International Journal of Electrical and Computer Engineering (IJECE)
Vol. 16, No. 2, April 2026, pp. 850~862
ISSN: 2088-8708, DOI: 10.11591/ijece.v16i2.pp850-862

Smartphone data privacy and security awareness among university students in Malaysia

Ahmed Al-Rassas[1], Zaheera Zainal Abidin[2]
[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
[2]Faculty of Artificial Intelligence and Cyber Security, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Article Info

Article history:

Received Apr 13, 2025
Revised Nov 26, 2025
Accepted Jan 15, 2026

Keywords:

Cyber-threat Malaysia
Data privacy awareness
Data protection
Mobile internet users
Smartphone privacy

ABSTRACT

This study examines the level of data privacy and security awareness (DPSA) among Malaysian university students who depend on smartphones for academic activities. An enhanced cybersecurity education (CE) technological proficiency–perceived control (CTP) model is proposed, incorporating technological innovation and cultural norms (TICN) as a mediating factor between technological proficiency (TP) and awareness. A total of 356 students from public and private institutions in Melaka participated. The Krejcie and Morgan table was used to determine the sample size. Descriptive analysis was conducted using IBM SPSS 27, and SmartPLS-SEM was used to evaluate both measurement and structural models. Reliability and validity were confirmed through a pilot study with 50 respondents. Findings show that TICN significantly strengthens the translation of technical skills into protective behavior, outperforming the original model that used frequency of smartphone usage (FSU) as a mediator. The enhanced model provides a deeper understanding of the socio-technical determinants of smartphone privacy awareness. Implications, limitations, and directions for future research are also discussed.

Corresponding Author:

Ahmed Al-Rassas
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM)
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
Email: M032310040@student.utem.edu.my

1. INTRODUCTION

Mobile technologies and the internet of things (IoT) have become indispensable to contemporary daily life, extending their influence beyond personal communication to the broader landscape of lifelong learning. In higher education, it has now become common practice to access course material, manage assignments, and participate in digital learning spaces using mobile devices [1]. Smartphones, in particular, serve as primary platforms through which students retrieve course materials, interact with peers, and participate in institutional digital ecosystems that facilitate academic progress [2]. However, the increasing dependence on mobile technologies has also brought substantial cybersecurity vulnerabilities. International studies consistently report rising incidences of phishing, malicious applications, data harvesting, and unsafe browsing practices, identifying low student cybersecurity awareness as a global concern [3]. Evidence from academic communities in the Middle East further reveals uneven levels of cybersecurity awareness, underscoring the need for structured initiatives that integrate technological innovation with cultural practices to cultivate secure digital behaviors [4]. These global trends illustrate a persistent challenge in higher education: ensuring that digital accessibility is balanced with robust security measures.

In Malaysia, the rapid growth of smartphone adoption has coincided with escalating cybercrime incidents. University students frequently access institutional portals, learning management systems, and

third-party applications, often exposing personal and institutional data due to carelessness or inadequate awareness. Studies show that many students underestimate cybersecurity risks or fail to apply essential protective measures, such as safeguarding Wi-Fi usage, regulating app permissions, or adopting strong authentication practices [5]. These behaviors are further exacerbated by the urgency associated with completing academic tasks on mobile devices, which leads students to prioritize speed over security checks [6]. Recent cases of information leakage in Malaysian universities affirm this fear, proving that students are unaware or underestimate the threats that have the potential to expose sensitive data such as email accounts and financial information [7], [8]. Thus, raising awareness of cybersecurity is not only necessary to protect institutional digital systems but also to improve students' sense of physical and academic security in a more digitized teaching space [9]. Without proactive efforts to promote awareness, it is probable that the cycle of breaches and reacting to them will continue [10]. Over time, repeated security breaches may also undermine students' confidence in digital services, thereby reducing their motivation to engage in online learning and collaboration [2].

Despite the growing focus on cybersecurity education (CE), a lack of security awareness among students remains a significant issue in online learning environments [4], [11]. This deficiency exposes learners to breaches that compromise sensitive information, including personal identifiers, authentication credentials, and location data [12]. Low technological proficiency (TP) and limited perceived control over personal data on smartphones further contribute to unsafe digital practices [13], [14]. Existing research, however, has not sufficiently examined how these factors, for instance, TP, perceived data control, and exposure to CE, interact within smartphone-based learning environments [15]. Previous models have also depended heavily upon behavior exposure (*e.g.*, smartphone usage frequency) as a mediator, which does not adequately capture the socio-technical influences shaping awareness and secure behavior [16].

To address these gaps, this study proposes an enhanced cybersecurity education–technological proficiency–perceived control (CE–TP–CTP) model by incorporating technological innovation and cultural norms (TICN) as a socio-technical mediator. TICN includes security features, such as security-by-default, such as encryption, multi-factor authentication, and privacy dashboards, alongside normative pressures encouraged by peers and institutional environments [17]. The enhanced model retains the core constructs of CE, TP, and perceived control over data (PCOD), but replaces the previous mediator, frequency of smartphone usage (FSU), with TICN. This socio-technical perspective posits that protective behavior arises not only from technical knowledge but also from cultural expectations and technologically embedded safeguards [18].

This study, therefore, investigates how university students understand and practice data privacy and security awareness (DPSA) in everyday smartphone use by comparing the explanatory power of the existing and enhanced CTP models. Based on empirical results from 356 students in three Malaysian universities, we investigate whether only behavioral exposure has explanatory power of awareness or if socio-technical constructs contribute to a more complete understanding of protective behavior in smartphone learning settings. The results extend the literature through the validation of an expanded socio-technical model and the provision of evidence-based knowledge to improve awareness initiatives for cybersecurity among Malaysian higher education institutions. The paper is structured as follows: section 1 is the introduction, section 2 presents the literature review and hypotheses, section 3 explains the methodology, section 4 displays the results and discussion, and section 5 concludes the study with implications, limitations, and avenues for future research.

2. LITERATURE REVIEW AND HYPOTHESES

2.1. Data privacy and security awareness

Students' extensive reliance on smartphones for online learning exposes them to significant data privacy and security risks. Previous studies emphasize that most students in universities are unaware of privacy policies and have low participation in cybersecurity training, as indicated at UiTM Terengganu [19], [20]. These findings indicate widespread unpreparedness and a general underestimation of cybercrime threats among higher education learners.

Empirical research further notes that breaches within educational institutions arise more frequently from human error than from system failure [8]. Even when privacy notifications are provided within learning management systems, third-party integrations often continue to collect student data beyond their consent [4], showing that institutional disclosures alone are insufficient to ensure privacy awareness. As prior research has discussed, raising privacy awareness is essential for building digital trust within learning contexts [12].

Accordingly, DPSA encompasses students' understanding of digital risks, their ability to recognize potential threats, and their readiness to adopt protective practices [21]. Despite this, many students remain unaware of the privacy implications associated with insecure smartphone behaviors. A study on Vietnamese students has shown a knowledge gap between perceived and actual privacy understanding, with over 50% of the participants unable to identify malware threats, and 20% did not recognize unsafe application permissions

while confidently claiming their true understanding of it [22]. These contrasting results across contexts underscore a behavioral gap that is not yet fully understood, thereby motivating the need for more comprehensive models of DPSA.

2.2. Cybersecurity education

Cybersecurity education (CE) plays a critical role in improving students' ability to recognize and respond to digital threats. A study conducted in multiple Nigerian universities revealed that most students have not been officially trained on cybersecurity, and when they claim to have had some experience with it, they were unable to identify basic threats like phishing and social-engineering attacks [4]. The authors recommended incorporating structured modules in the higher education curricula to foster defensive behavior.

Similar challenges have been reported in Saudi Arabia and other European, Middle Eastern countries [23], where students have a basic knowledge of cybersecurity, however, they are unable to utilize their knowledge in real-world scenarios. This vulnerability is driven by unsafe password practices, careless sharing habits, and an ongoing dependence on unsecured public Wi-Fi. All of these collectively increase students' exposure to being hacked and cyber threats, which are preventable by targeting cybersecurity awareness and education efforts [15].

Empirical findings consistently show that CE enhances students' threat detection abilities and the adoption of preventive measures [12]. However, many students continue to receive minimal formal training, leaving them exposed to persistent weaknesses in their digital behavior. Therefore, strengthening CE remains a crucial predictor of DPSA.

H1: CE positively influences DPSA.

2.3. Technological proficiency

Technological proficiency (TP) refers to students' ability to manage smartphone systems, configure security settings, and detect potential threats. And research shows that many students overestimate their proficiency in these areas. While many consider themselves competent technology users, their perceived proficiency often exceeds their actual skill levels [24]. Across-country comparisons show that students are consistently overconfident, although they do not look for phishing links, app permission access, or secure network connections despite the fact that they claim to be technically confident enough [15]. Likewise, active use of mobile-learning platforms by students was reported [3], but they were unable to handle system features like secure browsing, privacy settings, or updating device security.

Additional studies highlight that limited technical understanding increases susceptibility to sensor-based attacks, especially when students unknowingly install high-risk applications. Many continue to struggle with fundamental protective actions, such as managing permissions or avoiding unsecured Wi-Fi networks [12]. These findings collectively show that frequent smartphone use does not equate to proficiency and that technical skills are essential for safe digital behavior. Within the scope of this study, those findings would rationalize that technological skill should be associated with a positive effect on DPSA: higher proficiency allows students to perceive threats and manage settings properly in their devices, as well as develop proactive attitudes.

H2: TP positively influences DPSA.

2.4. Perceived control over data

Perceived control over data (PCOD) reflects the extent to which individuals believe they can regulate how their personal information is collected, used, and shared. Higher perceptions of control are associated with safer online practices and greater trust in digital platforms [25]. Research using validated cybersecurity awareness scales demonstrates that self-perceived control is a strong predictor of cautious digital behavior among university students [26].

However, studies caution that perceived control does not always align with actual protective behavior. Such inflated perceptions of risk can offer students a false sense of security and dismiss actual risks [27]. PCOD is successful when learners develop an understanding of privacy systems and access mechanisms in concert with system controls that are simple to understand and support informed actions [28].

H3: perceived control over data is positively associated with students' DPSA.

2.5. Technological innovation and cultural norms

Recent literature highlights the combined influence of technological innovation and cultural norms (TICN) in shaping students' secure smartphone practices. Technological innovation includes security-by-default features such as multi-factor authentication, device encryption, privacy dashboards, and automatic updates, while cultural norms encompass peer expectations, institutional practices, and campus guidelines that reinforce responsible digital behavior.

While TP enables students to recognize security features, prior studies show that technical ability alone does not ensure protective behavior [29]. Contrary to this assumption, prior studies have shown that even technically capable students may neglect security practices when cultural or contextual cues are weak, suggesting that competence requires reinforcement through social and institutional expectations [18]. For innovation, security features enhance students' knowledge and practical security skills [30], such as multi-factor authentication, privacy dashboards, and device encryption. On the cultural side, peer practices, institutional policies, and campus norms reinforce protective routines by showing that security actions are expected and valued [31]. Research conducted across Germany, South Korea, Spain, Sweden, and the United States identified that cultural values influenced students' notions of privacy, trust, and control in the digital learning ecosystem [32]. These variations demonstrate that behavior is not driven by technical ability alone but by how cultural environments build the importance of security. Together, these mechanisms shape the perspective in which students decide whether to apply their technical abilities [3]. Although existing models acknowledge technical skills and behavioral mediators, they do not consider socio-technical interaction. TICN addresses this gap by capturing the combined influence of technical capability and cultural reinforcement, explaining how proficiency is translated into sustained protective behavior. Hence, two hypotheses are proposed:

H4: TP is positively associated with TICN.

H5: TICN mediates the relationship between TP and students' DPSA.

2.6. Research framework

The existing CTP model conceptualizes CE, TP, and PCOD as direct predictors of DPSA, with FSU serving as a behavioral mediator. However, a major limitation in this model is that the frequency of use fails to consider the larger socio-technical context wherein technical competencies are converted into normative patterns of protection [33]. In contrast, FSU reflects only the exposure level and does not explain why some high-frequency users remain careless while others adopt consistent security awareness [24].

To address this gap, the enhanced CTP model introduces TICN as a mediator between (TP and DPSA) while retaining FSU to enable comparative analysis. This framework facilitates a systematic comparison between a behavioral exposure that is based on a model and one that incorporates socio-technical mechanisms. Prior behavioral cybersecurity research has shown that usable defaults and normative reminders influence everyday security choices, suggesting that TICN is a stronger mediator than frequent usage [34]. Thus, testing the pathway (TP→TICN→DPSA) allows the enhanced CTP model to clarify whether awareness improves from exposure alone or from the socio-technical conditions that foster secure behavior [7]. Figure 1 presents the existing CTP model, while Figure 2 illustrates the enhanced CTP model with TICN as a mediator.

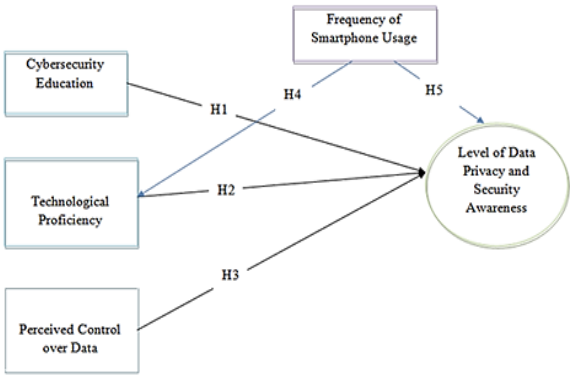

Figure 1. Existing CTP model

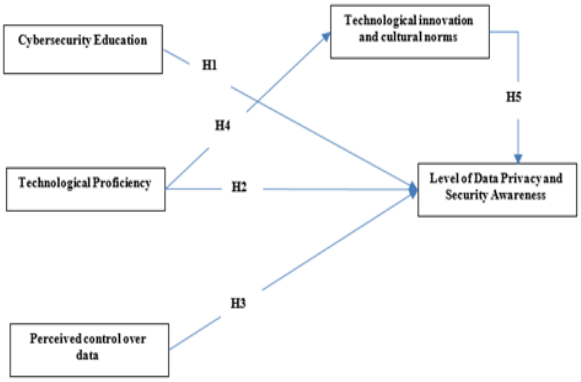

Figure 2. Enhanced CTP model with TICN mediator

3. RESEARCH METHOD

3.1. Sample and data

A cross-sectional approach was used in this study to explore the level of DPSA among Malaysian university students who use smartphones. This design is appropriate as it allows the relationships between multiple constructs to be examined at a single point in time without requiring repeated measurements. In February 2024, a pilot survey was conducted with 50 students from Universiti Teknikal Malaysia Melaka (UTeM) to evaluate the readability and reliability of the questionnaire. Based on feedback from two

cybersecurity experts, several items required rephrasing, and minor corrections were made. During this pilot stage, SPSS was used to conduct data screening, preliminary regression, and PCA to assess the item structure and reliability before distributing the full survey. After the completion of the pilot revisions, the final full-scale survey was conducted between March and May 2024 across three Malaysian institutions: UTeM, Multimedia University (MMU), and Universiti Teknologi MARA (UiTM). The survey questionnaire link was distributed online via WhatsApp groups. Random sampling was used to minimize sampling bias and improve representativeness across faculties, and the overall research process is summarized in Figure 3.

In total, 356 valid responses were collected. In section A of the questionnaire gathered demographic details of gender, age, program of study, smartphone ownership, and average daily usage. In Section B, five main variables were measured: CE, TP, perceived control over data, technological innovation and cultural norms, and DPSA, using a 5-point Likert scale.

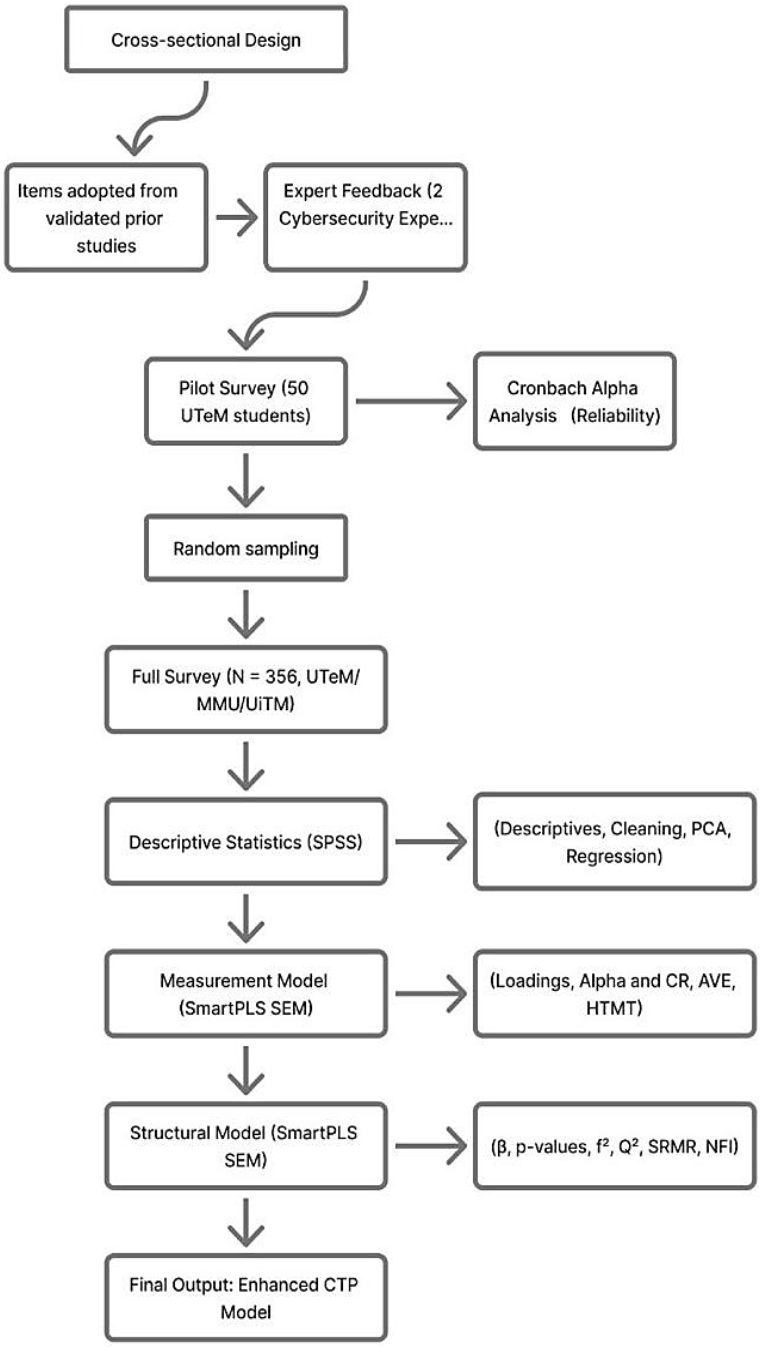

Figure 3. Research design and methodology flowchart

3.2. Measurement

The variables and their measurement items were adapted from prior validated studies to ensure reliability and validity. A total of 21 indicators were used to measure both independent, mediating, and dependent variables, adapted from prior studies [25], [26], [32], [34], [35]. Each variable met the recommended minimum item requirements for use in structural equation modeling as outlined by Hair *et al.* [36].

3.3. Data analysis technique

Descriptive statistics were first conducted using IBM SPSS statistics (v27) to summarize respondents' demographics (gender, age, program, smartphone ownership, and daily usage time). SPSS was also used for preliminary checks, including missing data screening and cleaning, means, and standard deviation to ensure accuracy. After preparing the dataset, the main analysis was to conduct SEM SmartPLS (version 4.0), and chosen for its suitability in handling complex models, latent variables, and non-normal data distributions. PLS-SEM was appropriate due to its ability to handle predictive modeling and complex mediation structures. The analysis followed a two-step procedure recommended by Hair *et al.* [36], first the measurement model, which was assessed for reliability, Cronbach's alpha (α), composite reliability (CR), convergent validity, average variance extracted (AVE), and discriminant validity Fornell Fornell-Larcker criterion, and Heterotrait–Monotrait (HTMT). Items with loadings below 0.70 were removed to improve the reliability of the constructs. Second, the structural model was used to evaluate the hypothesized relationships, including path coefficients, t-values, p-values, effect sizes, predictive relevance, and mediation effects, assessed using a 5,000-sample bootstrapping. These steps help to see which model improves security awareness better among university students. Model fit was assessed using the standardized root mean square residual (SRMR). Mediation analysis was performed to compare TICN with the previously used FSU mediator, identifying which mechanism better explains students' DPSA.

4. RESULTS AND DISCUSSION

This section presents the study findings in three parts: descriptive statistics, measurement model evaluation, and structural model assessment. Each part is discussed in relation to the research objectives and interpreted in line with prior studies.

4.1. Sample and descriptives

Table 1 summarizes the responses used to estimate both the existing and enhanced models have the same number of respondents to avoid bias (N=356). Table 2 presents the demographic profile of the respondents. Most participants were male (73.3%), while 26.7% were female. Ages were 18–20 (62.9%), 21–23 (27.0%), and above 23 (10.1%). By program, Diploma students accounted for 30.3%, Degree students for 46.9%, and master's students for 22.8%. Regarding device usage, 91.3% reported using a smartphone, 7.0% reported not using one, and 1.7% selected other. Daily usage patterns are reported with 43% using their devices for 1–3 hours daily and 34.8% for 4–6 hours, and a smaller proportion reported higher use, with 12.4% using their smartphones 7–8 hours per day, and 9.8% exceeding 8 hours.

Table 1. Number of respondents

Model	Number of respondents (N)
Existing model	356
Enhanced model	356

Table 2. Respondent's demographic profile

Category	Description	Count	Column N %
Gender	Male	261	73.3%
	Female	95	26.7%
Age	Teenager 18-20	224	62.9%
	Adults 21-23	96	27.0%
	Above 23	36	10.1%
Level of study	Diploma	108	30.3%
	Degree	167	46.9%
	Master	81	22.8%
Using any smartphone device	Yes	325	91.3%
	No	25	7.0%
	Other	6	1.7%
You frequently use the smartphone	1 to 3 hours a day	153	43.0%
	4 to 6 hours a day	124	34.8%
	7 to 8 hours	44	12.4%
	More than 8 hours a day	35	9.8%

4.1.1. Factor descriptives

Table 3 reports means and standard deviations for the study factors in both models. In general, the enhanced model shows higher mean values. CE increased from 2.391 to 3.306 and TP from 3.140 to 3.367, while PCOD was similar (3.394 vs. 3.381), and DPSA increased from 3.148 to 3.339. Frequency of smartphone usage (FSU) showed a mean value of 3.2918, whereas TICN was introduced as a stronger socio-technical mediator with a higher mean value of 3.3305, indicating better explanatory potential for how technical skills translate into secure behavior.

Table 3. Descriptive statistics: existing and enhanced CTP models

Variables	Mean (existing)	Std. Dev. (existing)	Mean (enhanced)	Std. dev. (enhanced)
CE	2.3914	0.680	3.3057	0.846
TP	3.1395	0.610	3.3670	0.868
PCOD	3.3937	0.700	3.3806	0.848
FSU (Existing)	3.2918	0.690	N/A	N/A
TICN (Enhanced)	N/A	N/A	3.3305	0.931
DPSA	3.1478	0.650	3.3394	0.875

Note: N/A indicates variable not included in the enhanced model.

4.2. Measurement model evaluation

4.2.1. Reliability and convergent validity

Table 4 summarizes the reliability and validity results for both the existing and enhanced CTP models. The existing model recorded weak reliability results for CE, TP, PCOD, and DPSA, and FSU performs poorly (α = 0.263, CR = 0.336, AVE = 0.209), indicating limited internal consistency and poor convergent validity. While the enhanced model showed improvement, with Cronbach's alpha values between 0.795 and 0.890 and AVE values above 0.50 for all variables. These statistics confirm that the enhanced model got acceptable reliability and validity thresholds (α > 0.70, CR > 0.70, AVE > 0.50).

Table 4. Reliability and convergent validity results

Variables	α (existing)	α (enhanced)	CR (existing)	CR (enhanced)	AVE (existing)	AVE (enhanced)
CE	0.579	0.858	0.668	0.903	0.381	0.700
TP	0.466	0.877	0.463	0.915	0.242	0.730
PCOD	0.348	0.825	0.451	0.896	0.224	0.741
FSU (existing)	0.263	N/A	0.336	N/A	0.209	N/A
TICN (enhanced)	N/A	0.890	N/A	0.919	N/A	0.694
DPSA	0.601	0.795	0.419	0.856	0.291	0.543

The notable improvement was observed in PCOD (α increased from 0.348 to 0.825) and TP (α from 0.466 to 0.877), while the introduced mediator TICN achieved high reliability (α = 0.890, CR = 0.919). These enhancements indicate that the revised constructs better capture their dimensions and that the enhanced CTP model offers a stable and valid framework for assessing DPSA among university students, supporting its use for further structural analysis in line with Hair *et al.* [37].

4.2.2. Indicator loadings

This test aimed to evaluate whether the individual items reliably measure their respective variables. Hair *et al.* [36] suggested that indicator loadings of 0.70 or higher provide strong evidence of indicator reliability. Figure 4 illustrates the standardized outer loadings, which all exceeded the recommended threshold. This confirms that the items load their intended factors and therefore support both indicator reliability and convergent validity.

4.2.3. Discriminant validity

Table 5 presents the Fornell–Larcker criterion results, with the square root of AVE values shown on the diagonal. These range from 0.737 (DPSA) to 0.861 (PCOD). In all cases, the square root of AVE is greater than the correlations between variables, confirming discriminant validity. The strongest correlation is observed between TICN and DPSA (0.718), but this remains lower than the AVE values for both factors, supporting the conclusion that each factor is empirically distinct.

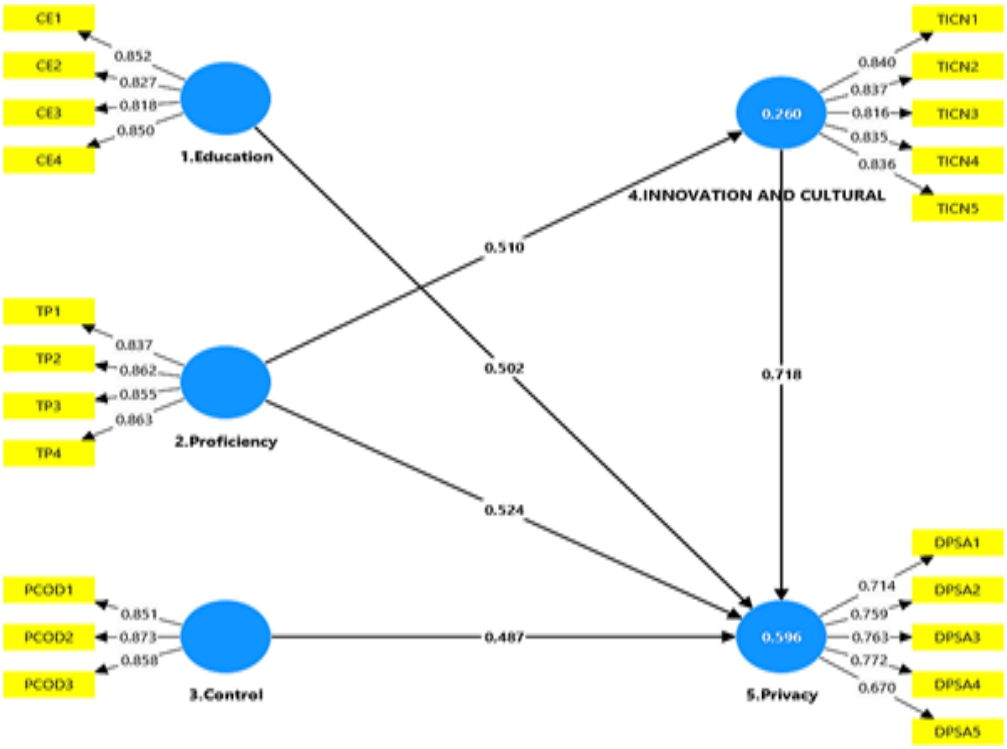

Figure 4. Standardized results of SEM analysis

Table 5. Fornell-Larcker criterion and discriminant validity

Variables	CE	TP	PCOD	TICN	DPSA
CE	**0.837**				
TP	0.345	**0.854**			
PCOD	0.326	0.444	**0.861**		
TICN	0.441	0.510	0.450	**0.839**	
DPSA	0.502	0.524	0.487	0.718	**0.737**

Note: the diagonal is the square root of the AVE (in bold) of the latent variables and indicates the highest in any column or row. LV = latent variable.

Table 6 presents the Heterotrait–Monotrait ratios (HTMT) for assessing discriminant validity. All HTMT values below 0.85, as recommended by Hair *et al.* [36], indicating adequate discriminant validity for all factors. The highest value is TICN with DPSA at 0.792. Other values include CE with TP at 0.398, CE with TICN at 0.504, and TP with PCOD at 0.520.

Table 6. HTMT of correlations for assessing discriminant

Variables	CE	TP	PCOD	TICN	DPSA
CE					
TP	0.398				
PCOD	0.387	0.520			
TICN	0.504	0.576	0.523		
DPSA	0.590	0.609	0.590	0.792	

4.2.4. Exploratory PCA

Table 7 reports the principal component analysis. The first component explains 75.247 percent of the variance, indicating a dominant latent dimension. Based on initial eigenvalues, the second component (eigenvalue 0.898) explains 17.953 percent, bringing the cumulative variance to 93.200 percent. Because the other components' eigenvalue is below one, this indicates that the measurement items are largely explained by one dominant factor, confirming the dominance of the first component supports unidimensional measurement, consistent with the SEM measurement results.

Table 7. Principal component analysis

Total variance explained						
Component	Initial eigenvalues			Extraction sums of squared loadings		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	3.762	75.247	75.247	3.762	75.247	75.247
2	.898	17.953	93.200			
3	.240	4.802	98.002			
4	.063	1.258	99.260			
5	.037	.740	100.000			

Extraction method: principal component analysis.

4.3. Structural model

4.3.1. Model fit

Table 8 compares the model fit indices of the existing and enhanced CTP models. The enhanced model achieved a better overall fit (chi-square = 834.217) compared to the existing model (chi-square = 1600.323). The enhanced model shows a lower d_ULS value (2.506 vs. 4.197) and acceptable d_G (1.422), indicating that the model-implied relationships reproduce the data more closely overall. The normed fit index (NFI) for the enhanced model is 0.848; the existing model's NFI = 0.561. The standardized root mean square residual (SRMR) is 0.088 for the enhanced model and 0.162 for the existing model. An SRMR around 0.08 to 0.10 and an NFI above 0.80, as suggested by [36], which is regarded as acceptable, thus the enhanced model meets this threshold, whereas the existing model does not. Overall, these indices indicate a good fit for the enhanced model and a better improvement over the existing.

Table 8. Model fit indices for the existing and enhanced CTP models

Model	Chi-square	d_ULS	d_G	NFI	SRMR
Enhanced model	834.217	2.506	1.422	0.848	0.088
Existing model	1600.323	4.197	0.929	0.561	0.162

4.3.2. Ordinary least squares regression

In this phase, we test direct effects, with DPSA as the dependent variable and CE, TP, PCOD, and TICN as predictors. All four predictors were statistically significant, $p < 0.001$. The enhanced CTP model showed better model fit (SRMR = 0.088; NFI = 0.848) and stronger predictive power for DPSA compared to the existing model. TICN showed the largest direct effect ($\beta = 0.388$) on DPSA, outperforming CE ($\beta = 0.268$), TP(β=0.133), and PCOD (β=0.108), as stated in Table 9.

Table 9. Multiple regression results for predictors of DPSA

Coefficients[a]								
Model		Unstandardized coefficients		Standardized coefficients	t	Sig.	95.0% confidence interval for B	
		B	Std. error	Beta			Lower bound	Upper bound
1	(Constant)	.381	.146		2.608	.010	.094	.668
	CE	.277	.047	.268	5.911	.000	.185	.369
	TP	.134	.055	.133	2.467	.014	.027	.242
	PCOD	.111	.054	.108	2.060	.040	.005	.218
	TICN	.365	.045	.388	8.086	.000	.276	.453

a. Dependent variable: DPSA

4.3.3. Hypotheses testing (direct and indirect relationships)

The test results on the hypotheses are presented in Table 10. On the first hypothesis, it was hypothesized that CE positively contributes to DPSA. Expectedly, the result for this hypothesis validated it by depicting a positive correlation between CE and DPSA ($\beta = 0.195$, $t = 3.959$, $p < 0.001$), a marked improvement over the existing model ($\beta = 0.044$). For the second hypothesis, it was hypothesized that TP has a significant positive correlation with DPSA. It was considerably supported ($\beta = 0.577$, $t = 13.121$, $p < 0.001$), thereby confirming effectiveness in awareness raising by digital skills. For the third hypothesis, perceived control over data was assumed to positively affect DPSA. This was supported in the results since there was a significant relationship ($\beta = 0.124$, $t = 2.078$, $p < 0.001$), with lower values compared to CE and TP. In hypothesis four, TP was presumed to have a positive prediction for TICN. The results confirmed this presumption, such that TP significantly predicted TICN ($\beta = 0.140$, $t = 2.293$, $p < 0.001$).

Hypothesis five is to test mediation by TICN between TP and DPSA. Mediation test for indirect effect confirmed TICN in transmitting a proportion of TP's influence on DPSA ($\beta = 0.603$, $t = 9.926$, $p < 0.001$). Bootstrapping generates robust confidence intervals for indirect effects without normality assumptions, which means these results demonstrate that technical skills (TP) enhance protective behavior through socio-technical conditions (TICN), underscoring the importance of supportive cultural and technological contexts in strengthening DPSA.

Table 10. Results of direct and indirect effect hypotheses

Hypothesis	Relationship	Std beta (existing)	Std beta (enhanced)	t-value (enhanced)	p-value (enhanced)	Decision (enhanced)
H1	CE →DPSA	0.044	0.195	3.959	$p < 0.001$	Supported
H2	TP → DPSA	0.011	0.577	13.121	$p < 0.001$	Supported
H3	PCOD→DPSA	0.062	0.124	2.078	$p < 0.001$	Supported
H4	TP → TICN	N/A	0.140	2.293	$p < 0.001$	Supported
H5	TP → TICN→DPSA	N/A	0.603	9.926	$p < 0.001$	Supported

4.3.4. Effect sizes and predictive relevance

The results in Table 11 show that both endogenous variables exhibit predictive relevance, as indicated by Q^2 values greater than zero with the thresholds recommended by Hair *et al.* [36]. Q^2 values above zero indicate predictive relevance. TICN ($Q^2 = 0.178$) and DPSA ($Q^2 = 0.288$) both show meaningful predictive relevance. TICN demonstrates the strongest effect on DPSA ($f^2 = 0.386$), which is considered large, while CE ($f^2 = 0.084$) and TP ($f^2 = 0.034$) have small-to-medium effects, and PCOD ($f^2 = 0.032$) has a small effect.

Table 11. Values of (Q^2) and Cohen's indicator (f^2) in the SEM model

Variables	Q^2	TICN (f^2)	DPSA (f^2)
CE			0.084
TP		0.352	0.034
PCOD			0.032
TICN	0.178		0.386
DPSA	0.288		

Note: large effect: 0.34; medium effect: 0.14; small effect: 0.01 (Cohen, 1988)

4.4. Discussion

The findings demonstrate that the enhanced CTP model provides a more comprehensive understanding of how students develop protective smartphone behavior. CE and TP significantly contribute to awareness. PCOD also plays a role, although weaker. TICN emerged as a powerful socio-technical mediator, indicating that awareness improves not merely through exposure or usage frequency but through supportive norms and secure-by-default technologies. These results align with global research and emphasize the need for institutions to create environments where secure behavior is expected, reinforced, and technologically facilitated.

The first notable finding is the effect of CE on DPSA ($\beta = 0.195$, $t = 3.959$, $p < 0.001$). This result is consistent with earlier studies [31], which demonstrates that structured awareness programs and formal instruction increase students' ability to recognize and mitigate digital threats. In the context of higher education, the growing emphasis on introducing cybersecurity training within curricula underscores the need for this relationship [12], suggesting that embedding cybersecurity courses, workshops, and micro modules into higher education can directly enhance security awareness.

Besides, those who are familiar with technical proficiency have safe behavior, which demonstrates greater confidence among students in dealing with their devices, making better use of built-in security mechanisms, and not practicing risky internet behavior [27]. They are also capable of recognizing potential threats and adopting preventive actions, such as adjusting privacy settings, using stronger passwords, or managing app permissions. This observation is supported by earlier studies, which link digital competence with safer decision-making in everyday tasks [38]. The results reflected in the statistical analysis showed that TP has a strong positive influence on DPSA ($\beta = 0.577$, $t = 13.121$, $p < 0.001$), indicating that practice-based digital training reinforces security behavior.

Moving to the finding related to PCOD, which showed a positive impact on DPSA ($\beta = 0.124$, $t = 2.078$, $p < 0.05$). This is supported by prior findings that individuals who feel in control of their personal data are more proactive in safeguarding it and can make wise decisions [25]. Students who believe they can

manage privacy settings, limit access, and monitor usage are more inclined to adopt protective strategies. Cybersecurity is also attitude-dependent: when students are in charge, their behavior is more protective, so building proficiency in navigating app permissions, privacy dashboards, and sharing settings might translate perceived control into protective behavior.

Another important finding is the role of TICN. The analysis showed that TP positively predicts TICN ($\beta = 0.140$, $t = 2.078$, $p < 0.001$), indicating that students with higher levels of TP are better equipped to adopt new security technologies, adjust their practices to safer behavior, and influence their peers by modeling protective behavior [31]. This aligns with prior socio-technical evidence that technical capability, institutional policies, and peer expectations jointly shape security behavior [17], [18], [39]. This suggests that Universities should aim not only to produce technical proficiency but integrate student systems with default-secure settings (encryption, MFA), such that technical skills are supplemented by facilitating environments.

Additionally, the mediation role further showed that TICN transmits part of the influence of TP onto DPSA ($\beta = 0.603$, $t = 9.926$, $p < 0.001$), reinforcing that technical skills alone are insufficient [16]. Supportive cultural and institutional contexts are crucial for transforming knowledge into sustainable protective behavior [11], [18], [39]. These socio-technical factors also help explain how student awareness differs for students who come from different educational and cultural backgrounds, as those with limited exposure to technology or CE may find it harder to adapt to secure practices. Hence, strengthening cultural and institutional support systems, such as university-wide awareness programs and secure-by-default environments, remains essential [23].

These combined results confirm that the enhanced CTP model outperforms the existing one by integrating TICN as a key mediating factor. The findings highlight the association between education, skill, control, and socio-technical conditions in improving awareness [15], [23]. Although CE and PCOD emphasize knowledge and perceived control as essential components, TP and TICN indicate practical skills and supportive settings. The mediation of TICN offers both theoretical and practical contributions by revealing how innovation and norms act as the bridge between technical ability and protective action [39]. By putting those findings in the context of existing research, this study contributes further insights into student behavior when learning via smartphones and offers practical implications for universities, policymakers, and organizations wanting to promote cybersecurity awareness.

6. CONCLUSION

This study contributes a validated enhanced CTP model for explaining DPSA among university students. The inclusion of TICN as a mediator substantially strengthens predictive power compared with the original model. Findings highlight that awareness is shaped not only by technical knowledge but also by socio-technical conditions that encourage secure behavior. Practical recommendations include integrating hands-on cybersecurity modules, enforcing secure-by-default campus technologies, and embedding cultural norms that reinforce responsible digital behavior. Future research may adopt experimental or cross-institutional designs to validate the model further.

The implications of this study emphasize that integrating TICN into digital-literacy initiatives can strengthen cybersecurity awareness. At the same time, efforts by governments to increase ICT training should include encouragement for socio-technical practices that tie secure-by-default technologies together with cultural norms. This integration supports the goal of fostering a digitally resilient society.

This study has several limitations. First, the results are based on university populations in Malaysia and may not apply to other student or cultural samples; therefore, replication with additional countries would ideally ensure the broader applicability of the enhanced CTP model. Second, the research used self-reported data, and these findings might differ from actual cybersecurity behavior. Future research might use behavioral methods such as (e.g., eye tracking, system logs) that could be utilized to compare actual behavior with self-reported awareness. Lastly, the English-only survey instrument may have limited understanding for some participants; therefore, multilingual instruments might enhance more precise responses in future research.

FUNDING INFORMATION

Authors state no funding involved.

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] I. Palamà, A. Amici, G. Bellicini, F. Gringoli, F. Pedretti, and G. Bianchi, "Attacks and vulnerabilities of Wi-Fi enterprise networks: user security awareness assessment through credential stealing attack experiments," *Computer Communications*, vol. 212, pp. 129–140, Dec. 2023, doi: 10.1016/j.comcom.2023.09.031.

[2] J. Garzón, Kinshuk, D. Burgos, and A. Tlili, "Advantages and challenges associated with mobile learning in education: a systematic literature review," *Journal of Computers in Education*, vol. 12, no. 4, pp. 1173–1205, Dec. 2024, doi: 10.1007/s40692-024-00342-x.

[3] F. Di Nocera, G. Tempestini, and M. Orsini, "Usable security: a systematic literature review," *Information*, vol. 14, no. 12, p. 641, Nov. 2023, doi: 10.3390/info14120641.

[4] I. Adeshola and D. I. Oluwajana, "Assessing cybersecurity awareness among university students: implications for educational interventions," *Journal of Computers in Education*, vol. 12, no. 4, pp. 1283–1305, Dec. 2025, doi: 10.1007/s40692-024-00346-7.

[5] M. Sangeen, N. A. Bhatti, K. Kifayat, A. A. Alsadhan, and H. Wang, "Blind-trust: raising awareness of the dangers of using unsecured public Wi-Fi networks," *Computer Communications*, vol. 209, pp. 359–367, 2023, doi: 10.1016/j.comcom.2023.07.011.

[6] Z. Muhammad, Z. Anwar, A. R. Javed, B. Saleem, S. Abbas, and T. R. Gadekallu, "Smartphone security and privacy: a survey on APTs, sensor-based attacks, side-channel attacks, google play attacks, and defenses," *Technologies*, vol. 11, no. 3, p. 76, Jun. 2023, doi: 10.3390/technologies11030076.

[7] A. Balapour, H. R. Nikkhah, and R. Sabherwal, "Mobile application security: role of perceived privacy as the predictor of security perceptions," *International Journal of Information Management*, vol. 52, Jun. 2020, doi: 10.1016/j.ijinfomgt.2019.102063.

[8] F. Schlackl, N. Link, and H. Hoehle, "Antecedents and consequences of data breaches: a systematic review," *Information & Management*, vol. 59, no. 4, p. 103638, Jun. 2022, doi: 10.1016/j.im.2022.103638.

[9] D. Amo *et al.*, "Local technology to enhance data privacy and security in educational technology," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 7, no. 2, pp. 262–273, Dec. 2021, doi: 10.9781/ijimai.2021.11.006.

[10] M. Spruit, D. Oosting, and C. Kreffer, "Factors that influence secure behaviour while using mobile digital devices," *Information & Computer Security*, vol. 32, no. 5, pp. 729–747, Nov. 2024, doi: 10.1108/ICS-02-2024-0035.

[11] K. Ramakrishnan, N. M. Yasin, and J. Periasamy, "Digital divide on cybersecurity awareness among the Malaysian higher learning institution students," in *AIP Conference Proceedings*, 2022, p. 40022, doi: 10.1063/5.0092796.

[12] N. A. Hasbullah, N. M. Zainudin, N. A. M. Razali, M. Wook, S. Ramli, and M. F. A. M. Fadzil, "Staying safe online: security measures by university students to secure privacy," in *2023 11th International Conference on Information and Education Technology (ICIET)*, Mar. 2023, pp. 572–576, doi: 10.1109/ICIET56899.2023.10111360.

[13] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the frontiers of cybersecurity behavior: a systematic review of studies and theories," *Applied Sciences*, vol. 13, no. 9, p. 5700, May 2023, doi: 10.3390/app13095700.

[14] L. De Kimpe, M. Walrave, P. Verdegem, and K. Ponnet, "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context," *Behaviour & Information Technology*, vol. 41, no. 8, pp. 1796–1808, Jun. 2022, doi: 10.1080/0144929X.2021.1905066.

[15] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: a comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, Jan. 2022, doi: 10.1080/08874417.2020.1712269.

[16] L. Li, L. Xu, and W. He, "The effects of antecedents and mediating factors on cybersecurity protection behavior," *Computers in Human Behavior Reports*, vol. 5, p. 100165, Mar. 2022, doi: 10.1016/j.chbr.2021.100165.

[17] M. Jamalova, "Cultural values and digital gap: overview of behavioral patterns," *PLOS ONE*, vol. 19, no. 10, p. e0311390, Oct. 2024, doi: 10.1371/journal.pone.0311390.

[18] N. S. Sulaiman, M. A. Fauzi, W. Wider, J. Rajadurai, S. Hussain, and S. A. Harun, "Cyber–information security compliance and violation behaviour in organisations: a systematic review," *Social Sciences*, vol. 11, no. 9, p. 386, 2022, doi: 10.3390/socsci11090386.

[19] R. Raju, N. H. A. Rahman, and A. Ahmad, "Cyber security awareness in using digital platforms among students in a higher learning institution," *Asian Journal of University Education*, vol. 18, no. 3, Jul. 2022, doi: 10.24191/ajue.v18i3.18967.

[20] M. R. Sanfilippo, N. Apthorpe, K. Brehm, and Y. Shvartzshnaider, "Privacy governance not included: analysis of third parties in learning management systems," *Information and Learning Sciences*, vol. 124, no. 9/10, pp. 326–348, Nov. 2023, doi: 10.1108/ILS-04-2023-0033.

[21] A. A. Pua'at and N. M. Yunus, "A study on awareness, exposure and attitude towards digital citizenship among university students in Malaysia," *Information Management and Business Review*, vol. 15, no. 1(I)SI, pp. 190–203, May 2023, doi: 10.22610/imbr.v15i1(I)SI.3397.

[22] A. Tick and P. T. Mai, "Cyber security awareness and the behaviors of higher education students, using smartphones in Vietnam," *Acta Polytechnica Hungarica*, vol. 21, no. 12, pp. 111–131, 2024.

[23] M. A. Alqahtani, "Factors affecting cybersecurity awareness among university students," *Applied Sciences*, vol. 12, no. 5, p. 2589, Mar. 2022, doi: 10.3390/app12052589.

[24] S. Getenet, R. Cantle, P. Redmond, and P. Albion, "Students' digital technology attitude, literacy and self-efficacy and their effect on online learning engagement," *International Journal of Educational Technology in Higher Education*, vol. 21, no. 1, p. 3, Jan. 2024, doi: 10.1186/s41239-023-00437-y.

[25] N. Rodríguez-Priego, L. Porcu, M. B. P. Peña, and E. C. Almendros, "Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure," *Journal of Retailing and Consumer Services*, vol. 72, p. 103284, May 2023, doi: 10.1016/j.jretconser.2023.103284.

[26] L. Bognár and L. Bottyán, "Evaluating online security behavior: development and validation of a personal cybersecurity awareness scale for university students," *Education Sciences*, vol. 14, no. 6, p. 588, May 2024, doi: 10.3390/educsci14060588.

[27] K. Degirmenci, "Mobile users' information privacy concerns and the role of app permission requests," *International Journal of Information Management*, vol. 50, pp. 261–272, Feb. 2020, doi: 10.1016/j.ijinfomgt.2019.05.010.

[28] A. Kumi-Yeboah, Y. Kim, B. Yankson, S. Aikins, and Y. A. Dadson, "Diverse students' perspectives on privacy and technology integration in higher education," *British Journal of Educational Technology*, vol. 54, no. 6, pp. 1671–1692, Nov. 2023, doi: 10.1111/bjet.13386.

[29] C. Rosales-Márquez, C. E. Carbonell-García, V. Miranda-Vargas, R. Diaz-Zavala, and K. M. Laura-De La Cruz, "Self-confidence

as a predictor of digital skills: a fundamental pillar for the digitalization of higher education," *Frontiers in Education*, vol. 9, Jan. 2025, doi: 10.3389/feduc.2024.1515033.
[30] M. Zhang, X. Zhao, Y. Xue, J. Yang, and Y. Zhang, "A meta-analysis of how the culture and technical development level influence citizens' adoption of m-government," *International Review of Administrative Sciences*, vol. 89, no. 1, pp. 129–144, Mar. 2023, doi: 10.1177/00208523211057358.
[31] W. C. H. Hong, C. Chi, J. Liu, Y. Zhang, V. N.-L. Lei, and X. Xu, "The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates," *Education and Information Technologies*, vol. 28, no. 1, pp. 439–470, Jan. 2023, doi: 10.1007/s10639-022-11121-5.
[32] O. Viberg *et al.*, "Cultural differences in students' privacy concerns in learning analytics across Germany, South Korea, Spain, Sweden, and the United States," *Computers in Human Behavior Reports*, vol. 14, p. 100416, May 2024, doi: 10.1016/j.chbr.2024.100416.
[33] H. Shaw, D. A. Ellis, K. Geyer, B. I. Davidson, F. V Ziegler, and A. Smith, "Quantifying smartphone 'use': choice of measurement impacts relationships between 'usage' and health," *Technology, Mind, and Behavior*, vol. 1, no. 2, pp. 114–128, 2020, doi: 10.1037/tmb0000022.
[34] A. Kumar *et al.*, "A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare," *Sensors*, vol. 22, no. 15, p. 5921, Aug. 2022, doi: 10.3390/s22155921.
[35] F. Donbesuur, G. O. A. Ampong, D. Owusu-Yirenkyi, and I. Chu, "Technological innovation, organizational innovation and international performance of SMEs: the moderating role of domestic institutional environment," *Technological Forecasting and Social Change*, vol. 161, p. 120252, Dec. 2020, doi: 10.1016/j.techfore.2020.120252.
[36] J. F. Hair Jr, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, "Partial least squares structural equation modeling (PLS-SEM): an emerging tool in business research," *European Business Review*, vol. 26, no. 2, pp. 106–121, Mar. 2014, doi: 10.1108/EBR-10-2013-0128.
[37] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, *Partial least squares structural equation modeling (PLS-SEM) using R*. Cham: Springer International Publishing, 2021.
[38] S. S. Shukla, M. Tiwari, A. C. Lokhande, T. Tiwari, R. Singh, and A. Beri, "A comparative study of cyber security awareness, competence and behavior," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, Dec. 2022, pp. 1704–1709, doi: 10.1109/IC3I56241.2022.10072880.
[39] L.-W. Wong, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and A. Sohal, "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: building supply chain capabilities," *International Journal of Information Management*, vol. 66, p. 102520, Oct. 2022, doi: 10.1016/j.ijinfomgt.2022.102520.

BIOGRAPHIES OF AUTHORS

Ahmed Al-Rassas received the B.Sc. degree in computer networks from Al Andalus University for Science and Technology Yemen, and is currently pursuing his M.Sc. degree in computer science with a specialization in cybersecurity at Universiti Teknikal Malaysia Melaka (UTeM), Malaysia. His research focuses on smartphone data privacy awareness among university students in Malaysia. He has also served as a district general manager in the local administration in Yemen. His academic interests include cybersecurity education, technological proficiency, smartphone security, social engineering, and data protection. He can be contacted at email: m032310040@student.utem.edu.my.

Zaheera Zainal Abidin holds a Ph.D. in information technology (quantitative sciences) and two M.Sc. degrees in computer networking and information technology (quantitative sciences), all from Universiti Teknologi MARA (UiTM), Malaysia. She obtained her bachelor's degree in information technology from the University of Canberra, Australia. She is currently a senior lecturer at the faculty of artificial intelligence and cyber security (FAIX), Universiti Teknikal Malaysia Melaka (UTeM), Malaysia. Her research interests include internet of things (IoT), network security, physical security, computer networking, and image processing. She is a member of the optimization modelling, analytic and simulation (OPTIMAS) research group. She can be contacted at email: zaheera@utem.edu.my.