**Journal of the Community Development in Asia (JCDA)**
**Vol. 9 No. 1, pp.80-95, January, 2026**
**E-ISSN: 2654-7279 P-ISSN: 2685-8819**
**https://ejournal.aibpmjournals.com/index.php/JCDA/index**

# Determinants of Trust in E-Wallet Security: A Study Among Malaysian Undergraduates

**Azura Abdullah Effendi[1], Haslindar Ibrahim[1], Garima Mathur[2], Muhammad Faiz Ameen Bin Bhurhanuddeen[1*], Muhammad Arif Bin Azahari[1], Muhammad Akram Bin Abdul Rahman[1], Muhammad Hasif Bin Azizan[1], Daisy Mui Hung Kee[1]**

[1]University Sains Malaysia, Jalan Sungai Dua,11800 Minden, Pulau Pinang, Malaysia
[2]Prestige Institute of Management, Scheme 54, Indore 452010, India
*Corresponding Email: faizameen@student.usm.my

## ARTICLE INFORMATION

**Publication information**

**Research article**

**HOW TO CITE**
Effendi, A. A., Ibrahim, H., Mathur, G., Ameen, M. F. B., Arif, M. A., Akram, M. A. R., …, & Kee, D. M. H. (2026). Determinants of trust in e-wallet security: A study among Malaysian undergraduates. *Journal of the Community Development in Asia, 9*(1), 80-95.

**DOI:**
**https://doi.org/10.32535/jcda.v9i1.4335**

Received: 14 November 2025
Accepted: 18 December 2025
Published: 20 January 2026

## ABSTRACT

The rapid adoption of e-wallets among Malaysian undergraduates has heightened concerns regarding digital security and user trust. This study examines the key factors influencing trust in e-wallet security among Malaysian undergraduate students. Using a quantitative approach, data were collected through an online survey administered to undergraduates from multiple universities in Malaysia. Regression analysis was employed to examine the effects of secure online transactions, data privacy protection, and account recovery and lock features on e-wallet security confidence. The results indicate that the model explains 78.6% of the variance in security confidence ($R^2$ = 0.786, F = 189.38). Data privacy protection emerged as the strongest predictor ($\beta$ = 0.401, $p < 0.01$), followed by account recovery and lock protection ($\beta$ = 0.373, $p < 0.01$) and secure online transactions ($\beta$ = 0.177, $p < 0.01$). These findings demonstrate that while transaction security remains essential, users place greater emphasis on personal data protection and recovery mechanisms. The study highlights the importance of strengthening privacy safeguards, enhancing user control features, and improving cybersecurity awareness to foster trust in e-wallet platforms. The results offer practical implications for policymakers, financial institutions, and e-wallet providers seeking to promote secure and sustainable digital payment adoption among young users in Malaysia.

**Keywords:** Data Privacy Protection; E-Wallet Security; Secure Online Transactions; Trust; Undergraduate Users

## INTRODUCTION

In today's rapidly evolving digital economy, consumers' financial habits have been significantly reshaped by the increasing adoption of digital payment systems. An e-wallet, or digital wallet, is an application installed on an electronic device that stores payment information and enables users to make secure purchases without carrying physical cash or cards. In Malaysia, e-wallet usage has increased rapidly, particularly since the onset of the COVID-19 pandemic (Rahman et al., 2022). This growth has been driven by factors such as increased smartphone penetration, government initiatives promoting cashless transactions, and the expansion of a tech-savvy population. As a result, e-wallets have emerged as a dominant mode of transaction, especially among younger generations such as university students. The most prominent e-wallets currently trending in Malaysia include GrabPay, InstaPay eWallet, Wise, Touch 'n Go, BigPay, and GoPayz (Fox, 2025). For instance, e-wallet usage among Generation Z undergraduates in Malaysia increased from 28% in 2019 to 57% by late 2024, effectively doubling pre-pandemic adoption rates (Nawang et al., 2025). However, many undergraduates prefer using third-party and direct banking applications such as Touch 'n Go, Maybank Anytime Everywhere (MAE) by Maybank, CIMB Bank, and RHB Bank. Digital payment systems offer several advantages, including convenience, flexibility, security (Hoo et al., 2023), cost savings, bill-splitting capabilities, and opportunities for toll payment discounts (Wei & Zhang, 2025). These benefits collectively contribute to the widespread adoption of e-wallets among Malaysian undergraduate students.

Despite the growing popularity of e-wallets, many users, particularly students, may be unaware of the long-term risks associated with relying entirely on digital payment systems. Recent academic studies indicate that digital wallet ecosystems are increasingly targeted by sophisticated phishing and impersonation attacks aimed at stealing one-time passwords, access tokens, and other sensitive credentials (Md. Waliullah et al., 2025). Security concerns, therefore, remain a critical issue, especially if such risks are not adequately addressed. Sahi et al. (2022) note that slower adoption of digital payment systems is often attributed to users' concerns regarding security and privacy. Digital payments may be exposed to various forms of risk, including service risk, device risk, network risk, and platform risk (Putrevu & Mertzanis, 2024). Unlike cash transactions, which occur instantly without the involvement of third-party platforms, e-wallet transactions require the transmission of personal and financial information through digital networks, potentially increasing users' vulnerability to unauthorized access, data breaches, fraud, and system failures. Undergraduate students, who may not be fully aware of the cybersecurity threats associated with digital payments, therefore need to pay closer attention to these security-related issues (Tick & Mai, 2024).

Although existing research has extensively examined the benefits and adoption of e-wallets, limited attention has been given to how Malaysian undergraduates perceive security risks associated with digital payments. Studies that comparatively examine cash and e-wallet usage in relation to perceived security remain scarce, highlighting a critical research gap that this study seeks to address. This research is particularly relevant as it positions security concerns as a key determinant influencing undergraduates' preferred payment methods. By examining students' perceptions of safety when using cash versus e-wallets, this study provides valuable behavioral insights into financial decision-making in an increasingly digitalized environment. Moreover, it contributes to the limited body of literature on how security perceptions shape the financial behavior of Malaysian undergraduates within the context of a developing economy.

The outcomes of this study are expected to have important implications for multiple stakeholders, as the findings aim to enhance understanding of cybersecurity threats associated with digital payment systems among Malaysian undergraduates. This study seeks to increase students' awareness of the risks related to e-wallet usage while also offering insights that may assist fintech companies and application developers in designing more targeted improvements related to transparency, data protection, and user control mechanisms. In addition, the findings may support policymakers and educators in strengthening cybersecurity education initiatives and promoting safer financial practices within the undergraduate community in Malaysia. Specifically, this study examines and compares the frequency and purposes of cash and e-wallet usage among undergraduates, identifies the key factors influencing students' preferences for payment methods with a particular emphasis on security-related concerns, and evaluates students' perceptions of security risks associated with e-wallet transactions in comparison to traditional cash-based payments.

## LITERATURE REVIEW

### Secure Online Transactions and MAE Security Confidence

Secure online transactions represent a foundational element in the development of user trust toward e-wallet systems, particularly in contexts where digital payments have become deeply embedded in everyday financial activities. The rapid growth of digital payment adoption, especially during the COVID-19 pandemic, significantly increased reliance on cashless transactions as a means of minimizing physical contact and maintaining public hygiene (Graziano et al., 2025). In Malaysia, the implementation of cashless payment solutions by Maybank enabled users to avoid physical contact and cash handling, highlighting the role of digital payments not only as financial instruments but also as practical public health responses during periods of heightened risk (Kee et al., 2021). As the usage of MAE e-wallet services continues to expand beyond pandemic-related motivations, users' expectations regarding transaction safety, system reliability, and fraud prevention have correspondingly intensified.

Consumers are increasingly concerned about how their payment data is processed, transmitted, and protected throughout digital transaction flows. Prior studies emphasize that advanced authentication mechanisms, encryption technologies, and real-time transaction notifications are essential components in safeguarding users' financial information and detecting unauthorized activities at early stages (Paul et al., 2023). These security features play a critical role in preventing fraud, which remains one of the major barriers to the broader adoption of digital payment systems, particularly among younger and financially active user groups (Janteng & Dino, 2022). In the absence of robust transaction security, even minor system vulnerabilities may undermine confidence and discourage continued usage.

Furthermore, as users become more digitally literate and experienced with financial technologies, they increasingly expect e-wallet providers to deliver not only transactional convenience but also high levels of transparency, accountability, and protection. Financial service providers that clearly communicate their transaction security measures and actively monitor suspicious activities are more likely to gain users' trust and long-term engagement. Research suggests that users perceive digital payment technologies as more beneficial and reliable when secure transaction processes are seamlessly embedded within the platform's design and functionality, leading to higher user satisfaction, retention, and continued usage (Kee et al., 2022a). The protection of users' financial resources and transaction data is therefore a critical determinant in building and sustaining trust in e-wallet systems, particularly in competitive digital payment markets (Kee et al., 2022b).

Taken together, these arguments suggest that secure online transaction mechanisms serve as a fundamental trust-building pillar in e-wallet adoption. By ensuring safe transaction execution, reducing perceived financial risk, and enhancing user confidence in digital payment environments, secure online transactions are expected to exert a positive influence on users' overall security confidence in MAE e-wallet services.

H1: Secure online transaction has a significant positive effect on MAE security confidence among Malaysian undergraduates.

**Data Privacy Protection and MAE Security Confidence**

Data privacy protection is widely recognized as a central factor in fostering trust in digital financial services, particularly within e-wallet platforms such as MAE by Maybank. As users increasingly shift from cash-based transactions to digital payment systems, expectations regarding the protection of personal and financial information have become more pronounced. Users seek strong assurances that their sensitive data will be safeguarded against unauthorized access, misuse, and cyber threats throughout the transaction lifecycle (Tee et al., 2024). In response to these expectations, mobile payment applications have increasingly incorporated biometric authentication mechanisms, such as fingerprint recognition and secure password-based login systems, which enhance both user convenience and security by restricting system access to authorized individuals only (Ramli, 2021). These mechanisms play an important role in shaping users' perceptions of safety when engaging in digital financial transactions.

Modern consumers are also increasingly aware of how their personal data is collected, stored, transmitted, and managed by financial service providers. Heightened public awareness of cybersecurity incidents and data breaches has reinforced the importance of compliance with stringent data protection standards and regulatory requirements to ensure the confidentiality and integrity of user information (Nayak et al., 2025). Without adequate privacy safeguards, the likelihood of data leakage or unauthorized data exploitation increases, which can severely undermine user trust and discourage the continued use of e-wallet services. As such, data privacy concerns remain a critical challenge for digital payment providers operating in highly competitive financial ecosystems.

While system usability and convenience remain important determinants of technology acceptance, prior research emphasizes that ease of use must be carefully balanced with robust privacy and security practices to achieve sustainable trust and long-term user engagement (Kee et al., 2022a). Users may initially adopt an e-wallet platform due to its convenience, but continued usage is more strongly influenced by perceptions of how well their personal information is protected. As e-wallet technologies continue to evolve and process increasing volumes of sensitive user data, maintaining strong data privacy protocols becomes a strategic necessity rather than a purely technical requirement (Chelvarayan et al., 2022). Therefore, data privacy protection is expected to exert a significant positive influence on users' confidence in the security of MAE e-wallet applications.

H2: Data privacy protection has a significant positive effect on MAE security confidence among Malaysian undergraduates.

**Account Recovery and Lock Features and MAE Security Confidence**

In digital financial environments, effective account recovery and lock features play a vital role in reducing user anxiety and strengthening trust in e-wallet platforms, particularly in situations involving potential security breaches or access-related issues (Sait et al., 2024). Users increasingly expect to regain access to their accounts quickly and securely in cases of forgotten credentials, device loss, or suspected fraudulent activities, as prolonged access disruptions may lead to financial losses and diminished trust in the platform (Kocabas et al., 2021). As a result, the availability of reliable recovery mechanisms has become a key determinant of perceived security in digital payment systems.

Previous research indicates that security practices such as multi-step account verification, email or SMS confirmation, and the use of strong personal identification numbers significantly reduce the risk of unauthorized access and account misuse (Omotunde & Ahmed, 2023). These practices provide users with reassurance that even if a security incident occurs, appropriate safeguards are in place to minimize potential damage. By enabling users to temporarily lock their accounts or initiate recovery procedures, e-wallet platforms empower users with a sense of control over their financial assets, which is essential for building confidence in digital financial environments.

Maybank's introduction of digital customer service innovations, such as the Maybank EzyQ online appointment management system, reflects broader institutional efforts to improve service accessibility, responsiveness, and user support in financial services (Ramli et al., 2021). Although such systems do not function as direct account recovery tools, they indirectly enhance users' confidence by facilitating timely assistance, issue resolution, and account-related inquiries. The availability of responsive support channels complements technical security features and reinforces users' perceptions of institutional reliability.

Empirical evidence further suggests that perceived risk, perceived ease of use, and perceived convenience are closely associated with users' intentions to adopt and continue using e-wallet services (Kee et al., 2022a). By lowering perceived risk and strengthening user control over account access, recovery, and lock features contribute to a more secure and reassuring user experience. Consequently, these features are expected to exert a positive influence on users' confidence in the overall security of MAE e-wallet platforms.

H3: Account recovery and lock features have a significant positive effect on MAE security confidence among Malaysian undergraduates.

### MAE Security Confidence Among Malaysian Undergraduates

An e-wallet is a digital payment tool that enables online transactions through computers or smartphones, functioning in a manner similar to debit or credit cards while offering greater flexibility, accessibility, and convenience for users (Kee et al., 2022a). Among Malaysian undergraduates, e-wallets have become an integral part of daily financial activities, including retail purchases, transportation payments, and peer-to-peer transfers. As reliance on digital financial services continues to increase, users' confidence in the security of these platforms has emerged as a critical concern, particularly in environments where financial data is continuously processed and stored digitally. This concern became more pronounced during periods of heightened risk, such as the COVID-19 pandemic, when physical transactions were discouraged, and digital payment platforms experienced accelerated adoption.

The widespread use of the Maybank2u application during the pandemic illustrates how digital financial platforms were leveraged to minimize physical interaction, reduce cash handling, and support public health initiatives in line with global recommendations (Sonali et al., 2025). For undergraduate users, who are generally technologically adept yet financially cautious, such platforms provide both convenience and safety. However, increased usage also heightened awareness of potential security vulnerabilities, making trust in system security a decisive factor in continued adoption.

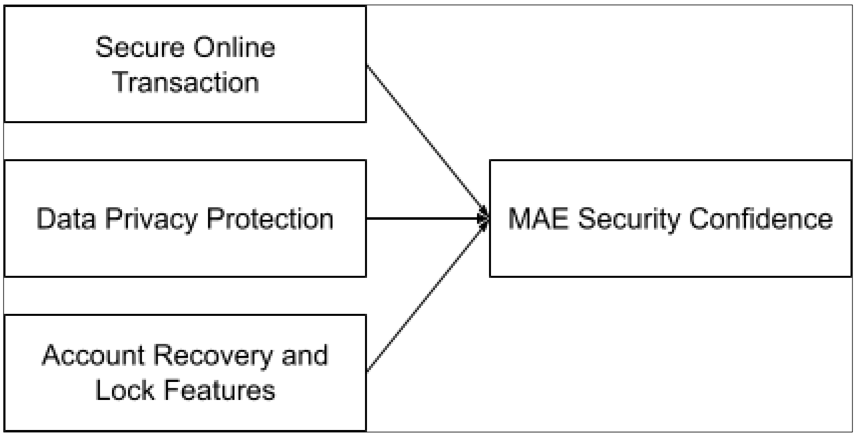
Security in digital payment systems encompasses a comprehensive set of programs, technologies, and procedures designed to verify information sources, protect user privacy, and maintain system integrity against network threats, fraud, and data breaches. These security considerations consistently rank among the most influential factors shaping users' decisions to adopt and continue using digital payment platforms (Karmaker et al., 2025). Although e-wallet applications are often perceived as secure due to features such as username authentication, password protection, and transaction monitoring, users continue to evaluate potential uncertainties related to privacy breaches and unauthorized access when engaging with these services (Edeh et al., 2021; Kee et al., 2022b).

Therefore, strengthening security confidence in platforms such as MAE is essential not only for fostering sustained user trust but also for encouraging broader adoption and supporting digital financial inclusion among Malaysian undergraduates. By addressing security concerns proactively, e-wallet providers can enhance user confidence, promote responsible usage, and contribute to the long-term sustainability of digital financial ecosystems.

### Conceptual Framework

The study framework model is depicted in Figure 1.

**Figure 1.** Research Framework



## RESEARCH METHOD

There exist three basic research approaches employed when conducting research: quantitative, qualitative, and mixed methods. The three approaches vary in terms of data collection and analysis, and the choice greatly depends on the research objectives as well as the kind of variables being employed. For this study, we employed a quantitative research strategy in examining the determinants of trust in the security of e-wallets among Malaysian undergraduates with specific reference to the MAE e-wallet. With this strategy, we can collect and analyze tabular numerical data to establish correlations and quantify levels of trust in terms of key security features.

Quantitative research is particularly appropriate for this topic as it provides a means of collecting data from a large population, and hence generalization to a broader undergraduate population can be achieved. According to Kee et al. (2022a), quantitative methods are best in obtaining trends in e-wallet adoption through surveys and statistical analysis. This method is certain in hypothesis testing and enables one to define relationships between variables such as secure online transactions, protection of data privacy, account recovery functionality, and overall security confidence.

To recruit participants, we used a convenience sampling method. This non-probability technique involves selecting respondents who are readily available and willing to participate. Convenience sampling was the effective method to use here because our target group, university students, is easily reachable via social media channels. Hence, this method allows us for rapid data rapidly without extensive logical planning. Although convenience sampling does not guarantee full representativeness, it is effective for exploratory research among tech-savvy undergraduates.

Data were gathered using an online questionnaire created using Google Forms, which was distributed through WhatsApp, Telegram, and Instagram. The questionnaire had four sections that covered the respondents' background information and perceptions regarding safe online transactions, data privacy, recovery features of accounts, and, in general, their trust in MAE's security. Online distribution was utilized because it is easy, cost-effective, and has good reach, especially among tech-literate undergraduate students. According to Kee et al. (2021), internet-based surveys are particularly convenient among students because they are flexible in terms of time and place and eliminate logistical costs associated with traditional surveying.

A five-point Likert scale was used to collect the responses, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). This research collected 160 valid responses. This scale permitted respondents to show the degree of agreement or disagreement with various statements regarding e-wallet security features.

This study used IBM SPSS Statistics in analyzing the data, which is a commonly used software for statistical analysis in the social sciences. SPSS allowed us to perform data cleaning, descriptive analysis, reliability testing (Cronbach’s alpha), and inferential tests such as Pearson correlation and multiple regression. SPSS is commonly used in digital financial behaviour studies because it is reliable and efficient in handling large datasets, according to Kee et al. (2022b). With the use of SPSS, we had the capacity to test our hypotheses, quantify the correlations between variables, and draw data-driven inferences about the most significant determinants of e-wallet security trust among Malaysian undergraduates.

## RESULTS

**Table 1.** Respondents’ Profile Summary (N=160)

| Response | Category | Frequency | Percentage (%) |
|---|---|---|---|
| Gender | Male | 51 | 31.9 |
| | Female | 109 | 68.1 |
| Age Group | 18–20 | 16 | 10.0 |
| | 21–23 | 130 | 81.3 |
| | 24–26 | 11 | 6.9 |
| | Above 26 | 3 | 1.9 |
| Race | Malay | 115 | 71.9 |
| | Chinese | 26 | 16.3 |
| | Indian | 17 | 10.6 |
| | Others | 2 | 1.2 |
| Monthly Allowance | Below RM500 | 68 | 42.5 |
| | RM500 – RM1,000 | 69 | 43.1 |
| | RM1,001 – RM1,500 | 13 | 8.1 |
| | Above RM1,501 | 10 | 6.3 |

| | | | |
|---|---|---|---|
| How Often Do You Use E-Wallet? | Daily | 143 | 89.4 |
| | Weekly | 10 | 6.3 |
| | Monthly | 4 | 2.5 |
| | Rarely | 2 | 1.3 |
| | Never | 1 | 0.6 |
| Average Spending per E-Wallet Use | Less than RM10 | 21 | 13.1 |
| | RM10 – RM50 | 79 | 49.4 |
| | RM51 – RM100 | 37 | 23.1 |
| | RM101 – RM200 | 10 | 6.3 |
| | More than RM200 | 13 | 8.1 |

Table 1 presents the demographic characteristics and e-wallet usage patterns of the respondents (N = 160). The sample consists predominantly of female students, accounting for 68.1% (N = 109), while male respondents represent 31.9% (N = 51). In terms of age distribution, the majority of respondents fall within the 21–23 age group (N = 130, 81.3%), followed by those aged 18–20 (N = 16, 10.0%), 24–26 (N = 11, 6.9%), and above 26 years old (N = 3, 1.9%). This age profile is appropriate given the study's focus on undergraduate students, who are typically active users of digital payment platforms.

With regard to ethnicity, most respondents are Malay (N = 115, 71.9%), followed by Chinese (N = 26, 16.3%), Indian (N = 17, 10.6%), and others (N = 2, 1.2%). In terms of monthly allowance, 43.1% (N = 69) of respondents receive between RM500 and RM1,000, while 42.5% (N = 68) report receiving below RM500. A smaller proportion receives allowances between RM1,001 and RM1,500 (N = 13, 8.1%) or above RM1,501 (N = 10, 6.3%). These figures indicate that most respondents fall within the low- to moderate-income category, which may influence their spending behavior and reliance on e-wallet services.

Regarding usage frequency, e-wallet adoption among respondents is notably high. A large majority of students report using e-wallets daily (N = 143, 89.4%), followed by weekly (N = 10, 6.3%), monthly (N = 4, 2.5%), and rare usage (N = 2, 1.3%), while only one respondent (0.6%) reports never using an e-wallet. In terms of average spending per transaction, most respondents spend between RM10 and RM50 (N = 79, 49.4%), followed by RM51–RM100 (N = 37, 23.1%), less than RM10 (N = 21, 13.1%), more than RM200 (N = 13, 8.1%), and RM101–RM200 (N = 10, 6.3%). Overall, these findings suggest that MAE is widely integrated into students' daily activities, including food purchases, bill payments, shopping, transportation, and online services, reinforcing the relevance of examining security confidence in e-wallet usage.

**Table 2.** Descriptive statistics, Cronbach's Coefficient Alpha, and Zero-order Correlations for all study variables

| | Variable | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 1 | Secure Online Transaction | 0.890** | | | |
| 2 | Data Privacy Protection | 0.801** | 0.888** | | |
| 3 | Account Recovery and Lock Protection | 0.736** | 0.820** | 0.904** | |
| 4 | MAE Security Confidence | 0.771** | 0.847** | 0.831** | 0.943** |
| Number of Items | | 5 | 5 | 5 | 5 |
| Mean | | 4.3417 | 4.2177 | 4.1500 | 4.2426 |
| Standard Deviation | | 0.66003 | 0.69035 | 0.77369 | 0.74834 |

Note: N = 160; *p < 0.05, **p < 0.01, ***p < 0.001. The diagonal entries represent Cronbach's Coefficient Alpha.

Table 2 reports the descriptive statistics, Cronbach's alpha coefficients, and zero-order correlations among the study variables. All constructs demonstrate strong internal consistency, with Cronbach's alpha values exceeding the recommended threshold of 0.70. Specifically, Secure Online Transaction ($\alpha = 0.890$), Data Privacy Protection ($\alpha = 0.888$), Account Recovery and Lock Protection ($\alpha = 0.904$), and MAE Security Confidence ($\alpha = 0.943$) indicate high reliability, confirming the adequacy of the measurement instruments.

The mean scores for all variables range from 4.1500 to 4.3417, suggesting that respondents generally hold positive perceptions toward e-wallet security features and express a high level of confidence in the MAE platform. Secure Online Transaction records the highest mean value, indicating that transaction safety is particularly important to Malaysian undergraduates. The relatively low standard deviation values (0.66003–0.77369) reflect consistency in respondents' perceptions.

Correlation analysis shows that all independent variables are positively and significantly associated with MAE Security Confidence at the 0.01 significance level. Data Privacy Protection exhibits the strongest correlation ($r = 0.847$), followed by Account Recovery and Lock Protection ($r = 0.831$) and Secure Online Transaction ($r = 0.771$). Significant positive correlations are also observed among the independent variables, indicating that while these constructs are interrelated, they remain conceptually distinct. These results provide preliminary empirical support for the proposed research framework and justify further hypothesis testing through regression analysis.

**Table 3.** Regression Results for Determinants of MAE Security Confidence

| Variable | | MAE Security Confidence |
|---|---|---|
| 1 | Secure Online Transaction | 0.177 |
| 2 | Data Privacy Protection | 0.401 |
| 3 | Account Recovery and Lock Protection | 0.373 |
| $R^2$ | | 0.786 |
| F-value | | 189.38 |
| Durbin–Watson Statistic | | 2.222 |

Table 3 presents the regression results examining the effects of Secure Online Transaction, Data Privacy Protection, and Account Recovery and Lock Protection on MAE Security Confidence. The model explains a substantial proportion of variance in MAE Security Confidence, with an $R^2$ value of 0.786, indicating that 78.6% of the variation in the dependent variable is accounted for by the three predictors. The F-value of 189.38 confirms that the model is statistically significant, while the Durbin–Watson statistic of 2.222 suggests no serious autocorrelation issues.

With respect to the proposed hypotheses, Secure Online Transaction has a positive and statistically significant effect on MAE Security Confidence ($\beta = 0.177$, $p < 0.01$), supporting H1. This result indicates that secure transaction mechanisms, such as authentication and encryption, enhance users' confidence in the MAE platform.

Data Privacy Protection demonstrates the strongest positive effect on MAE Security Confidence ($\beta = 0.401$, $p < 0.01$), providing strong support for H2. This finding suggests that Malaysian undergraduates place considerable importance on how their personal and financial data are collected, stored, and protected when forming security confidence.

Similarly, Account Recovery and Lock Protection show a significant positive effect on MAE Security Confidence ($\beta = 0.373$, $p < 0.01$), thereby supporting H3. The result implies that features enabling users to regain control of their accounts and prevent unauthorized access play a critical role in reinforcing trust in the platform.

Overall, although all three security-related factors significantly contribute to MAE Security Confidence, the results indicate that users place the greatest emphasis on data privacy protection, followed by account recovery and lock features, while secure online transactions, although significant, exert a comparatively smaller influence.

## DISCUSSION

### H1: Secure Online Transaction and MAE Security Confidence

This study examined the determinants influencing MAE security confidence among Malaysian undergraduates and found that secure online transactions, data privacy protection, and account recovery and lock protection all significantly affect users' trust in e-wallet security. These findings reinforce existing literature, which suggests that security-related factors are central to digital payment adoption, particularly in emerging economies where trust remains a critical concern (Putrevu & Mertzanis, 2024; Ramli, 2021).

Although secure online transactions demonstrated the smallest standardized effect among the three predictors, it remains a statistically significant contributor to MAE security confidence. This finding suggests that secure transaction processes, including authentication, encryption, and real-time monitoring, are increasingly perceived as baseline requirements rather than differentiating features. Previous studies have similarly noted that as users become more experienced with digital payments, transaction security is often taken for granted unless a failure occurs (Kee et al., 2022a; 2022b). Nonetheless, secure transaction mechanisms continue to underpin overall trust, as weaknesses in this area can quickly erode confidence and discourage continued usage (Edeh et al., 2021; Karmaker et al., 2025).

### H2: Data Privacy Protection and MAE Security Confidence

Among the predictors, data privacy protection emerged as the strongest determinant of MAE security confidence. This result is consistent with prior studies indicating that users' willingness to adopt and continue using e-wallets is highly dependent on how well their personal and financial data are protected (Hoo et al., 2023; Rahman et al., 2022). As digital payment platforms increasingly collect and process sensitive user information, concerns related to data misuse, unauthorized access, and regulatory compliance have become more prominent (Nayak et al., 2025; Omotunde & Ahmed, 2023). For undergraduate users, who are generally digitally literate but still vulnerable to cyber threats, strong data protection mechanisms serve as a key signal of platform reliability and trustworthiness. This finding aligns with Sahi et al. (2022), who highlighted security and privacy as dominant themes in digital payment research and key barriers to adoption when inadequately addressed.

### H3: Account Recovery and Lock Protection and MAE Security Confidence

Account recovery and lock protection were identified as the second most influential factor in shaping MAE security confidence. This supports earlier research emphasizing the importance of user control and protection strategies in mitigating perceived risk (Kocabas et al., 2021). Features such as account recovery, verification procedures, and lock mechanisms provide users with reassurance that potential security breaches can be managed effectively. Similar findings have been reported among university students and young adults, where perceived control over financial accounts significantly enhances trust in cashless payment systems (Chelvarayan et al., 2022; Nawang et al., 2025). In the context of Malaysia, where e-wallet usage surged during and after the COVID-19 pandemic, these recovery features play a crucial role in maintaining users' confidence amid increasing reports of digital fraud (Kee et al., 2021; Md. Waliullah et al., 2025).

### Integrated Interpretation of Security Confidence Determinants

Overall, the findings indicate that MAE security confidence is not shaped by a single security feature but rather by a combination of complementary safeguards that collectively reduce perceived risk. This supports earlier research suggesting that trust in digital payment systems is multidimensional, encompassing privacy assurance, transaction security, and user empowerment (Janteng & Dino, 2022; Sonali et al., 2025). As e-wallet adoption continues to expand among Malaysian undergraduates, service providers must align technological advancements with evolving user expectations regarding safety, transparency, and control. From a broader perspective, strengthening security confidence in e-wallet platforms contributes not only to individual user trust but also to the sustainability of cashless ecosystems in emerging digital economies (Fox, 2025; Wei & Zhang, 2025).

## CONCLUSION

This study examined the key factors influencing trust in the security of e-wallet services, with specific attention to the MAE application by Maybank among Malaysian undergraduate students. The findings indicate that undergraduates are active users of e-wallets for routine financial transactions and demonstrate a high level of awareness regarding the importance of security in digital payment environments. Security considerations remain a primary determinant in users' selection of digital payment platforms, reflecting heightened concerns over the protection of personal and financial information in an increasingly cashless economy.

Among the examined factors, data privacy protection emerged as the most influential determinant of security confidence in MAE usage. Strong data protection standards play a critical role in assuring users that their personal and financial information is handled confidentially and safeguarded against unauthorized access. This finding highlights the growing sensitivity of young users to issues of data misuse, surveillance, and cyber threats. Account recovery and lock protection mechanisms were also found to significantly enhance trust, as these features provide users with a sense of control over their accounts through effective safeguards such as identity verification procedures and account-locking functions in response to suspicious activity. Secure online transaction mechanisms, including authentication processes, encryption technologies, and real-time transaction notifications, further contribute to users' security confidence by enabling continuous monitoring and early detection of potentially fraudulent activities.

The statistical results confirm that data privacy protection exerts the strongest influence on MAE security confidence, underscoring the importance young users place on responsible data governance by financial service providers. In addition, the significance of account recovery and lock protection reflects users' expectations for proactive and responsive security features that minimize financial risk. Although secure online transaction demonstrates a comparatively smaller standardized effect, it remains a fundamental component of overall trust, as consistent and secure transaction execution supports continued usage and reduces perceived uncertainty in digital payment activities.

Despite the widespread adoption and convenience of e-wallet services, Malaysian undergraduates continue to express concerns regarding risks such as digital fraud, unauthorized access, and data breaches. Without robust and continuously updated security measures, these risks have the potential to undermine user confidence and slow the sustained adoption of cashless payment systems. The potential exposure of sensitive information reinforces the need for ongoing improvements in security infrastructure, transparent communication of protection mechanisms, and enhanced user awareness regarding digital safety practices. Accordingly, e-wallet providers, banking institutions, and policymakers should collaborate to strengthen regulatory frameworks, improve platform security standards, and promote responsible digital payment behavior.

Overall, this study contributes to the growing body of literature on e-wallet security by providing empirical evidence on how specific security-related factors shape trust among Malaysian undergraduates. The findings offer practical insights for system developers, financial institutions, and policymakers seeking to foster a safer and more trustworthy digital payment ecosystem. As digital financial services continue to expand among younger populations, maintaining strong security confidence will be essential for long-term sustainability. Trust in e-wallet platforms should therefore be regarded not only as a technical requirement but also as a strategic priority for ensuring continued engagement and stability in the digital financial sector.

## LIMITATION

Despite the valuable findings of this study, several limitations should be acknowledged. This research employed a cross-sectional design based on self-reported survey data collected at a single point in time, which limits the ability to establish causal relationships or observe changes in perceptions of e-wallet security over time. In addition, the sample was confined to Malaysian undergraduates, which may restrict the generalizability of the results to other population groups with different demographic or socioeconomic characteristics. The study also focused on a limited set of determinants of MAE security confidence, potentially overlooking other relevant factors such as regulatory awareness, institutional trust, or prior experiences with digital fraud. Furthermore, the exclusive use of quantitative methods may not fully capture the depth of users' personal experiences and concerns regarding e-wallet security. These limitations should be considered when interpreting the findings and may provide directions for future research.

## ACKNOWLEDGMENT

The authors would like to express their heartfelt gratitude to everyone who helped and contributed to this research. Their valuable cooperation, guidance, and assistance throughout the study were greatly appreciated.

## DECLARATION OF CONFLICTING INTERESTS

The authors have declared no potential conflicts of interest concerning the study, authorship, and/or publication of this article.

## REFERENCES

Chelvarayan, A., Yeo, S. F., Yi, H. H., & Hashim, H. (2022). E-wallet: A study on cashless transactions among university students. *F1000Research, 11*, 687. https://doi.org/10.12688/f1000research.73545.1

Edeh, F. O., Aryani, D. N., Subramaniam, T., Kee, D. M. H., Samarth, T., Nair, R. K., Kannappan, T., Tan, Y. S., & Teh, Y. C. (2021). Impact of COVID-19 pandemic on consumer behavior towards the intention to use e-wallet in Malaysia. *International Journal of Accounting & Finance in Asia Pacific, 4*(3), 42–59. https://doi.org/10.32535/ijafap.v4i3.1205

Fox, L. (2025, July 15). *Malaysia top 10 e-wallets comparison: Features, use cases & selection guide*. Hawk Insight. https://hawkinsight.com/en/article/malaysia-top-10-e-wallets-guide

Graziano, E. A., Musella, F., & Petroccione, G. (2025). Cashless payment: behavior changes and gender dynamics during the COVID-19 pandemic. *EuroMed Journal of Business*, *20*(5), 54-74. https://doi.org/10.1108/EMJB-11-2023-0299

Hoo, W. C., Yee, Y. F., Chan, A. H. A., Mubaarique, A. R., Shina, A., & Khan, M. S. (2023). Factors influencing the adoption of e-wallet among the general public in Malaysia. *International Journal of Academic Research in Business and Social Sciences, 13*(7). https://doi.org/10.6007/ijarbss/v13-i7/17313

Janteng, J., & Dino, N. F. N. (2022). Investigating the determinants of e-wallet adoption intention in Malaysia: An empirical study. *International Journal of Academic Research in Business and Social Sciences, 12*(6), 561–575. https://doi.org/10.6007/IJARBSS/v12-i6/13855

Karmaker, S., Oishi, M. E. F., Qasem, A., Sami, S. B. S., & Noor, J. (2025). Exploring influential factors of consumer purchase behavior on the adoption of digital payment apps in Bangladesh. *Computers in Human Behavior Reports*, *17*, 100587. https://doi.org/10.1016/j.chbr.2025.100587

Kee, D. M. H., Hisam, N. N. B. N., Rashid, N. H. B. A., Aziz, N. S. B. A., Mazlan, N. A. B., & Mahadi, N. A. Z. B. (2021). The impact of using cashless payment during the COVID-19 pandemic: A case study of Maybank. *International Journal of Accounting & Finance in Asia Pacific, 4*(2), 107–117. https://doi.org/10.32535/ijafap.v4i2.1118

Kee, D. M. H., Lai, K. H. H., Chin, H. L., Lee, K. J., Long, J. L., Yosantini, I., & Aryani, D. N. (2022a). Do you have a digital wallet? A study of e-wallet during the COVID-19 pandemic. *International Journal of Accounting & Finance in Asia Pacific, 5*(1), 24–38. https://doi.org/10.32535/ijafap.v5i1.1413

Kee, D. M. H., Ow, A. L., Ooi, Z. J., Sathiaselan, P., Pang, K., Ashaari, S. K., & Madhan, M. (2022b). Have you touched? A case study of Touch 'n Go e-wallet. *International Journal of Accounting & Finance in Asia Pacific, 5*(1), 84–94. https://doi.org/10.32535/ijafap.v5i1.1416

Kocabas, H., Nandy, S., Tamanna, T., & Al-Ameen, M. N. (2021). Understanding users' behavior and protection strategy upon losing or identifying unauthorized access to online accounts. In A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust* (Lecture Notes in Computer Science, Vol. 12788). Springer. https://doi.org/10.1007/978-3-030-77392-2_20

Md. Waliullah, M. Z. H. G., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions, 1*(1), 226–257. https://doi.org/10.63125/fh49gz18

Nawang, W. R. W., Abdillih, M. A. A. M., & Mursidi, A. (2025). Embracing e-wallet applications among Generation Z in Malaysia: The mediating role of trust. *Journal of Nusantara Studies (JONUS), 10*(1), 373–398. https://doi.org/10.24200/jonus.vol10iss1pp373-398

Nayak, R., Ghugar, U., Gupta, P., Dash, S., & Gupta, N. (2025). Data Privacy and Compliance in Information Security. *Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics*, 17-33. https://doi.org/10.1002/9781394268917.ch2

Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115-133. https://doi.org/10.58496/MJCSC/2023/016

Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16. https://doi.org/10.5121/ijsc.2023.14301

Putrevu, J., & Mertzanis, C. (2024). The adoption of digital payments in emerging economies: challenges and policy responses. *Digital Policy, Regulation and Governance*, *26*(5), 476-500. https://doi.org/10.1108/DPRG-06-2023-0077

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. *International Journal of Academic Research in Business & Social Sciences*, *12*(7), 983-994. https://doi.org/10.6007/IJARBSS/v12-i7/14327

Ramli, F. A. A. (2021). Mobile payment and e-wallet adoption in emerging economies: A systematic literature review. *Journal of Emerging Economies and Islamic Research, 9*(2), 1–39. https://doi.org/10.24191/jeeir.v9i2.13617

Sahi, A. M., Khalid, H., Abbas, A. F., Zedan, K., Khatib, S. F. A., & Amosh, H. A. (2022). The research trend of security and privacy in digital payment. *Informatics, 9*(2), 32. https://doi.org/10.3390/informatics9020032

Sait, M. A., Ali, M. A., Almunawar, M. N., & Haji Masri, H. M. (2024). Understanding factors to digital wallet discontinuance intention among past users: an exploratory study. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-01-2024-0005

Sonali, S., Hussain, S., Gupta, S., & Bhardwaj, S. (2025). A helping hand in banking: How off-site customer-to-customer interactions impact the mobile banking usage behaviour and financial well-being. *International Journal of Bank Marketing*, 1–29. https://doi.org/10.1108/IJBM-02-2025-0125

Tee, Y. Y., Ting, M. S., & Talib, A. A. (2024). Facilitating the influence on adopting E-wallets: An extended technology acceptance model (TAM) approach. *International Journal of Academic Research in Business and Social Sciences*, *14*(2), 883. https://doi.org/10.6007/IJARBSS/v14-i2/20587

Tick, A., & Mai, P. T. (2024). Cyber Security Awareness and the Behaviors of Higher Education Students, using Smartphones in Vietnam. *Acta Polytechnica Hungarica*, *21*(12), 111-131. https://doi.org/10.12700/APH.21.12.2024.12.7

Wei, L., & Zhang, B. (2025). A bundled dilemma: explaining the adoption paradox of digital vouchers in supply chain. *International Journal of Production Research*, 1–21. https://doi.org/10.1080/00207543.2025.2579767

## ABOUT THE AUTHOR(S)

### 1st Author

Dr. Azura Abdullah Effendi is a Senior Lecturer at Universiti Sains Malaysia (USM), specializing in Management and Organizational Behavior. An accomplished academic, she teaches undergraduate and postgraduate courses, supervises Master’s and PhD candidates, and conducts research in Emotional Intelligence, Leadership, and Work Values. Her work has been published in journals such as the American Journal of Economics and Business Administration (AJEBA) and Journal of Global Business and Economics (JOGBE), and she serves as a journal editor and peer reviewer for several academic publications. A co-author of books on Organizational Behavior, she also contributes as a consultant, external examiner, and research trainer for universities and government agencies. An active member of MIM, MIHRM, and AAM, Dr. Azura is a recognized speaker and module developer for USM and other institutions. Beyond academia, she is a community advocate, having won an award for her welfare initiatives and organized multiple charitable projects.

Email: azura_e@usm.my
ORCID ID: https://orcid.org/0000-0003-3849-2912

**2nd Author**
Haslindar Ibrahim is currently an associate professor in finance at the School of Management, Universiti Sains Malaysia, and she earned her Ph.D from the University of Malaya in 2009. Her current research interests include ownership concentration (family ownership), corporate governance, capital structure, green finance, digital finance, and Islamic finance. Her publications appeared in, among others, Pacific-Basin Finance Journal, Corporate Social Responsibility and Environmental Management, Resource Policy, Transnational Corporations Review, Journal of Multinational Financial Management, and many more. She has also presented her research works in various conferences locally and internationally. She is also supervising Ph.D and master's students and is currently conducting research in corporate governance, financial literacy among young and ageing society, and green and digital finance-related fields.
Email: haslindar@usm.my
ORCID ID: https://orcid.org/0000-0002-0134-1486

**3rd Author**
Dr. Garima Mathur is a Professor in Management (HR & OB). She is a PhD, UGC-NET qualified, Master's in Psychology (MA) and Management (MBA). She is the Head of the HR Department & MBA Program with more than 20 years of research and academic experience. Her areas of interest are Organizational Behaviour, Human Resource Management & Research Methodology. She is a corporate and academic trainer in a variety of industries. She has chaired sessions/delivered keynote speeches at various conferences, including overseas conferences in Indonesia, Malaysia, Singapore, etc. Dr. Garima is a Jiwaji University-approved PhD guide, and twelve research scholars under her have already been awarded PhD degrees. Being an active researcher, more than ninety national and international refereed publications, including 24 Scopus (including Q1), 10 Web of Sciences, ABDC, etc., are due to her credit. She is an active Member of APA, AIB, ISTD, IAA, and GMA. Dr. Garima has also published five edited books. She is the editor of 'Prestige International Journal of Management & IT- Sanchayan' and a member of the editorial and review boards of many reputed journals, including the Academy of Management, Inderscience Journals, Emerald, Sage, etc.
Email: garima.mathur@prestigegwl.org
ORCID ID: https://orcid.org/0000-0003-1166-2192

**4th Author**
Muhammad Faiz Ameen Bin Bhurhanuddeen is a current undergraduate at Universiti Sains Malaysia.
Email: faizameen@student.usm.my

**5th Author**
Muhammad Arif Bin Azahari is a current undergraduate at Universiti Sains Malaysia.
Email: arif.azahari87@student.usm.my

**6th Author**
Muhammad Akram Bin Abdul Rahman is a current undergraduate at Universiti Sains Malaysia.
Email: muhdakramm27@student.usm.my

**7th Author**
Muhammad Hasif Bin Azizan is a current undergraduate at Universiti Sains Malaysia.
Email: mhdhasif@student.usm.my

**8th Author**
Dr. Daisy Mui Hung Kee is an Associate Professor at the School of Management, Universiti Sains Malaysia (USM). She earned her Ph.D. from the University of South Australia and an MBA from USM. A prolific scholar with over 75 Web of Science and 113

Scopus-indexed publications, she also serves as the Country Director for AIBPM (Indonesia) and the STAR Scholars Network (USA).
Email: daisy@usm.my
ORCID ID: https://orcid.org/0000-0002-7748-8230