

PERCEIVED SECURITY RISK AND E-PAYMENT ADOPTION IN HIGHER EDUCATION: EVIDENCE FROM UiTM STUDENTS

SHAIFUL BAHARIN, S. N.¹ – MASRUDI, S. H.¹ – OTHMAN, Z.² – KEDIN, N. A.³ – BAKHTIAR, M. F. S.^{1*}

¹ Faculty of Hotel and Tourism Management, Universiti Teknologi MARA, Selangor, Malaysia.

² Faculty of Hotel and Tourism Management, Universiti Teknologi MARA Cawangan Pulau Pinang, Pulau Pinang, Malaysia.

² Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Selangor, Malaysia.

*Corresponding author
e-mail: mfaeez[at]uitm.edu.my

(Received 18th October 2025; revised 28th November 2025; accepted 05th December 2025)

Abstract. The RHB MySiswa Debit i-Card was introduced to encourage cashless transactions among Malaysian public university students. Despite its benefits, security concerns such as fraud, privacy breaches, and data protection continue to limit its adoption. This study investigates how perceived security risk influences intention to use and actual usage of the card among Universiti Teknologi MARA (UiTM) Puncak Alam students. A quantitative cross-sectional survey from 162 respondents was conducted, with data analyzed via correlation, multiple regression, and Sobel mediation testing. Results reveal significant positive relationships between perceived security risks, intention to use and actual usage; with intention to use fully mediating the relationship between perceived security risks and actual usage behavior. These findings underscore the importance of building user trust through clear communication of security features and targeted awareness campaigns. The study extends adoption theory by integrating perceived security risk and provides actionable insights for enhancing e-payment uptake in higher education settings.

Keywords: *perceived security risks, intention to use, actual usage, MySiswa Debit i-Card*

Introduction

Digital innovations in business transactions have progressively supplanted cash-based payments with electronic alternatives, offering enhanced convenience, speed, security, and cost-efficiency (Bakar et al., 2024; Lai and Liew, 2021). Many nations now aim to achieve a cashless society, a goal embraced by individuals, organizations, and governmental bodies alike (Lai and Liew, 2021). Electronic payment, or e-payment, denotes any payment mechanism that does not involve physical cash, banknotes, or cheques. It encompasses online payment platforms and channels enabling consumers to pay for goods and services via the Internet (Tian et al., 2024). These systems, including mobile wallets and digital platforms provide users with secure, efficient means to conduct financial transactions virtually, aligning with growing demands for seamless, user-centric digital experiences (Lai and Liew, 2021). To boost e-payment adoption among Malaysian youth particularly students at higher learning institution, the government launched the RHB MySiswa Debit i-Card initiative in 2024. While this campaign is expected to elevate adoption levels, it may also heighten the exposure to potential cybersecurity vulnerabilities. Despite notable benefits and rising e-payment adoption, Malaysian consumers continue to express concerns regarding security risks

(Bakar et al., 2024). These apprehensions extend beyond transactional threats to include issues of privacy, identity theft, and the integrity of digital financial systems (Waliullah et al., 2025; Bakar et al., 2024). Such risks can adversely affect consumer trust and dampen adoption rates. Hence, addressing these challenges is vital to fostering broader acceptance and usage of e-payment technology.

For that matter, this study investigated users' perceived security risks related to e-payment platforms and examines how these perceptions influence their intention to use and actual usage behavior. Specifically, it explores perceived security risk, intention to use and actual usage behavior of e-payments among UiTM Puncak Alam students in light of the RHB MySiswa Debit i-Card campaign.

Literature review

The shift toward electronic payments is offering convenience but raising concerns over privacy and fraud (Gupta et al., 2023; Ali et al., 2021). In Malaysia, public and private initiatives such as the RHB MySiswa Debit i-Card which aim to increase cashless transactions among youth particularly students at higher learning institutions, making it timely to examine how perceived security risk influences both the intention to use and actual usage behavior of e-payment solutions. In the subsequent section, each variable examined in this study is reviewed. The Theory of Planned Behavior is discussed. It provides the basis for the formulation of the study's hypotheses.

Perceived security risk

Perceived security risk refers to an individual's subjective expectation that a service or transaction could expose them to financial loss, privacy invasion, identity theft, or data breaches (Gupta et al., 2023; Ali et al., 2021). In Malaysia, this concern is especially noticeable. As such, Sidek et al. (2024) found that despite convenience, university students hesitate to use cashless payments due to concerns about reliability, privacy, and data security. Similarly, a study among UiTM Melaka students suggests that e-wallet acceptance is undermined by perceived lack of security features; even when other benefits are evident (Seng et al., 2023). These findings underscore that security risk is a real barrier among Malaysian students, reinforcing the need to explicitly measure its impact on intention and usage behavior.

Intention to use

Behavioral intention captures an individual's stated readiness or plan to perform a behavior (Fishbein and Ajzen, 1977), and it is the proximal predictor of actual behavior in many technology-acceptance models. In e-payment research, intention is influenced by perceived usefulness, perceived ease of use, social influence, facilitating conditions and perceived risk/trust trade-offs (Liu et al., 2025; Gupta et al., 2023). Within the context of Malaysian university students, behavioral intention has been shown to hinge not only on perceived usefulness and ease of use but also on trust dimensions. Seng et al. (2023) reported that although perceived usefulness drives intention, the presence of security and trust concerns may temper uptake. When students doubt the system's safety or institutional assurance, even with promising features; they delay or avoid adoption. These dynamics suggest that students' intention to use the MySiswa Debit i-Card will be influenced heavily by how secure they believe it is, in addition to intrinsic factors like convenience.

Actual usage behavior

Actual usage behavior denotes the frequency and scope of real transactions made with an e-payment instrument such as number of purchases, breadth of merchant acceptance. Theory and evidence indicate that behavior follows intention when situational constraints are minimal and facilitating conditions are present (Ajzen, 1991). From the perspective of Malaysian student contexts, intention does not always translate into use unless trust is established. For example, if students remain uneasy about digital safety, they may avoid using e-payment tools despite expressing intent. Research suggests that supporting conditions such as secure infrastructure are necessary to bridge the gap from intention to use (Sidek et al., 2024). Therefore, in studying UiTM Puncak Alam students, assessing perceived security is essential to explain actual usage behavior.

Study framework and hypothesis

In order to gain an improved understanding on the determinants of MySiswa Debit i-Card perceived security risks, intention to use and actual usage behavior, a study framework is developed originating from Theory of Planned Behavior (TPB). According to TPB, behavioral intention is the immediate antecedent of actual behavior, shaped by attitude, subjective norms, and perceived behavioral control (Ajzen, 1991). In this study, perceived security risks would influence students' attitudes toward MySiswa Debit i-Card, thus affecting intention to use. Among Malaysian students, attitudes toward e-payment are highly sensitive to transaction safety and privacy perceptions; higher security perceptions foster positive attitudes and stronger intentions (Seng et al., 2023), while high perceived risks suppress both (Sidek et al., 2024). Subjective norms, particularly peer influence and university endorsement, also play a pivotal role. Peer approval and positive campus narratives can normalize e-payment usage and reduce hesitation (Bakar et al., 2024). Perceived behavioral control reflecting students' confidence in using the card and the availability of necessary resources, further strengthens the intention and behavior link. Hence, if secure payment channels and technical support are readily accessible, students would be more capable of adopting and regularly using the card.

In line with TPB, this study hypothesizes that intention to use mediates the relationship between perceived security risk and actual usage behavior. That is, even if students perceive high security, actual usage is unlikely unless they first form a strong intention to use. Based from all earlier deliberation, the following hypotheses were proposed for evaluation: (H1): There is a relationship between perceived security risk and actual usage behavior of MySiswa Debit i-Card; (H2): There is a relationship between perceived security risk and intention to use MySiswa Debit i-Card; (H3): There is a relationship between intention to use and actual usage behavior of MySiswa Debit i-Card; (H4): Intention to use mediates the relationship between perceived security risk and actual usage behavior of MySiswa Debit i-Card.

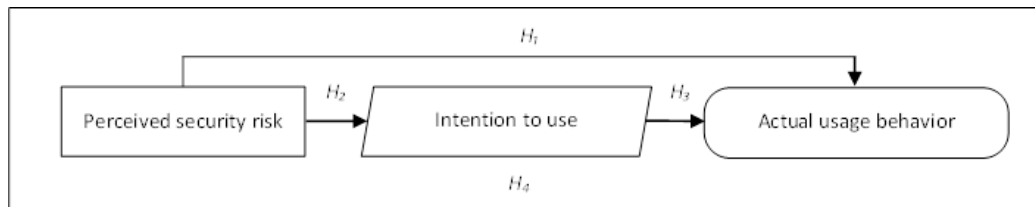


Figure 1. Research framework.

Materials and Methods

In this research, primary data were collected using survey. Quantitative research design was employed to examine the influence of perceived security risks on the intention to use as well as actual usage behavior of the RHB MySiswa Debit i-Card among students at Universiti Teknologi MARA (UiTM) Puncak Alam. A cross-sectional survey approach was applied, with data collected at a single point in time. The target population comprised students who were eligible and had access to MySiswa Debit i-Card. Using convenience sampling, a total of 162 valid responses were successfully obtained. Data were collected via a structured survey consisting four sections: (1) demographic information, (2) perceived security risks, (3) intention to use, and (4) actual usage behavior. All variables were measured using established scales adapted from prior literature, with minor modifications to suit the study context. Responses were recorded on a five-point Likert scale ranging from “strongly disagree” to “strongly agree.” The survey was pre-tested for clarity and content validity, and its reliability was assessed through Cronbach’s alpha. Data analysis was conducted using SPSS to obtain descriptive statistics, correlation analysis, and multiple regression results. Sobel test was employed to examine the mediating role of intention to use in between perceived security risks and actual usage behavior.

Results and Discussion

The profile of respondents

(Table 1) indicates that the sample was predominantly female undergraduate students, with most aged between 21 and 23 years. The majority were undergraduate students enrolled in various academic programs at Universiti Teknologi MARA (UiTM) Puncak Alam. A significant proportion of them reported being aware of the RHB MySiswa Debit i-Card. While some reported prior experience using the card, all acknowledged being introduced to it through campus initiatives during enrollment.

Table 1. Demographic info of respondents.

Category		Frequency	Percentage
Gender	Male	35	21.6
	Female	127	78.4
Age Group	Under 20 years old	37	22.8
	Between 21 to 25 years old	110	67.9
	Between 26 to 30 years old	7	4.3
	Between 31 to 35 years old	1	0.6
	Above 36 years old	7	4.3
Education Level	Bachelor Degree	130	80.2
	Master	31	19.1
	PhD	1	0.6
Faculty	Faculty of Hotel and Tourism Management	53	32.7
	Faculty of Health Sciences	12	7.4

Faculty of Accountancy	19	11.7
Faculty of Education	18	11.1
Faculty of Art and Design	6	3.7
Faculty of Business Management	47	29.0
Faculty of Architecture, Planning and Surveying	3	1.9
Faculty of Pharmacy	4	2.5
Total	162	100

Descriptive statistics

The descriptive statistics (*Table 2*) show that respondents generally reported moderately high perceptions of security when using the RHB MySiswa Debit i-Card. Mean scores for perceived security risk indicated that students felt reasonably confident in the card's ability to safeguard against fraud, data breaches, and privacy violations. Similarly, intention to use scored high, suggesting that students were generally willing to use the card for transactions both on and off campus. However, the mean score for actual usage behavior was slightly lower compared to perceived security and intention to use, indicating a potential gap between students' willingness to use the card and their actual transaction behavior. This pattern suggests that while positive perceptions and intentions exist, certain barriers such as limited merchant acceptance, habit persistence with cash, or lingering security concerns may still hinder consistent and widespread usage of the MySiswa Debit i-Card among UiTM students.

Table 2. Descriptive statistics.

Category	Mean	SD
Perceived risk		
I perceive MySiswa Debit i-Card is secure.	3.8951	0.82363
I perceive that the info relating to user and MySiswa Debit i-Card transactions are secure.	4.0370	0.77930
I believe that an inappropriate party will not be able to access my MySiswa Debit i-Card transaction.	3.8272	0.88872
It is acceptable for me to share personal information during online transactions.	3.2099	1.11139
The possibility of online fraud transactions is low for me.	3.1173	1.07707
I will continue using MySiswa Debit i-Card even when issues relating to security system breach is highlighted.	2.8457	1.13974
I trust the ability of MySiswa Debit i-Card to protect my personal privacy.	3.7346	0.89020
I am not worried about the security of my MySiswa Debit i-Card.	3.1049	1.25904
Intention to use		
I would use my MySiswa Debit i-Card for any purchase in the future.	3.7222	1.01081
I would use MySiswa Debit i-Card for online shopping.	3.6235	1.05745
I would use MySiswa Debit i-Card for physical/point of sale purchases.	3.7037	0.98365
I intend to use MySiswa Debit i-Card to make payments for purchases in the near future shall I have access to it.	3.7778	1.00310
I intend to use other kinds of MySiswa Debit i-Card services in the future.	3.7407	0.94937
I intend to use MySiswa Debit i-Card more frequently in the future.	3.6111	1.02908
I intend to try out latest MySiswa Debit i-Card services in the future.	3.7716	0.96700
I intend to recommend MySiswa Debit i-Card to my family and friends in the future.	3.6420	1.02525
Actual usage behavior		
I use MySiswa Debit more often than others.	3.1728	1.15064
I am currently using and will continue to use MySiswa Debit.	3.5556	0.95228
I make online transactions mainly via MySiswa Debit.	3.3951	1.09973
I have considerable experience using MySiswa Debit.	3.3580	1.03730
I have considerable experience in doing payments via debit cards over the internet.	3.6111	1.08204
I have been using MySiswa Debit i-Card for quite sometimes.	3.3457	1.13838
I frequently benefited from using MySiswa Debit i-Card.	3.4630	1.06403
Overall, I made many transactions using MySiswa Debit i-Card.	3.3889	1.10476

Correlation analysis

The correlation analysis (*Table 3*) revealed significant positive relationships among perceived security risk, intention to use, and actual usage behavior of RHB MySiswa Debit i-Card. Higher perceptions of security were associated with stronger intentions to use, and stronger intentions were linked to higher actual usage behavior. Additionally,

perceived security risk also showed a direct positive correlation with actual usage behavior, although the relationship was weaker compared to its correlation with intention to use. These results provide empirical support for the study’s proposed hypotheses. Specifically, the findings confirm that perceived security risk is significantly related to both intentions to use and actual usage behavior (supporting H1 and H2), and that intention to use is significantly related to actual usage behavior (supporting H3). The strength and significance of these relationships suggest that perceived security risks play a critical role in shaping students’ adoption behavior, as outlined in the study framework.

Table 3. Correlation analysis.

Variables	Perceived risk	Intention to use	Actual usage behavior
Perceived Risk	1	.569**	.484**
Intention to Use	.569**	1	.733**
Actual Usage Behavior	.484**	.733**	1
Sig. (2-tailed)	.000	.000	.000
N	162	162	162

Note: ** Correlation is significant at the 0.01 level (2-tailed).

Mediation analysis

According to Baron and Kenny (1986), a variable can function as a mediator in the causal sequence if regression analyses reveal statistically significant relationships at the first three levels under the following conditions (refer Mediation Diagram in Figure 2: (1) The independent variable significantly predicts the dependent variable ($X \rightarrow Y$); (2) The independent variable significantly predicts the mediator ($X \rightarrow M$), where the mediator acts as a dependent variable; (3) The mediator significantly predicts the dependent variable while controlling for X ($M \rightarrow Y$). If any of these relationships are not significant, mediation is unlikely; (4) Mediation is assessed as full or partial. Full mediation occurs when X no longer significantly affects Y after controlling for M. Partial mediation occurs when X still affects Y but the effect is reduced. The smaller the coefficient “c,” the greater the mediator’s effect. Table 4 shows that the independent variable (Perceived Risk) is a significant predictor of the dependent variable (Actual Usage) ($t = 7.001, p < 0.05$). In other words, “c” (unstandardized coefficient = 0.607) is statistically significant. The Table 4 shows that the independent variable (Perceived Risk) is a significant predictor of the mediating variable (Intention to Use) ($t = 8.762, p < 0.05$). That is, “a” (unstandardized coefficient = 0.669) is statistically significant. The Table 4 shows that while controlling for the independent variable (Perceived Risk), the mediating variable (Intention to Use) is a significant predictor of the dependent variable (Actual Usage Behavior) ($t = 10.368, p < 0.05$). That is, “b” (unstandardized coefficient = 0.721) is statistically significant.

Table 4. Regression analysis of perceived risk and intention to use on actual usage behavior.

Model	Predictor	Dependent Variable	B	Std. Error	β	t	Sig.
<i>Perceived Risk (X) \rightarrow Actual Usage Behavior (Y)</i>							
Model 1	Constant	Actual Usage Behavior	1.299	0.307	–	4.232	.000
	Perceived Risk (X)	Actual Usage Behavior	0.607	0.087	0.484	7.001	.000
<i>Perceived Risk (X) \rightarrow Intention to Use (M)</i>							
Model 2	Constant	Intention to Use	1.359	0.270	–	5.030	.000
	Perceived Risk (X)	Intention to Use (M)	0.669	0.076	0.569	8.762	.000
<i>Perceived Risk (X) \rightarrow Actual Usage Behavior (Y); Intention to Use (M) \rightarrow Actual Usage Behavior (Y)</i>							
Model 3	Constant	Actual Usage Behavior	0.318	0.256	–	1.244	.215

Perceived Risk (X)	Actual Usage Behavior	0.124	0.082	0.099	1.524	.130
Intention to Use (M)	Actual Usage Behavior	0.721	0.070	0.676	10.368	.000

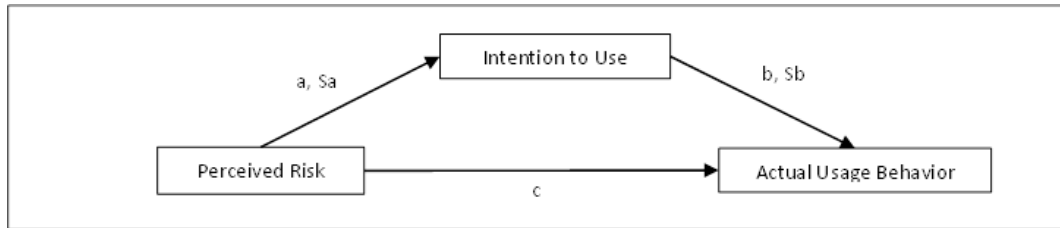


Figure 2. Mediation diagram.

Sobel test

Sobel test was utilized to examine if Intention to Use mediated the relationship between Perceived Risk and Actual Usage Behavior (refer Figure 3 Sobel Test Result). First, results of simple linear regression show that Perceived Risk was a statistically significant predictor of Actual Usage Behavior ($b = 0.607$, $\beta = 0.484$, $t = 7.001$, $p < 0.05$). Next, when the mediator, Intention to Use, was entered in the regression analysis, Perceived Risk then is not a significant predictor of Actual Usage Behavior ($b = 0.124$, $\beta = 0.099$, $t = 1.524$, $p > .05$). On the other hand, the mediator, Intention to Use, emerged as a significant predictor of Actual Usage Behavior ($b = 0.721$, $\beta = 0.676$, $t = 10.368$, $p < .05$). These results suggest Intention to Use fully mediates the relationship between Perceived Risk and Actual Usage Behavior. To further investigate the mediator, the Sobel test was utilized. The result confirmed that Intention to Use significantly mediates the relationship between Perceived Risk and Actual Usage Behavior ($Z = 6.692$, $p < .05$). The mediation results suggest that students’ perceptions of security primarily shape their behavior by first influencing their intention, which in turn drives actual usage. These findings confirm the study’s mediation hypothesis (H4), supporting the Theory of Planned Behavior’s assertion that behavioral intention serves as the proximal predictor of actual behavior.

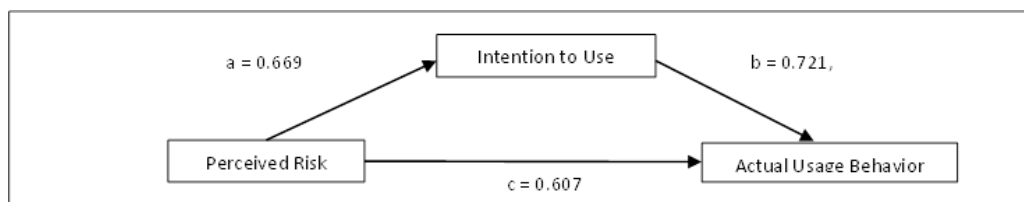


Figure 3. Sobel test result.

This study explored the influence of perceived security risk on intention to use and actual usage behavior of RHB MySiswa Debit i-Card among UiTM Puncak Alam students, grounded in the Theory of Planned Behavior (TPB). Empirical results confirmed that perceived security risk significantly predicted both intentions to use and actual usage behavior (supporting H1 and H2). Intention to use, in turn, significantly influenced actual usage behavior (supporting H3), and mediated the relationship between perceived security risk and actual usage behavior (supporting H4). These results affirm that security perceptions shape behavior primarily through motivational intention, consistent with TPB’s postulate that intention is a proximal determinant of action (Ajzen, 1991). The positive links between perceived security risks and intention to use align with international and Malaysian findings. Gupta et al (2023) as well as Ali

et al. (2021) similarly documented that strong security perceptions boost user intention and uptake in financial technology, or FinTech (computer programs and other technology used to support or enable banking and financial services) contexts. Within Malaysia, Bakar et al. (2024) and Seng et al. (2023) reported that students' trust and security beliefs substantially influence e-payment adoption. This study results reinforce these patterns, specifically within the MySiswa Debit i-Card study framework, by showing that even when students find the system convenient or endorsed by their institution, they still hesitate if security doubts persist. This underscores that convenience must be complemented by robust security assurance to convert interest into usage behavior.

Moreover, the mediation effect of intention to use enhances the TPB application in this domain. TPB suggests that attitudes (reflected by perceived security risk in this research), along with subjective norms and perceived behavioral control, shape intention and subsequently behavior (Ajzen, 1991). Usman et al. (2025) similarly found that intention to use serves as a crucial conduit between attitudes and usage in Malaysian e-payment adoption. This study findings extend this insight by specifying that security-induced attitude changes operate through intention to yield usage; particularly relevant in campus environments where institutional support can amplify or moderate these relationships.

Conclusion

By situating the study within TPB and emphasising perceived security as an antecedent attitude construct, this research enriches both TPB and technology acceptance literature. It demonstrates the salience of security perceptions in shaping attitudes and how those attitudes translate into both intentions to use and actual usage behavior among young, educated users. The mediation result adds nuance to TPB by illustrating a clear pathway whereby security perceptions influence behaviour indirectly via motivation. This helps bridge TPB with FinTech-specific variables, offering conceptual refinement for future theoretical integration. For policy-makers and university administrators, the findings suggest that promoting cashless payment systems among students requires more than launching the product. It necessitates robust security messaging and trust-building. Campaigns should transparently communicate encryption standards, fraud protection policies, and user support channels to strengthen security perceptions. Peer-led awareness programs and testimonials from early adopters may further bolster confidence. Moreover, ensuring readily available technical support and visible security cues (such as alerts, transaction notifications) can enhance perceived behavioral control, which TPB suggests is crucial for intention formation and follow-through.

Several limitations must be noted. First, the cross-sectional design precludes causal inference; longitudinal study would better capture how perceptions, intentions, and usage evolve over time. Second, the use of convenience sampling at a single campus limits generalizability. Other campuses or student demographics may exhibit different dynamics. Third, while perceived security perception was central, researcher didn't quantitatively measure subjective norms or perceived behavioral control, TPB's other two constructs which may also play significant roles. Finally, self-reported usage can be prone to bias; future research could incorporate transaction logs or system analytics for objective measures. Future work should adopt longitudinal or experimental designs to

track how interventions (such as security education campaigns) influence security perception, intention, and usage over time. Expanding the sample to multiple universities and including demographic subgroups (including international students) could enhance external validity. Researchers might also integrate full TPB constructs (subjective norms, perceived behavioral control) and explore moderating influences such as prior e-payment experience or technological familiarity. Finally, including behavioral economics insights such as incentives, could identify ways to bridge the remaining intention-behavior gaps. In conclusion, this study confirms that perceived security risk significantly shapes UiTM students' intention to use and actual usage behavior of MySiswa Debit i-Card, with intention to use serving as a key mediator. Strengthening security perceptions and fostering strong adoption intentions are essential strategies for promoting sustained e-payment usage in higher education contexts.

Acknowledgement

This research is self-funded.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

- [1] Ajzen, I. (1991): The theory of planned behavior. – *Organizational Behavior and Human Decision Processes* 50(2): 179-211.
- [2] Ali, M., Raza, S.A., Khamis, B., Puah, C.H., Amin, H. (2021): How perceived risk, benefit and trust determine user Fintech adoption: a new dimension for Islamic finance. – *Foresight* 23(4): 403-420.
- [3] Bakar, N.A., Rosbi, S., Norizan, S.N., Yusoff, M.M., Ali, M.A. (2024): Factors influencing customer acceptance towards electronic wallets (E-Wallets) in Malaysia: Perceived security as focus variable. – *International Journal of Business and Technology Management* 6(1): 399-412.
- [4] Baron, R.M., Kenny, D.A. (1986): The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. – *Journal of Personality and Social Psychology* 51(6): 1173-1182.
- [5] Fishbein, M., Ajzen, I. (1977): *Belief, attitude, intention, and behavior: An introduction to theory and research.* – Addison-Wesley Publishing Company 578p.
- [6] Gupta, K., Wajid, A., Gaur, D. (2023): Determinants of continuous intention to use FinTech services: the moderating role of COVID-19. – *Journal of Financial Services Marketing* 29: 517-538
- [7] Lai, P.C., Liew, E.J. (2021): Towards a cashless society: The effects of perceived convenience and security on gamified mobile payment platform adoption. – *Australasian Journal of Information Systems* 25: 26p.
- [8] Liu, K., Li, Q., Tao, D. (2025): Determinants of continuous use intention of smart healthcare services: Evidence from a commitment-trust theory perspective. – *Health Informatics Journal* 31(3): 17p.
- [9] Seng, N.D., Ibrahim, N.F., Yin, L.S., Maiyus, M.B. (2023): An empirical study on acceptance of e-wallet among malaysian university students. – *International Journal of Academic Research in Business and Social Sciences* 13(12): 1099-1112.

- [10] Sidek, N.Z.M., Anuar, A., Othman, M.H., Ahmarofi, A.A. (2024): CASHLESS PAYMENT HESITANCY AMONGST UNIVERSITY STUDENTS. – *Management* 9(36): 134-148.
- [11] Tian, Y., Chan, T.J., Fadzilah, A.H.H., Ng, M.L., Zainudin, S.S.S., Jalis, F.M.M. (2024): Factors influencing malaysian university students' intention to use online payment systems: an application of the extended perceived value theory. – *Journal of Logistics, Informatics and Service Science* 11(9): 19-36.
- [12] Usman, B., Rianto, H., Aujirapongpan, S. (2025): Digital payment adoption: A revisit on the theory of planned behavior among the young generation. – *International Journal of Information Management Data Insights* 5(1): 17p.
- [13] Waliullah, M., George, M.Z.H., 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. – *Applied Journal of Advanced Technology and Engineering Science (AJATES)* 1(1): 226-257.