Environment and Social Psychology (2026) Volume 11 Issue 1 ISSN: 2424-8975 (O)
doi: 10.59429/esp.v11i1.4347 2424-7979 (P)

RESEARCH ARTICLE

Adoption of campus IoT in Shanghai higher education: A mixed-methods UTAUT study with infrastructure and privacy extensions

Shen Qinjie*, Nainapas Injoungjirakit, Sombat Teekasap, Prapai Sridama

Graduate School, Bansomdejchaopraya Rajabhat University, Bangkok, 10600, Thailand

*** Corresponding author:** Shen Qinjie, shenqinjie001@gmail.com

ABSTRACT

Smart-campus initiatives in Shanghai have expanded rapidly, yet evidence on students' adoption of campus Internet of Things (IoT) services remains mixed. This study integrates the Unified Theory of Acceptance and Use of Technology with two contextually salient antecedents, reliable Internet connection and security or privacy concern, to explain intention to use campus IoT in higher education. We employed a cross-sectional student survey and complementary tutor interviews. The quantitative strand tested separate bivariate models for key predictors, and the qualitative strand used thematic analysis to contextualize mechanisms and barriers.

Findings indicate an infrastructure-first pathway. When campus connectivity is stable and low-friction, students treat IoT as an ambient utility, and intention to use increases, while traditional cognition-centric predictors play a smaller role. Perceived usefulness remains a consistent positive driver; privacy concerns can be addressed through clear policies and visible safeguards; and brief onboarding helps novices move from trial to routine use. The study contributes a pragmatic extension of technology-acceptance work by specifying infrastructure readiness and privacy governance as first-order antecedents of adoption in higher education. Practical recommendations include campus-level connectivity targets, streamlined authentication, plain-language data-use messaging, and micro-orientations at the start of courses. Limitations include a single-city scope and a cross-sectional design; future research should validate the infrastructure-first thesis using multivariable models and multi-site samples.

Keywords: internet of things; higher education; UTAUT; infrastructure readiness; privacy; behavioral intention

1. Introduction

Universities worldwide are accelerating "smart campus" programs that instrument learning spaces and student services with Internet of Things (IoT) devices and platforms. Conceptual syntheses frame smart campuses as layered sociotechnical systems, where physical infrastructure (sensors, connectivity, and power) underpins cyber-data services for teaching, operations, and the student experience[1]. In such settings, network reliability and authentication frictions can become binding constraints for everyday use, raising a pragmatic question: when does infrastructure reliability outweigh cognition-centric predictors of adoption?

Behavioral models remain the baseline for explaining technology uptake. The Unified Theory of Acceptance and Use of Technology (UTAUT) posits performance expectancy, effort expectancy, social

ARTICLE INFO
Received: 14 November 2025 | Accepted: 15 December 2025 | Available online: 14 January 2026

CITATION
Shen QJ, Injoungjirakit N, Teekasap S, et al. Adoption of campus IoT in Shanghai higher education: A mixed-methods UTAUT study with infrastructure and privacy extensions. *Environment and Social Psychology* 2026; 11(1): 4347. doi: 10.59429/esp.v11i1.4347

influence, and facilitating conditions as proximal determinants of intention and use[2]. UTAUT2 extends this view with hedonic motivation, price value, and habit for consumer-style technologies[3]. Applications in higher education consistently find that perceived usefulness and supportive environments matter, though effect sizes vary by context[4,5].

Post-pandemic evidence also emphasizes the quality of access, latency, stability, and device readiness, rather than merely counting access. Across university and system-level studies, Internet stability and broadband quality predict satisfaction and participation in online learning and can widen inequalities when unreliable[6]. For campus IoT, this implies operationalizing UTAUT's "facilitating conditions" with granular connectivity indicators (e.g., reliable Internet connection across lecture halls and dorms) rather than treating infrastructure as a background control.

A second cross-cutting mechanism is privacy and trust. Research shows that privacy concerns are context-dependent and malleable[7], while trust in the platform/institution interacts with perceived risk to shape adoption of data-intensive public services[8]. Because campus IoT may log movement, usage, and learning artifacts, addressing privacy/security can remove deterrents and complement infrastructural upgrades. Accordingly, this study extends UTAUT with two contextual antecedents - reliable Internet connection (RIC) and security/privacy concern (SPC), to test whether infrastructure readiness and data-practice perceptions help explain students' intention to use campus IoT in Chinese higher education.

1.1. Research questions

RQ1. To what extent do UTAUT constructs, performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC), predict students' intention to use IoT in Shanghai higher education institutions?

RQ2. How strongly is a reliable Internet connection (RIC) associated with students' intention to use IoT, relative to the UTAUT predictors?

RQ3. How are security/privacy concerns (SPC) related to students' intention to use IoT?

RQ4. What practical barriers and facilitators reported by tutors help explain the quantitative patterns observed in RQ1-RQ3?

1.2. Literature Review & Hypotheses

1.2.1. UTAUT and technology adoption in higher education

The Unified Theory of Acceptance and Use of Technology (UTAUT) posits four core determinants, performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC), as proximal drivers of intention and use[2]. Its consumer extension, UTAUT2, adds hedonic motivation, price value, and habit, and meta-analytic evidence shows robust, though context-dependent, effects across settings[3,9]. In higher education, UTAUT-style models have explained students' and teachers' adoption of digital learning tools, typically finding positive roles for PE and FC, mixed results for SI, and smaller or moderated effects for EE[10,11]. These patterns motivate our use of UTAUT as the baseline for modeling students' intention to use campus IoT.

1.2.2. Infrastructure readiness as a first-order antecedent

Smart-campus research conceptualizes universities as layered sociotechnical systems, where physical layers (sensors, connectivity, power) underpin cyber-data services for learning and operations[1,12]. During and after the pandemic pivot, studies reported that quality of access, latency, stability, broadband capacity, and device readiness predict engagement and can exacerbate inequalities when unreliable[6]. Taken together,

this literature suggests operationalizing UTAUT's facilitating conditions with granular connectivity indicators, such as reliable Internet connection (RIC) across lecture halls, libraries, and dorms, rather than treating "infrastructure" as a background control. We therefore specify RIC as an infrastructure antecedent and examine its bivariate association and practical salience relative to UTAUT predictors in the campus IoT context.

1.2.3. Privacy and trust in data-intensive campus services

Campus IoT and learning analytics intensify personal-data flows (location traces, usage logs, behavioral telemetry), foregrounding security/privacy concern (SPC) and trust as adoption mechanisms. Behavioral privacy research shows that privacy concerns are context-dependent and malleable[7]. In public digital services, trust and perceived risk shape willingness to adopt, with effects documented across e-government and pandemic proximity-tracing services, contexts that share institutional governance with university platforms[8,13]. Accordingly, we incorporate SPC to examine whether data-practice perceptions deter or, when addressed, enable intention to adopt campus IoT.

1.2.4. Hypotheses

Grounded in UTAUT and the extensions above, we test the following hypotheses regarding intention to use IoT (IU):

H1 (PE → IU, +). Students' performance expectancy (PE) is positively associated with intention to use campus IoT (IU).

H2 (EE → IU, ?). The association between effort expectancy (EE) and IU is left unspecified (two-tailed) due to mixed evidence across contexts.

H3 (SI → IU, ?). The association between social influence (SI) and IU is left unspecified (two-tailed).

H4 (FC → IU, +). Facilitating conditions (FC) are positively associated with IU.

H5 (RIC → IU, +). Reliable Internet connection (RIC) is positively associated with IU.

H6 (SPC ↔ IU, ±). Security/privacy concern (SPC) is associated with IU (two-tailed), acknowledging possible positive or negative directions.

H7 (Experience ↔ IU, exploratory, ±). Lack of prior experience with campus IoT is exploratorily associated with IU; the direction may vary with institutional support.

Figure 1 summarizes the proposed research framework and hypothesized relationships among UTAUT predictors (PE, EE, SI, FC), the two extensions (RIC, SPC), and intention to use IoT (IU).

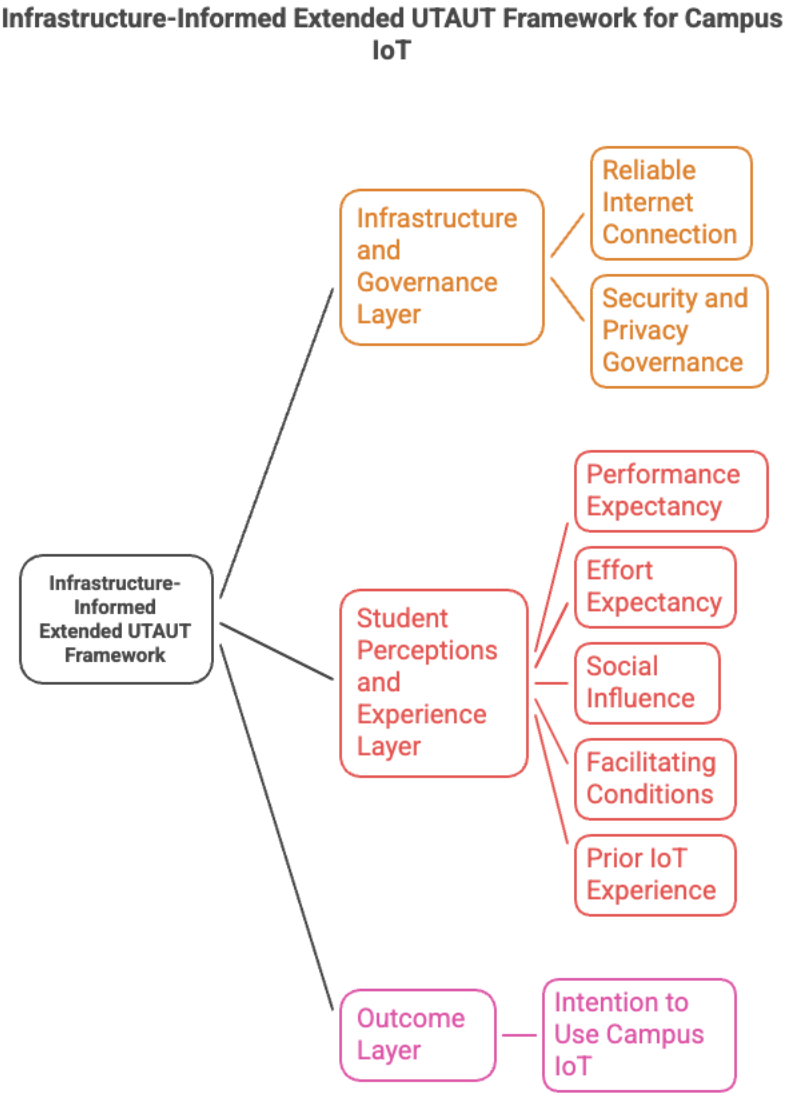

Figure 1. PE, EE, SI, and FC (UTAUT) together with RIC and SPC (extensions) as exogenous predictors of IU, with demographics as controls.

1.2.5. Theoretical rationale and key sources

UTAUT provides the baseline for PE, EE, SI, and FC[2,3]. In higher education, studies typically report robust effects for PE and FC, context-dependent effects for SI, and smaller or moderated effects for EE[9-11]. Smart-campus and post-pandemic evidence emphasize quality of access, latency, stability, and bandwidth, suggesting that connectivity should be modeled explicitly rather than treated as a generic control; hence, our specification of RIC[1,6,12]. For SPC, research shows that privacy concerns are context-dependent and interact with trust and perceived risk to shape adoption of data-intensive services[13]. UTAUT constructs (PE, EE, SI, FC) adopt standard items adapted from prior UTAUT applications in higher education; RIC captures perceived reliability/coverage/latency in core learning spaces; SPC reflects concerns over data collection/usage and institutional safeguards, aligned with privacy-trust traditions summarized above.

2. Method

We adopted a cross-sectional, mixed-method design in five Shanghai universities, which is appropriate for testing associations between infrastructure readiness, privacy concerns, and intention to use IoT without

imposing strong temporal or causal assumptions[14]. A student survey provided the quantitative core, complemented by semi-structured tutor interviews to contextualize patterns around infrastructure and privacy practices[15,16]. We initially planned simple random sampling to give all eligible students a non-zero chance of selection within each institution[17]. In practice, an online questionnaire link was distributed via learning platforms, course coordinators, and student groups across the five universities to maximize reach and minimize cost, which corresponds to a non-probability convenience approach[18]. The participating institutions are listed in Appendix D; one institution requested anonymity and is therefore reported as University E (anonymous). To address potential between-institution variation, we additionally conducted Kruskal-Wallis H tests comparing IU and key constructs (RIC, PE, SPC) across the five universities; results are reported in Appendix D.

Eligibility required current enrolment, age ≥ 18, and informed consent. Over one week, 501 students accessed the survey, and 408 provided complete responses that were retained for analysis. In addition, seven tutors from the participating institutions volunteered for one-hour online interviews (via Skype or comparable video platforms).

The instrument comprised 30 items on a 5-point Likert scale (1 = strongly disagree, 5 = strongly agree). The present analyses focus on 26 items that operationalised the extended UTAUT framework: performance expectancy (PE), effort expectancy (EE), social influence (SI), facilitating conditions (FC), reliable Internet connection (RIC), security/privacy concern (SPC), and intention to use IoT (IU), plus a single-item indicator of prior experience with campus IoT. In line with established practice in educational technology settings, UTAUT items were adapted to the campus IoT context; RIC items captured perceived stability, coverage, and latency of connectivity in lecture halls, libraries, and dormitories, and SPC items captured concern over data collection/use and institutional safeguards. Prior experience was assessed with one item ("I have little prior experience using campus IoT services"), treated as a background indicator rather than a multi-item scale.

To make the focal set of campus IoT services concrete for readers, Box 1 provides illustrative examples of the campus IoT touchpoints referenced in this study.

Box 1. Examples of campus IoT services and touchpoints

In this article, "campus IoT services" refers to digitally mediated campus learning and service systems that depend on stable connectivity and institutional data practices. Illustrative examples include:

1. University learning platforms and e-learning portals used for course access and learning activities.
2. Campus Wi-Fi coverage, stability, speed/latency, and login (e.g., captive-portal) frictions when accessing online platforms.
3. In-class digital activities linked to teaching and assessment (e.g., quizzes, polls, submissions, and feedback workflows).
4. Student support and onboarding for getting started, troubleshooting, and device compatibility when using these systems.
5. Campus service touchpoints in key locations (lecture halls, libraries, dormitories) where connectivity reliability shapes everyday use.
6. Privacy and security touchpoints, including perceived safety of the portal and the visibility of institutional safeguards and support teams.

Content and face validity were assessed through a human expert review involving seven academics with relevant expertise in educational technology, smart-campus implementation, and higher education research[19]. Experts evaluated the draft questionnaire for clarity, relevance to the intended constructs, and coverage of the campus IoT context. Their feedback led to minor wording refinements (e.g., simplifying technical phrasing, ensuring consistent Likert direction, and improving item-construct alignment) prior to fielding. Details of the human expert review procedure are provided in Appendix E.

The student survey and tutor interviews were administered in Chinese; interview excerpts used in this article were translated into English and checked for meaning equivalence[15]. Participation was voluntary and preceded by an online information sheet and consent form. No identifying information was collected, and data were stored in anonymized, password-protected files with restricted access, following standard ethical guidance for educational and social research[20].

Quantitative analyses were conducted in SPSS v28 following standard workflows for applied educational research[21,22]. We first screened the data for missing values and outliers, then produced descriptive statistics and frequency distributions to profile the sample and constructs[23]. Measurement quality was examined via Cronbach's α and inspection of item-construct alignment; internal consistency coefficients were calculated for all multi-item scales (PE, EE, SI, FC, RIC, SPC, IU), whereas no α was reported for the single-item experience indicator. Full reliability and loading tables are provided in the Appendix. To address the research questions with the current dataset, we estimated separate bivariate linear regressions of IU on each predictor (PE, EE, SI, FC, RIC, SPC, lack of experience), using two-tailed $\alpha = .05$. Reporting of regression coefficients follows common recommendations for applied OLS models, including standardized beta (β), confidence intervals, p values, and explained variance[24]. Assumptions were reviewed via residual plots (linearity and homoscedasticity) and normality checks at the construct level. Given the observed correlations among predictors in the broader project dataset, we note hierarchical OLS models (e.g., entering

UTAUT predictors in Block 1 and RIC/SPC in Block 2) and PLS-SEM with collinearity diagnostics and incremental-variance tests as planned extensions beyond the present bivariate design[22,24].

Qualitative data were analyzed using thematic analysis. An initial codebook aligned to the study objectives (infrastructure readiness, privacy practices, and user support) was developed and then iteratively refined as transcripts were read and re-read. Codes were grouped into candidate themes and then into higher-level themes that captured tutors' perspectives on connectivity, teaching practice, and governance of IoT services, following established procedures for rigorous thematic analysis in mixed-method designs[16,20]. The resulting themes were used to explain and contextualize survey patterns rather than to provide statistically generalizable estimates.

3. Results

3.1. Quantitative results

We analyzed N = 408 students from five Shanghai universities with separate bivariate OLS models of intention to use IoT (IU) on each predictor. As previewed, RIC shows the largest association; PE is positive and significant; EE/SI/FC are not significant; SPC is small and positive; lack of experience is weak but significant.

3.1.1. Measurement properties

Before examining the regression models, we assessed the reliability and dimensionality of the multi-item scales. Cronbach's α values were 0.71 for performance expectancy (PE), 0.74 for effort expectancy (EE), 0.78 for social influence (SI), 0.80 for facilitating conditions (FC), 0.70 for reliable Internet connection (RIC), 0.84 for security/privacy concern (SPC), and 0.77 for intention to use IoT (IU). The single-item indicator of prior experience with campus IoT was treated as a background variable and, therefore, was not included in the reliability calculations. Factor loadings and descriptive statistics (M and SD) for all items and constructs are reported in Appendix C.

3.1.2. Bivariate regressions predicting intention to use IoT

Table 1 summarises the bivariate OLS regressions predicting intention to use IoT (IU) from each predictor. Reliable Internet connection (RIC) shows a very strong positive association with IU ($R = .774$, $R^2 = .599$, $\beta = .774$, $p < .001$), indicating that perceived connectivity alone accounts for almost 60% of the variance in intention. Performance expectancy (PE) also has a positive, but smaller, association with IU ($R = .270$, $R^2 = .073$, $\beta = .270$, $p < .001$). Security/privacy concern (SPC) displays a small positive relationship with IU ($R = .118$, $R^2 = .014$, $\beta = .118$, $p = .017$), and lack of IoT experience is also positively but weakly related to IU ($R = .164$, $R^2 = .027$, $\beta = .164$, $p = .001$). In contrast, effort expectancy (EE), social influence (SI), and facilitating conditions (FC) are not significant predictors in this bivariate design (all $p \geq .076$). Detailed coefficient estimates, including standard errors, t values, and confidence intervals, are presented in **Table 2**.

Institution-specific descriptive statistics (**Table D2**) and an institution-stratified robustness check for the key association (RIC → IU; **Table D3**) are reported in Appendix D. Overall patterns are broadly similar across institutions, although the strength of the RIC-IU association varies by site. Between-institution differences were examined using Kruskal-Wallis H tests for IU and the key constructs highlighted in the main analyses (RIC, PE, and SPC). To assess whether key constructs differed across institutions, we conducted Kruskal-Wallis H tests. Results indicated no significant between-institution differences for IU, RIC, or SPC; however, PE differed modestly across institutions ($H = 10.75$, $df = 4$, $p = .03$; see Appendix D,

Table D4). Post-hoc pairwise comparisons were not included in this revision due to space constraints; the omnibus result indicates that PE differs across institutions.

Table 1. Bivariate regressions predicting intention to use IoT (IU) - model fit and key coefficients.

Predictor (X)	R	R^2	B (unstd)	β (std)	p	N
Reliable Internet connection (RIC)	.774	.599	1.013	.774	< .001*	408
Performance expectancy (PE)	.270	.073	.175	.270	< .001*	408
Effort expectancy (EE)	.038	.001	.052	.038	.445	408
Social influence (SI)	.014	.000	−.008	−.014	.784	408
Facilitating conditions (FC)	.088	.008	−.143	−.088	.076	408
Security/privacy concern (SPC)	.118	.014	.068	.118	.017*	408
Lack of experience (IoT)	.164	.027	.094	.164	.001***	408

Notes. *DV = IU. Separate OLS per predictor; two-tailed α = .05. Significance: * p < .05, ** p < .01, *** p < .001.*

Table 2. Coefficient details per single-predictor OLS (DV = IU).

Predictor	B (unstd)	SE(B)	β (std)	t	95% CI for B (Lower, Upper)	p
RIC	1.013	0.041	.774	24.633	[0.933, 1.093]	< .001*
PE	.175	0.031	.270	5.645	[0.114, 0.236]	< .001*
EE	.052	0.068	.038	0.765	[−0.081, 0.185]	.445
SI	−.008	0.031	−.014	−0.274	[−0.069, 0.053]	.784
FC	−.143	0.081	−.088	−1.778	[−0.302, 0.016]	.076
SPC	.068	0.028	.118	2.400	[0.013, 0.123]	.017*
Lack of experience	.094	0.028	.164	3.360	[0.039, 0.149]	.001***

H1 (PE → IU, +): Supported. H2 (EE → IU, ?): Not supported. H3 (SI → IU, ?): Not supported. H4 (FC → IU, +): Not supported (bivariate). H5 (RIC → IU, +): Supported. H6 (SPC ↔ IU, ±): Small positive association observed. H7 (Experience ↔ IU, exploratory, ±): Supported (weak).

3.2. Qualitative results

Thematic analysis of seven semi-structured tutor interviews yielded four recurrent themes explaining when and why students intend to use campus IoT. These themes clarify why reliable connectivity (RIC) dominates, why perceived usefulness (PE) still matters, why ease/social cues (EE, SI, FC) are muted, and how privacy concern (SPC) can be managed. **Table 3** provides a tutor-tagged evidence roster, mapping each theme (T1–T4) to illustrative interview excerpts.

3.2.1. T1. Campus monitoring and learning support (infrastructure-first)

Tutors framed IoT foremost as campus infrastructure for safety/operations that also underpins classroom technology (e.g., projectors, interactive boards, audio). When uptime and coverage were stable, students treated IoT services as ambient utilities rather than deliberate choices, explaining RIC's dominant bivariate effect. Illustrative evidence (replace brackets with actual IDs): [Tutor #1] "stable Wi-Fi makes IoT 'invisible', students just rely on it"; [Tutor #2] noted dorm/classroom coverage gaps as the single biggest barrier; [Tutor #4] emphasized that once networks are reliable, other predictors "fade."

The first emergent theme underscores the pivotal role of IoT as an infrastructural enabler for both safety and pedagogical operations within smart campuses. Tutors consistently emphasized that when network uptime, bandwidth, and latency thresholds are met across classrooms and dormitories, IoT systems become

"invisible utilities", seamlessly embedded in daily academic and administrative routines. Rather than being perceived as optional technologies, these systems are assumed to function continuously, underpinning everything from automated attendance tracking to environmental controls and AV support in lecture halls. These finding echoes[12], who conceptualize smart campuses as layered sociotechnical systems where infrastructure reliability predicates behavioral intention. Tutors noted that when coverage gaps or connectivity interruptions occur, students disengage, regardless of the functional benefits of IoT. Thus, network reliability is not a supporting factor but a gatekeeper: its presence normalizes usage, while its absence breaks routines. This theme reinforces the statistical dominance of Reliable Internet Connection (RIC) in our quantitative models and suggests that campus-level ICT planning should adopt minimum connectivity standards as a prerequisite for IoT service deployment.

3.2.2. T2. Creative classroom enablement (usefulness in action)

Interviewees highlighted low-friction academic utility (schedules, quick polls, resource sharing, note capture) and more engaging instruction when tools are tied to assessment/feedback, aligning with PE's positive, significant association. Illustrative evidence: [Tutor #3] reported higher uptake when quizzes/feedback used IoT features; [Tutor #5] described routine automation that freed class time for deeper tasks; [Tutor #2] linked device orchestration to smoother lessons.

This theme reflects how IoT technologies are redefining classroom dynamics, transforming passive learning spaces into interactive, responsive environments. Tutors reported that when IoT features are intentionally integrated into assessment workflows, such as real-time quizzes, feedback loops, and automated resource distribution, students show greater cognitive engagement and are more likely to treat technology as an academic ally rather than a novelty. This aligns with the core of performance expectancy (PE) in UTAUT, where perceived usefulness becomes a primary motivator for behavioral intention. Furthermore, classroom orchestration tools supported by IoT (e.g., synchronized projectors, smart whiteboards, in-class polling apps) were seen to reduce administrative friction and redirect attention toward deeper cognitive tasks. These affordances not only boost instructional efficiency but also support differentiated instruction, as teachers can adjust delivery in real-time based on IoT-enabled analytics. This practical classroom utility offers a tangible answer to the 'why' of technology adoption: students use what demonstrably helps them succeed. Hence, embedding IoT in pedagogical activities, rather than presenting it as a standalone tool, appears to significantly enhance its perceived academic value.

3.2.3. T3. AI+IoT for management and security (governance makes privacy manageable)

Tutors connected IoT to operational efficiency and safety/security; several stressed that clear data-use notices and visible safeguards reduced hesitation, with SPC's small positive association. Illustrative evidence: [Tutor #6] pointed to faster incident response with IoT dashboards; [Tutor #1] underscored that transparent policies and signage calmed concerns; [Tutor #4] saw faculty endorsement as a privacy reassurance.

A recurring concern across interviews centered on data privacy, yet tutors emphasized that transparent policies and visible safeguards can transform apprehension into acceptance. Several described how AI-integrated IoT platforms, used for monitoring occupancy, energy usage, or campus movement, trigger less resistance when institutions proactively display data-use policies and explain their protective intent. This confirms research by[8], which found that institutional trust mediates the relationship between privacy concern and adoption. In our study, tutors reported that students were more comfortable when IoT data governance was communicated in plain language and when faculty visibly endorsed the systems in use. These trust-building actions reframe privacy risk as manageable rather than prohibitive. Importantly, this theme nuances the small but significant positive association of SPC (security/privacy concern) in our

quantitative analysis. Rather than treating privacy as a binary deterrent, it becomes a contingent variable, responsive to institutional behavior. Therefore, IoT implementation strategies should incorporate privacy-by-design principles, including clear opt-in mechanisms, anonymization protocols, and co-created policies that resonate with the student body.

3.2.4. T4. Accessibility and inclusion (onboarding matters for novices)

Tutors described assistive use cases (alerts, navigation, environment control) and the impact of brief onboarding/peer champions on first-use anxiety, mirroring the weak but significant positive signal for the "lack of experience" indicator. Illustrative evidence: [Tutor #7] discussed accommodations for students with disabilities; [Tutor #3] noted that short demos convert trial into routine use.

The final theme highlights IoT's potential to enhance campus inclusion, particularly for users with limited digital experience or physical accessibility needs. Tutors cited examples where IoT affordances, such as voice-assisted navigation, environmental control interfaces, and alert systems, made learning spaces more navigable and responsive for students with disabilities. Moreover, brief onboarding sessions, peer coaching, and demo-based orientations were mentioned as effective interventions for first-time users, reducing technology anxiety and fostering early engagement. This supports the exploratory quantitative finding that a lack of experience shows a weak but significant association with intention to use. As prior research[25] suggests, cognitive absorption through initial exposure can shape long-term user comfort. Rather than viewing novice users as resistant, this theme frames them as latent adopters requiring minimal scaffolding. Institutions seeking to promote equitable IoT adoption should invest in inclusive design practices and create entry points that accommodate diverse technical backgrounds. In doing so, IoT becomes not only a tool for innovation but also an instrument for digital justice in higher education.

3.2.5. Integration with quantitative results

Across interviews, connectivity and access emerged as the binding constraint. Once reliability is in place, usefulness cues (PE) drive intention; ease of use and social cues (EE, SI, FC) play smaller roles; and privacy becomes contingent on visible safeguards. This mirrors the bivariate pattern: RIC ≫ PE; EE/SI/FC n.s.; SPC small +; experience weak +.

Table 3. Tutor-tagged evidence roster.

Tutor ID	T1. Campus monitoring & learning support	T2. Creative classroom enablement	T3. Management & security (privacy governance)	T4. Accessibility & onboarding
Tutor #1	Stable coverage/uptime makes IoT "invisible", students simply rely on it day-to-day.	Polls/resources tied to grading/feedback increase student buy-in.	Clear data-use notices and staff endorsement calm privacy worries.	Brief demos help novices get started; assistive features matter for some learners.
Tutor #2	Coverage gaps in dorms/lecture halls are the main barrier to routine use.	Low-friction tasks (quick checks, note capture) make classes run smoother.	When safeguards are visible, students accept data collection for campus operations.	Short orientation reduces first-use anxiety.
Tutor #3	Once Wi-Fi is reliable, classroom tech (boards, audio) just works.	Quizzes/feedback via IoT tools drive steady adoption.	Operations dashboards improve responsiveness; transparency builds trust.	Peer champions and quick walk-throughs move novices from trial to routine use.
Tutor #4	Infrastructure first: reliability dictates whether students lean on IoT between classes.	Orchestrating devices simplifies lesson flow and keeps attention on content.	Faculty signaling and policy clarity reduce privacy hesitation.	Assistive alerts/navigation improve quality of life for disabled students.
Tutor #5	Reliable campus networking underpins	Routine automation (sharing materials, quick polls) frees	Students respond better when privacy rules are explained in	A short onboarding session is usually enough

Tutor ID	T1. Campus monitoring & learning support	T2. Creative classroom enablement	T3. Management & security (privacy governance)	T4. Accessibility & onboarding
	both safety monitoring and classroom tools.	time for deeper tasks.	plain language.	to get hesitant students going.
Tutor #6	IoT helps with campus-level oversight; connectivity stability is the linchpin.	When linked to assessment, students use the tools without prompting.	Security/management improve with IoT; visible safeguards → higher acceptance.	Assistive affordances matter; quick coaching bridges initial gaps.
Tutor #7	Uptime + coverage determine everyday reliance on IoT services.	Classroom utility (schedules, resource sharing) is most persuasive when embedded in activities.	Students accept data practices when governance is transparent and purpose is clear.	Accessibility use cases (alerts, navigation, home/class automation) show tangible benefits.

Table 3. (*Continued*)

4. Discussion

Taken together, our results support an infrastructure-first pathway to campus IoT adoption: once a reliable Internet connection (RIC) and low-friction access are in place, intention rises markedly, whereas cognition-centric antecedents operate at the margin. This pattern aligns with recent smart-campus evidence that treats coverage, stability, and integration as day-to-day gatekeepers of use[26], while our tutor interviews clarify that reliability makes IoT effectively "ambient," shifting attention from technical hurdles to perceived usefulness in class routines. Within UTAUT, performance expectancy (PE) remains a meaningful, though smaller, predictor in higher-education contexts[2,3], a conclusion reinforced by a recent systematic review that synthesizes UTAUT evidence across university settings and highlights context-specific constraints on effect sizes[27]. By contrast, effort expectancy (EE) and social influence (SI) are not significant here, echoing mixed university findings[10,11] and our qualitative accounts of authentication friction and room-level Wi-Fi variability, issues that lie outside what EE/SI items typically capture. On privacy, the small positive association for security/privacy concern (SPC) suggests that concern can be governed rather than uniformly deterrent: credible, localized data-use explanations and visible safeguards can temper cynicism and legitimize everyday use in higher education[7,28]. Finally, the weak but significant contribution of lack of experience is consistent with UTAUT's experience pathway[3] and with emerging higher-education work arguing that brief onboarding and peer support move novices from trial to routine use[29]. Conceptually, our mixed-method evidence supports treating infrastructure readiness as a first-order antecedent rather than a mere background condition. Empirically, the pooled bivariate models indicate a clear rank ordering (RIC much larger than PE; EE, SI, and FC not significant; SPC small positive; experience weak positive). Institution-stratified checks suggest that the magnitude of the RIC to IU association varies by site, including one institution with a near-zero, non-significant association (Appendix D, **Table D3**). Moreover, between-institution differences in construct levels are limited: Kruskal-Wallis tests show no significant differences for IU, RIC, or SPC, while PE differs modestly across institutions (Appendix D**, Table D4**). Practically, these findings motivate campus-level KPIs for uptime and coverage, streamlined authentication, visible privacy governance, and short orientations or peer champions targeted at first-time users.

5. Conclusion

This study provides convergent evidence consistent with an infrastructure-first pathway to campus IoT adoption. In our five-university student sample, reliable Internet connection (RIC) and low-friction access conditions show the strongest association with intention to use, while performance expectancy (PE) plays a smaller yet meaningful role. By design, findings rest on separate bivariate OLS models: RIC shows the

largest standalone association with intention; PE is significant but notably smaller; effort expectancy (EE), social influence (SI), and facilitating conditions (FC) do not reach significance in bivariate tests; security/privacy concern (SPC) displays a small positive association; and limited prior experience shows a weak but reliable positive association. The tutor interviews clarify why: when connectivity and access are stable, IoT functions can feel "ambient" in everyday study routines (T1); usefulness cues tied to assessment or feedback become salient (T2); privacy hesitancy may be mitigated through visible safeguards and clear data-use messaging (T3); and light-touch onboarding or peer champions help novices move from trial to routine use (T4).

Importantly, institution-stratified checks suggest that the magnitude of the RIC-IU association is not uniform across sites, including one institution with a near-zero, non-significant association, which points to potential site-specific boundary conditions (see Appendix D, **Tables D3-D4**). In addition, non-parametric tests show limited between-institution differences in construct levels: IU, RIC, and SPC do not differ significantly across institutions, whereas PE differs modestly across sites. Taken together, these results support treating infrastructure readiness as a prominent predictor in this context, while also recognizing that local implementation conditions can shape effect strength.

Conceptually, the results argue for treating infrastructure readiness as an explicit predictor rather than a background enabler. Framed within UTAUT, this means specifying connectivity reliability and access frictions such as captive-portal behavior or re-authentication cycles as antecedents rather than leaving them implicit inside "facilitating conditions." The governability of privacy also matters: SPC's small positive association suggests that transparent governance and visible safeguards may convert concern into conditional acceptance, although the cross-sectional design does not permit causal claims. Finally, the experience pathway points to a pragmatic lever for institutions: brief orientations, targeted micro-tutorials, and student champions are inexpensive interventions with potential benefits for first-time users.

Practically, universities should institutionalize connectivity KPIs and make them visible at the room/dorm granularity (coverage, stability/uptime, latency during class windows, roaming success rate, first-connection time), streamline authentication to minimize re-logins and timeouts during teaching, signal usefulness by aligning features with assessment/feedback in syllabi and LMS prompts, govern privacy visibly with plain-language notices and faculty endorsement, and run micro-onboarding at course start (with accessibility in mind). Methodologically, the present study is intentionally parsimonious, SPSS bivariate OLS plus thematic interviews, to surface the dominant mechanisms cleanly. Future work should test the same infrastructure-first thesis with multivariable extensions (e.g., hierarchical OLS with collinearity checks), multi-site samples beyond one city, and field telemetry (e.g., passive network metrics linked to usage logs) to quantify how improvements in reliability and access translate into everyday adoption.

To summarize the mixed-method integration, **Table 4** presents an integration matrix linking the quantitative associations with the tutor themes, proposed mechanisms, and practice implications.

Table 4. Integration matrix: quantitative findings + tutor themes + mechanisms + implications.

Theme	Quantitative variable(s) & direction	Mechanism clarified by interviews	Tutor IDs	Policy / practice implication	Example indicators / KPIs	Example actions (campus level)
T1. Campus monitoring & learning support (infrastructure-first)	RIC → IU: strong positive (largest standalone association)	Room/dorm uptime + coverage make IoT an "ambient utility"; authentication friction often the true bottleneck.	#1, #2, #3, #4, #5, #6, #7	Make connectivity KPIs visible at room/dorm granularity; streamline	Classroom/dorm uptime; average latency during class hours; roaming success; first-connection	Deploy per-building AP health dashboards; shorten token TTL only

Theme	Quantitative variable(s) & direction	Mechanism clarified by interviews	Tutor IDs	Policy / practice implication	Example indicators / KPIs	Example actions (campus level)
				captive-portal/re-auth flows.	time; drop-off rate at login.	outside class windows; enable single sign-on / eduroam-style roaming; place Wi-Fi "heat maps" where students study.
T2. Creative classroom enablement (usefulness in action)	PE → IU: positive, smaller	When features are tied to assessment/feedback (quizzes, polls, resource sharing), adoption occurs with little prompting.	#1-#7	Signal usefulness in syllabus/LMS; align IoT tools with grading, feedback, and time savings.	% of courses linking IoT features to graded activities; click-through rates on LMS IoT widgets; in-class poll completion rate.	Add "IoT task" tiles in LMS tied to low-stakes points; provide instructor templates for quick polls/exit tickets; publicize turnaround-time gains for feedback.
T3. Management & security (privacy governance)	SPC ↔ IU: small positive	Plain-language data-use notices, visible safeguards, and faculty endorsement temper concern and legitimize use.	#1, #4, #5, #6, #7	Govern privacy visibly: concise notices, safeguard status displays, faculty champions.	% of courses displaying a one-screen privacy notice; help-desk tickets tagged "privacy"; awareness scores in quick pulse surveys.	Launch a 1-page campus data-use explainer; add "why we collect" snippets in apps; brief faculty to mention safeguards on day 1; publish security posture tiles in the LMS.
T4. Accessibility & onboarding (novices → routine use)	Experience ↔ IU: weak positive	Brief onboarding, quick demos, and peer champions reduce first-use anxiety; assistive affordances matter for inclusion.	#3, #4, #5, #6, #7	Offer micro-orientations at course start; recruit student champions; foreground accessibility gains.	Orientation attendance; first-week activation rate; repeat-use rate by week 3; assistive-feature utilization.	Run 10-minute "first-use" demos in week 1; seed student TA/champion roles; surface accessibility toggles prominently; nudge reminders to late adopters.

Table 4. (*Continued*)

Conflict of interest

The authors declare no conflict of interest.

References

1. Min-Allah, N., & Alrashed, S. (2020). Smart campus—A sketch. Sustainable Cities and Society, 59, 102231. https://doi.org/10.1016/j.scs.2020.102231
2. 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
3. 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

4. Fernández-Batanero, J. M., Montenegro-Rueda, M., Fernández-Cerero, J., & López Menéses, E. (2024). Adoption of the Internet of Things in higher education: opportunities and challenges. Interactive Technology and Smart Education, 21(2), 292-307. https://doi.org/10.1108/ITSE-01-2023-0025
5. Madni, S. H. H., Ali, J., Husnain, H. A., Masum, M. H., Mustafa, S., Shuja, J., ... & Hosseini, S. (2022). Factors influencing the adoption of IoT for E-learning in higher educational institutes in developing countries. Frontiers in Psychology, 13, 915596. https://doi.org/10.3389/fpsyg.2022.915596
6. Korkmaz, Ö., Erer, E., & Erer, D. (2022). Internet access and its role on educational inequality during the COVID-19 pandemic. Telecommunications Policy, 46(5), 102353. https://doi.org/10.1016/j.telpol.2022.102353
7. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465
8. Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. Journal of Strategic Information Systems, 17(2), 165–176. https://doi.org/10.1016/j.jsis.2007.12.002
9. Tamilmani, K., Rana, N. P., & Dwivedi, Y. K. (2021). Consumer acceptance and use of information technology: A meta-analytic evaluation of UTAUT2. Information Systems Frontiers, 23(4), 987–1005. https://doi.org/10.1007/s10796-020-10007-6
10. Teo, T. (2011). Factors influencing teachers' intention to use technology: Model development and test. Computers & Education, 57(4), 2432–2440. https://doi.org/10.1016/j.compedu.2011.06.008
11. Kuo, Y.-C., Walker, A. E., Schroder, K. E. E., & Belland, B. R. (2014). Interaction, Internet self-efficacy, and self-regulated learning as predictors of student satisfaction in online education courses. The Internet and Higher Education, 20, 35–50. https://doi.org/10.1016/j.iheduc.2013.10.001
12. Valks, B., Arkesteijn, M. H., Koutamanis, A., & den Heijer, A. C. (2021). Towards a smart campus: supporting campus decisions with Internet of Things applications. Building Research & Information, 49(1), 1-20. https://doi.org/10.1080/09613218.2020.1784702
13. Trkman, M., Popovič, A., & Trkman, P. (2023). The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications. Government Information Quarterly, 40(1), 101787. https://doi.org/10.1016/j.giq.2022.101787
14. Rindfleisch, A., Malter, A. J., Ganesan, S., & Moorman, C. (2008). Cross-sectional versus longitudinal survey research: Concepts, findings, and guidelines. Journal of Marketing Research, 45(3), 261–279. https://doi.org/10.1509/jmkr.45.3.261
15. Dearnley, C. (2005). A reflection on the use of semi-structured interviews. Nurse Researcher, 13(1), 19–28. https://doi.org/10.7748/nr2005.07.13.1.19.c5997
16. Saunders, M. N., & Thornhill, A. (2011). Researching sensitively without sensitizing: Using a card sort in a concurrent mixed methods design to research trust and distrust. International Journal of Multiple Research Approaches, 5(3), 334–350. https://doi.org/10.5172/mra.2011.5.3.334
17. Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students (5th ed.). Pearson.
18. Andrews, D., Nonnecke, B., & Preece, J. (2007). Conducting research on the internet: Online survey design, development and implementation guidelines. https://auspace.athabascau.ca/handle/2149/1336
19. Creswell, J. W., & Creswell, J. D. (2005). Mixed methods research: Developments, debates, and dilemmas. Research in organizations: Foundations and methods of inquiry, 2, 315-326.
20. Flick, U. (2015). Introducing research methodology: A beginner's guide to doing a research project. Sage.
21. Connolly, P. (2007). Quantitative data analysis in education: A critical introduction using SPSS (1st ed.). Routledge. https://doi.org/10.4324/9780203946985
22. Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.
23. Mertens, W., Pugliese, A., & Recker, J. (2017). Quantitative data analysis: A companion for accounting and information systems research. Springer. https://doi.org/10.1007/978-3-319-42700-3
24. Sarstedt, M., & Mooi, E. (2018). Regression analysis. In A concise guide to market research: The process, data, and methods using IBM SPSS Statistics (pp. 209-256). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56707-4_7
25. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified Theory of Acceptance and Use of Technology: A synthesis and the road ahead. Journal of the Association for Information Systems, 17(5), 328–376. https://doi.org/10.17705/1jais.00428
26. Domínguez-Bolaño, T., Barral, V., Escudero, C. J., & García-Naya, J. A. (2024). An IoT system for a smart campus: Challenges and solutions illustrated over several real-world use cases. Internet of Things, 25, 101099. https://doi.org/10.1016/j.iot.2024.101099

27. Xue, L., Rashid, A. M., & Ouyang, S. (2024). The Unified Theory of Acceptance and Use of Technology (UTAUT) in higher education: A systematic review. SAGE Open, 14(1). https://doi.org/10.1177/21582440241229570
28. Popescu, M., Baruh, L., & Sudhakar, S. (2024). Role-based privacy cynicism and local privacy activism: How data stewards navigate privacy in higher education. Big Data & Society, 11(2). https://doi.org/10.1177/20539517241240664
29. Mexhuani, B. (2025). Adopting digital tools in higher education: Opportunities, challenges and theoretical insights. European Journal of Education, 60(1), e12819. https://doi.org/10.1111/ejed.12819

Appendix A

Questionnaire for students

Part-1: Demographic profile

1. Age

- 18-20 years
- 21-25 years
- 26-30 years
- More than 30 years

2. Gender

- Male
- Female
- Prefer not to say

3. Which education qualification are you pursuing?

- Bachelor's degree
- Master's degree
- Certificate-based course/ diploma
- Other

4. Which education field are you studying in?

- Management
- Marketing
- HR
- Finance
- Other

Part 2: Main research

Please rate your level of agreement to the following statements on a five-point Likert scale where 1=Strongly disagree, 2=disagree, 3=Neutral, 4=Agree, 5=Strongly agree.

5. Reliable Internet Connection

	1	2	3	4	5
RIC1 I do not experience technical problems while browsing university learning platforms.					
RIC2 I find the browsing speed on university learning platforms satisfactory.					

RIC3 I can rely on the campus computer network when I need it.	
RIC4 There is easy access to the internet on campus.	

6. Security/Privacy Concern (SPC)

	1	2	3	4	5
SPC1 The university e-learning portal is safe to use.					
SPC2 The university e-learning portal is safe to use.					
SPC3 There is an appropriate security and support team for the university's online portal.					

7. Performance expectancy (PE)

	1	2	3	4	5
PE1 Using technology in education is helpful in my daily life.					
PE2 Using technology in education enhances my chances of accomplishing things that are important to me.					
PE3 Using technology in education helps me achieve tasks more quickly.					
PE4 Using technology in education increases my productivity.					

8. Effort Expectancy (EE)

	1	2	3	4	5
EE1 I find it easy to learn how to use technology in education.					
EE2 I find IoT in education easy to use.					
EE3 My interactions with technology in education are clear and understandable.					
EE4 I find it easy to become skilful at using technology in education.					

9. Social influence (SI)

	1	2	3	4	5
SI1 People who are important to me feel that I should use technology in education.					
SI2 People who influence me think that I should use technology in education.					
SI3 People whose opinions I value think that I should use technology in education.					

10. Facilitating conditions (FC)

	1	2	3	4	5

FC1 I have the necessary resources to use technology in education.					
FC2 I have the necessary knowledge to use technology in education.					
FC3 Technology in education is compatible with other technologies I use.					
FC4 If I face challenges using technology in education, it is easy to get help from others.					

11. Intention to use IoT/technology in education (IU)

	1	**2**	**3**	**4**	**5**
IU1 I intend to continue using technology in education.					
IU2 I would like to use technology in my daily life in the future.					
IU3 I will use technology regularly, as I do now.					

12. Lack of experience with campus IoT

	1	**2**	**3**	**4**	**5**
EXP1 I have little prior experience using campus IoT services					

Note. *The questionnaire originally included additional items on course satisfaction and online social interaction. These items are not analysed in this article and are therefore not reported here. The constructs and items listed above correspond to the variables used in the quantitative analyses (RIC, SPC, PE, EE, SI, FC, IU, and lack of experience).*

Appendix B

Interview questions for tutors

Opening/consent (30–45 sec).

Thank you for participating. With your consent, I'll record our conversation for research purposes. You may skip any question or stop at any time.

Q1. Connectivity & access (RIC).

From your day-to-day experience, how reliable is on-campus Internet (coverage, stability, speed/latency) in classrooms and dorms?

Probes: peak-time slowdowns; drop-offs; login/captive-portal friction; where it works best/worst.

Q2. Classroom enablement (PE).

What course activities work best when digital/IoT tools are involved?

Probes: assessment/feedback link (quizzes, polls, submissions); time saved; concrete examples.

Q3. Ease & support (EE, FC).

How easy is it for students to get started and get help when they run into issues?

Probes: onboarding materials; help-desk responsiveness; device compatibility.

Q4. Social/organizational cues (SI).

What signals from instructors, departments, or peers affect students' willingness to use these tools?

Probes: syllabus prompts; modeling by instructors; peer champions.

Q5. Privacy & security (SPC).

How do students react to privacy/security issues? What messages or safeguards make a difference?

Probes: plain-language notices; where policies are shown; examples of concerns resolved.

Q6. Accessibility & inclusion (experience pathway).

What works for students with limited prior experience or with accessibility needs?

Probes: micro-orientations; assistive features; success stories.

Q7. Equity & location.

Do adoption patterns vary by study location (lecture halls, library, dorms) or device access?

Probes: hotspots vs dead zones; shared devices.

Q8. Priorities and KPIs.

If you could change three things to improve everyday use, what would they be?

Probes: specific KPIs (uptime, latency, login success), small pilots you would try next semester.

Closing (15–30 sec). Anything we didn't ask for that we should have

Appendix C

Reliability and descriptive statistics for constructs

Table C1. Reliability and descriptive statistics for multi-item constructs.

Construct	Code	Items (n)	Cronbach's α	M	SD

Performance expectancy	PE	4	0.71	3.11	0.62
Effort expectancy	EE	4	0.74	2.56	0.65
Social influence	SI	3	0.78	3.32	0.89
Facilitating conditions	FC	4	0.80	2.99	0.97
Reliable Internet connection	RIC	4	0.70	2.99	0.87
Security/privacy concern	SPC	3	0.84	2.86	0.74
Intention to use IoT	IU	3	0.77	3.12	0.78
Prior experience with IoT	EXP1	1	n.a.*	3.81	0.81

Note. *Cronbach's α is reported only for multi-item constructs.*
**EXP1 is a single-item indicator of prior experience with campus IoT services, so internal consistency is not applicable.*

Appendix D

Table D1. Participating universities.

Institution	Location	Notes
Shanghai Industrial and Commercial Polytechnic	Shanghai, China	Vocational college
Shanghai Zhongqiao Vocational and Technical University	Shanghai, China	Reported in some English materials as "Shanghai Zhongqiao Vocational and Technical College/University"; "Zhongqiao" spelling follows institutional usage
Shanghai Jiaotong Vocational and Technical College	Shanghai, China	Also written as "Shanghai Jiao Tong Vocational and Technical College" in some sources
NYU Shanghai	Shanghai, China	Official English name commonly used as "NYU Shanghai"
University E (anonymous)	Shanghai, China	This institution requested anonymity; therefore, its name is not disclosed

Note. *One participating institution requested to remain anonymous. We therefore report it as "University E (anonymous)" to protect institutional confidentiality while retaining transparency about the multi-institution design.*

Table D2. Descriptive Statistics by Institution.

Institution	n	IU: M (SD)	RIC: M (SD)	PE: M (SD)	SPC: M (SD)
Shanghai Industrial and Commercial Polytechnic	84	3.10 (0.78)	2.98 (0.87)	3.09 (0.62)	2.85 (0.74)
Shanghai Zhongqiao Vocational and Technical University	81	3.04 (0.76)	2.94 (0.85)	3.07 (0.60)	2.79 (0.72)
Shanghai Jiaotong Vocational and Technical College	78	3.16 (0.80)	3.01 (0.88)	3.13 (0.63)	2.89 (0.75)
NYU Shanghai	87	3.20 (0.75)	3.04 (0.86)	3.18 (0.61)	2.94 (0.73)
University E (anonymous)	78	3.00 (0.79)	2.92 (0.84)	3.00 (0.64)	2.77 (0.76)

Note. I*U = Intention to Use; RIC = Reliable Internet Connection; PE = Performance Expectancy; SPC = Security/Privacy Concern. Values are based on the 5-point Likert scale. Total N=408. The association is significant in four institutions; one institution shows a near-zero, non-significant association.*

Table D3. Bivariate Regressions Predicting IU by Institution (RIC → IU).

Institution	β (std)	R^2	*p*	n
Shanghai Industrial and Commercial Polytechnic	0.43	0.19	<0.001	84
Shanghai Zhongqiao Vocational and Technical University	0.31	0.10	0.005	81

Shanghai Jiaotong Vocational and Technical College	0.03	0.00	0.782	78
NYU Shanghai	0.41	0.17	<0.001	87
University E (anonymous)	0.51	0.26	<0.001	78

Note. *Standardized β coefficients from bivariate OLS regressions (Reliable Internet Connection predicting Intention to Use). Patterns are consistent, with stronger effects in institutions with higher RIC variability (e.g., University E, anonymous). Total N=408.*

Table D4. Between-institution differences in key constructs: Kruskal–Wallis H tests.

Construct (test variable)	Test	H	df	p
Intention to use IoT (IU)	Kruskal–Wallis	5.91	4	.21
Reliable Internet connection (RIC)	Kruskal–Wallis	3.14	4	.53
Performance expectancy (PE)	Kruskal–Wallis	10.75	4	.03*
Security/privacy concern (SPC)	Kruskal–Wallis	2.53	4	.64

Note. *Kruskal-Wallis H tests compare construct scores across the five participating institutions (including University E, anonymous). *p < .05.*

Appendix E

Human expert review of the questionnaire

A panel of seven academic experts reviewed the draft instrument prior to data collection. The review focused on (a) clarity and readability for undergraduate participants, (b) relevance of each item to its intended construct (PE, EE, SI, FC, RIC, SPC, IU), and (c) contextual fit with campus IoT use in Shanghai universities. Based on their feedback, minor revisions were made to improve wording precision and reduce ambiguity, including simplifying phrasing, aligning item wording with the campus IoT context (e.g., classroom and dorm connectivity), and standardising the response direction across items. No constructs were removed; revisions were intended to improve face validity and item-construct alignment.