MUNI FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Tsai, C.-Y. (2024). Is undergraduates' adoption of the Internet of Things rational? The role of risk perception. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18*(4), Article 8.
https://doi.org/10.5817/CP2024-4-8

Is Undergraduates' Adoption of the Internet of Things Rational? The Role of Risk Perception

Chun-Yen Tsai

Center for General Education / Research Center for Promoting Civic Literacy, National Sun Yat-sen University, Taiwan

Abstract

Users' intentions and behavior when using the Internet of Things (IoT) are essential issues in contemporary technology research. This research used the Theory of Planned Behavior (TPB) model to predict undergraduates' IoT use intention and behavior in the smart home context. A total of 412 undergraduates at four universities in Taiwan participated in this study. The Structural Equation Modeling (SEM) approach was utilized to test the hypotheses. The results revealed that undergraduates' attitudes and subjective norms had a positive effect on their IoT use intention, which, in turn, had effects on their IoT use behavior. This study also found that undergraduates' risk perception of behavioral control had a negative effect on their IoT use intention. In contrast, their perceived risk of behavioral control had a positive direct effect on their IoT use behavior. This research contributes to the current state of knowledge since the proposed model revealed that undergraduates' adoption of the Internet of Things might not be entirely rational. Their risk perception of behavioral control might play particular role.

Keywords: Internet of Things; risk perception; SEM; theory of planned behavior

Editorial Record

First submission received:
February 6, 2023

Revisions received:
October 10, 2023
April 5, 2024
June 30, 2024

Accepted for publication:
July 10, 2024

Editor in charge:
David Smahel

Introduction

The Internet of Things (IoT) technology brings both convenience and new challenges, as it enables interconnected products, data collection, and customization with risk issues. The IoT refers to devices with microprocessors that can be connected to the Internet (George et al., 2021; van Deursen et al., 2021). On the one hand, this new technological development brings convenience and improves work performance; on the other hand, it poses several new problems and challenges (Hsu & Lin, 2016; Mani & Chouk, 2018; Philip et al., 2022; Roe et al., 2022). People only need to understand what a standalone technology product does or how to use it before deciding to buy or adopt it. However, the advent of the IoT era has complicated this decision-making since IoT technology can connect products to products and products of third parties through the Internet or other connection technologies (Paupini et al., 2022; F. Zhang et al., 2023). These processes collect and integrate data to customize technology products according to consumer needs (Hsu & Lin, 2016; Kim et al., 2019; F. Zhang et al., 2023). For example, in addition to providing the functions of traditional watches, smart watches can also record users' health statuses and store data in cloud storage through the network. IoT technology brings unprecedented convenience, while on the other hand, it requires users to rethink its risks and costs (Cheryl et al., 2021).

Risk issues are significant in Internet use, especially with IoT growth, driving government regulation and education efforts. The rapid development of IoT makes transmitting and receiving information more frequent, making risk issues more complex (Cheryl et al., 2021; George et al., 2021; F. Zhang et al., 2023). These risk perceptions may stem from the *Big Brother effect*, which refers to individuals' awareness of being monitored and controlled by powerful organizations (F. Zhang et al., 2023). When accessing information products, personal digital footprints may be collected by big data systems (Henry et al., 2022; Q. Yang, 2021). The customized services formed by big data systems accordingly may make people overly dependent on these information services and may end up controlling their lives (van Deursen et al., 2021). Relevant government departments try to protect users' rights by formulating laws (Cheryl et al., 2021) or promoting formal and informal education (Y. T. Chen et al., 2021; Tsai et al., 2022). Past studies have found that different age groups have different attitudes and behaviors regarding using the Internet or technology products (Kim et al., 2019; van Deursen et al., 2021). Highly educated people may be more receptive to emerging technologies than less educated people (Baudier et al., 2020). The current study aimed to understand and explore undergraduates' attitudes towards and use behaviors of the IoT.

The Theory of Planned Behavior (TPB; Ajzen, 1985, 2002) is a behavioral decision model primarily applied to understand individuals' behavior. In the TPB model, behavioral intentions are rational and are assumed to predict behaviors, and several antecedents predict behavioral intentions. TPB has been successfully applied to interpretive research on technology use, including online behavior (e.g., Aderibigbe et al., 2021), technology product consumption (e.g., Perri et al., 2020), and IoT use intention (e.g., Almazroi, 2023; Alraja, 2022; Hasan et al., 2023; Pal et al., 2020, 2021; H. Yang et al., 2017; W. Zhang & Liu, 2022). However, the intention variable is more often included in the models tested in these studies than the actual behavior variable. In addition, fewer studies have discussed the rational process of IoT adoption behavior. Therefore, the current study focused on exploring the use of the TPB model to predict undergraduates' IoT use intentions and behaviors in the smart home context, and explored the role of perceived risk in this model. The following research question was addressed: Could the TPB model incorporating the risk perception variable explain undergraduates' rational adoption of the IoT?

Perceived Benefits and Risks of IoT Usage

Risk perception refers to an individual's subjective judgment about the extent of risk associated with a specific product or event (Aggarwal et al., 2020; Binder et al., 2012). The threats and risks of technological products are related to IoT users' change in attitude toward adoption (Aggarwal et al., 2020; Pal et al., 2021; Philip et al., 2022; van der Zeeuw et al., 2023; van Deursen et al., 2021). Users often increase their risk perception and tend to have negative attitudes toward products requiring sensitive personal data (Cheryl et al., 2021; Pal et al., 2021) and digital footprints (Henry et al., 2022). In this case, it may affect users' willingness to provide personal data, thereby reducing the intention to adopt the product. The individual's knowledge of the technology may also affect their use intention (Aggarwal et al., 2020; Alkawsi et al., 2020). Therefore, if service providers intentionally conceal what information is taken from users, or if individuals have limited knowledge and understanding of the technology, it may also affect their risk perception.

The crucial factors that influence users' adoption behavior of technology products may originate from their perceptions of the benefits of the product or the consideration of user costs. The Privacy Calculus Theory asserts that an individual's behavioral motivation is affected by dual driving forces: perceived benefit and perceived risk (Alraja, 2022; Kim et al., 2019; Lünich et al., 2023; Ostendorf et al., 2022; Pal et al., 2021; Princi & Krämer, 2020). The former has a positive driving force, while the latter has an opposing one (Hsu & Lin, 2016; Kim et al., 2019). For example, individuals may consider the positive drive generated by benefits such as improving performance (Hsu & Lin, 2016; Kim et al., 2019) before deciding whether to use IoT services. In contrast, the risk of personal data leakage (Hsu & Lin, 2016; Kim et al., 2019; Pal et al., 2021; Princi & Krämer, 2020) or device failure (Alraja, 2022) in using IoT services is an opposing driving force. When individuals' positive drive is much higher than their negative drive, IoT services may be used, but not vice versa (Kim et al., 2019).

Risk perception has a considerable influence on the motivation of IoT technology product users. Users with certain risk perceptions may reduce their willingness to adopt such products (Aggarwal et al., 2020; Hasan et al., 2023; Pal et al., 2021; Princi & Krämer, 2020; H. Yang et al., 2017; W. Zhang & Liu, 2022). For Privacy Calculus Theory, related IoT studies (Kim et al., 2019; Princi & Krämer, 2020) have revealed that when individuals perceive the benefits of technology products, they might have a higher tolerance for risks, which could prompt them to be willing to provide their data to obtain the services or benefits provided by suppliers. Recent studies have also revealed that the impact of benefit perception on IoT users was more stable than that of risk perception (Kim et al., 2019; Princi

& Krämer, 2020). A concept related to the Privacy Calculus Theory is the privacy paradox, which concerns users' privacy-related decisions and behaviors (Cloarec et al., 2024). The privacy paradox refers to the divergence between privacy attitudes and actual behavior, in which users may indicate that they care about their privacy but rarely take protective actions (Barth & de Jong, 2017; F. Zhang et al., 2023). Regarding the privacy paradox, people may be more inclined to pursue immediate benefits and ignore potential long-term privacy risks in some cases (Barth & de Jong, 2017). Accordingly, Privacy Calculus Theory is an explanatory framework used to describe users' rational calculation processes in information disclosure decisions, while the privacy paradox is an observational phenomenon used to describe the contradiction between users' privacy attitudes and their actual behaviors. This behavior may be inconsistent with their initial trade-offs when making privacy calculations, thus presenting a privacy paradox phenomenon (Cloarec et al., 2024).

The Models Depict the Adoption of IoT Technology

The Theory of Planned Behavior (TPB; Ajzen, 1985, 2002) is a behavioral decision model primarily used to predict and understand human behavior in marketing, advertising, and public relations (Mital et al., 2018). The TPB has also been applied to research on prosocial behaviors, nutritional interventions, and pro-environmental psychology (Mital et al., 2018; W. Zhang & Liu, 2022). The Technology Acceptance Model (TAM; Davis et al., 1989) is another widely used model for exploring an individual's behavior or intention to adopt an IoT technology product (Kumar et al., 2023). These two theories were inspired by the Theory of Rational Action (TRA; Ajzen & Fishbein, 1973), which has been used to explain how attitudes rationally influence individual behavior. The Unified Theory of Acceptance and Use of Technology (UTAUT/2; Venkatesh et al., 2003, 2012) is a synthesis of several theories, such as TAM and TPB. The UTAUT2 has been widely applied in IoT research (Kumar et al., 2023). These four models have been applied to explain emerging technology adoption behavior or intention (Kumar et al., 2023; Mital et al., 2018; Pal et al., 2020).

Several related studies have shown that the TAM fails to adequately explain the behavioral intention of IoT technology adoption behavior (e.g., Almazroi, 2023; Pal et al., 2020; H. Yang et al., 2017). The antecedent factors of the TAM are benefit perceptions, which have a positive driving force. Nevertheless, the TAM does not include the factor of subjective norms and ignores the psychological factor of social influence, which TRA focuses on. On the contrary, the TPB is a TRA modification, adding a behavioral control factor (Hansen et al., 2018). Additionally, nine factors in the UTAUT2 model may fail to fit the parsimony principle of Structural Equation Modeling (SEM; Kline, 2011). Based on the above discussion, the TPB may be more suitable for predicting users' IoT intentions and behavior (W. Zhang & Liu, 2022). However, as technology evolves, new technologies and products require more user information or digital footprints to provide customized services (Henry et al., 2022; Q. Yang, 2021). These models gradually fail to comprehensively explain technology adoption behavior (Zhang & Liu, 2022). Therefore, the TPB may need to be modified to include the risk perception factor for explaining IoT adoption (Hasan et al., 2023; H. Yang et al., 2017; W. Zhang & Liu, 2022).

The TPB assumes that behavior is predicted by behavioral intention, which refers to an individual's tendency and degree of action to engage in a particular behavior. Use intentions are predicted by attitudes, subjective norms, and behavioral control (Ajzen, 2002). Attitude is an individual's predisposition to perceive a particular thing or idea positively or negatively. Subjective norms refer to the social influence of significant others an individual perceives when adopting a particular behavior. Behavioral control is one's perceived ability to control the processes when engaging in a specific activity. In addition, the TPB assumes that behavior is predicted by behavioral control. This model was proposed several decades ago. Early technology products may not have required users to provide so much personal data, so risk perception may not have been a critical prerequisite at that time. This discussion also shows the need to adjust the TPB with risk perception in the current research on IoT usage (Hasan et al., 2023; H. Yang et al., 2017; W. Zhang & Liu, 2022).

Several studies have incorporated the TPB to explain users' IoT adoption (e.g., Almazroi, 2023; Alraja, 2022; Hasan et al., 2023; Pal et al., 2020; H. Yang et al., 2017; W. Zhang & Liu, 2022). Among these studies, the risk perception factor was considered in some (e.g., Alraja, 2022; Hasan et al., 2023; H. Yang et al., 2017; W. Zhang & Liu, 2022). For example, Alraja (2022) combined the TPB and Privacy Calculus Theory to examine healthcare providers' behavioral intention to use IoT-enabled healthcare applications. However, the actual behavior factor was rarely incorporated into models in these studies. Besides, the proposed models in these studies were extended to a more complex extent to include risk perception or other factors. Such a complex model may not comply with the

parsimony principle of SEM (Kline, 2011). Therefore, to explain the adoption behavior of IoT, the proposed model in the current study needs to follow the parsimony principle of SEM.

This study adopted the TPB to explore undergraduates' IoT use behavior. The model was revised, refined, and incorporated with the risk perception factor by discussing findings from previous studies. Furthermore, the application of the TPB in IoT usage research is limited (Kumar et al., 2023; Mital et al., 2018). In addition to providing empirical evidence for the rational process of this model, this study may also improve its inferences.

The Antecedent Factors of IoT Adoption Intention and Behavior

If people have a positive attitude toward IoT, they may have the intention to invest time and resources in understanding and using IoT devices (George et al., 2021; Mital et al., 2018; H. Yang et al., 2017; W. Zhang & Liu, 2022). In addition, the correlation between attitude and intention factors has always existed in the TRA, TPB, and TAM models (H. Yang et al., 2017). Attitudes toward the perceived benefits or usefulness have been found to affect IoT technology adoption intentions (e.g., Almazroi, 2023; George et al., 2021; Hasan et al., 2023; Hsu & Lin, 2016; Mital et al., 2018; H. Yang et al., 2017; W. Zhang & Liu, 2022). A study by van der Zeeuw et al. (2023) revealed that IoT remote access and scheduling functions could provide households with convenience, which determined their intentions to use IoT devices. For example, if people have the attitude that the robot vacuum can effectively clean the floor and improve their work efficiency, they may intend to adopt this technology. However, some studies also found that attitudes were not necessarily an essential antecedent of IoT technology adoption intentions in some cohorts (e.g., Alraja, 2022). For example, robot vacuums may be too expensive for some people to afford. Such a relationship may appear inconsistent. Thus, the first hypothesis (H) is as follows:

H1: Attitudes have a positive effect on IoT use intention.

Potential users of emerging technologies lack sufficient information to decide to adopt technology. Therefore, users' adoption of emerging technologies may be affected by the opinions of their peers (H. Yang et al., 2017). Such a factor mainly includes subjective norms or social influences. Users' intentions may increase when IoT services have social influences or high subjective norms (George et al., 2021). Subjective norms have been found to affect IoT technology adoption intentions (e.g., Alraja, 2022; George et al., 2021; Mital et al., 2018; H. Yang et al., 2017). For example, if people's peers use robot vacuums, they may intend to adopt them. However, some studies also found that subjective norms were not necessarily an essential antecedent of IoT technology adoption intentions (e.g., W. Zhang & Liu, 2022). For example, a study by van der Zeeuw et al. (2023) revealed that users of vacuum cleaners felt these machines were intrusive to the homemakers' domain and perceived a loss of control and quality in this domain. If people's significant others have negative opinions about robot vacuums after using them, this situation may influence people's intention to adopt them. Accordingly, the hypothesis is as follows:

H2: Perceived subjective norms have a positive effect on IoT use intention.

Relevant scholars (Aggarwal et al., 2020; Hasan et al., 2023; H. Yang et al., 2017; W. Zhang & Liu, 2022) have pointed out that benefit perception alone cannot effectively predict IoT behavioral intentions. Since IoT technology can interconnect products and third parties through the Internet or other connection technologies (Paupini et al., 2022), risk perception impacts individuals' IoT behavioral intentions. Moreover, the risk perceptions have been included in the Privacy Calculus Theory to explain the adoption of IoT (e.g., Alraja, 2022; Hsu & Lin, 2016; Kim et al., 2019; Pal et al., 2021; Princi & Krämer, 2020). Therefore, to correctly predict current IoT behavior intentions, factors related to risk perception should be added to the TPB model (Hasan et al., 2023; H. Yang et al., 2017; Zhang & Liu, 2022). The factor of behavioral control in the TPB was modified to risk perception of behavioral control in the current study. The risk perception of behavioral control is defined as users' risk perceptions of controlling a particular technology when adopting these technology products (Hansen et al., 2018; Hsu & Lin, 2016; Kim et al., 2019; van Deursen et al., 2021). Risk perception has been found to affect IoT technology adoption intentions both negatively (e.g., Aggarwal et al., 2020; Hsu & Lin, 2016; W. Zhang & Liu, 2022) and positively (e.g., Hasan et al., 2023). Such a relationship may appear inconsistent. In addition, risk perception has been found to affect actual IoT use negatively (e.g., Princi & Krämer, 2020). For example, a robot vacuum typically scans a home layout and stores it in a cloud system to help it navigate and clean. This measure may cause users to worry about sensitive information in the home setting being leaked or controlled by information equipment companies. These concerns may reduce the intended and actual use of the device. Accordingly, the following are hypothesized:

H3: Risk perceptions of behavioral control have a negative effect on IoT use intention.

H4: Risk perceptions of behavioral control have a negative effect on IoT use behavior.

Usually, users' intentions signal preparation for behavioral action (Ronaghi & Forouharfar, 2020). When users have a specific usage intention, they may take corresponding behavioral actions to satisfy this intention (J. H. Chen et al., 2020). In addition, the relationship between these two factors has always existed in the TRA, TPB, and TAM models. This relationship has been studied and verified in IoT research (Kumar et al., 2023). Intentions have been found to affect IoT technology adoption behaviors (e.g., Alkawsi et al., 2020; Princi & Krämer, 2020; Ronaghi & Forouharfar, 2020). For example, if people intend to adopt a robot vacuum, they may be more likely to actually adopt this technology product. However, some studies also found that intentions were not necessarily an essential antecedent of IoT technology adoption behaviors (e.g., J. H. Chen et al., 2020). For example, people trying to use a robot vacuum may be too busy to actually go to a store to select and purchase the product. Accordingly, the hypothesis is as follows:

H5: Use intention has a positive effect on IoT use behavior.

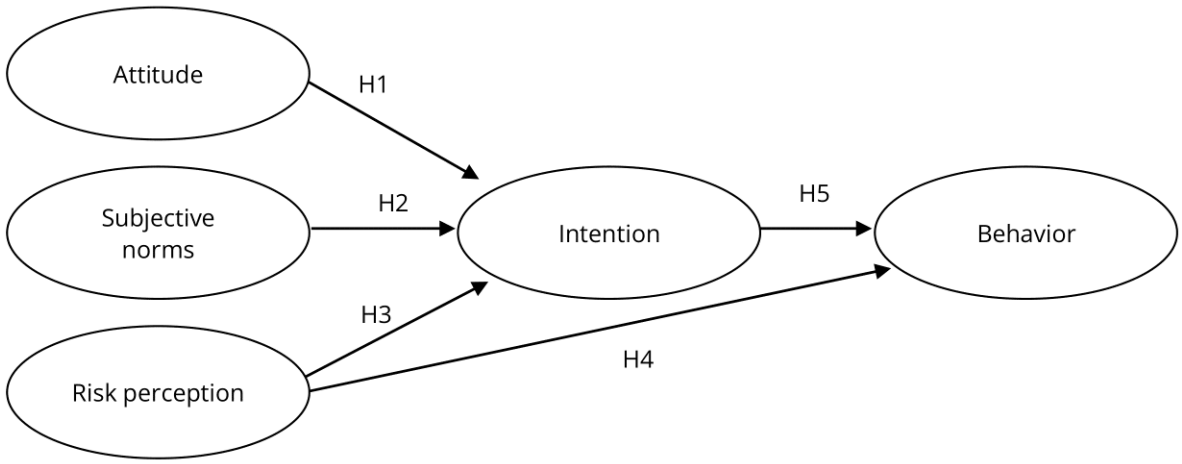
From the above discussion, the literature review of the TPB and Privacy Calculus Theory shows that both benefit and risk perceptions are essential and cannot be ignored (Hasan et al., 2023; H. Yang et al., 2017; W. Zhang & Liu, 2022). Therefore, the interactive relationship between benefit and risk perceptions should be explored more clearly in this study to further understand their effect on IoT users' intentions and behavior. Thus, this study assumed that the antecedent factors of IoT use intentions and behaviors included users' attitudes, subjective norms, and perceived risk of behavioral control.

Methods

Research Method and Framework

The survey research method was adopted in this study, and data were collected using questionnaires. SEM was used to verify the TPB model and predict undergraduates' IoT use intentions and behaviors. According to the theoretical basis discussed above, the research framework was proposed in this study, as shown in Fig. 1; it comprises the five research hypotheses mentioned above (H1~H5).

Figure 1. *Research Framework of This Study.*



Participants

The research team selected three universities in northern, central, and southern Taiwan as participant sources by purposive sampling. In purposive sampling, the researcher directly (rather than randomly) selects a subset representing the entire population (Fraenkel et al., 2012). Since Taiwan has several science and technology universities, one university of science and technology in southern Taiwan was also selected. A total of 412 questionnaires were returned from November 2021 to March 2022. Among them, 246 (59.7%) were from male, and 166 (40.3%) were from female respondents. Science majors accounted for 285 (69.1%) responses, and non-science majors for 127 (30.9%). These undergraduates ranged in age from 18 to 27 years old, with an average age of 20.3 years.

Instrument

The instrument in this study included five subscales: *attitude*, *subjective norms*, *risk perception of behavioral control*, *intention*, and *behavior* (see Table 1). The instrument was designed based on the idea of the *IoT ecosystem*, which includes users, devices, and services (Shin & Park, 2017). In the preface of the questionnaire, the context of using devices or services, including smart watches, smart bracelets, robot vacuums, and wireless cameras, was set in a smart home. Using a Likert-scale item, respondents may more frequently declare themselves neutral on a 5-point Likert scale, while a 4-point Likert scale without a neutral point may force respondents to be more thoughtful and express more accurate ratings (Adelson & McCoach, 2010). Some scholars, therefore, used 4-point scales in their studies (e.g., Caspi et al., 2019; Xu & Leung, 2018). The 4-point Likert scale was thus applied in this study. The first four subscales were scored using the 4-point Likert scale. These options were designed as *strongly disagree, disagree, agree*, and *strongly agree*, and each option was scored as 1 to 4 points. The *behavior* subscale, for instance, was scored using the 4-point Likert scale. The options were *never, rarely, sometimes*, and *often*, and a score of 1 to 4 was given.

The *attitude* subscale (Kim et al., 2019) consisted of five items, with Cronbach's α reliability of .87. An example item is: *Using this IoT service would improve my performance*. The *subjective norms* subscale (Hsu & Lin, 2016), which consisted of four sub-items, had a Cronbach's α reliability of .94. An example item is: *Most people in my peer group frequently use IoT devices*. The *risk perception of behavioral control* subscale (van Deursen et al., 2021) consisted of three items, and its Cronbach's alpha reliability was .79. An example item is: *Using IoT will control our lives*. The use *intention* subscale (Hsu & Lin, 2016) consisted of three items, and Cronbach's α reliability was .87. An example item is: *I intend to continue using IoT services*. The *behavior* subscale was designed according to Durndell and Haag's (2002) study. There were three items in this subscale, and Cronbach's alpha reliability was .87. An example item is: *I have used IoT products in the past year*.

Table 1. *The Sub-Scales, Example Items, and Cronbach's α of the Instrument.*

Scales	Example items	Number of items	Cronbach's α
Attitude	Using this IoT service would improve my performance.	5	.87
Subjective norms	Most people in my peer group frequently use IoT devices.	4	.94
Risk perception of behavioral control	Using IoT will control our lives.	3	.79
Intention	I intend to continue using IoT services.	3	.87
Behavior	I have used IoT products in the past year.	3	.87

Research Process

The research team first emailed the four university staff to obtain consent to issue the questionnaires. The Google Forms system was the online platform to create and distribute the questionnaires. When administering the questionnaire, the instructor or teaching assistant explained the study and obtained students' consent. After that, they explained that the context of IoT was focused on smart homes and their devices. Meanwhile, the questionnaire link was sent to students who agreed to fill in the questionnaire. Students who completed the questionnaire received a stationery gift. The collected data were converted from the Google Forms system into Excel and SPSS files for later analyses.

Data Analyses

SEM was adopted to test the model fit of the theoretical model in this study, using the software AMOS 18 with Maximum Likelihood for parameter assessment. The measurement and structural model fit from two aspects of external and internal quality were examined: The external quality index was as follows: The root mean square error of approximation (RMSEA) was less than .06, the standardized root mean square residual (SRMR) was less than .08 (Hu & Bentler, 1999). The measure fits included the goodness-of-fit index (GFI) and the comparative fit index (CFI) greater than .90 (Hu & Bentler, 1999). The internal quality was as follows: the average variance extracted (AVE) values of the latent variables were above .5, and the composite reliability was above .6 (Fornell & Larcker,

1981). Moreover, the bootstrap analysis of SEM, based on Baron and Kenny's (1986) approach, was used to confirm mediation effects (Cheung & Lau, 2008).

Results

Assessment of the Measurement Model Fit

Regarding the correlation of observed variables, a correlation matrix was analyzed according to Pearson's product-moment correlation, as shown in Table 2. These correlation coefficients among latent variables ranged from .03 to .62. Correlation coefficients below .80 indicate no multicollinearity issues (Hutcheson & Sofroniou, 1999). The mean, standard deviation (*SD*), skewness, and kurtosis coefficients of the observed variables in this study are also listed in Table 2. The range of skewness coefficients is between −0.41 and −0.03. The range of kurtosis coefficients is between −0.73 and 2.69. The cases of skewness under 3 and kurtosis under 10 show that the observed variables align with normal distribution (Kline, 2011).

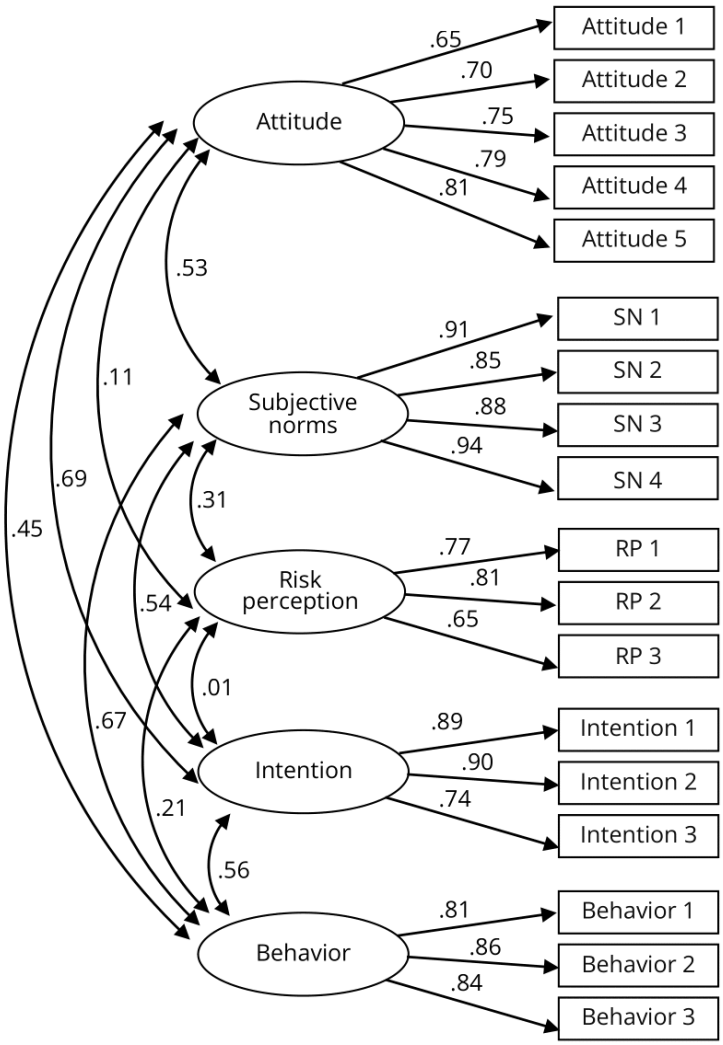
Table 2. *Descriptive Statistics and Pearson's Correlation Matrix of the Variables.*

Latent variables	1	2	3	4	5
1. Attitude	.74				
2. Subjective norms	.43***	.89			
3. Risk perception of behavioral control	.09	.29***	.75		
4. Intention	.60***	.50***	.03	.85	
5. Behavior	.36***	.62***	.19***	.52***	.84
M	3.06	2.93	2.49	3.03	2.67
SD	0.43	0.68	0.61	0.52	0.85
Skewness	−0.19	−0.28	−0.03	−0.41	−0.26
Kurtosis	2.69	0.17	0.26	1.94	−0.73
AVE	.55	.80	.56	.72	.70
CR	0.86	0.94	0.79	0.88	0.88

Note. ***p < .001; the coefficients on the diagonal represent the root of AVE of each variable.

The measurement model is shown in Fig. 2. The model fit analysis results of the measurement model (confirmatory factor analysis, CFA) were GFI = .93, CFI = .97, RMSEA = .06, and SRMR = .05, all of which met the model fit standard regarding external quality. All factor loadings ranged from .65 to .94. In terms of internal quality (see Table 2), the reliability test results showed that the AVE coefficients of the five latent variables of *attitude*, *subjective norms*, *risk perception of behavioral control*, *intention*, and *behavior* were .55, .80, .56, .72, and .70, respectively, which were all above the criterion of .5. In addition, the composite reliability coefficients of the five latent variables were .86, .94, .79, .88, and .88, respectively, which were also all above the criterion of .6. As shown in Table 2, the correlation coefficients of each variable with other variables were less than the square root of the AVE of that variable. This result means that the requirements for discriminant validity were satisfied (Fornell & Larcker, 1981). The above results indicate that the internal quality was acceptable. This model conforms to acceptable criteria for external and internal quality, representing that the factors can explain all latent variables.

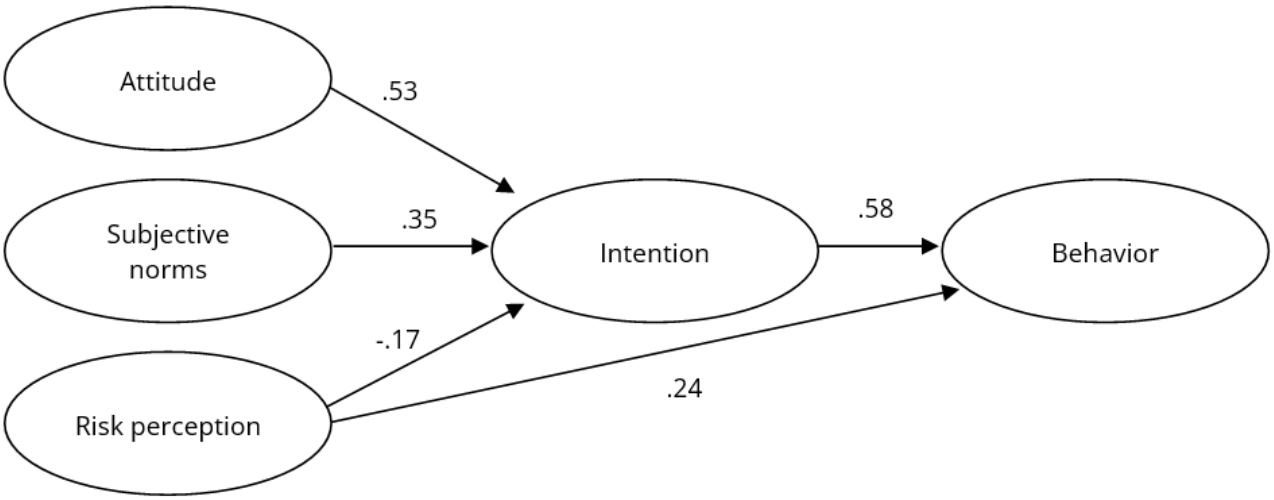
Figure 2. *The Measurement Model of Scales in This Study*.



Assessment of the Structural Model Fit

In this study, the relationships among factors of students' IoT use intention and behavior were investigated. Fig. 3 shows the tested model with standardized path coefficients, which all reached significance (p < .001). The test results of the structural model were GFI = .92, CFI = .95, RMSEA = .06, and SRMR = .07, all of which met the model fit standards. This model conforms to acceptable criteria for structural model quality and represents the factors that can be used to explain undergraduates' IoT use behavior and intentions.

Figure 3. *The Result of the Structural Model in This Study*.



The effects of each latent variable in the model were analyzed as shown in Fig. 3. The *attitude* and *subjective norms* variables had direct positive effects on *intention,* respectively (β = .53 and β = .35), while *risk perception of behavioral control* had a direct negative effect on *intention* (β = −.17). The *intention* variable had a direct positive effect on the *behavior* variable (β = .58). This result showed that if undergraduates perceived higher attitudes and subjective norms, they also had higher IoT use intention. However, undergraduates with a higher risk perception of IoT products had lower intentions to use them. In addition, the results showed that if the undergraduates had higher IoT use intentions, they also had a higher frequency of behavior.

The indirect effects of each latent variable were tested using bootstrap analysis, as shown in Table 3. The total effect of the first path was .31. The overall effect of the second path was .20. The third path could be confirmed as a partial mediation effect. The above analysis shows that undergraduates' *risk perception of behavioral control* variable had an effect on the IoT *behavior* variable. In addition, it also shows that the effect of undergraduates' *risk perception of behavioral control* variable on the *behavior* variable included a direct effect (.24) and an indirect effect (−.10) through the *intention* variable. The total effect of the fourth path was .14, while the total effect of the fifth path was .58. This model explained 56% of the variance in IoT use *intention* (R^2 = .56) and 39% of the variance in IoT use *behavior* (R^2 = .39).

Table 3. *Indirect Effect Analysis by Using Bootstrapping.*

Paths	Direct effects	Indirect effects	Total effects
1. Attitude → Intention → Behavior	—	.31 [.23, .39]	.31 [.23, .39]
2. Subjective norms → Intention → Behavior	—	.20 [.12, .29]	.20 [.12, .29]
3. Risk perception of behavioral control → Intention → Behavior	—	−.10 [−.18, −.04]	—
4. Risk perception of behavioral control → Behavior	.24 [.12, .33]	—	.14 [.02, .25]
5. Intention → Behavior	.58 [.48, .67]	—	.58 [.48, .67]

Note. Standardized coefficient [95% confidence interval].

Discussion

The results of the current study showed that undergraduates' *attitudes* had a direct effect on their IoT use *intention* (β = .53); thus, H1 was accepted. This result is in line with previous IoT research on the relationship between attitude and intention (Almazroi, 2023; George et al., 2021; Hasan et al., 2023; Hsu & Lin, 2016; Mital et al., 2018; H. Yang et al., 2017; W. Zhang & Liu, 2022). Scholars have found that attitude is a critical antecedent factor influencing the intention of individuals to adopt IoT products (Hsu & Lin, 2016; van Deursen et al., 2021). The perceived benefits of IoT products have a positive effect on the intention to use them (Hsu & Lin, 2016; Kim et al., 2019). If undergraduates perceive IoT to improve their daily and homework performance, they might intend to use it.

Moreover, the results of the current study showed that *subjective norms* had a direct effect on the *intention* to use IoT products (β = .35); thus, H2 was accepted. This result is roughly in line with previous studies on the relationship between subjective norms or social influence and the use intention of IoT (Alraja, 2022; George et al., 2021; Mital et al., 2018; H. Yang et al., 2017). Schepers and Wetzels (2007) conducted a meta-analysis of 63 technology adoption studies and found that subjective norms were an essential factor in the intention to adopt technology. Social psychologists believe that users' significant others can change their opinions about product adoption (Schepers & Wetzels, 2007). IoT products have become more diverse in recent years, and their users are increasing. Family or friends of undergraduates may become facilitators of their intention to use IoT products.

Furthermore, the results of the current study showed that *risk perception of behavioral control* had a direct effect on undergraduates' IoT use *intention* (β = −.17); thus, H3 was accepted. This result was consistent with related research on IoT usage (Aggarwal et al., 2020; Hsu & Lin, 2016; W. Zhang & Liu, 2022). These results also echo the Privacy Calculus Theory that asserts the dual driving forces of perceived benefit and risk on technology adoption intention. If undergraduates had a risk perception that IoT may control their lives, their future use intentions might be lower. This perception may be related to IoT products connecting to the Internet to exchange data (Hsu & Lin, 2016; Kim et al., 2019). However, regarding the predictive power of users' intention to use the IoT, the effect of perceived benefit (*attitude* variable) was higher than that of risk perception. Hsu and Lin (2016) speculated that IoT is still a new technology service. Users may have a limited understanding of this technology and be unable to accurately assess the seriousness of the risks. It is easy for users to imagine that the benefits outweigh the costs

(risks). Recent studies revealed a similar result (Kim et al., 2019; Princi & Krämer, 2020), in which the users' perceived benefit was a stronger antecedent of intention to provide private information than perceived risk. Kim et al. (2019) explained that if the product provides some services and benefits that users need, users may reduce their risk perception and be willing to provide their private information. The qualitative interview data of Hsu and Lin (2016) showed that the convenience and benefits of IoT technology were unprecedented and might make individuals underestimate the importance of risk issues.

IoT technology adoption studies (e.g., Aggarwal et al., 2020) have shown that users sometimes overestimate the advantages of the perceived benefits, and underestimate the threat of risk perceptions when making decisions. Users may exchange personal information for specific services or benefits (W. Zhang & Liu, 2022). Another possible reason is that the risk issues are hypothetical events that have not occurred to users, so they differ from the realistic consideration (Distler et al., 2020). Besides, some studies (Kim et al., 2019) have shown that users' cognitive changes may also be one of the reasons for adopting technology in different time and space scales. Contemporary people's trust in technology products is higher than before, reducing their risk perception (Hansen et al., 2018).

In addition, the results of the current study showed that users' *intentions* had a direct effect (β = .58) on their *behavior* related to IoT products; thus, H5 was accepted. This result was consistent with previous IoT research on the relationship between users' intentions and behavior (Alkawsi et al., 2020; Princi & Krämer, 2020; Ronaghi & Forouharfar, 2020). Intention is the degree to which people consciously plan to execute certain future behaviors (Ronaghi & Forouharfar, 2020). Intention has been recognized by some important models (e.g., TRA and TAM) as an essential factor in predicting technology use. In emerging IoT technology, users' intentions are still essential to their behavior.

The results of the current study showed that users' *risk perception of behavioral control* had a positive effect on their IoT *behavior* (β = .24); thus, H4 was rejected. Previous studies mostly observed the behavior of IoT technology use from the perspective of benefit perception, while fewer studies have focused on this relationship (Hsu & Lin, 2016). The current study thus provides additional insights into this research area. The current study showed inconsistent results with Princi and Krämer's (2020) study, which found that users' perceived risks in using IoT healthcare devices negatively affected their actual use. Unlike the data collected from smart home IoT devices, the data collected by IoT healthcare devices is special personal data. Once users perceive a risk, it might affect their actual use. This factor might be the reason why the result of the current study differed from Princi and Krämer's (2020) findings. Additionally, the *risk perception of behavioral control* variable in the current study was used to replace the behavioral control variable in the original TPB model. The updated model suggests that undergraduates' risk perception of behavioral control might play a role in their IoT use intentions and behaviors. The results of the current study contribute to understanding the relationship among undergraduates' risk perceptions, use intention, and use behavior of IoT products. Undergraduates might have prior experience with other digital products, and could understand and bear the potential risks of these products. Undergraduates with higher risk perceptions might have higher IoT usage but less intention to use it in the future and to recommend it to friends. This relationship caused a *suppression effect* between the risk perception and the user behavior variables. In the statistics, the suppression effect reduced the effect in the relationship between the independent and dependent variables since the mediating variable explained part of the effect (Cheung & Lau, 2008; MacKinnon et al., 2000). The prediction effect of undergraduates' risk perceptions of their IoT behavior may reduce the overall predictive effect due to the mediating variable of intention.

Observed from the overall theoretical model, the TPB was modified from the TRA (Hansen et al., 2018; Pal et al., 2020), which assumes that users' behavior is generated after obtaining some information and rational thinking. In addition, the Privacy Calculus Theory also assumes that users' behavior when using information products is based on rational judgments (Ostendorf et al., 2022; Princi & Krämer, 2020). However, from the results of the current study, undergraduates' IoT use intention and behavior might not be entirely rational, but rather contradictory in nature due to the risk perception. The results revealed that under rational judgment, undergraduates' IoT use intention would be predicted by benefit perception (H1) and social influence (H2). Undergraduates with higher risk perceptions might have a lower intention to use IoT in the future and might be less likely to recommend it to their peers (H3). Hansen et al. (2018) had similar findings that perceived trust positively and perceived risk negatively predicted an individual's risk-taking propensity to use technology. However, undergraduates with higher risk perceptions in the current study used more IoT (H4). The results of H3 and H4 seem to be contradictory. These results might echo the privacy paradox phenomenon (Barth & de Jong, 2017; Cloarec et al., 2024; F. Zhang et al., 2023). Individuals' perceived risk and trust in this decision-making process using technology products are complex, finally counterbalancing a person's identified risk-taking propensity (Hansen et al., 2018). Perceptions of these

risks meant that the use of these IoT devices with considerable caution by undergraduates influenced their future use intentions, or they were less likely to recommend the devices to their peers. Nonetheless, undergraduates with higher risk awareness might have a demand or impulse to use IoT devices (Ostendorf et al., 2022), could bear this kind of risk, and have a higher frequency of IoT device usage.

Conclusions

The TPB model was used in this study to explain undergraduates' use intention and behavior of IoT in the smart home context. The behavioral control variable in the original TPB model was replaced with the *risk perception of behavioral control* variable. The results revealed that undergraduates' *attitudes* and *subjective norms* had a positive effect on their intention to use IoT, which, in turn, had effects on their IoT use *behavior*. It was also found that undergraduates' *risk perception of behavioral control* had a negative effect on their IoT use *intention*. However, undergraduates' *risk perception of behavioral control* had a positive direct effect on their IoT use *behavior*. The current study contributes to the current state of knowledge since the proposed model revealed that undergraduates' adoption of the Internet of Things might not be entirely rational. Their risk perception of behavioral control might play a particular role.

Undergraduates intensify their intention to use IoT because of their perceived benefits and the use of these technologies by significant others. In everyday life, however, risks are ubiquitous, and the same is true when using IoT products. Undergraduates might have experience with other digital products and understand the possible risks. Regarding technology education, the perception of these risks means that IoT users had considerable caution but reduced their intention to use IoT. From the perspective of promoting technology use, IoT device vendors may provide users with awareness programs to avoid problematic use. This strategy may gain users' trust and reduce the impact of risk perception on intention (Hansen et al., 2018). In addition, IoT system vendors may promote user-centered product design (Q. Yang, 2021). They may encourage developers to consider users' needs and rights when designing IoT products and services and fully consider users' opinions and feedback. This design includes providing reliable control and management capabilities that allow users to tailor the behavior of IoT systems to their preferences and needs. Moreover, IoT systems may provide transparent mechanisms to allow users to manage their usage records and digital footprints in a convenient way (Henry et al., 2022), such as providing a user interface or control panel. Individuals may have the right to control their digital footprints, including viewing, modifying, and deleting them. This measure may enable individuals to weigh the balance between risk and reward when sharing data for IoT services. Governments and businesses may take this into consideration when designing and implementing IoT systems to ensure that the collection and use of digital footprints are reasonable and beneficial to the overall interests of individuals and society.

Several research limitations of the current study should be noted. To strengthen the representativeness of the sample, the research team selected universities in northern, central, and southern Taiwan as the source of participants. The number of male and female participants was uneven due to the purposive sampling of the universities. This process might have caused bias in the study results. Future studies may duplicate the same research framework to confirm the results. The sample was limited to undergraduates. If the model of this study were used with other cohorts, the predictive effect might be different. In addition, the TPB model was updated to include a risk perception variable in the current study, replacing the behavioral control variable. However, risk perception is not conceptually equivalent to perceived behavioral control. This premise should be recognized when using the structural model of the current study to infer other technology adoption behaviors. Moreover, the proposed model in this study explained 56% of the variance in IoT use intention, and 39% of the variance in IoT use behavior. These results mean additional research is required to comprehend the remaining 44% and 61% of the variances. Finally, follow-up experimental studies may be conducted to confirm the exact causal relationship between the variables.

Conflict of Interest

The author has no conflicts of interest to declare.

Author's Contribution

This study was devised and conducted by **Chun-Yen Tsai**.

Acknowledgement

The work reported here was supported by the National Science and Technology Council, Taiwan, under grants MOST 110-2511-H-110-010-MY2. The authors also greatly appreciate the assistance of Mr. Po-jen Hsieh and the valuable suggestions of the journal reviewers and editors.

References

Adelson, J. L., & McCoach, D. B. (2010). Measuring the mathematical attitudes of elementary students: The effects of a 4-point or 5-point Likert-type scale. *Educational and Psychological Measurement, 70*(5), 796–807. https://doi.org/10.1177/0013164410366694

Aderibigbe, N., Ocholla, D., & Britz, J. (2021). Differences in ethical cyber behavioural intention of Nigerian and South African students: A multi-group analysis based on the theory of planned behaviour. *Libri-International Journal of Libraries and Information Studies, 71*(4), 389–406. https://doi.org/10.1515/libri-2019-0062

Aggarwal, N., Albert, L. J., Hill, T. R., & Rodan, S. A. (2020). Risk knowledge and concern as influences of purchase intention for Internet of things devices. *Technology in Society, 62*, Article 101311. https://doi.org/10.1016/j.techsoc.2020.101311

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11–39). Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-69746-3_2

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I., & Fishbein, M. (1973). Attitudinal and normative variables as predictors of specific behavior. *Journal of Personality and Social Psychology, 27*(1), 41–57. https://doi.org/10.1037/h0034440

Alkawsi, G. A., Ali, N., & Baashar, Y. (2020). An empirical study of the acceptance of IoT-based smart meter in Malaysia: The effect of electricity-saving knowledge and environmental awareness. *IEEE Access, 8*, 42794–42804. https://doi.org/10.1109/ACCESS.2020.2977060

Almazroi, A. A. (2023). An empirical investigation of factors influencing the adoption of Internet of things services by end-users. *Arabian Journal for Science and Engineering, 48*(2), 1641–1659. https://doi.org/10.1007/s13369-022-06954-8

Alraja, M. (2022). Frontline healthcare providers' behavioural intention to Internet of things (IoT)-enabled healthcare applications: A gender-based, cross-generational study. *Technological Forecasting and Social Change, 174*, Article 121256. https://doi.org/10.1016/j.techfore.2021.121256

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. https://doi.org/10.1037/0022-3514.51.6.1173

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Baudier, P., Ammi, C., & Deboeuf-Rouchon, M. (2020). Smart home: Highly-educated students' acceptance. *Technological Forecasting and Social Change, 153*, Article 119355. https://doi.org/10.1016/j.techfore.2018.06.043

Binder, A. R., Cacciatore, M. A., Scheufele, D. A., Shaw, B. R., & Corley, E. A. (2012). Measuring risk/benefit perceptions of emerging technologies and their potential impact on communication of public opinion toward science. *Public Understanding of Science, 21*(7), 830–847. https://doi.org/10.1177/0963662510390159

Caspi, A., Gorsky, P., Nitzani-Hendel, R., Zacharia, Z., Rosenfeld, S., Berman, S., & Shildhouse, B. (2019). Ninth-grade students' perceptions of the factors that led them to major in high school science, technology, engineering, and mathematics disciplines. *Science Education, 103*(5), 1176–1205. https://doi.org/10.1002/sce.21524

Chen, J. H., Ha, N. T. T., Tai, H. W., & Chang, C. A. (2020). The willingness to adopt the Internet of things (IoT) conception in Taiwan's construction industry. *Journal of Civil Engineering and Management, 26*(6), 534–550. https://doi.org/10.3846/jcem.2020.12639

Chen, Y. T., Shih, W. L., Lee, C. H., Wu, P. L., & Tsai, C. Y. (2021). Relationships among undergraduates' problematic information security behavior, compulsive Internet use, and mindful awareness in Taiwan. *Computers & Education, 164*, Article 104131. https://doi.org/10.1016/j.compedu.2021.104131

Cheryl, B.-K., Ng, B.-K., & Wong, C.-Y. (2021). Governing the progress of Internet-of-things: Ambivalence in the quest of technology exploitation and user rights protection. *Technology in Society, 64*, Article 101463. https://doi.org/10.1016/j.techsoc.2020.101463

Cheung, G. W., & Lau, R. S. (2008). Testing mediation and suppression effects of latent variables: Bootstrapping with structural equation models. *Organizational Research Methods, 11*(2), 296–325. https://doi.org/10.1177/1094428107300343

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2024). Transformative privacy calculus: Conceptualizing the personalization-privacy paradox on social media. *Psychology & Marketing, 41*(7), 1574–1596. https://doi.org/10.1002/mar.21998

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Distler, V., Lallemand, C., & Koenig, V. (2020). How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs. *Computers in Human Behavior*, *106*, Article 106227. https://doi.org/10.1016/j.chb.2019.106227

Durndell, A., & Haag, Z. (2002). Computer self efficacy, computer anxiety, attitudes towards the Internet and reported experience with the Internet, by gender, in an East European sample. *Computers in Human Behavior, 18*(5), 521–535. https://doi.org/10.1016/S0747-5632(02)00006-7

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2012). *How to design and evaluate research in education* (8th ed.). McGraw-Hill.

George, J. F., Chen, R., & Yuan, L. (2021). Intent to purchase IoT home security devices: Fear vs privacy. *PLoS One, 16*(9), Article e0257601. https://doi.org/10.1371/journal.pone.0257601

Hansen, J. M., Saridakis, G., & Benson, V. (2018). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior*, *80*, 197–206. https://doi.org/10.1016/j.chb.2017.11.010

Hasan, N., Bao, Y., Miah, S. J., & Fenton, A. (2023). Factors influencing the young physicians' intention to use Internet of things (IoT) services in healthcare. *Information Development, 39*(4), 902–919. https://doi.org/10.1177/02666669211064114

Henry, C., Gohdes, A., & Dorff, C. (2022). Digital footprints and data-security risks for political scientists. *PS: Political Science & Politics, 55*(4), 804–808. https://doi.org/10.1017/S1049096522000543

Hsu, C.-L., & Lin, J. C.-C. (2016). An empirical examination of consumer adoption of Internet of things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, *62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

Hu, L., & Bentler, P. M. (1999). Cut off criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Hutcheson, G. D., & Sofroniou, N. (1999). *The multivariate social scientist: Introductory statistics using generalized linear models*. Sage Publications. https://uk.sagepub.com/en-gb/eur/the-multivariate-social-scientist/book205684

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior, 92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

Kline, R. B. (2011). *Principles and practice of structural equation modeling* (3rd ed.). Guilford Press. https://psycnet.apa.org/record/2010-18801-000

Kumar, A., Sanjay Dhingra, A., & Falwadiya, H. (2023). Adoption of Internet of things: A systematic literature review and future research agenda. *International Journal of Consumer Studies, 47*(6), 2553–2582. https://doi.org/10.1111/ijcs.12964

Lünich, M., Marcinkowski, F., & Kieslich, K. (2023). It's now or never! Future discounting in the application of the online privacy calculus. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15*(3), Article 11. https://doi.org/10.5817/CP2021-3-11

MacKinnon, D. P., Krull, J. L., & Lockwood, C. M. (2000). Equivalence of the mediation, confounding and suppression effect. *Prevention Science, 1*(4), 173–181. https://doi.org/10.1023/A:1026595011371

Mani, Z., & Chouk, I. (2018). Consumer resistance to innovation in services: Challenges and barriers in the Internet of things era. *Journal of Product Innovation Management, 35*(5), 780–807. https://doi.org/10.1111/jpim.12463

Mital, M., Chang, V., Choudhary, P., Papa, A., & Pani, A. K. (2018). Adoption of Internet of things in India: A test of competing models using a structured equation modeling approach. *Technological Forecasting & Social Change, 136*, 339–346. https://doi.org/10.1016/j.techfore.2017.03.001

Ostendorf, S., Meier, Y., & Brand, M. (2022). Self-disclosure on social networks: More than a rational decision-making process. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16*(4), Article 2. https://doi.org/10.5817/CP2022-4-2

Pal, D., Arpnikanondt, C., Funilkul, S., & Chutimaskul, W. (2020). The adoption analysis of voice-based smart IoT products. *IEEE Internet of Things Journal, 7*(11), 10852–10867. https://doi.org/10.1109/JIOT.2020.2991791

Pal, D., Zhang, X., & Siyal, S. (2021). Prohibitive factors to the acceptance of Internet of things (IoT) technology in society: A smart-home context using a resistive modelling approach. *Technology in Society, 66*, Article 101683. https://doi.org/10.1016/j.techsoc.2021.101683

Paupini, C., van der Zeeuw, A., & Fiane Teigen, H. (2022). Trust in the institution and privacy management of Internet of things devices. A comparative case study of Dutch and Norwegian households. *Technology in Society, 70*, Article 102026. https://doi.org/10.1016/j.techsoc.2022.102026

Perri, C., Giglio, C., & Corvello, V. (2020). Smart users for smart technologies: Investigating the intention to adopt smart energy consumption behaviors. *Technological Forecasting and Social Change, 155*, Article 119991. https://doi.org/10.1016/j.techfore.2020.119991

Philip, S. J., Luu, T., & Carte, T. (2022). There's no place like home: Understanding users' intentions toward securing Internet-of-things (IoT) smart home networks. *Computers in Human Behavior, 139*, Article 107551. https://doi.org/10.1016/j.chb.2022.107551

Princi, E., & Krämer, N. C. (2020). Out of control – privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology, 11*, Article 582054. https://doi.org/10.3389/fpsyg.2020.582054

Roe, M., Spanaki, K., Ioannou, A., Zamani, E. D., & Giannakis, M. (2022). Drivers and challenges of Internet of things diffusion in smart stores: A field exploration. *Technological Forecasting and Social Change, 178*, Article 121593. https://doi.org/10.1016/j.techfore.2022.121593

Ronaghi, M. H., & Forouharfar, A. (2020). A contextualized study of the usage of the Internet of things (IoTs) in smart farming in a typical Middle Eastern country within the context of Unified Theory of Acceptance and Use of Technology model (UTAUT). *Technology in Society, 63*, Article 101415. https://doi.org/10.1016/j.techsoc.2020.101415

Schepers, J., & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information & Management, 44*(1), 90–103. https://doi.org/10.1016/j.im.2006.10.007

Shin, D.-H., & Park, Y. J. (2017). Understanding the Internet of things ecosystem: Multi-level analysis of users, society, and ecology. *Regulation & Governance, 19*(1), 77–100. https://doi.org/10.1108/DPRG-07-2016-0035

Tsai, C.-Y., Shih, W.-L., Hsieh, F.-P., Chen, Y.-A., Lin, C.-L., & Wu, H.-J. (2022). Using the ARCS model to improve undergraduates' perceived information security protection motivation and behavior. *Computers & Education, 181*, Article 104449. https://doi.org/10.1016/j.compedu.2022.104449

van der Zeeuw, A., van Deursen, A. J., & Jansen, G. (2023). The irony of the smart home: How the IoT shifts power balances and reinforces household values. *The Information Society, 39*(3), 171–182. https://doi.org/10.1080/01972243.2023.2189896

van Deursen, A. J., van der Zeeuw, A., de Boer, P., Jansen, G., & van Rompay, T. (2021). Digital inequalities in the Internet of things: Differences in attitudes, material access, skills, and usage. *Information, Communication & Society, 24*(2), 258–276. https://doi.org/10.1080/1369118X.2019.1646777

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178. https://doi.org/10.2307/41410412

Xu, M. L., & Leung, S. O. (2018). Effects of varying numbers of Likert scale points on factor structure of the Rosenberg Self-Esteem Scale. *Asian Journal of Social Psychology, 21*(3), 119–128. https://doi.org/10.1111/ajsp.12214

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: An extension of the theory of planned behavior. *Industrial Management and Data Systems, 117*(1), 68–89. https://doi.org/10.1108/IMDS-01-2016-0017

Yang, Q. (2021). Toward responsible AI: An overview of federated learning for user-centered privacy-preserving computing. *ACM Transactions on Interactive Intelligent Systems, 11*(3–4), Article 32. https://doi.org/10.1145/3485875

Zhang, F., Pan, Z., & Lu, Y. (2023). AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. *Information & Management, 60*(2), Article 103736. https://doi.org/10.1016/j.im.2022.103736

Zhang, W., & Liu, L. (2022). Unearthing consumers' intention to adopt eco-friendly smart home services: An extended version of the theory of planned behavior model. *Journal of Environmental Planning and Management, 65*(2), 216–239. https://doi.org/10.1080/09640568.2021.1880379

About Author

Chun-Yen Tsai is a professor at National Sun Yat-sen University. His research focuses on educational technology and science education. Currently, he participates in some projects granted by the National Science and Technology Council in Taiwan related to educational technology and information education studies.

https://orcid.org/0000-0002-4016-5614

Correspondence to
Chun-Yen Tsai, National Sun Yat-sen University, No.70, Lianhai Rd., Gushan Dist., Kaohsiung City 80424, Taiwan,
ctsai@mail.nsysu.edu.tw