, and it is enhanced with access control to ensure the security of user transactions. This financial mobility innovation decreases reliance on the usage of computers for transactions and payments. Users can also lower their fees by dealing at the counter or using cash withdrawal machines at the bank. One advantage of utilizing an e-wallet is the preservation of the user's time, as it eliminates the need for physical transactions and the associated waiting period.

The use of digital wallets enables the transfer and receiving of funds, in addition to facilitating the acquisition of products and services. Without the availability of a desktop computer or laptop, this transaction can solely be completed via smartphone. The e-wallet application enhances the practicality of banking transactions by providing users with immediateaneous responses. The beneficiary of an e-wallet application installed on a smartphone can also benefit in the absence of a conventional bank account. Through the implemented e-wallet, funds can be transferred to the recipient using phone number reference, business registration, QR sharing, or other suitable forms of identification. As is customary, the bank will assess additional fees for banking activities such as fund transfer transactions conducted through user accounts (Ying et al., 2020). When performing fund transfer transactions via the e-wallet application, the user account is exempt from any additional charges.

E-wallets enable the transmission and receipt of funds in addition to simplifying the purchase of goods or services. Banking transactions using this e-wallet are regarded as more practical because consumers receive real-time responses. Installing an e-wallet application on a smartphone also allows the recipient who does not have a regular bank account to profit. Transfers to recipients can be made based on phone number reference, business registration, QR sharing, and other acceptable identification using the installed e-wallet. Banking activities such as fund transfer transactions through user accounts will, as usual, incur additional bank costs (Ying et al., 2020).

The use of electronic wallets also offers users the opportunity to adapt supplementary activities to diverse digital requirements. This covers additional demands that enhance social activities by utilizing e-wallets, such as entertainment, travel, reward collecting, and other services (Sabli et al., 2021). Users strategically manage and harmonize their social engagements using the advantages of e-wallet applications, since these platforms provide organized and methodical coordination of activities and leisure pursuits. The meal-ordering service garnered significant attention, particularly during the COVID-19 pandemic, coinciding with the increasing adoption of e-wallets (Ojo et al., 2022). A climate conducive to the e-economy is

now in place. The mentality of industry players, particularly in pushing the use of digital technology in daily operations, continues to increase. Because there is an infinite amount of space and opportunity for transactions, using electronic platforms has become popular.

One of the reasons for the rise in e-wallet usage as a substitute form of payment for products and services is this peak. Additionally, a variety of facilities that can be implemented through the e-wallet application are included in the transmission of influence using the application (Ojo et al., 2022). These facilities include transportation, tourism, and recreation.

A multitude of electronic wallet applications are available in the current market. The market's selection of e-wallet applications indicates how seriously the service business takes encouraging the usage of digital payments. This potential serves as one of the driving forces for society's digitization through a variety of cashless payment methods.

2. ENCOURAGE THE USE OF E-WALLET

The collaboration between the government, facilitated by the Government Linked Company (GLC), and the commercial sector is crucial in fostering opportunities aimed at realizing the objective of digitalizing society. To enhance the proficiency in the advancement of the nation's digital economy ecosystem, the agreement to clarify the responsibilities of each organization is established as a standard. The parties involved in this development of the nation's financial digital sector are network service providers, banking institutions, companies that build applications for e-wallets, and stakeholders.

The Financial Sector Blueprint 2022-2026 is an initiative of the Bank Negara Malaysia (BNM) aimed at bringing together stakeholders to encourage the growth of the digital economy. A necessary strategy for preserving the financial sector's stability in an uncertain economic environment. Disclosure of the financial system's use of technology necessitates direction to streamline market-based governance and community capacities. Strategic Core 3 of the Financial Sector Blueprint 2022-2026 - Advance the digitization of the financial sector, which is the focus of the government, particularly BNM, in order to integrate the pace of technology based on the financial ecosystem.

In order to effectively navigate the increasingly intricate issues and hazards associated with financial systems, users, and markets, it is imperative to engage in thorough preparation (Financial Sector Blueprint, 2022-2026, p. 68). The Financial Sector Blueprint 2022-2026 places significant importance on data security in digital transactions. It highlights the need to ensure the protection of user data and emphasizes the implementation of controls, such as the review of fundamental requirements, to safeguard user interests. The blueprint also suggests that the government should provide guarantees in this regard (Financial Sector Blueprint, 2022-2026, p. 69).

Figure 1 depicts a series of stages aimed at establishing the user's identity by means of an integrated identity verification mechanism, hence prioritizing the user's interests. The use of this measure can effectively mitigate the incidence of identity manipulation, a phenomenon that is increasingly likely due to the rapid advancement of technology. The government's proactive measure demonstrates a

commitment to positioning digital technology as the primary catalyst for economic growth, while also recognising the significance of consumers and the advancement of the digital financial industry.

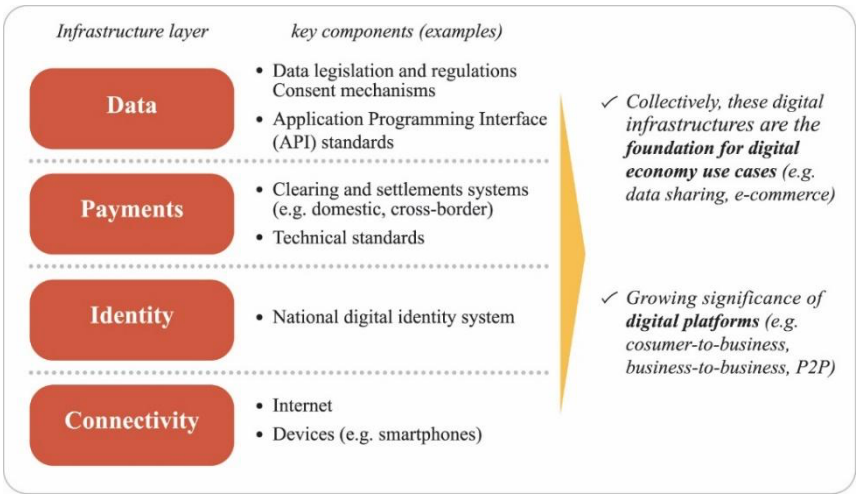

Fig.1. The main infrastructure layers in the digital economy

(Source: Financial Sector Blueprint 2022-2026)

As stated by Merchantrade Asia's Managing Director and Founder, the process of enhancing the digital ecosystem environment is a comprehensive endeavor that does not exclude the less fortunate, including B40 and people with disabilities (Malaysia Fintech Report 2022, p. 3). By involving the B40 and OKU groups, who also gain from and preserve their competitiveness in the age of the digital economy, this emphasis serves to further fuel the financial market's openness. The foreword of the Malaysian Fintech Report 2022, on page 4, expressed the hope that digital transformation would be integrated with efforts to streamline processes and enhance the customer experience, rather than being viewed as a standalone catalyst for the growth of the digital economy by Sean Hesh, Group Chief Executive Officer, GHL.

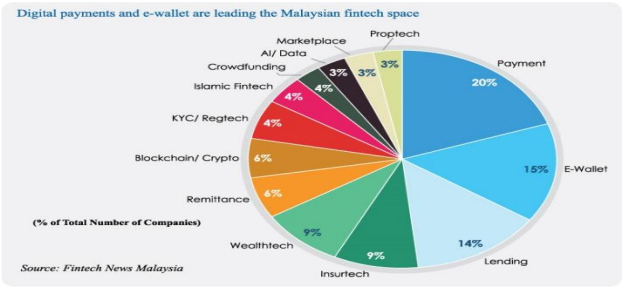

Fig.2. (Source: Malaysia Fintech Report 2021)

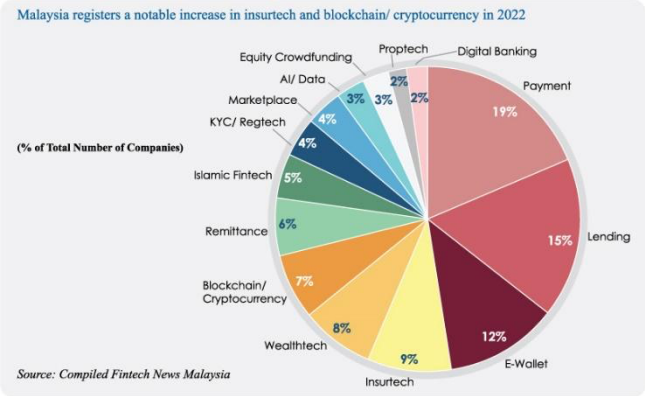

Fig.3. (Source: Malaysia Fintech Report 2022)

The percentage of Malaysians using fintech (financial technology) applications is seen in Figure 2. The analysis pertains to the proportionality of the sequence within the time frame encompassing the years 2021 and 2022. According to the Malaysian Fintech Report 2022 (p. 7), the utilization of e-wallets has attained a notable degree of acceptance, standing at 12%, which represents the third highest percentage. The proportion shown in Figure 1, which depicts e-wallet usage in 2021, serves as a benchmark for the acceptance of e-wallet users. The increasing reliance of individuals on smartphone-based digital payment applications has resulted in the prominent adoption of this technique as the primary preference. According to the study conducted by Amin et al. (2022), A number of variables contributed to the 2022 decline in the percentage of applications used. One notable inclusion is the presence of digital banking applications. According to fintech news sources, the emergence of digital banks represents a technologically advanced approach to banking that provides cost-effective, efficient, and secure services. According to Fintech news sources, digital banks are a sophisticated technology that delivers banking at a cheap cost, quickly, securely, and as an option because it surpasses the services offered by traditional banks (Rebecca Oi. 2023 Feb 21).

The initiative by BNM to establish a digital bank involves licensing five different consortiums: Boost Holdings Sdn Bhd and RHB Bank Bhd, YTL Digital Capital Sdn Bhd and Sea Ltd, GXS consortium Bank Pte Ltd and Kuok Brothers Sdn Bhd, AF Investment Bank Sdn Bhd and MoneyLion Inc, AEON Financial Service Co Ltd and AEON Credit Service (M) Bhd. This particular combination was chosen due to its ability to meet the needs of relationships with current users, infrastructure competence primarily in the digital economy, and—above all—financial governance experience. Based on the expertise and capacities of the five consortiums that were chosen, Digital Bank can further broaden the range of services it provides through the network of digital financial services (Dr. Chow Yee Peng, 2022, Oct 24).

In order to further promote the adoption of e-wallet applications, the central bank, BNM, intends to enhance the utilization of digital payment technology by initiating an e-money campaign. As to the official statement issued by Bank Negara, the aforementioned campaign serves as the foundation for the objective of augmenting the number of e-payment transactions per capita from 221 to 400 within the corporate community and households by the year 2026 (Bank Negara Malaysia,

2022). The endeavors to incorporate digital payment systems are not solely targeted at individual consumers.

The presence of finance facilities is necessary due to the existence of low-income micro-entrepreneurs. Hence, the imperative for a financing effort that prioritizes social considerations and has the potential to enhance social resilience is paramount. Based on it, BNM translated the creation of a social finance program that assisted in enhancing corporate capabilities and was supported by eight national financial institutions. According to Bank Negara Malaysia (2023), there are a total of eight financial institutions available as options for individuals seeking a more flexible financing alternative compared to the conventional approach. These institutions include AmBank Islamic, Bank Islam, Bank Muamalat, CIMB Islamic Bank, Public Islamic Bank, RHB Islamic Bank, Bank Simpanan Nasional, Bank Rakyat, Agrobank, and SME Bank. ITekad has implemented initiatives aimed at mitigating the digital divide by enhancing its online sales capabilities. Based on the statement provided by BNM, it can be inferred that a significant majority, specifically 95%, of micro-entrepreneurs affiliated with iTekad have effectively demonstrated the ability of the digital business landscape to enhance their sales capabilities.

The significance of utilizing personal information as a valuable resource for purposes beyond user identity verification. The Government, particularly through the Ministry of Finance, has placed significant emphasis on the importance of coordinating security measures in the advancement of digital financial technology. This is evident in the launch of the Financial Sector Blueprint (FSB) 2022 - 2026 by Bank Negara Malaysia (BNM). The objective of this initiative is to enhance the capabilities and efficiency of all stakeholders involved in the digital economy ecosystem, thereby serving as a catalyst for navigating the progressively complex financial landscape.

The government is placing a strong focus on its obligation to implement the best access control and resolve any vulnerabilities in the application of technology to digital banking. The implementation of FSB 2022-2026 presents an opportunity to enhance the efficacy of competitive application development through the alignment of recommendations. Users of e-wallets are guaranteed access control features that are thought to be able to safeguard the security of their financial and personal data (Hossain et al., 2022). This is demonstrated by the way that many layers of authentication are combined with passwords, biometric authentication, and other forms of interwoven access control (Sabli et al., 2021).

3. THREATS IN THE USE OF E-WALLET

There are a number of hazards to online financial transaction services including online banking and e-commerce (Busse, N. 2023). Users get disinterested in instances of intrusion such as online fraud, hacked user accounts, and other incidents affecting the digital economy. The operating system, which serves as the installation base for e-wallet applications, is a source of potential dangers. Threats to the e-wallet application installation platform include the following:

- Attacks involving the alteration of instructions are designed to undermine the operating system's ability to execute the original code instructions as intended (Vučinić, M., & Luburić, R. (2022). The presence of a potential information incursion

and unauthorized access creates a vulnerability that can be exploited in the operations of e-wallet applications.

• Continuous innovation and functional function enhancement are part of application development. The Software Development Life Cycle, or SDLC, depends heavily on the coding stage (Humayun et al., 2022). The pursuit of a functional application amidst competition may entail a potential compromise to the stability of the resulting code. Applications for e-wallets that involve security of usage in particular will be impacted in terms of operational stability.

• Vulnerabilities in the e-wallet software itself may also provide an opening for penetration. The occurrence of direct threats in e-wallets, namely those related to access control security disruptions, pertains to the compromise of fingerprint or facial data of users. Biometric data is also susceptible to attacks using contemporary methods due to the digital environment, which puts one of the access control cores at risk (Adler et al., 2008). Failure to verify the authenticity of the biometric system can have the dual consequence of preventing users from using it and creating uncertainty over the identification of the true owner (Jain et al., 2012). Adversaries have the potential to exploit instances of system functionality failures, which may lead to detrimental consequences for users of the program.

• The device used for installing applications is susceptible to being exploited as a means for compromising application security. In conjunction with technological advancements, there exists the potential for data theft through the utilization of air-gap attack techniques, as discussed by Park et al. (2023). By altering activities through intermediaries inside user device components, attackers take advantage of remote access technologies to target devices. In the realm of smartphone connectivity, an ideal strategy entails the utilization of many transmission modalities, including radio frequency, wireless communication, infrared technology, and Bluetooth connectivity.

Numerous strategies and endeavors have been undertaken to promote the widespread adoption of digital technology in everyday life, with particular emphasis on the utilization of e-wallets as a means of payment. However, there are certain communities that have yet to adopt methods aimed at identifying potential hazards that may pose risks to their economic endeavors. Despite the enhanced security measures implemented by e-wallet program providers, the potential for financial loss remains a concern. Sinar Harian (Roshila Murni Rosli, March 15, 2020) reported an instance of fraudulent activity involving the utilization of electronic wallets. The projected financial loss amounts to approximately RM600,000. The aforementioned figure is of considerable magnitude, encompassing a total of 50 individuals utilizing e-wallet services who have willingly surrendered their identity cards to the syndicate. The operational strategy employed by the syndicate involves enticing individuals with the offer of RM300 credit upon registration through their platform. The syndicate successfully persuaded consumers to grant permission for the utilization of their mobile phones in the distribution of Transaction Authorization Code (TAC) numbers.

The presence of manipulation in digital economic activities is a persistent phenomenon. However, it is crucial to recognize the significance of identifying potential risks and implementing suitable control measures in order to ensure the secure utilization of digital economic technologie.

4. METHODOLOGY

The level of security provided by an e-wallet application is extremely reliant on the capacity for motivation and the influence of supply on development. According to Hatamleh et al. (2023), the role highlighted by the e-wallet brand in the market influences the rise in consumer acceptance based on the features provided. Without positioning the brand as a means of attracting the interest of consumers alone, the benefits of use must go beyond the desires of consumers and consider the advantages that merchants can obtain.

User confidence in e-wallets can be tied to the degree to which the applied access control is truly effective and can protect user interests. Consumer acceptance is influenced by the utility of a product's defense capability, according to culture. The perception of security (Chong et al., 2023), one of the factors influencing user attitudes towards the use of e-wallet applications, is one of the factors influencing user attitudes positively.

The purpose of this study is to determine the access control principles used by e-wallet applications. Generally, standard procedures must be completed before an application is available for use. To initiate the installation of an application, the user must have their personal information available as a reference. Banking information is a component of e-wallet applications because it is the primary source for making digital payments on mobile devices.

The selection of electronic wallet applications consists four popular brands, namely Touch 'n Go, Boost, GrabPay, and MAE. In order to avoid any possibility of misinterpretation and preserve a level of sensitivity among application providers, each of the brands is referred to as Brand A, Brand B, Brand C, and Brand D. Furthermore, the brand arrangement is not translated in the ordered sequence.

4.1. Installation of e-wallet application

Prior to the completion of installation and configuration, the initial phase entails the use of user-related data and information. Users must ensure that the application provider complies with applicable laws during their proprietorship of user data. This is necessary because every commercial transaction involving users must adhere to the Personal Data Protection Act 2010 (Act 709) and its enforcement and compliance.

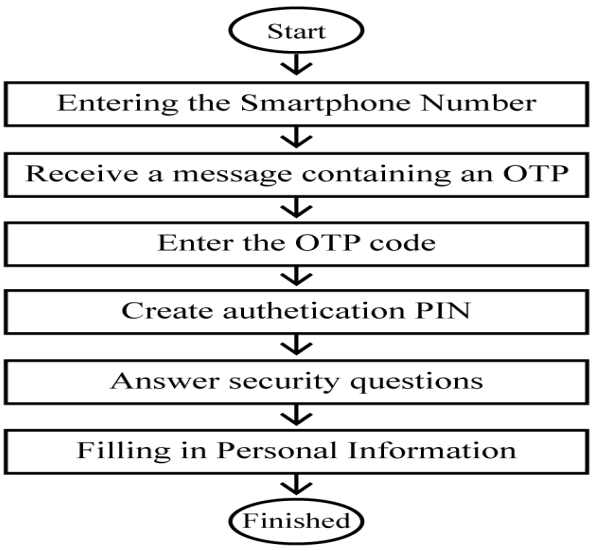

Fig.4.Installation Flow

The Android operating system is used to install applications. In general, the installation process follows the pattern depicted in figure 4. Nevertheless, according to the security requirements of each brand, there are variations in the implementation methods or security components that must be added. Before using the application, the user must register. Initial registration of the application is required.

Application installation permission needs to be approved by the actual owner of the device. The main purpose is to ensure the interests of users and obtain full usage rights as e-wallet account owners. There is a field where the user fills in personal information. The information that will be stored will be a reference to facilitate the use of the application and will be linked to the user's e-wallet account database.

The smartphone number becomes the medium of communication for the process of sending the security code. Therefore, users need to ensure that the smartphone number used is a valid and accessible number during the registration process. This e-wallet application will be linked to the smartphone number where the installation of the application is done.

The application server will send a response for one-time password (OTP) verification. The receipt of the OTP code is proof of successful verification of the smartphone number. The user needs to enter the received OTP code into the space provided on the registration interface. Next is the provision of a security pin to ensure access control to the application, which is the generation of a Personal Identification Number (PIN). The process of creating a 6-digit PIN is required to perform account access and authentication activities when using the e-wallet application later. The user's smartphone will display an interface for entering the created PIN. There are several access control methods to ensure the security of e-wallet accounts, including the use of Multi-Factor authentication involving biometrics.

Once the pin verification is successful, the user will be given a question and must fill in the answer field. The authentication method using questions is a security alternative to recovery support for applications (Eliasi et al., 2019). Recovery refers

to the process of repairing a broken application or reinstalling an application on an existing device and installing a new application using the same e-wallet account.

4.2. Verification Process

Completing the authentication process is the last step in getting the system configured to start any transaction via the e-wallet. To initiate the verification procedure, the user must present an identity document, such as a passport or identity card. To finish the account verification process, additional security elements are required in addition to the use of identity documents. This is contingent upon the extra verification specifications established. This is a result of the fact that every brand controls user account security using a distinct strategy and degree of development. Table 1 displays the process for verifying e-wallet accounts for brands A, B, C, and D.

Table 1:Authentication requirements

Verification method	Brand A	Brand B	Brand C	Brand D
Generate a 6-digit PIN.	*	*	*	*
Scan and upload identification documents.	*		*	*
Biometric identification;				
▪ Selfie face	*		*	
▪ Selfie video	*			
▪ Voice	*			

Brand A employs an authentication approach, beginning with the upload of a picture of the user's identity identification, such as an ID card or passport. Users must use their smartphone's camera to scan the front and back of their ID card or the information in their passport book. The next step is biometric authentication, which incorporates identification by facial selfie recording, video selfie recording, voice recording, and user-side recording. During the recognition process, the user must perform the following tasks with the smartphone's camera:

- Capture a facial self-portrait to authenticate the legitimate user.
- Initiate the activation of the microphone function on the smartphone device, so enabling the continuation of the ongoing process of speech recording. The procedure necessitates the user to capture a segment of their facial features and audibly articulate the numerical value exhibited on the screen of their mobile device.
- After turning on the video mode, capture a video selfie by slowly sliding up to the user's side from the front of their face. The video begins with the user's face and then pans gently to reveal their side.

In brand A applications, biometric identification is a component of the enhanced security authentication process.

As part of the registration procedure, Brand B generates PINs as a means of authentication. It is ensured that the verification process can be completed by employing a 6-digit PIN (Ying et al., 2020). To finish the verification procedure, the user must input a six-digit PIN into the field on the smartphone's application display.

Brand C employs a method of authentication that involves uploading a scan of the user's identity card or passport, both front and back. The owner of the e-wallet account's smartphone camera must be used for scanning. The user must snap a selfie for biometric identification once the upload procedure has been successful. Once the self-portrait satisfies the application prerequisites and is prepared for usage, the verification procedure concludes.

Brand D employs the same way of uploading a scanned image of the user's identification document for the purpose of authenticating the e-wallet account. To access brand D's e-wallet account, however, this brand requires a 6-digit PIN that must be generated to access its e-wallet account.

Each e-wallet brand relies primarily on personal and biometric data for its authentication approach. The uploaded identity is designed to fulfill the application's security requirements. This control strategy seeks to prevent irresponsible parties from misusing their identities. The cross-checking process can guarantee the safety of using mobile applications that are open to cyber attacks.

5. ACCESS CONTROL

Prior to utilizing the electronic wallet, it is imperative for the account holder to comply with access control measures. The primary objective of enabling access control in the e-wallet application is to regulate and enhance the security measures pertaining to transactions. Table 2 displays the access controls used by each e-wallet application. In addition to enhancing brands' marketing capabilities, more access control techniques can lower the likelihood of account abuse.

Table 2: E-wallet access control

Type of Access Control	Brand A	Brand B	Brand C	Brand D
Add e-wallet funds;				
▪ Authentication based on a PIN	*	*	*	*
▪ Device-based authentication				
▪ Biometric verification	*	*	*	
Payment;				
▪ Authentication based on a PIN	*	*	*	*
▪ Device-based authentication			*	*
▪ Biometric verification	*	*	*	

Users make purchases through brand A using the e-wallet application by scanning QR code offered at the business premises. After completing the purchase selection process, a PIN is entered to confirm the transaction. The PIN comprises a sequence of 6 numerical digits that is inputted by the user during the installation process of the application. The same method is used to add funds to the wallet when a 6-digit confirmation number needs to be entered to complete a transaction.

For brand B, the purchase method is identical; once the goods and services have been selected, the user must input the 6-digit PIN sent to their smartphone to complete the transaction. To expedite the payment procedure when visiting the

location, a QR code scanner is the preferred method. The payment transaction will be successful once the user inputs the 6-digit PIN that was established during the installation of the application.

Brand C employs the same method for payment transactions by scanning a QR code on the user's website or when conducting business on the premises. The final verification step requires the user to input the 6-digit PIN generated during e-wallet account creation. The C-brand provider's advantage is the enhancement of the approval feature that necessitates the assignment of the application to a registered device. Using this method, only an activated device can access the application for authentication purposes. However, only certain payment amounts are subject to this form of verification.

Brand D, on the other hand, employs the OTP code verification method that is sent to mobile phones (Muhtasim et al., 2022). This control provides a secure area for identifying users of devices that only allow for transactions. Before proceeding with payment, the user must verify the account configuration image icon. This identifying procedure is a method of security control employed in situations such as online banking

According to Bosamia et al. (2019), the e-wallet application provider offers access control measures that allow for the utilization of multiple factors, including a multi-factor authentication layer. The utilization of passwords and biometric factors as means of authentication, when combined, serves as an access control mechanism for conducting transactions. The utilization of biometric authentication technology is closely aligned with the demands of the digital realm as it relies on the process of confirming the physical characteristics of the user's face (Ibsen et al., 2022). Furthermore, audio has been used as a security component for authentication (Markowitz, J. A. 2000). The utilization of the owner's voice recording as a means to regulate unwanted access enhances the complexity of infiltration on the electronic wallet application. Particularly when it comes to the advancement of access control, this innovation adds value and fosters healthy competition.

As the legal owner of an e-wallet account, users must be aware of the evolving requirements for fundamental security. Users are responsible for maintaining the security of their e-wallet account against external intrusions. Users should select difficult-to-guess passwords to place pressure on intruders. Users should always adhere to password standards that comply with security requirements. Sensitivity to the ability of hacking techniques, such as brute-force attacks, rainbow table attacks, dictionary attacks, and others, to obtain passwords, particularly those that do not meet the minimum security requirements (Hassan et al., 2021).

6. CONCLUSION

The integration of e-wallets as an electronic payment method is considered a viable substitute for promoting a cashless society. The expansion of business interactions involving the digital economy has entered a new chapter thanks to electronic transactions conducted through smartphones. The transition of society to a more technologically relevant phase is primarily driven by the government and the private sector's proactive support through the production space of electronic integrated applications in commercial concerns. The utilization of e-wallets has gradually transformed the landscape of financial transactions, leading to a shift from

traditional payment methods such as credit/debit cards and Internet banking services. More e-wallet companies are now on the market, and they offer the same level of ease as banking institutions while being completely operational.

The strength of the provided security system is a crucial format for digital payments or financial activities. Security concerns are crucial in e-wallet apps, from the very beginning to the end of the installation procedure. This is due to the fact that, in addition to the appealing features provided, there is a great deal of responsibility associated with protecting user data. If access control features are not given priority during the creation of e-wallet applications, for instance, it would directly affect user confidence.

Users are equally responsible for maintaining the security of the data stored in the e-wallet application as application providers are for creating platforms that permit financial transactions. The specifics of the procedure and the degree of access security offered use a variety of techniques. Users must make sure that device information, personal data, and banking are integrated, much like with the Internet banking system. A more adaptable installation platform that does not restrict the place of use is the main distinction, but the cross-checking technique is still used. It was previously mentioned that some users enable third parties to register their e-wallet applications, which makes them easily manipulable into divulging personal information. This mistake offers a way for information related to e-wallet accounts to be misused. As a result, users ought to feel accountable for not disclosing information carelessly.

REFERENCES

Singh, G. (2019). A review of factors affecting digital payments and adoption behaviour for mobile e-wallets. International Journal of Research in Management & Business Studies, 6(4), 89-96.

Widayat, W., Marsudi, M., & Masudin, I. (2023). QR-code-based payment. Does the consumer intend to adopt a retail buying transaction?. Banks and Bank Systems, 18(3), 1-13.

Mahomed, P. M. D. A. S. B. (2021, April 24). Insentif khas kerajaan rangsang perkembangan ekonomi digital. Berita Harian. https://www.bharian.com.my/rencana/lain-lain/2021/04/810160/insentif-khas-kerajaan-rangsang-perkembangan-ekonomi-digital

Shamsuddin, M. M. J., Sitiris, M., & Yunus, S. M. (2022). E-Wallet in Malaysia: A Proposed Structure of Contracts According to The Juristic Adaptation (Takyif Fiqhi). Malaysian Journal Of Islamic Studies (MJIS), 6(2), 15-37.

Hatamleh, A., Kanaan, A. G., Majdalawi, Y. I., & El-Ebiary, Y. A. B. (2023). The Efficiency and Effectiveness of E-Wallet Systems in E-Commerce Platforms. Journal of Survey in Fisheries Sciences, 10(2S), 2634-2644.

Ying, W. C., & Mohamed, M. I. K. P. (2020). Understanding the factors influences users continuous intention towards e-wallet in Malaysia: Identifying the gap. Research in Management of Technology and Business, 1(1), 312-325.

Sabli, N., Pforditen, N. E., Supian, K., Azmi, F. N., & Solihin, N. A. I. M. (2021). The acceptance of E-Wallet in Malaysia. Selangor Business Review, 1-14.

Ojo, A. O., Fawehinmi, O., Ojo, O. T., Arasanmi, C., & Tan, C. N. L. (2022). Consumer usage intention of electronic wallets during the COVID-19 pandemic in Malaysia. Cogent Business & Management, 9(1), 2056964.

Bank Negara Malaysia (2023). Financial Sector Blueprint 2022 -2026 https://www.bnm.gov.my/documents/20124/5915429/fsb3_en_book.pdf

Fintech New Malaysia (2022). Malaysia Fintech Report. https://fintechnews.my/wp-content/uploads/2022/07/Fintech-Report-Malaysia-2022-Fintech-News-Malaysia-x-Merchantrade-2.pdf

Amin, S. I. M., Ab Hamid, S. N., & Norhisam, N. H. (2022). Faktor Penentu Niat Penggunaan e-Dompet pasca Pandemik COVID-19 di Malaysia: Integrasi Model UTAUT dan MAT. Jurnal Pengurusan, 66, 0_1-13.

Rebecca Oi (2023, Feb 21). Fintech New Malaysia : Digital Banks Could Be the Key to Promoting Financial Inclusion for Malaysia's B40. https://fintechnews.my/34216/financial-inclusion/digital-banks-could-be-the-key-to-promoting-financial-inclusion-for-malaysias-b40/

Dr. Chow Yee Peng (2022, Oct 24). The Star : Digital banks in Malaysia: Prospects and lessons from China. https://www.thestar.com.my/opinion/columnists/search-scholar-series/2022/10/24/digital-banks-in-malaysia-prospects-and-lessons-from-china

Bank Negara Malaysia (2022, October 29) BNM further advancing e-payment adoption and financial inclusion [Press release]. https://www.bnm.gov.my/-/e-duit-itekad-launch

Hossain, M. M., Akter, S., & Adnan, H. M. (2022). Does the trust issue impact the intention to use e-wallet technology among students?. Journal of Entrepreneurship and Business (JEB), 10(1), 57-71.

Busse, N. (2023). The impact of cashless societies on business and society (Bachelor's thesis, University of Twente).

Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. Journal of Central Banking Theory and Practice, 11(2), 27-53.

Humayun, M., Jhanjhi, N., Almufareh, M. F., & Khalil, M. I. (2022). Security threat and vulnerability assessment and measurement in secure software development. Comput. Mater. Contin, 71, 5039-5059.

Adler, A. (2008). Biometric system security. Handbook of biometrics, 381-402.

Jain, A. K., & Nandakumar, K. (2012). Biometric authentication: System security and user privacy. Computer, 45(11), 87-92.

Roshila Murni (2020, Mac 15). Sinar Harian : Perdaya mangsa guna e-wallet https://www.sinarharian.com.my/article/73930/berita/jenayah/perdaya-mangsa-guna-e-wallet.

Hatamleh, A., Kanaan, A. G., Majdalawi, Y. I., & El-Ebiary, Y. A. B. (2023). The Efficiency and Effectiveness of E-Wallet Systems in E-Commerce Platforms. Journal of Survey in Fisheries Sciences, 10(2S), 2634-2644.

Chong, M. H., Chow, W. Y., Chow, X. Q., & Lim, C. C. H. (2023). Consumer satisfaction in E-shopping: shopee Malaysia case. Asia Pacific Journal of Management and Education (APJME), 6(1), 94-107.

Eliasi, B., & Javdan, A. (2019). Comparison of blockchain e-wallet implementations.

Muhtasim, D. A., Tan, S. Y., Hassan, M. A., Pavel, M. I., & Susmit, S. (2022). Customer satisfaction with digital wallet services: an analysis of security factors. Int. J. Adv. Comput. Sci. Appl, 13, 195-206

Bosamia, M., & Patel, D. (2019). Wallet payments recent potential threats and vulnerabilities with its possible security measures. Int. J. Comput. Sci. Eng, 7(1), 810-817.

Ibsen, M., Rathgeb, C., Fischer, D., Drozdowski, P., & Busch, C. (2022). Digital face manipulation in biometric systems. In Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks (pp. 27-43). Cham: Springer International Publishing.

Markowitz, J. A. (2000). Voice biometrics. Communications of the ACM, 43(9), 66-73.

Hassan, M. A., & Shukur, Z. (2021). Device identity-based user authentication on electronic payment system for secure E-wallet apps. Electronics, 11(1), 4.

Karniawati, N. P. A., Darma, G. S., Mahyuni, L. P., & Sanica, I. G. (2021). Community Perception of Using QR Code Payment in Era New Normal. PalArch's Journal of Archaeology of Egypt/Egyptology, 18(1), 3986-3999.

Yong, C., Tham, J., Azam, S. F., & Khatibi, A. (2021). The Factors Influencing College Students' Acceptance Of Mobile Payment In Malaysia. European Journal of Management and Marketing Studies, 7(1). https://doi.org/10.46827/ejmms.v7i1.1192

Lim, R. J., & Zulkipli, H. (2023). The Relationship Between Factors Affecting E-Wallets Adoption Among Adults in Kuantan, Pahang. Research in Management of Technology and Business, 4(1), 458-470.

Asmelash, L. (2019, August 14). Social media use may harm teens' mental health by disrupting positive activities, study says. CNN. https://www.cnn.com/2019/08/13/health/social-media-mental-health-trnd/index.html

Kadir, H. A., Ismail, R., Wok, S., & Manan, K. A. (2022). The Mediating Effect of Attitude on E-Wallet Usage Among Users in Malaysia. Journal of Communication Education, 2(1), 58-77.

Ramli, F. A. A., Hamzah, M. I., Wahab, S. N., & Shekhar, R. (2023). Modeling the Brand Equity and Usage Intention of QR-Code E-Wallets. FinTech, 2(2), 205-220.

Rahman, N. L. A., Abd Mutalib, H., Sabri, S. M., Annuar, N., Mutalib, S. K. M. S. A., & Rahman, Z. S. A. (2022). Factors Influencing E-Wallet Adoption among Adults During Covid-19 Pandemic in Malaysia: Extending The Tam Model. Sciences, 12(7), 983-994.

Park, J., Yoo, J., Yu, J., Lee, J., & Song, J. (2023). A Survey on Air-Gap Attacks: Fundamentals, Transport Means, Attack Scenarios and Challenges. Sensors, 23(6), 3215.

Yathiraju, N., & Dash, B. (2023). Gamification Of E-Wallets With The Use Of Defi Technology-A Revisit To Digitization In Fintech. International Journal of Engineering, Science, 3(1).

VT, A., & George, J. (2023). Acceptance Of E-Wallet Humanities And Social Science Studies. Peer-Reviewed, Bi-annual, Interdisciplinary UGC CARE List Journal.

Ismail, S., & Yahaya, N. A. (2023). An Exploratory Study O Human Behavior Towards Intention To Use Facial Biometric Payment Among Malaysia Consumers. International Journal of Technology Management and Information System, 5(2), 16-29.