Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# EXPLORING DIGITAL WALLET CONTINUANCE: INSTRUMENT DEVELOPMENT BASED ON TASK-TECHNOLOGY FIT THEORY AND PRIVACY CALCULUS THEORY

**ADIBAH AHMAD[1], RAHAYU AHMAD[2], SYAHIDA HASSAN[3]**

[1]PhD Candidate, School of Computing, Universiti Utara Malaysia, Malaysia

[2]Associate Professor, School of Computing, Universiti Utara Malaysia, Malaysia

[3]Senior Lecturer, School of Computing, Universiti Utara Malaysia, Malaysia

E-mail: [1]adibah6122@gmail.com, [2]rahayu@uum.edu.my, [3]syahida@uum.edu.my,

**ABSTRACT**

With the growing adoption of digital wallets, increasing attention has been directed toward the challenges associated with their continued use, particularly regarding security and user privacy. This study extends prior research by integrating concerns related to technology fit and privacy through the lens of Task-Technology Fit (TTF) Theory and Privacy Calculus Theory, which serve as the study's theoretical foundations. To address emerging factors influencing the sustained use of digital wallets, new constructs have been proposed. The measurement instruments employed in this study consist of both adapted items from existing literature and newly developed items tailored to the proposed constructs. The development process included expert evaluations to ensure content validity, involving five Information Systems scholars who assessed the relevance and clarity of the items. A pilot test was conducted involving 38 university students who participated through an online survey. Validity and reliability testing were conducted using SPSS software. Results from validity and reliability analyses demonstrate robust measurement properties, indicating that the items effectively capture the intended constructs. A subsequent pilot test further confirmed the appropriateness of the instruments for use in future empirical research.

**Keywords:** *Cashless, E-Wallet, TTF, PCT, Continuous Use*

## 1. INTRODUCTION

Since the introduction of debit cards in the late 1960s, cashless payment methods have undergone significant transformation, consequently influencing payment practices. The evolution of payment systems—from debit cards to credit cards, followed by online banking, mobile applications, and Near Field Communication (NFC) technology—has revolutionized cashless transactions. This revolution has led to the emergence of digital wallets, which serve as repositories for payment method information, coupons, gift cards, and other financial data. Digital wallets enable users to store various forms of payment-related information in one accessible location while eliminating the need to carry physical items [1], [2].

Furthermore, the emergence of digital wallets has contributed to a shift in cashless payment patterns. Generally, instead of carrying multiple physical cards—such as credit and debit cards—users only need to carry a digital wallet installed on their smartphones. The convenience of use has also contributed to the increasing number of digital wallet users [3]. Globally, it is estimated that there will be more than 5.3 billion digital wallet users by 2026 [4]. This statistic indicates a positive trend in the acceptance of digital wallets.

In parallel with the growing number of digital wallet users, associated issues have also gained increased attention. Security concerns, trust, interoperability, and integration with existing systems are among the key challenges facing digital wallets [5].

Given this reality, the integration of technological efficiency and security in digital payment systems is becoming increasingly vital. Accordingly, this study aims to examine the relationship between digital wallet technology's effectiveness and its privacy features in continuously using it by exploring the instruments involve in the study.

The skeleton of this paper as follow: (1) introduction, (2) literature review, (3) methodology, (4) findings, (5) discussion, (6) conclusion, (7) implications, (8) limitation, and (9) recommendation.

## 2. LITERATURE REVIEW

This section discusses about the literature related to the study. It involves task-technology theory (TTF), privacy calculus theory (PCT), and continuous use of digital wallet.

### 2.1 Task-Technology Fit (TTF) Theory

Task-Technology Fit (TTF) Theory explains the alignment between a technology's capabilities and the tasks it is designed to support. This theory was introduced by Goodhue and Thompson in 1995. Unlike earlier studies, which primarily focused on the antecedents of usage and user intention, TTF was the first framework to examine the post-adoption phase of technology utilization [6]. Since its inception, numerous studies have sought to refine and extend the original theory to accommodate advancements in technology and evolving work environments.

In addition to investigating the direct relationship between task and technology performance, prior research has explored various contextual factors that influence the degree to which a technology is suited to its intended purpose. These contextual factors include individual aspects, such as user experience, skills, and preferences, as well as organizational factors, such as culture, structure, and processes. Furthermore, TTF has been integrated with other theoretical frameworks, demonstrating that it is neither a static nor a unidimensional concept, but rather one influenced by various dynamic factors. The emergence of new technologies—such as artificial intelligence (AI) and social technologies—has further shaped the application of TTF. Additionally, the increasing prominence of these technologies has underscored the importance of user experience and technological adaptability as critical determinants of technological fit.

Originally, the core components of TTF Theory consisted of task characteristics, technology characteristics, task-technology fit, utilization, and performance. However, in the current era of digitalization, relying solely on task and technology characteristics to assess technological functionality is insufficient, as security concerns have become a widely recognized issue. The security of a technology is crucial in ensuring its suitability for continued use. Thus, there is a growing need to revisit and expand TTF Theory by introducing new components that align with the digital era, namely data security characteristics and application characteristics.

Beyond technological fit, concerns related to digital technology have also gained significant attention. One of the most pressing issues in this domain is privacy, and digital wallets are no exception [7]. Privacy-related challenges, such as data breaches, insecure authentication mechanisms, and vulnerabilities in third-party services, pose critical risks to digital wallet security [8], [9], [10], [11].

Given the increasing significance of privacy concerns, this study seeks to explore the interplay between the technological fit and privacy aspects of digital wallets by integrating Task-Technology Fit Theory with Privacy Calculus Theory. While TTF emphasizes the alignment between users' payment-related tasks and the functionalities provided by digital wallets, Privacy Calculus Theory complements this perspective by examining how users weigh perceived benefits against privacy concerns.

This paper focuses on the continuous use of digital wallets. The following sections elaborate on the core and newly introduced constructs underpinning Task-Technology Fit Theory, namely task characteristics, technology characteristics, data security characteristics (new), application characteristics (new), task-technology fit, and financial transaction performance.

#### 2.1.1 Task characteristics

Tasks are broadly defined as actions performed by individuals to transform inputs into outputs. A task can be conceptualized as a specific piece of work executed through a series of actions to achieve a particular goal [6], [12], [13]. Task characteristics refer to the distinct attributes and requirements of tasks that influence the extent to which technology can effectively support them, thereby enhancing performance and utilization [14], [15].

According to Oliveira, Faria, Thomas and Popovič [16], task characteristics represent a fundamental construct in explaining task-technology fit. Empirical studies have demonstrated that task characteristics positively impact task-technology fit [17], [18], [19]. In the context of financial technology, task characteristics have also been identified as significantly influencing task-technology fit. For instance, Tam and Oliveira [20] found that the task characteristics associated with

mobile banking positively affect task-technology fit. Similarly, Baabdullah, Alalwan, Rana, Patil, and Dwivedi [21] reported that task characteristics exert a positive influence on task-technology fit among mobile banking users.

Within the realm of digital wallets, task characteristics can be operationalized as the circumstances, complexity, and requirements associated with users' interactions with digital wallets, including activities such as making payments, transferring funds, and tracking expenses. These characteristics determine whether digital wallet-related tasks are perceived as straightforward or complex.

**2.1.2 Technology characteristics**

Technology characteristics refer to the inherent attributes and functionalities of a technological system [6]. Previous studies have demonstrated that technology characteristics positively influence task-technology fit [22], [18]. In the context of digital wallets, technology characteristics refer to the features and functionalities embedded in digital wallet systems. This including processing speed, integration with other platforms or applications, compatibility with various devices, and other performance-related attributes [23].

User interface, Near Field Communication (NFC), QR code, and two-factors authentication are among the technology characteristics involved in digital wallet [24], [25]. In research related to financial technology, technology characteristics have also been found to significantly impact task-technology fit. Specifically, the features and capabilities of mobile banking have been shown to positively affect task-technology fit [26], [21], [16], [27].

**2.1.3 Data security characteristics**

Data security is defined as the process of safeguarding data from loss, modification, or unauthorized access throughout its lifecycle [28]. In the context of mobile applications, data security pertains to the protection of sensitive information stored locally on devices and within system databases, ensuring resilience against unauthorized access, security breaches, and data loss [29], [30], [31].

From the perspective of digital wallets, data security characteristics can be operationalized as the measures implemented to protect users' sensitive information. These measures include multi-factor authentication, privacy safeguards, encryption protocols, and other security mechanisms designed to enhance data protection [32], [33], [34].

**2.1.4 Application characteristics**

In the context of mobile applications, application characteristics refer to the distinct features and qualities that define how mobile apps operate and are perceived by users [35], [36], [37], [38]. In the specific context of digital wallets, application characteristics can be operationalized as the essential features and functionalities of digital wallet applications, including availability, responsiveness, personalization options, user-friendliness, and other relevant attributes [39], [40], [41].

The quality of application characteristics in digital wallets directly influences user experience and adoption. When users perceive an application as efficient, intuitive, and responsive, their satisfaction with its functionalities increases, subsequently enhancing their intention to continue using the digital wallet in the future [42], [43], [44].

**2.1.5 Task-technology fit**

Task-technology fit is defined as the degree to which technological capabilities align with task requirements [45]. In the context of digital wallets, task-technology fit refers to the extent to which a digital wallet's features correspond to users' functional needs [46]. The effectiveness of a digital wallet plays a crucial role in sustaining its quality and usability. Users are more likely to continue using a digital wallet when its technological capabilities adequately support the tasks they need to perform [47], [48].

**2.1.6 Financial transaction performance**

In general, financial transaction performance refers to the efficiency, accuracy, and reliability of financial transactions within an organization or system. In the context of financial technology (FinTech), financial transaction performance pertains to the effectiveness and efficiency of executing financial transactions, facilitated by technological innovations [49], [50].

Within the domain of digital wallets, financial transaction performance can be defined as the extent to which digital wallets successfully facilitate payments and money transfers with respect to speed, accuracy, and reliability [34], [51].

## 2.2 Privacy Calculus Theory (PCT)

Privacy Calculus Theory was introduced by Laufer and Wolfe in 1977. According to their framework, individuals make decisions regarding the disclosure of personal information by rationally weighing the costs and benefits associated with such actions [52]. However, Culnan and Armstrong [53] were among the pioneering scholars who utilized the term "privacy calculus" to describe the process of balancing perceived benefits and risks, particularly

in the context of personal information disclosure in online settings.

Since the introduction of this theory, numerous studies have examined the privacy trade-off, particularly in digital environments, as technological advancements continue to reshape data-sharing practices. Research has explored this privacy trade-off across various domains, including e-commerce, social media, online learning, and mobile payment systems [54], [55], [56], [57].

In the context of digital wallets, this theory has been instrumental in analyzing how users navigate the balance between convenience and privacy-risks. Privacy trade-offs issues often arise due to data collection practices, transaction tracking, and third-party access, which may lead to potential privacy vulnerabilities [58], [59].

#### 2.2.1 Benefits of information disclosure

The benefits of information disclosure refer to the advantages individuals receive when they provide their personal information to a party or system. These benefits can be categorized into extrinsic and intrinsic rewards. Extrinsic benefits encompass external incentives that individuals gain from sharing their personal information, such as time efficiency, financial savings, promotional incentives, and other tangible rewards. Conversely, intrinsic benefits refer to internal rewards derived from information disclosure, including enjoyment, self-esteem enhancement, and personal satisfaction.

In the context of digital wallets, providing personal information to service providers enables users to access various benefits offered by these platforms, such as discount promotions, loyalty rewards, point accumulation, and a seamless user experience, all of which contribute to greater satisfaction and enjoyment. When users perceive that the benefits of disclosing their information outweigh potential risks, they are more likely to engage in information-sharing behaviors [60], [61].

#### 2.2.2 Risks of information disclosure

The risks associated with information disclosure refer to the potential disadvantages individuals may encounter when sharing their personal data with entities or systems. In the context of digital wallets, these risks include data breaches, insecure authentication mechanisms, and vulnerabilities in third-party services, all of which pose significant security concerns for users. When users perceive that the risks associated with digital wallet usage outweigh the benefits, they may be reluctant to adopt or continue using e-wallet services [62], [63].

#### 2.2.3 Intention to disclose personal information

In general, the intention to disclose personal information refers to an individual's willingness to share their personal data with another party or organization. This intention is often influenced by various psychological and contextual factors, including trust, transparency, perceived benefits, attitudes, and other relevant considerations [64], [65], [66].

In the context of digital wallets, the intention to disclose personal information specifically refers to a consumer's willingness to share their personal data with a digital wallet service provider to access and utilize the platform's services.

### 2.3 Continuous Use of Digital Wallet

Generally, continuous use refers to the ongoing utilization of a product, service, or system over time. In the context of digital wallets, continuous use denotes users' recurring engagement with the platform for financial transactions and related activities. The decision to continue using a digital wallet is influenced by several factors, including user satisfaction, perceived benefits, security perceptions, perceived risks, and perceived usefulness [67], [68], [69], [70].

In addition, the sustained use of digital wallets is shaped by the degree to which users' expectations align with actual performance, further reinforcing engagement with the technology [68].

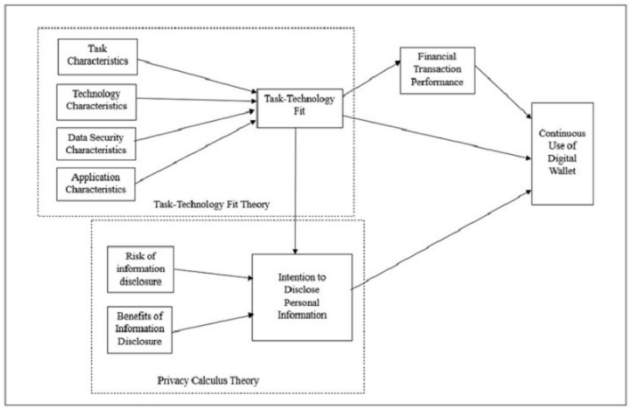


*Figure 1: Conceptual Model of the Study*

## 3. METHODOLOGY

This section discusses about the methodology involved in the study. It involves instrument, validity, reliability, exploratory factor analysis (EFA), and pilot study.

### 3.1 Instrument

The instruments involved in this study were primarily adapted and adopted from previous research related to Task-Technology Fit Theory, Privacy Calculus Theory, Digital Financial Literacy, Government Incentives, and Continuous Use of Digital Wallet as shown in Table 1. Additionally, several new items were developed to better align with the specific context of the study. The questionnaire was divided into four sections. The first section captured the demographic information of the respondents. The second section included items based on the Task-Technology Fit Theory and Privacy Calculus Theory. The third section addressed the dependent variable, namely the Continuous Use of Digital Wallet. The fourth section comprised items related to the two moderating variables: Digital Financial Literacy and Government Incentives.

*TABLE 1: QUESTIONNAIRE ITEMS*

| Construct | Number of Items | Reference |
|---|---|---|
| Task Characteristics (TAC) | 3 | Zhou, Lu & Wang (2010) |
| Technology Characteristics (TEC) | 3 | Zhou, Lu & Wang (2010) |
| Data Security Characteristics (DSC) | 6 | Three items from Seberger, Shklovski, Swiatek & Patil (2022); three items newly proposed |
| Application Characteristics (AppC) | 3 | European Central Bank (2023) |
| Task-Technology Fit (TTF) | 4 | Zhou, Lu & Wang (2010) |
| Financial Transaction Performance (FTP) | 5 | El-Gayar, Deokar & Wills (2010) |
| Benefits of Information Disclosure (BEN) | 3 | Wang, Duong & Chen (2016) |
| Risks of Information Disclosure (RISK) | 3 | Wang, Duong & Chen (2016) |
| Intention to Disclose Personal Information (INT) | 3 | Wang, Duong & Chen (2016) Dinev & Hart (2006) |
| Continuous Use of Digital Wallet (CUDW) | 4 | Rahi & Ghani (2021) |

### 3.2 Validity

Validity refers to the extent to which a concept is accurately measured in a quantitative study and the validity of a research study refers to how well the results among the study participants represent true findings among similar individuals outside the study [71], [72].

#### 3.2.1 Content validity

Content validity refers to the degree to which an assessment instrument is relevant to and representative of the targeted construct it is intended to measure [73]. Content validation provides evidence regarding the validation of an instrument by evaluating the degree to which it accurately measures the targeted construct [74]. This process enables the instrument to support meaningful and appropriate inferences and/or decisions based on the instrument scores given, in accordance with the assessment's purpose [75], [76], [73]. An expert panel typically consists of subject matter experts and professionals with experienced in survey design, data collection, coding, and data analysis [77], [78]. Accordingly, five expert reviewers were selected to evaluate all the items within the constructs.

The five expert reviewers, each with a background in Information System, were asked to access all the construct items by assigning a score of 1,2, or 3, where 1 = poorly match (the item is unrelated to the study and should be removed), 2 = moderately match (the item is relevant but requires revision to better align with the study), and 3 = perfectly matched (the item is highly relevant to the study). In addition to scoring, the expert reviewers were also invited to provide additional relevant comments regarding the items under review.

### 3.3 Reliability

Reliability refers to the consistency of a measurement instrument [79]. According to Price, Jhangiani and Chiang [79], there are three types of consistency: over time (test-retest reliability), across items (internal consistency), and across different researchers (inter-rater reliability). The internal consistency pertains to the extent to which respondents consistently answer similar items within a multi-item scale [79]. The test scores are considered reliable if they remain consistent across (a) different testing occasions, (b) different editions of the test containing different questions or problems designed to measure the same general skills or types of knowledge, and (c) different scoring of the test taker's responses, by different raters [80]. According to Hair, Babin and Anderson [81], an instrument's reliability is defined as its capacity to consistently

yield trustworthy results across measurement executions. Moreover, to access the instrument's internal consistency, the Cronbach's alpha value was computed for every item [82], [83]. Sekaran and Bougie [85] noted that a Cronbach's alpha value is considered good if it exceeds 0.80, acceptable if it falls between 0.60 and 0.70, and poor if it below 0.60.

### 3.4 Exploratory factor analysis (EFA)

Exploratory factor analysis (EFA) is a statistical technique used to identify items that specifically represent the underlying construct measured by a questionnaire [85], [83]. According to Hair et al. [81] and Mindrila [85], EFA can be conducted with a minimum sample size of 100 respondents. Prior to performing EFA, the Kaiser-Meyer-Olkin sample adequacy test (KMO) and the Bartlett's Test of Sphericity should be conducted to access the suitability of the dataset for factor analysis. These tests evaluate whether the data meet the assumptions required for factor extraction. In addition, for a factor to be considered valid, its eigenvalue – which reflects the amount of variance explained by each component – must be at least one. The threshold values and relevant sources for these criteria are summarized in Table 2.

*TABLE 2: FACTOR ANALYSIS CRITERIA CUT-OFF*

| The Criterion | Satisfactory Level |
|---|---|
| KMO | > 0.5 |
| Bartlett's Test of Sphericity | < 0.05 |
| Eigenvalue | > 1.0 |
| Factor Loading | > 0.4 |

### 3.5 Pilot test

A pilot study is a preliminary investigation conducted to evaluate various aspects of the approaches intended for a more extensive, rigorous, or confirmatory study [86]. The pilot study primary objective is not to address specific research questions but rather to ensure that researchers do not commence a large-scale study without adequate understanding of proposed methods, and it also serves to prevent potential critical flaws in a study that may be costly in in terms of time and resources [87]. Additionally, researchers also use pilot study to access the effectiveness and feasibility of the intended research techniques and procedures [87].

In this study, the pilot study was conducted via an online questionnaire, which was distributed through an official class group chat. The questionnaire was distributed among higher education students, as this study focused on individuals aged 18 years and above. To be eligible, participants were required to be users of digital wallet. A total of 38 students expressed interest and participated in the pilot study.

## 4. Findings

This section discusses about the finding of the study. It involves results of validity, reliability, and exploratory factor analysis (EFA).

### 4.1 Validity result

Based on the evaluation scores and comments provided by the five experts reviewers, the instruments were revised to enhance the study's accuracy and significance. Table 3 presents the feedback from the expert reviewers. the expert reviewers' feedback. However, not all constructs are included in the table as several received uniformly positive feedback. Only selected items that received substantial commentary are presented in Table 3. All items within the construct of application characteristics, financial transaction performance, and intention to disclose personal information were unanimously approved by the expert reviewers. Therefore, these constructs are excluded from the table.

*TABLE 3: REVIEWERS FEEDBACK AND ITEMS CORRECTION*

| Construct | Original Item | Feedback | Corrected Item |
|---|---|---|---|
| Task Characteristics | I need to pay my purchasing real-time. | ER4: Need to rephase to ease understandin g | I need to pay my purchasing on the spot. |
| Technology Characteristics | I can count on digital wallet to be "up" and available when I need it. | ER4: The choice of word. | My digital wallet is often "up" and available when I need it. |
| Data Security Characteristics | Control of personal information lies at the heart of mobile app users' privacy control. | ER3: Too general. | My digital wallet enables me to control my personal information through the privacy control settings. |
| Task-Technology Fit | In helping complete my payment tasks, the functions of digital wallet are enough. | ER1: Consider replacing the word "enough" with sufficient and rephrase the whole sentence. | The functions of my digital wallet are able to complete my payment tasks. |
| Benefit of Information Disclosure | The digital wallet application provides personalized | ER4: Ambiguous statement. | My digital wallet application provides offers and |

| | | | |
|---|---|---|---|
| | offers tailored to the context of individual activity. | | promotions based on my previous activities and transactions. |
| Risk of Information Disclosure | The potential loss in disclosing my personal information to digital wallet would be high. | Rephrase to make it clearer. | Disclosing personal information to my digital wallet could result in a high potential loss, such as the theft of personal information. |
| Continuous Use of Digital Wallet | In future, because of need, I would like to continue use of digital wallet even though digital wallet facing data breach issues. | EX2: Not that suitable. Maybe it is good to rephrase. | In the future, because of necessity, I would like to continue using a digital wallet, even though it may face data leakage issues. |

*(EX = Expert)*

Table 4 presents the Content Validity Index (CVI) for all items included in this study. Based on the results shown in the Table 4, it can be concluded that all expert reviewers agree with the proposed items, although minor revisions were recommended. The Scale-Level Content Validity Index (S-CVI) scores range from 0.80 to 1.00, which is considered acceptable according to established benchmarks [88], [89], [90], [91].

*TABLE 4: CONTENT VALIDITY INDEX*

| Item | EX 1 | EX 2 | EX 3 | EX 4 | Numbers of Relevance | I-CVI | Agree-ment |
|---|---|---|---|---|---|---|---|
| TAC1 | 2 | 2 | 2 | 2 | 5 | 1 | Agree |
| TAC2 | 2 | 2 | 2 | 3 | 5 | 1 | Agree |
| TAC3 | 2 | 3 | 2 | 3 | 5 | 1 | Agree |
| | | | | | S-CVI | 1 | |
| TEC1 | 3 | 3 | 1 | 2 | 4 | 0.8 | Agree |
| TEC2 | 2 | 3 | 1 | 3 | 4 | 0.8 | Agree |
| TEC3 | 3 | 3 | 1 | 3 | 4 | 0.8 | Agree |
| | | | | | S-CVI | 0.8 | |
| DSC1 | 2 | 3 | 3 | 2 | 5 | 1 | Agree |
| DSC2 | 2 | 3 | 3 | 3 | 5 | 1 | Agree |
| DSC3 | 3 | 3 | 3 | 2 | 5 | 1 | Agree |
| DSC4 | 3 | 3 | 3 | 2 | 5 | 1 | Agree |
| DSC5 | 3 | 2 | 2 | 2 | 5 | 1 | Agree |
| DSC6 | 3 | 3 | 2 | 2 | 5 | 1 | Agree |
| | | | | | S-CVI | 1 | |
| AppC1 | 3 | 3 | 3 | 3 | 5 | 1 | Agree |
| AppC2 | 3 | 3 | 3 | 3 | 5 | 1 | Agree |
| AppC3 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| | | | | | S-CVI | 1 | |
| TTF1 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| TTF2 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| TTF3 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| TTF4 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| | | | | | S-CVI | 1 | |
| FTP1 | 3 | 3 | 3 | 3 | 5 | 1 | Agree |
| FTP2 | 3 | 3 | 3 | 3 | 5 | 1 | Agree |
| FTP3 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| | | | | | S-CVI | 1 | |
| BEN1 | 3 | 3 | 3 | 2 | 5 | 1 | Agree |
| BEN2 | 3 | 3 | 3 | 2 | 5 | 1 | Agree |
| BEN3 | 3 | 3 | 1 | 2 | 4 | 0.8 | Agree |
| | | | | | S-CVI | 0.93 | |
| RISK1 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| RISK2 | 2 | 3 | 2 | 3 | 5 | 1 | Agree |
| RISK3 | 2 | 3 | 2 | 3 | 5 | 1 | Agree |
| | | | | | S-CVI | 1 | |
| INT1 | 3 | 2 | 3 | 3 | 5 | 1 | Agree |
| INT2 | 3 | 2 | 3 | 3 | 5 | 1 | Agree |
| INT3 | 3 | 2 | 1 | 3 | 4 | 0.8 | Agree |
| | | | | | S-CVI | 0.93 | |
| CONT1 | 3 | 3 | 3 | 3 | 5 | 1 | Agree |
| CONT2 | 3 | 3 | 1 | 3 | 4 | 0.8 | Agree |
| CONT3 | 3 | 3 | 2 | 3 | 5 | 1 | Agree |
| CONT4 | 2 | 3 | 2 | 2 | 5 | 1 | Agree |
| | | | | | S-CVI | 0.95 | |

(1 = Poorly match – unrelated and need to remove, 2 = Moderately match - relevant but need to review, 3 = Perfectly match – highly relevant)

## 4.2 Reliability

The reliability analysis was also performed using SPSS version 29. Table 5 reports the Cronbach's alpha values for all items included in the study. As shown, the Cronbach's alpha for the overall items exceeds 0.70, demonstrating an acceptable level of internal consistency. The table further provides a comparison between the original Cronbach's alpha values and the values obtained when individual items were deleted. The "Cronbach's alpha if item is deleted" analysis suggests that the reliability coefficient would improve slightly if certain items were removed.

*TABLE 5: RELIABILITY TEST*

| Construct | Number of items | Original Cronbach's Alpha | Cronbach's Alpha if item is deleted | Items to be deleted |
|---|---|---|---|---|
| Task Characteristics | 3 | .803 | .803 | 0 |
| Technology Characteristics | 3 | .730 | .875 | TEC1 |
| Data Security Characteristics (new) | 6 | .896 | .905 | DSC5 |
| Application Characteristics (new) | 3 | .804 | .948 | AppC3 |
| Task-Technology Fit | 4 | .974 | .975 | TTF1 |
| Financial Transaction Performance | 3 | .928 | .938 | FTP1 |
| Benefits of Information Disclosure | 3 | .863 | .904 | BEN3 |
| Risks of Information Disclosure | 3 | .941 | .980 | RISK1 |
| Intention to Disclose Personal Information | 3 | .844 | .890 | INT3 |
| Continuous Use of Digital Wallet | 4 | .881 | .970 | CUDW4 |

Journal of Theoretical and Applied Information Technology
28th February 2026. Vol.104. No.4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

### 4.3 Exploratory Factor Analysis (EFA)

Exploratory Factor Analysis (EFA) was conducted SPSS version 29. As presented in Figure 2, the Kaiser-Meyer-Olkin (KMO) value exceeds 0.5, indicating the data meet the minimum threshold for sampling adequacy, as a KMO value of 0.5 or higher is generally considered acceptable.

*TABLE 6: KMO AND BARTLETT'S TEST*

**KMO and Bartlett's Test**

| | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .766 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 235.355 |
| | df | 45 |
| | Sig. | <.001 |

Table 7 reports the communality values for all items. Communality serves as a useful indicator of how well each item is represented by the extracted factors [92]. As shown, all communalities exceed the threshold of 0.5, with values ranging from a minimum of 0.523 to a maximum of 0.923, thereby indicating satisfactory item representation.

*TABLE 7: COMMUNALITY OF COMPONENTS*

| Components | Initial | Extraction |
|---|---|---|
| 1 | 1.000 | .721 |
| 2 | 1.000 | .656 |
| 3 | 1.000 | .816 |
| 4 | 1.000 | .844 |
| 5 | 1.000 | .923 |
| 6 | 1.000 | .797 |
| 7 | 1.000 | .750 |
| 8 | 1.000 | .877 |
| 9 | 1.000 | .523 |
| 10 | 1.000 | .638 |

Table 8 presents the total variance explained by the extracted components. As shown, three factors were extracted. Among the ten components, the first component alone accounts for 44.259% of the total variance. These three factors were retained based on the criterion of eigenvalues greater than one. Collectively, the three factors explain 75.454% of the total variance.

*TABLE 8: TOTAL VARIANCE EXPLAINED*

**Total Variance Explained**

| Component | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 4.426 | 44.259 | 44.259 | 4.426 | 44.259 | 44.259 | 3.895 | 38.955 | 38.955 |
| 2 | 1.901 | 19.035 | 62.264 | 1.901 | 19.035 | 62.264 | 1.994 | 19.936 | 58.891 |
| 3 | 1.219 | 13.189 | 75.454 | 1.219 | 13.189 | 75.454 | 1.656 | 16.563 | 75.454 |
| 4 | .948 | 9.481 | 84.935 | | | | | | |
| 5 | .468 | 4.676 | 89.610 | | | | | | |
| 6 | .381 | 3.814 | 93.424 | | | | | | |
| 7 | .245 | 2.446 | 95.870 | | | | | | |
| 8 | .176 | 1.703 | 97.573 | | | | | | |
| 9 | .164 | 1.644 | 99.217 | | | | | | |
| 10 | .078 | .783 | 100.000 | | | | | | |

Extraction Method: Principal Component Analysis.

Table 9 presents the scree plot of the components, in which the eigenvalues are arranged in descending order. The highest eigenvalue is 4.426, while the lowest is 0.780.

*TABLE 9: SCREE PLOT*

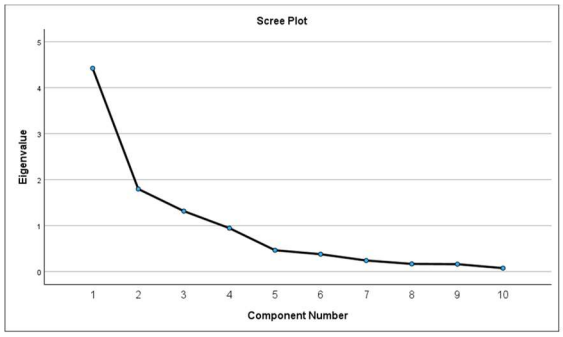


Table 10 presents the rotated component matrix of the study. The matrix compromises ten components distributed across three extracted factors.

*TABLE 10: ROTATED COMPONENTS MATRIX*

| | Factor | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Task Characteristics | .346 | -.105 | .768 |
| Technology Characteristics | .075 | .237 | .771 |
| Data security characteristics | .868 | .088 | .232 |
| Application characteristics | .903 | .129 | .103 |
| Task-technology fit | .890 | .038 | .360 |
| Financial transaction performance | .838 | .088 | .294 |
| Benefits of information disclosure | .105 | .839 | .189 |
| Risks of information disclosure | -.004 | .933 | .086 |
| Intention to disclose personal information | .346 | .551 | -.317 |
| Continuous use of digital wallet | .758 | .128 | -.217 |

## 5. DISCUSSION

This study involved a pilot investigation comprising 38 respondents. The respondents were digital wallet users aged 18 years and above.

To validate the content of the instrument, expert reviewers were consulted. These reviewers consisted of five specialists with backgrounds in Information Systems. They were asked to evaluate the instrument's content by assigning scores ranging from one to three. A score of one indicated a poor

match, suggesting that the item was unrelated and should be removed; a score of two indicated a moderate match, meaning the item was relevant but required revision; and a score of three indicated a perfect match, signifying that the item was highly relevant. In addition to assigning scores, the expert reviewers were also permitted to provide comments to further improve the content of the items. Based on the evaluations, it can be concluded that all expert reviewers agreed with the content of the items in this study. However, the comments provided by the reviewers must be taken into consideration. Accordingly, modifications to the items were made based on the expert reviewers' feedback.

In terms of the reliability test, all items of the constructs scored above 0.6, indicating that the item loadings are acceptable, as suggested by Hair, Hult, Ringle, and Sarstedt [93]. In addition, the Cronbach's alpha values were examined under the condition of item deletion. Based on these results, one item from each construct (except task characteristics) required deletion to improve the overall Cronbach's alpha value.

With respect to exploratory factor analysis (EFA), the Kaiser–Meyer–Olkin (KMO) value obtained in this study was 0.766, which exceeds the satisfactory threshold of 0.5. This result confirms that the sampling adequacy of the study is acceptable. Furthermore, the communality values for all items demonstrated satisfactory results, ranging from a minimum of 0.523 to a maximum of 0.923. According to the total variance explained, only three components had eigenvalues greater than one, while the remaining components had eigenvalues below one. The cumulative percentage of variance explained was 75.454%, indicating that the three components with eigenvalues greater than one accounted for 75.454% of the variance in the study. The remaining percentage was explained by seven components with eigenvalues below one. The eigenvalues were also illustrated graphically through the scree plot. The rotated component matrix revealed the loading values for each component. Five items—data security characteristics (.868), application characteristics (.903), task–technology fit (.890), financial transaction performance (.838), and continuous use of digital wallet (.758) - loaded onto Factor 1, which represents digital wallet usage. Three items - benefits of information disclosure (.839), risks of information disclosure (.933), and intention to disclose personal information (.551) - loaded onto Factor 2, which represents privacy. Factor 3 comprised task characteristics (.768) and technology characteristics (.771), representing the alignment between task and technology.

Based on the overall results, the implications this study suggest that the instrument offers valuable insights. The findings demonstrate that the items associated with the two proposed constructs – Data Security Characteristics and Application Characteristics – are both appropriate and applicable for use in the main study. Indirectly, these findings contribute to a new perspective to the Task-Technology Fit (TTF) Theory.

## 6. CONCLUSION

In conclusion, instrument development and validation are critical processes, as they serve to establish construct validity. Moreover, they constitute an essential component of survey validation, ensuring that a multi-item survey accurately measures the intended constructs.

The results of this preliminary study offer initial support for the model constructs and measurement instruments intended for use in the main study. However, revisions to certain items are necessary to address identified shortcomings prior to full implementation. Furthermore, this initial investigation lays the groundwork for the inclusion of the newly proposed constructs – Data Security Characteristics and Application Characteristics – give the promising performance of the related items.

## 7. IMPLICATIONS

This study establishes a new foundation for future research in terms of instrument development. The introduction of data security characteristics and application characteristics as novel constructs within task-technology fit theory enhances current investigations related to technological fitness. Indirectly, these two constructs also provide fresh insights into the existing task-technology fit framework.

Furthermore, the integration of task-technology fit theory with privacy calculus theory offers new perspectives on how the fitness of digital wallets and their associated privacy dimensions influence continuous usage. The notion of service-privacy fit may also be regarded as an innovative extension for current practice.

In addition, this study offers a holistic lens through which fintech adoption can be understood. The development of the instrument further enables digital wallet service providers to identify and address gaps in sustaining user engagement with digital wallet services.

## 8. LIMITATION

This study is limited to instrument development. The findings are limited to analyses pertaining to the development of the instrument, without the inclusion of any hypotheses. Although the results of this study indicate positive outcomes, the generalizability of these findings may be constrained by the limited sample size employed.

## 9. RECOMMENDATION

It is recommended that future research adopt or adapt this instrument as a foundational tool for further exploration. The utilization of this instrument is expected to enhance existing findings related to the fitness of digital wallets, the privacy of digital wallets, and the continuous use of digital wallets. Moreover, it is advisable that the instrument be applied to a large-scale population sample, as the present study was limited to the use of a pilot test sample.

## 10. ACKNOWLEDGEMENT

This research was supported by Ministry of Higher Education (MOE) of Malaysia through Fundamental Research Grant Scheme (FRGS/1/2024/ICT03/UUM/02/1).

## REFERENCES:

[1] F. A. A. Ramli and M. I. Hamzah, "Mobile payment and e-wallet adoption in emerging economies: A systematic literature review," *Journal of Emerging Economies and Islamic Research*, vol. 9, no. 2, p. 1, May 2021, doi: 10.24191/jeeir.v9i2.13617.

[2] S. Kumar, "Transforming Financial Transactions: The Leading Role Of Digital Wallets," *Iosr Journal Of Economics And Finance (Iosr-Jef) E-Issn*, vol. 15, pp. 30–33, 2024, doi: https://doi.org/10.9790/5933-1503033033.

[3] "Are digital wallets safe?," *Microsoft 365*. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/are-digital-wallets-safe

[4] Bank of America . (n.d.) *Digital wallets adoption and growth – digital payments strategy*. https://business.bofa.com/en-us/content/digital-wallets-adoption-digital-payments-strategy.html

[5] A. A. Mohmmed, A. M. S. Rahma, and H. B. AbdulWahab, "Digital Wallets Evolution: Navigating Challenges, Innovation and the Future Landscape," *Al-Qadisiyah Journal of Pure Science*, vol. 29, no. 1, Jan. 2024, doi: https://doi.org/10.29350/2411-3514.1248.

[6] D. L. Goodhue and R. L. Thompson, "Task-Technology Fit and Individual Performance," *MIS Quarterly*, vol. 19, no. 2, pp. 213–236, Jun. 1995, doi: https://doi.org/10.2307/249689.

[7] "8 Key Concerns About Digital Wallet Privacy and Security," *Acceta-fintech.com*, 2024. https://acceta-fintech.com/blog/8-key-concerns-about-digital-wallet-privacy-and-security

[8] PayPal, "Digital wallet privacy: What you need to know," *Paypal.com*, Aug. 30, 2024. https://www.paypal.com/uk/money-hub/article/digital-wallet-privacy (accessed Aug. 04, 2025).

[9] "CYBER RISKS IN FAST PAYMENT SYSTEMS," *World Bank Group*, 2025. Available: https://fastpayments.worldbank.org/sites/default/files/2025-02/Cybersecurity%20Focus%20Note_Feb%2019_Final.pdf

[10] F. International, "Digital Wallet Fraud - What is it and how it's prevented," *Fraud.com*, Aug. 11, 2023. https://www.fraud.com/post/digital-wallet-fraud

[11] "The Digital Identity Regulation Enters into Force - EU Digital Identity Wallet -," *EU Digital Identity Wallet*, 2024. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+Digital+Identity+Regulation+Enters+into+Force

[12] H.-P. Lu and Y.-W. Yang, "Toward an understanding of the behavioral intention to use a social networking site: An extension of task-technology fit to social-technology fit," *Computers in Human Behavior*, vol. 34, pp. 323–332, May 2014, doi: https://doi.org/10.1016/j.chb.2013.10.020.

[13] Fu, R.-A. Shang, A. Jeyaraj, Y. Sun, and F. Hu, "Interaction between task characteristics and technology affordances," *Journal of Enterprise Information Management*, vol. 33, no. 1, pp. 1–22, Oct. 2019, doi: https://doi.org/10.1108/jeim-04-2019-0105.

[14] S. Ratna, E. S. Astuti, H. N. Utami, K. Rahardjo, and Z. Arifin, "Characteristics of tasks and technology as a driver of task-technology fit and the use of the hotel

reservation information system," *VINE Journal of Information and Knowledge Management Systems*, vol. 48, no. 4, pp. 579–595, Nov. 2018, doi: https://doi.org/10.1108/vjikms-05-2018-0035.

[15] S. Ulfa, E. Surahman, I. Fatawi, and H. Tsukasa, "Task-Technology Fit Analysis: Measuring the Factors that influence Behavioural Intention to Use the Online Summary-with Automated Feedback in a MOOCs Platform," *The Electronic Journal of e-Learning*, vol. 22, no. 1, pp. 63–77, Mar. 2024, doi: 10.34190/ejel.22.1.3094.

[16] T. Oliveira, M. Faria, M. A. Thomas, and A. Popovič, "Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM," *International Journal of Information Management*, vol. 34, no. 5, pp. 689–703, Oct. 2014, doi: https://doi.org/10.1016/j.ijinfomgt.2014.06.004.

[17] Z. Zaremohzzabieh, S. Roslan, Z. Mohamad, I. A. Ismail, H. Ab Jalil, and S. Ahrari, "Influencing Factors in MOOCs Adoption in Higher Education: A Meta-Analytic Path Analysis," *Sustainability*, vol. 14, no. 14, p. 8268, Jul. 2022, doi: https://doi.org/10.3390/su14148268.

[18] A. Bere, "Applying an Extended Task-Technology Fit for Establishing Determinants of Mobile Learning: An Instant Messaging Initiative," *AIS Electronic Library (AISeL)*, 2018. https://aisel.aisnet.org/jise/vol29/iss4/4/

[19] X. Lin, R. Wu, Y.-T. Lim, J. Han, and S.-C. Chen, "Understanding the sustainable usage intention of mobile payment technology in Korea: Cross-Countries Comparison of Chinese and Korean users," *Sustainability*, vol. 11, no. 19, p. 5532, Oct. 2019, doi: 10.3390/su11195532.

[20] C. Tam and T. Oliveira, "Does culture influence m-banking use and individual performance?," Information & Management, vol. 56, no. 3, pp. 356–363, Apr. 2019, doi: https://doi.org/10.1016/j.im.2018.07.009.

[21] A. M. Baabdullah, A. A. Alalwan, N. P. Rana, P. Patil, and Y. K. Dwivedi, "An integrated model for m-banking adoption in Saudi Arabia," International Journal of Bank Marketing, vol. 37, no. 2, pp. 452–478, Mar. 2019, doi: 10.1108/ijbm-07-2018-0183.

[22] S. Rahi, M. M. Khan, and M. Alghizzawi, "Extension of technology continuance theory (TCT) with task technology fit (TTF) in the context of Internet banking user continuance intention," *International Journal of Quality & Reliability Management*, vol. 38, no. 4, pp. 986–1004, Sep. 2020, doi: 10.1108/ijqrm-03-2020-0074.

[23] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. Al-Khaleefa, "A Review on Electronic Payments Security," *Symmetry*, vol. 12, no. 8, p. 1344, Aug. 2020, doi: https://doi.org/10.3390/sym12081344.

[24] F. A. A. Ramli, M. I. Hamzah, S. N. Wahab, and R. Shekhar, "Modeling the Brand Equity and Usage Intention of QR-Code E-Wallets," *FinTech*, vol. 2, no. 2, pp. 205–220, Mar. 2023, doi: https://doi.org/10.3390/fintech2020013.

[25] K. Marky, K. Ragozin, G. Chernyshov, A. Matviienko, M. Schmitz, M. Mühlhäuser, C. Eghtebas, and K. Kunze, ""Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication," *ACM Transactions on Computer-Human Interaction*, vol. 29, no. 5, Feb. 2022, doi: https://doi.org/10.1145/3503514.

[26] C. Tam and T. Oliveira, "Performance impact of mobile banking: using the task-technology fit (TTF) approach," *International Journal of Bank Marketing*, vol. 34, no. 4, pp. 434–457, Jun. 2016, doi: https://doi.org/10.1108/ijbm-11-2014-0169.

[27] T. Zhou, Y. Lu, and B. Wang, "Integrating TTF and UTAUT to explain mobile banking user adoption," *Computers in Human Behavior*, vol. 26, no. 4, pp. 760–767, Jul. 2010, doi: https://doi.org/10.1016/j.chb.2010.01.013.

[28] D. M and J. Dhiipan, "A Meta-Analysis of Efficient Countermeasures for Data Security," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 1303-1308, doi: 10.1109/ICACRS55517.2022.10029302.

[29] B. Nadji, "Data Security, Integrity, and Protection," *Signals and communication technology*, pp. 59–83, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-61117-9_4.

[30] T. Aghaunor, P. Eshua, T. Obah, and O. Aromokeye, "Data security strategies to avoid data breaches in modern information systems," *World Journal of Advanced Research and Reviews*, vol. 20, no. 3, pp. 2122–2144, Dec. 2023, doi: https://doi.org/10.30574/wjarr.2023.20.3.2515.

[31] D. M. Kesa, "Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations," *World Journal of*

*Advanced Research and Reviews*, vol. 18, no. 3, pp. 970–992, Jun. 2023, doi: https://doi.org/10.30574/wjarr.2023.18.3.1166.

[32] S. Khan, "Enhancing User Trust in FinTech: A Multi-Factor Authentication Study | *Journal of Applied Information Science*, vol. 12 Issue 2," Publishingindia.com, 2024. http://www.publishingindia.com/jais/71/enhancing-user-trust-in-fintech-a-multi-factor-authentication-study/32170/87745/

[33] J. Peeters, "Data Protection in Mobile Wallets," *European Data Protection Law Review*, vol. 6, no. 1, pp. 56–65, 2020, doi: https://doi.org/10.21552/edpl/2020/1/8.

[34] D. A. Muhtasim, S. Y. Tan, M. A. Hassan, M. I. Pavel, and S. Susmit, "Customer Satisfaction with Digital Wallet Services: An Analysis of Security Factors," International *Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, Jan. 2022, doi: 10.14569/ijacsa.2022.0130124.

[35] A. K. Patidar and U. Suman, "A survey on mobile app development approaches with the industry perspective," *International Journal of Open Source Software and Processes*, vol. 13, no. 1, pp. 1–17, May 2022, doi: 10.4018/ijossp.300754.

[36] V. Maia, Taisa Gonçalves, and A. R. Rocha, "Quality Evaluation of Mobile Applications," *Simpósio Brasileiro de Qualidade de Software (SBQS)*, pp. 21–30, 2020, Available: https://sol.sbc.org.br/index.php/sbqs_estendido/article/view/14189

[37] J. Kim and H. Bahn, "Maintaining Application Context of Smartphones by Selectively Supporting Swap and Kill," *IEEE Access*, vol. 8, pp. 85140–85153, Jan. 2020, doi: https://doi.org/10.1109/access.2020.2992072.

[38] P. Lew and L. Olsina, "Relating User Experience with MobileApp Quality Evaluation and Design," in *Lecture Notes in Computer Science*, 2013, pp. 253–268. doi: 10.1007/978-3-319-04244-2_23.

[39] N. M. E. Pusparani, T. Setiyorini, and F. Frieyadie, "Usability testing analysis on digital wallet applications to measure user satisfaction," *Jurnal Riset Informatika*, vol. 5, no. 4, pp. 529–542, Sep. 2023, doi: 10.34288/jri.v5i4.119.

[40] H. Moksin, Z. H. Hudi, and M. A. Malek, "Wallet Go Digital: Exploring service quality and customer satisfaction in E-Wallet apps," *International Journal of Academic Research in Business and Social Sciences*, vol. 14, no. 12, Dec. 2024, doi: 10.6007/ijarbss/v14-i12/23771.

[41] S. Shari, Airul Shazwan Norshahimi, Siti Aqilah Yop, Asmad Rizal Umar, and Mohd, "Conceptualizing User Interface Satisfaction in the Touch 'n Go E-Wallet Mobile Application," *International Conference on Business and Technology* Cham: Springer Nature Switzerland, pp. 292–302, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-55911-2_28.

[42] D. Amoroso, R. Lim, J. Lei, and A. Saxena, "A study of satisfaction and loyalty for continuance intention of mobile wallet in India," *International Journal of E-Adoption*, vol. 15, no. 1, pp. 1–18, Mar. 2023, doi: 10.4018/ijea.319313.

[43] N. N. D. Phuong, L. T. Luan, V. Van Dong, and N. L. N. Khanh, "Examining Customers' Continuance Intentions towards E-wallet Usage: The Emergence of Mobile Payment Acceptance in Vietnam," *Journal of Asian Finance Economics and Business*, vol. 7, no. 9, pp. 505–516, Sep. 2020, doi: 10.13106/jafeb.2020.vol7.no9.505.

[44] S. Chaveesuk, B. Khalid, and W. Chaiyasoonthorn, "Continuance intention to use digital payments in mitigating the spread of COVID-19 virus," *International Journal of Data and Network Science*, vol. 6, no. 2, pp. 527–536, Jan. 2022, doi: 10.5267/j.ijdns.2021.12.001.

[45] R. Kishokumar and P. T. Thiyagarajan, "Influence of task - Technology fit on individual job performance in insurance industry: Special reference to Batticaloa District," *SSRN Electronic Journal*, Jan. 2015, doi: 10.2139/ssrn.2699795.

[46] C. O. Baxi, K. J. Patel, K. M. Patel, V. B. Patel, and V. A. Acharya, "Consumers' digital wallet adoption," *International Journal of Asian Business and Information Management*, vol. 15, no. 1, pp. 1–23, Nov. 2023, doi: 10.4018/ijabim.334016.

[47] K. R. Siregar and A. P. R. Ayulia, "Factors affecting user continued usage intention for the GoPay application using the task-technology fit model," in *Routledge eBooks*, 2022, pp. 63–68. doi: 10.1201/9781003222927-9.

[48] N. A. Narendrar, J. E. Suseno, and D. M. K. Nugraheni, "Factors influencing interest in continuing use of e-Wallet using the Technology Acceptance Model and Task-Technology FIT," *Mimbar Ilmu*, vol. 28, no. 2, pp. 221–230, Aug. 2023, doi: 10.23887/mi.v28i2.61228.

[49] T. Kniazieva and A. Maryna, "Fintech In Information And Analytical Support Of Decision-Making Of Financial Institutions," Jan. 2023, doi: https://doi.org/10.30525/978-9934-26-268-5-12.

[50] D. W. Firdaus and R. K. Aryanti, "The influence of financial technology in financial transactions," *IOP Conference Series Materials Science and Engineering*, vol. 662, no. 2, p. 022012, Nov. 2019, doi: 10.1088/1757-899x/662/2/022012.

[51] S. Purnama, C. S. Bangun, and S. A. Faaroek, "The effect of transaction experience using digital wallets on user satisfaction in millennial generation," *Aptisi Transactions on Management (ATM)*, vol. 5, no. 2, pp. 161–168, Apr. 2021, doi: 10.33050/atm.v5i2.1593.

[52] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: a multidimensional developmental theory," *Journal of Social Issues*, vol. 33, no. 3, pp. 22–42, Jul. 1977, doi: 10.1111/j.1540-4560.1977.tb01880.x.

[53] M. J. Culnan and P. K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, vol. 10, no. 1, pp. 104–115, 1999, Available: https://www.jstor.org/stable/2640390

[54] T. Dinev and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006, Available: https://www.jstor.org/stable/23015781

[55] H.-T. Chen, "Revisiting the privacy paradox on social media with an extended privacy calculus model: the effect of privacy Concerns, Privacy Self-Efficacy, and Social Capital on privacy management," *American Behavioral Scientist*, vol. 62, no. 10, pp. 1392–1412, Aug. 2018, doi: 10.1177/0002764218792691.

[56] X. Jiang, T.-T. Goh, and M. Liu, "On Students' willingness to use Online Learning: A Privacy Calculus Theory approach," *Frontiers in Psychology*, vol. 13, Jun. 2022, doi: 10.3389/fpsyg.2022.880261.

[57] D. C. Pham and T. Nguyen, "Understanding peer-to-peer mobile payment continuance intention: a privacy calculus perspective," *International Journal of Electronic Business*, vol. 20, no. 2, pp. 210–243, Jan. 2025, doi: 10.1504/ijeb.2025.145342.

[58] M. Prasetya, S. Shuhidan, S. Alam, and U. Teknologi, "Security, Risk and Trust in E-wallet Payment Systems: Empirical Evidence from Indonesia," *Management And Accounting Review*, vol. 22, no. 1, 2023, Available: https://mar.uitm.edu.my/images/Vol-22-1/14.pdf

[59] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. Al-Khaleefa, "A review on electronic payments security," *Symmetry*, vol. 12, no. 8, p. 1344, Aug. 2020, doi: 10.3390/sym12081344.

[60] S. Zhou and Y. Liu, "Effects of Perceived Privacy Risk and Disclosure Benefits on the Online Privacy Protection Behaviors among Chinese Teens," *Sustainability*, vol. 15, no. 2, p. 1657, Jan. 2023, doi: 10.3390/su15021657.

[61] M. Chen, X. Huang, and X. Qi, "To disclose or to protect? Predicting social media users' behavioral intention toward privacy," *Industrial Management & Data Systems*, vol. 124, no. 6, pp. 2091–2119, May 2024, doi: 10.1108/imds-05-2023-0337.

[62] W. A. Khan and Z. U. Abideen, "Effects of behavioural intention on usage behaviour of digital wallet: the mediating role of perceived risk and moderating role of perceived service quality and perceived trust," *Future Business Journal*, vol. 9, no. 1, Sep. 2023, doi: 10.1186/s43093-023-00242-z.

[63] H. Zhao, S. T. Anong, and L. Zhang, "Understanding the impact of financial incentives on NFC mobile payment adoption," *International Journal of Bank Marketing*, vol. 37, no. 5, pp. 1296–1312, Apr. 2019, doi: 10.1108/ijbm-08-2018-0229.

[64] S. H. Yoseph and G. Chongyan, "Antecedents of consumers' privacy protection behavior and intention to disclose personal information: Mediating role of personal information transparency," *International Journal of Science and Business*, vol. 37, no. 1, pp. 96–118, Jan. 2023, doi: 10.58970/ijsb.2388.

[65] L. Dogruel, S. Joeckel, and J. Henke, "Disclosing personal information in mHealth apps. testing the role of privacy attitudes, app habits, and social norm cues," *Social Science Computer Review*, vol. 41, no. 5, pp. 1791–1810, Jun. 2023, doi: 10.1177/08944393221108820.

[66] M. Degutis, S. Urbonavičius, I. Zimaitis, V. Skare, and D. Laurutytė, "Willingness to Disclose Personal Information: How to Measure it?," *Engineering Economics*, vol. 31, no. 4, pp. 487–494, Oct. 2020, doi: 10.5755/j01.ee.31.4.25168.

[67] A. Daragmeh, J. Sági, and Z. Zéman, "Continuous intention to use E-Wallet in the context of the COVID-19 pandemic: integrating the Health Belief Model (HBM) and

Technology Continuous Theory (TCT)," *Journal of Open Innovation Technology Market and Complexity*, vol. 7, no. 2, p. 132, May 2021, doi: 10.3390/joitmc7020132.

[68] D. Palullungan, "Pemodelan Continuance Intention Dalam Kasus Penggunaan Dompet Digital Di Kalangan Mahasiswa," *JIEMS (Journal of Industrial Engineering and Management Systems)*, vol. 15, no. 2, Oct. 2022, doi: 10.30813/jiems.v15i2.3768.

[69] N. Shanmugavel, N. P. Rana, S. Parayitam, and K. Kumar, "Assessing continuance intention to use digital wallet," *Journal of Global Information Management*, vol. 32, no. 1, pp. 1–29, Nov. 2024, doi: 10.4018/jgim.361120.

[70] Indrawati, R. H. Dharmawan and S. K. B. Pillai, "Analyzing Factors Influencing Continuance Intention of a Digital Walet: a Study of Digicash by Using Modified UTAUT 2 Model," *2023 International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS)*, Bali, Indonesia, 2023, pp. 1-6, doi: 10.1109/ICADEIS58666.2023.10270902.

[71] C. M. Patino and J. C. Ferreira, "Internal and external validity: can you apply research study results to your patients?," *Jornal Brasileiro De Pneumologia*, vol. 44, no. 3, p. 183, May 2018, doi: 10.1590/s1806-37562018000000164.

[72] R. Heale and A. Twycross, "Validity and reliability in quantitative studies," *Evidence-Based Nursing*, vol. 18, no. 3, pp. 66–67, May 2015, doi: 10.1136/eb-2015-102129.

[73] S. Rusticus, "Content validity," in *Springer eBooks*, 2014, pp. 1384–1385. doi: 10.1007/978-3-031-17299-1_553.

[74] E. Almanasreh, R. Moles, and T. F. Chen, "Evaluation of methods used for estimating content validity," *Research in Social and Administrative Pharmacy*, vol. 15, no. 2, pp. 214–221, Feb. 2019, doi: https://doi.org/10.1016/j.sapharm.2018.03.066.

[75] S. Messick, "Meaning and Values in Test Validation: The Science and Ethics of Assessment," Educational Researcher, vol. 18, no. 2, pp. 5–11, Mar. 1989, doi: 10.3102/0013189x018002005.

[76] P. A. Moss, "Themes and Variations in Validity Theory," Educational Measurement Issues and Practice, vol. 14, no. 2, pp. 5–13, Jun. 1995, doi: 10.1111/j.1745-3992.1995.tb00854.x.

[77] R. Czaja, "Questionnaire Pretesting Comes of Age," Marketing Bulletin, vol. 9, no. 5, pp. 52–66, 1998, Available: https://marketing-bulletin.massey.ac.nz/V9/MB_V9_A5_Czaja.pdf

[78] S. Hashim, S. F. Mohamad, S. A. H. Lim, and N. H. C. Ahmat, "Pretesting Survey Questionnaire: A guide on dissemination," International Journal of Academic Research in Economics and Management Sciences, vol. 11, no. 3, Sep. 2022, doi: 10.6007/ijarems/v11-i3/15228.

[79] I.-C. A. Chiang, R. S. Jhangiani, and P. C. Price, "Reliability and validity of measurement," Pressbooks, Oct. 13, 2015. https://opentextbc.ca/researchmethods/chapter/reliability-and-validity-of-measurement/

[80] S. Livingston, "Test Reliability-Basic Concepts," 2018. Available: https://www.ets.org/Media/Research/pdf/RM-18-01.pdf

[81] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, "Multivariate Data Analysis (7th Edition)", Pearson, New York, 2010.

[82] J. H. McMillan, and S. Schumacher, "Research in education: Evidence-based inquiry", Pearson, 2014. https://books.google.com.my/books/about/Research_in_Education.html?id=JSavAgAAQBAJ&redir_esc=y

[83] W. N. F. A. Jani, F. Razali, N. Ismail, and N. Ismawi, "Exploratory Factor Analysis: Validity and reliability of teacher's knowledge construct instrument," Jan. 21, 2023. https://hrmars.com/index.php/IJARPED/article/view/16236/Exploratory-Factor-Analysis-Validity-and-Reliability-of-Teachers-Knowledge-Construct-Instrument

[84] U. Sekaran, and R. Bougie, "Research methods for business: A skill building approach", 2016. John Wiley & Sons.

[85] D. Mindrila, "Exploratory factor analysis: An overview. Exploratory factor analysis", pp. 1-25, 2017.

[86] M. Arain, M. J. Campbell, C. L. Cooper, and G. A. Lancaster, "What is a pilot or feasibility study? A review of current practice and editorial policy," BMC Medical Research Methodology, vol. 10, no. 1, Jul. 2010, doi: 10.1186/1471-2288-10-67.

[87] D. F. Polit, and C. T. Beck, "Nursing research: Generating and assessing evidence for nursing practice (10th ed.)", Philadel-phia, PA: Wolters Kluwer/Lippincott Williams & Wilkins, 2017.

[88] L. L. Davis, "Instrument review: Getting the most from a panel of experts," Applied Nursing Research, vol. 5, no. 4, pp. 194–197, Nov. 1992, doi: 10.1016/s0897-1897(05)80008-4.

[89] D. F. Polit and C. T. Beck, "The content validity index: Are you sure you know what's being reported? critique and recommendations," Research in Nursing & Health, vol. 29, no. 5, pp. 489–497, Jan. 2006, doi: 10.1002/nur.20147.

[90] D. F. Polit, C. T. Beck, and S. V. Owen, "Is the CVI an acceptable indicator of content validity? Appraisal and recommendations," Research in Nursing & Health, vol. 30, no. 4, pp. 459–467, Jul. 2007, doi: 10.1002/nur.20199.

[91] M. S. B. Yusoff, "ABC of content validation and content validity index calculation", Education in Medicine Journal, vol. 11, no. 2, Jun. 2019, doi: https://doi.org/10.21315/eimj2019.11.2.

[92] M. Sarstedt and E. Mooi, "Cluster Analysis," Springer Texts in Business and Economics, pp. 273–324, 2014, doi: https://doi.org/10.1007/978-3-642-53965-7_9.

[93] J. F. Hair Jr., G. T. M. Hult, C. Ringle, and M. Sarstedt, (2016). "*A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*", Thousand Oaks, CA: Sage Publications, 2016.