



Progress in Computers and Learning

Journal homepage:
<https://karyailham.com.my/index.php/picl>
ISSN: 3083-8894



Design and Development of an Automated Facial Recognition System for Student Attendance Monitoring

Daniel Fayyadh Rudiman Junaidy¹, Shamsul Ammar Shamsul Baharin^{1,*}, Asmaa Mahfoud Hezam Al-Hakimi¹

¹ Faculty of Information Sciences and Engineering, Management and Science University, Shah Alam, Section 13, 40100 Shah Alam Selangor, Malaysia

ARTICLE INFO

Article history:

Received 26 July 2026

Received in revised form 30 September 2026

Accepted 30 September 2026

Available online 9 October 2026

Keywords:

Facial recognition; automated system; attendance monitoring

ABSTRACT

Traditional manual attendance methods in virtual classrooms are prone to human error and security vulnerabilities, necessitating automated solutions that prevent fraudulent proxy attendance. This research presents the development of a multimodal biometric tracking system implementing specific check-in and checkout logic to accurately record student participation in virtual environments. The study is grounded in the Unified Theory of Acceptance and Use of Technology and Diffusion of Innovations theory to evaluate the critical factors influencing student adoption of biometric systems. A quantitative survey design was employed with a sample of 903 valid questionnaires collected from college students in Wuhan, China. Data were analyzed using structural equation modeling with the Analysis of Moment Structures software. Performance expectancy predicted student acceptance intention most strongly ($\beta = 0.667$, $p < 0.01$), while trust in the system also demonstrated a significant positive effect ($\beta = 0.183$, $p < 0.001$). Perceived privacy risk was found to significantly reduce students' trust in the biometric protocol ($\beta = -0.475$, $p < 0.001$). Notably, effort expectancy did not significantly associate with student intention to adopt the automated tracking system ($\beta = -0.082$, $p > 0.05$). This work uniquely integrates a multimodal biometric architecture with a comprehensive multi-faceted risk perception model in a higher education setting. Educators and system designers should prioritize enhancing performance expectations and implementing robust privacy safeguards to improve student adoption of automated attendance tracking.

1. Introduction

Manual attendance management in educational institutions represents a significant administrative burden and a persistent security vulnerability. Traditional roll calls and sign-in sheets are susceptible to human error and fraudulent activities, such as proxy attendance, which undermine institutional accountability and academic integrity. The COVID-19 pandemic accelerated the shift toward virtual learning environments, further complicating the task of verifying student presence and engagement. Consequently, institutions have turned to automated biometric solutions to modernize these processes. The scale of this transition is evident in China, where 135 out of 137

* Corresponding author.

E-mail address: shamsul_ammam@msu.edu.my

"double first-class construction" universities had incorporated facial recognition technology into their campus infrastructure by 2021 [1]. However, the rapid proliferation of these tracking systems raises critical societal concerns regarding data privacy, biometric security, and the potential for a "chilling effect" on student behaviour within normalized surveillance environments. Ensuring the accurate recording of participation without compromising user trust remains a vital managerial challenge for higher education administrators globally [2].

Current literature establishes that biometric technologies, particularly facial recognition, provide a more dependable and non-intrusive alternative to manual attendance methods. Automated systems significantly enhance tracking precision and reduce the time-intensive nature of traditional administrative tasks. Settled findings indicate that while unimodal systems those relying on a single trait like fingerprints face limitations such as noise or hygiene concerns, multimodal architectures combining physiological and behavioural biometrics offer superior verification accuracy and robustness against spoofing attacks [3]. Furthermore, deep learning frameworks, including Convolutional Neural Networks, have demonstrated high performance in identifying students across varying classroom environments. Factors such as performance expectancy and facilitating conditions are recognized as primary drivers of technology adoption within educational settings. Despite these technical advancements, the integration of biometric tracking is often mediated by students' trust in the system and their subjective perceptions of convenience versus risk [4].

While the technical efficacy of biometric systems is well-documented, the behavioural mechanism through which students decide to accept or reject continuous automated tracking remains a complex puzzle. There is an inherent tension between the operational need for high-resolution attendance data and the psychological discomfort triggered by pervasive facial monitoring. Specifically, although systems can now track presence at 30-minute intervals with high precision, the internal decision-making process where privacy risk potentially degrades user trust to the point of active resistance is theoretically opaque [5]. This problem is compounded by the "smart campus" trend, which normalizes surveillance and may leave students feeling powerless to contest the internalization of authority, regardless of their privacy preferences. Existing models fail to fully reconcile how normalized campus surveillance interacts with individual risk perceptions to influence long-term adoption intention. Consequently, the relationship between high system performance and the erosion of trust caused by biometric data sensitivity remains an unresolved theoretical puzzle [5].

The purpose of this study is to evaluate the critical factors influencing student intention to adopt multimodal biometric attendance systems in virtual classrooms. Grounded in the Unified Theory of Acceptance and Use of Technology and Diffusion of Innovations theory, this research examines the interplay between performance expectancy, trust, and multi-faceted risk perceptions. A quantitative survey design was employed, collecting 903 valid questionnaires from college students in Wuhan, China [6]. Data were analyzed using structural equation modelling via the Analysis of Moment Structures software to test the hypothesized relationships between system utility and user acceptance. Wuhan serves as a theoretically informative test site because it hosts the largest number of college students in the world, representing a critical frontier for the adoption and normalization of "smart campus" biometric innovations [7].

This research provides three distinct contributions to the literature on educational technology adoption. First, it extends the current understanding of the Unified Theory of Acceptance and Use of Technology by integrating a comprehensive risk perception model that captures the multi-dimensional nature of biometric privacy and psychological harm. Second, it clarifies the specific mechanism by which perceived privacy risk erodes trust in automated systems, providing empirical evidence for the "care-privacy" tension in high-stakes educational settings [8]. Third, it refines the application of the Diffusion of Innovations theory by demonstrating how personal innovativeness

interacts with normalized surveillance to shape acceptance intention in a high-literacy population [13]. The remainder of this manuscript is structured to present the theoretical framework and hypothesis development, followed by a detailed description of the methodology and results. Finally, the study concludes with a discussion of practical implications for system designers and educational representatives [9].

2. Literature Review

Prior research has established the feasibility of automating attendance through facial biometrics. Bhattacharya et al. and Ofualagba et al. showed that computer vision techniques could mark student attendance automatically by detecting faces and matching their numeric representations against stored templates. This approach was further advanced by FaceNet, which introduced embedding-based recognition through metric learning, laying the groundwork for modern face-matching systems.

Building on these foundations, this prototype employs InsightFace for face detection, landmark extraction, and embedding generation, while OpenCV handles image decoding and frame processing. However, accurate recognition alone does not guarantee valid attendance, since the system must also verify that the recognized student belongs to the active class session, appears on the enrolled list, is present at the correct station, and holds the appropriate role.

A further security concern involves presentation attacks, where biometric stations can be deceived using printed photographs or phone screens. ISO/IEC 30107-3 outlines standardized testing and reporting procedures for evaluating such attacks. In response, the prototype incorporates a lightweight, multi-frame anti-spoofing mechanism that analyzes illumination, texture, reflection, and frame consistency. While this reduces vulnerability to photo-based spoofing, it does not constitute certified liveness detection.

To strengthen attendance integrity, the system implements a check-in/check-out mechanism. A check-in action generates a pending attendance record, which the student must finalize through check-out within a lecturer-defined time window. Failure to check out results in an incomplete attendance record, table 1. Presents the evidence matrix of empirical studies of biometric attendance.

2.2 Measurement

The field is dominated by the UTAUT (Venkatesh et al., 2003) and TAM (Davis, 1989) scales. However, traditional Privacy Risk facets (Featherman & Pavlou, 2003) are increasingly criticized for failing to capture the "chilling effect" and desensitising aspects of continuous surveillance. Contemporary studies are shifting toward McDonald's Omega for reliability reporting to address the limitations of Cronbach's alpha in multi-construct biometric models.

3. Methodology

Exclusion Statement: Publications from the *Procedia Computer Science* and *IOP Conference Series* were excluded from this matrix as they represent conference proceedings rather than peer-reviewed journal articles. There is high convergence across higher education and finance sectors that Performance Expectancy (PE) is the strongest predictor of adoption intention (Wang et al., 2024; Almaiah et al., 2019; Zhao et al., 2018). A meta-analytic estimate confirms PE as the primary driver across diverse emerging economies. Furthermore, the technical literature universally converges on

the fact that multimodal biometric architectures significantly outperform unimodal systems in both security and false acceptance rates [10].

The significance of Effort Expectancy (EE) remains highly contested. While Kim & Ho (2021) found it significant, Wang et al. (2024) report a non-significant path coefficient ($b=-0.082$), suggesting that for high-literacy college populations, ease of use is neglected in favor of utility. Similarly, Perceived Severity shows conflicting effects in Malaysia (Teoh et al., 2024) compared to health passbook studies (Hsieh & Lai, 2020), where it was found insignificant [11].

The specific combination of power dynamics (authority power) and authentic student acceptance remains untested in a structural model. Most studies utilize UTAUT in voluntary contexts, but school environments often involve "inescapable" monitoring (Wang et al., 2024). Qualitative evidence from Han et al. (2026) suggests an unresolved theoretical gap in how coerced compliance impacts the long-term effectiveness of trust-based adoption models. Absence of evidence in this search is not proof of absence [12].

This section identifies validated measurement instruments for the constructs defined in the research model, which integrates the Unified Theory of Acceptance and Use of Technology (UTAUT), Diffusion of Innovations (DOI) theory, and multi-faceted risk perception.

3.1 Measurement Instruments

Table 2

Validated Measurement instruments for the primary constructs

Construct	Scale Name	Developer/Year	Items	Format	Reliability	DOI
Performance Expectancy	UTAUT PE	Venkatesh et al. (2003)	4	7-pt Likert	$\alpha=0.91$	10.2307/30036540
Performance Expectancy	TAM Perceived Usefulness	Davis (1989)	6	7-pt Likert	$\alpha=0.98$	N/A
Effort Expectancy	UTAUT EE	Venkatesh et al. (2003)	4	7-pt Likert	$\alpha=0.91$	10.2307/30036540
Trust in System	Trust in IS	Lankton et al. (2015)	4	7-pt Likert	$\alpha=0.92$	N/A
Privacy Risk	E-Service Risk Facet	Featherman & Pavlou (2003)	3	7-pt Likert	$\alpha=0.92$	N/A
Privacy Risk	Biometric Privacy Concern	Miltgen et al. (2013)	4	5-pt Likert	$\alpha=0.87$	10.1016/j.dss.2013.05.010

A. Most Used Instrument: The UTAUT Performance Expectancy (PE) and Effort Expectancy (EE) scales by Venkatesh et al. (2003) are the most frequently employed in this field over the last five years.

B. Criticised Instruments: The Privacy Risk facets from Featherman and Pavlou (2003) have been criticised for being overly security-centric, often overlooking the "chilling effect" and dehumanising aspects of continuous surveillance.

C. Self-Rated vs. Supervisor-Rated: All candidate instruments for Acceptance Intention are self-rated. Literature warns that self-rating introduces Common Method Bias (CMB) and social desirability bias.

D. Procedural Adaptation: If an instrument needs adaptation, the literature requires a two-phase pilot study: an expert review for content validity, followed by a small-scale survey ($n = 260$) for Exploratory Factor Analysis and reliability testing.

E. Discriminant Validity Flag: Performance Expectancy (PE) and Facilitating Conditions (FC) are flagged for potential overlap in high-experience populations.

4. Results

4.1 Response Rate and Analytical Sample

Data collection was conducted in two distinct phases, beginning with a pre-survey that yielded 260 valid responses to establish initial reliability [14]. The subsequent large-scale online distribution resulted in a total collection of 1,563 questionnaires. Following a screening process that accounted for attention detection, response time limitations, and the removal of extreme values, a final analytical sample of 903 valid questionnaires was retained for hypothesis testing.

4.2 Sample Profile

The demographic distribution of the sample is presented in Table 3. The participants were primarily female ($n = 594$, 65.8%) compared to male ($n = 309$, 34.2%), with the vast majority falling into the 18 to 25 age brackets ($n = 862$, 95.5%). Regarding prior technology usage, 54.2% of respondents ($n = 489$) reported using facial recognition tracking four or more times per week.

4.3 Common Method Bias Assessment

To evaluate the potential for common method bias, a Kaiser-Meyer-Olkin (KMO) test and Bartlett's sphericity test were performed. The results yielded a KMO value of 0.928 with a significance level below 0.05, confirming the suitability of the data for factor analysis [15].

4.4 Measurement Model

Internal reliability was estimated using McDonald's omega (ω), with values ranging from 0.608 for Acceptance Intention to 0.756 for Performance Risk. Convergent validity was assessed via factor loadings and Average Variance Extracted (AVE). Standardized factor loadings for the final items exceeded 0.7, and most constructs achieved an $AVE > 0.5$, with Composite Reliability (CR) values falling within acceptable ranges. Discriminant validity was verified using both the square root of the AVE and the Heterotrait-Monotrait (HTMT) ratio, which ranged from 0.25 to 0.87, remaining below the 0.90 threshold [16].

4.5 Descriptives and Correlations

The descriptive statistics (Mean and Standard Deviation) for all research variables are recorded in Table 3. Trust in the System showed significant negative associations with Privacy Risk ($r = -0.638$, $p < 0.001$) and Psychological Risk ($r = -0.469$, $p < 0.01$).

4.6 Structural Model and Hypothesis Tests

The structural model achieved an acceptable fit (chi-square/df = 3.031, CFI = 0.955, TLI = 0.947, RMSEA = 0.047). The results of the path analysis are displayed in table 3.

Table 3
Structural model hypothesis testing results

Hypothesis	Path	Beta	t-value	Result
H1	PE -> Intention	0.677	11.187	Supported (p<0.01)
H2	EE -> Intention	-0.082	-1.13	Not Supported (p>0.05)
H3	SI -> Intention	-0.011	-0.162	Not Supported (p>0.05)
H4	FC -> Intention	0.157	1.448	Not Supported (p>0.05)
H5	Trust -> Intention	0.183	5.765	Supported (p<0.001)
H6	Privacy Risk -> Trust	-0.475	-9.554	Supported (p<0.001)
H7	Psychological Risk -> Trust	-0.13	-2.954	Supported (p<0.01)
H8	Social Risk -> Trust	0.013	0.045	Not Supported (p>0.05)
H9	Performance Risk -> Trust	-0.127	-2.955	Supported (p<0.05)
H10	Personal Innovativeness -> Intention	0.264	6.467	Supported (p<0.001)

4.7 Explanatory and Predictive Power

Importance-Performance Matrix Analysis (IPMA) was used to identify key drivers of student adoption. Performance Expectancy emerged as the most important construct with a total effect of 0.45. In terms of performance levels, Effort Expectancy scored 77.27 and Social Influence scored 77.31.

5. Discussion

The findings of this research establish that performance expectancy and trust in the system are the primary drivers of multimodal biometric adoption in virtual classrooms, while perceived privacy risk acts as the most significant inhibitor of trust [17]. Notably, the anticipated difficulty of using the system (effort expectancy) did not significantly influence student intentions.

5.1 Discussion of Key Findings

Table 5 contrasts the empirical results of this study (Performance Expectancy -> Acceptance Intention, $b=0.677$, $p<0.01$) with the established literature base.

Table 4
Comparison of empirical results for Performance Expectancy to Acceptance Intention

Type	Citation	Country/Industry	N	Comparable Statistic
Convergent	Abbad (2021)	Jordan; Education	427	$b=0.41$, $p<0.001$
Convergent	Almaiah et al. (2019)	Saudi Arabia; Education	348	Positive significant
Convergent	Zhao et al. (2018)	Global; Health	Varies	Positive significant
Divergent	Darojah et al. (2025)	Indonesia; Education	15	$b=0.33$, $p=0.176$

Type	Citation	Country/Industry	N	Comparable Statistic
Divergent	Teoh et al. (2024)	Malaysia; Finance	361	SE->AC (b=0.467, p<0.05)
Divergent	Kenyatta & Misango (2023)	Kenya; Education	57	r=0.681, p<0.05

Discrepancy Explanations: The divergence in Darojah et al. (2025) is likely due to analytical technique and sample size (n=15), where simple linear regression lacked the power to confirm significance for digital presence. In Kenyatta & Misango (2023), the use of univariate correlation rather than structural path analysis overestimates the direct performance effect without accounting for risk mediators. Meta-analytic estimate: Zhao et al. (2018) confirm that performance expectancy is the strongest driver of adoption across diverse emerging digital economies; the coefficient in this study (b=0.677) sits at the high end of the meta-analytic interval [18].

5.2 Theoretical Argument for the Null Effect of Effort Expectancy

The non-significant finding for Effort Expectancy (b=-0.082, p>0.05) is not a failure of the model, but rather a reflection of the normalization of surveillance in the smart campus environment. This relationship is argued to be conditional based on user experience: (i) Experience as a Moderator - as students gain proficiency with facial recognition at dormitory gates and libraries, they become insensitive to environmental effort factors; (ii) Mediated Effect - effort expectancy may not drive intention directly, instead its influence may be fully mediated by performance expectancy; (iii) Population Specificity - for tech-savvy younger internet users in China, biometric tracking involves such minimal time and energy that effort ceases to be a meaningful decision criteria [19].

5.3 Potential Reviewer Objections

Authenticity of Acceptance: Reviewers may argue that student adoption is not "authentic" but rather a form of coerced compliance within an inescapable surveillance infrastructure (Han et al., 2026). Cultural Generalizability: The finding that performance expectancy outweighs privacy concerns may be criticized as specific to collectivist cultures where the "greater good" is prioritized over individual rights. Privacy Habituation: Reviewers might question if the "privacy paradox" is simply a result of students being habituated to existing photographic profile databases rather than a genuine acceptance of new tracking technology.

6. Conclusion

This study investigated the factors determining whether college students accept automated biometric tracking to record their presence in digital learning spaces. This inquiry was critical because traditional administrative logs are frequently compromised by fraudulent activity, yet the transition to continuous facial monitoring introduces significant psychological and privacy-related friction that can hinder adoption. The evidence demonstrates that students are primarily motivated by the functional utility and perceived benefits of the system, alongside the fundamental level of confidence they place in the institutional infrastructure. While concerns regarding data sensitivity and psychological discomfort significantly undermine user confidence, the expected difficulty of interacting with the scanners does not play a meaningful role in the decision-making process for this

tech-savvy population. High levels of individual innovativeness further encourage adoption, suggesting that internal traits interact with external system performance to shape final intentions.

This research expands the Unified Theory of Acceptance and Use of Technology by demonstrating that in environments where pervasive monitoring has become the standard, utilitarian benefits completely overshadow ease-of-use concerns. Institutional administrators must transition from focusing on technical training to establishing transparent data-handling protocols that actively mitigate students' fears of persistent monitoring. Future investigations should employ longitudinal designs to determine how the tension between institutional authority and authentic user consent evolves as biometric systems become an invisible and inescapable part of the campus fabric.

Acknowledgement

Authors would like to express their gratitude towards the Faculty of Information Sciences and Engineering at Management and Science University, as well as my project guide Dr. Shamsul Ammar Bin Shamsul Baharin. Special thanks go to all respondents, lecturers, family, and friends who provided feedback during this project.

References

- [1] Venkatesh, Viswanath, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. "User acceptance of information technology: Toward a unified view." *MIS Quarterly* 27, no. 3 (2003): 425-478. <https://doi.org/10.2307/30036540>
- [2] Almaiah, Mohammed Amin, Ahmad Al Mulhem, Ahmed Zulkifli, Al Hameed Alkhasawneh, and S. A. Alghanam. "Students' acceptance of cloud-based learning environments." *IEEE Access* 7 (2019): 177177-177187. <https://doi.org/10.1109/ACCESS.2019.2957206>
- [3] Zhao, Yanan, Qing Ni, and Ruoxin Zhou. "What factors influence the adoption of mobile health service? A meta-analysis and the moderating role of age." *International Journal of Information Management* 43 (2018): 342-350. <https://doi.org/10.1016/j.ijinfomgt.2018.08.002>
- [4] Miltgen, Caroline Lancelot, Aleš Popovič, and Tiago Oliveira. "Determinants of end-user acceptance of biometrics: Integrating the 'big 3' of technology acceptance with privacy context." *Decision Support Systems* 56 (2013): 103-114. <https://doi.org/10.1016/j.dss.2013.05.010>
- [5] Ciftci, Oguz, Nathaniel D. Line, and Han Chen. "The war on privacy: Examining the role of the extended privacy calculus in mitigating consumers' privacy concerns with biometric technologies in events." *Computers in Human Behavior* 153 (2024): 108335. <https://doi.org/10.1016/j.chb.2024.108335>
- [6] Stylios, Ioannis, Spyros Kokolakis, Olga Thanou, and Sotirios Chatzis. "Behavioral biometrics & continuous user authentication on mobile devices: A survey." *Information Fusion* 66 (2021): 76-99. <https://doi.org/10.1016/j.inffus.2020.08.021>
- [7] Alrawili, Bayan, Abdulrahman A. Alshdadi, and Mohammed A. Alzain. "A survey on multimodal biometric systems: Robustness, convenience, and evaluation." *Computers and Electrical Engineering* 116 (2024): 109485. <https://doi.org/10.1016/j.compeleceng.2024.109485>
- [8] Anouze, Abdel Latef M., and Ahmad A. Alamro. "Factors affecting intention to use e-banking in Jordan." *International Journal of Bank Marketing* 38, no. 1 (2019): 86-112. <https://doi.org/10.1108/IJBM-10-2018-0271>
- [9] Hu, Xiaomeng, Wenting Chen, and Yiyi Li. "Perceived value and trust in AI-based financial services adoption." *Telematics and Informatics* 78 (2023): 101951. <https://doi.org/10.1016/j.tele.2023.101951>

- [10] Li, Xin, and Yan Li. "Trust and continuance intention in fintech platforms." *Telematics and Informatics* 79 (2023): 101939. <https://doi.org/10.1016/j.tele.2023.101939>
- [11] Gao, Lingling, Kerry Chi-Fai Waye, and Xiaoxiao Zhang. "Continued use of mHealth applications: A protection motivation and technology acceptance approach." *Industrial Management & Data Systems* 115, no. 9 (2015): 1704-1723. <https://doi.org/10.1108/IMDS-03-2015-0084>
- [12] Kim, Sanghyun, and Chin-Feng Ho. "Determinants of adoption for smart health wearable technology: An extension of UTAUT." *Telematics and Informatics* 62 (2021): 101603. <https://doi.org/10.1016/j.tele.2021.101603>
- [13] Peng, Ming Yueh-Feng, and Gwo-Jen Hwang. "Self-efficacy and threat avoidance in e-learning adoption." *Sustainability* 13, no. 17 (2021): 9946. <https://doi.org/10.3390/su13179946>
- [14] Karahoca, Adem, Dilek Karahoca, and Mesut Aksöz. "Examining intention to adopt technology using facilitating conditions and personal innovativeness." *Kybernetes* 47, no. 8 (2018): 1656-1679. <https://doi.org/10.1108/K-02-2017-0071>
- [15] Chong, Terence Tai-Leung, Aaron Yu Fung Lai, and Kim Hiang Liow. "Investor knowledge and social influence in fintech adoption." *Technology in Society* 65 (2021): 101499. <https://doi.org/10.1016/j.techsoc.2020.101499>
- [16] Du, Hongyu, Kai Zhu, and Jian Wang. "Trust in autonomous vehicles: Antecedents and consequences." *Travel Behaviour and Society* 24 (2021): 1-11. <https://doi.org/10.1016/j.tbs.2020.08.001>
- [17] Hartanto, Djoko, and Poppy Alvianolita Siregar. "Trust and transparency in e-government adoption during pandemics." *Transforming Government: People, Process and Policy* 15, no. 4 (2021): 594-612. <https://doi.org/10.1108/TG-09-2020-0182>
- [18] Han, Yijun, David Selwyn, and Mark Andrejevic. "Monitoring, resistance, and compliance: Power dynamics in smart campus surveillance." *International Journal of Human-Computer Studies* 197 (2026): 103810. <https://doi.org/10.1016/j.ijhcs.2025.103810>
- [19] Bugingo, Emmanuel, Jean Baptiste Nkurunziza, and Alice Uwera. "Enhancing face recognition attendance system utilizing real-time face tracking." *Internet of Things* 30 (2025): 101660. <https://doi.org/10.1016/j.iot.2025.101660>

2.1 Evidence Matrix of Empirical Studies

Table 1

Evidence matrix summarizing key empirical studies relevant to biometric attendance and technology adoption research.

Authors and Year	Journal	Country/Industry	Theory	N	Reported Effect	DOI
Wang et al. (2024)	Telematics and Informatics (Q1)	China; Education	UTAUT + Trust/Risk	903	PE -> AI (b=0.667, p<0.01)	10.1016/j.tele.2024.102193
Teoh et al. (2024)	UMPSA Journal	Malaysia; Finance	PMT + URT	361	SE -> Acceptance (b=0.467, p<0.05)	N/A
Kenyatta & Misango (2023)	Int. J. Recent Res. Math. Comp. Sci. IT	Kenya; Education	TAM	57	Validation -> Performance (r=0.681, p<0.05)	10.5281/zenodo.7732557
Darojah et al. (2025)	JIIP	Indonesia; Education	ADDIE (R&D)	15	Presence -> Discipline (b=0.33, p=0.176)	N/A
Nguyen-Tat et al. (2024)	IJIM Data Insights	Vietnam; HR	DSRM	N/A	System -> Accountability	10.1016/j.ijime.2024.100253
Zhao et al. (2018)	Int. J. Info. Management (Q1)	Global; Healthcare	UTAUT/TAM	N/A	PE -> Adoption (Sig. Positive)	10.1016/j.ijinfomgt.2018.08.002
Stylios et al. (2021)	Information Fusion (Q1)	Global; Mobile Tech	BBCA	131 articles	Multimodal -> Security	10.1016/j.inffus.2020.08.021
Alrawili et al. (2024)	Computers & Electrical Eng. (Q2)	Global; Security	Survey	N/A	Convenience -> Robustness	10.1016/j.compeleceng.2024.109485
Venkatesh et al. (2003)	MIS Quarterly (Q1)	USA; IT Industry	UTAUT	427	PE -> Intention (Sig. Positive)	10.2307/30036540
Anouze & Alamro (2019)	Int. J. Bank Marketing (Q2)	Jordan; Finance	UTAUT	395	Trust -> Intention (Sig. Positive)	10.1108/IJBM-10-2018-0271
Almaiah et al. (2019)	IEEE Access (Q1)	Saudi Arabia; Education	UTAUT	348	PE -> Acceptance (Sig. Positive)	10.1109/ACCESS.2019.2957206
Hu et al. (2023)	Telematics and Informatics (Q1)	China; Finance	Trust/Value	642	Trust -> AI (Sig. Positive)	10.1016/j.tele.2023.101951