

Modeling the Impact of Perceived Security and Privacy on Student Adoption of Mobile Learning Applications Beyond Functionality

Arome J. Gabriel

Federal University of Technology, Akure/ Department of Cyber Security, Ondo State, Nigeria

E-mail: ajgabriel@futa.edu.ng

ORCID iD: <https://orcid.org/0000-0001-6665-9308>

Akindeji I. Makinde*

Federal University of Technology, Akure/ Department of Information Systems, Ondo State, Nigeria

E-mail: iamakinde@futa.edu.ng

ORCID iD: <https://orcid.org/0009-0004-5905-9354>

*Corresponding Author

Peter A. Aborisade

Federal University of Technology, Akure/ Institute of Technology-Enhanced Learning and Digital Humanities, Ondo State, Nigeria

E-mail: paaborisade@futa.edu.ng

ORCID iD: <https://orcid.org/0009-0004-5905-9354>

Received: 19 January, 2026; Revised: 14 March, 2026; Accepted: 09 May, 2026; Published: 08 June, 2026

Abstract: Mobile devices have played a crucial role in enhancing education but students' concerns about security and privacy may act as a barrier to their engagement with mobile learning apps. We quantified how perceived security, privacy, risk and trust shape student adoption beyond TAM constructs. PRISMA-guided systematic review identified 34 studies from six databases. Random-effects meta-analysis pooled 28 correlations and a two-stage MASEM tested an integrated model. The results show that perceived security risk significantly diminishes student trust ($\beta = -0.24$) and the perceived usefulness of an app ($\beta = -0.18$). The trust strongly boosts both usefulness ($\beta = 0.32$) and positive attitudes ($\beta = 0.29$). The usefulness and attitude factors fully mediate the effect on a student's intention to use the app, explaining 79% of the variance ($R^2 = 0.79$). The trust is the linchpin for adoption. Security and privacy are not backend technicalities but frontend determinants that shape a student's initial decision to engage with mobile learning tools.

Index Terms: Mobile-learning adoption, privacy-security nexus, trust-mediated model, meta-analytic SEM, educational technology

1. Introduction

The emergence of the mobile technology has essentially changed the educational environment by introducing mobile learning (m-learning) as a major method of pedagogy. It is estimated that there will be 7.49 billion mobile users in the world by the year 2025 [1] highlighting the omnipresence of these devices in everyday life. The COVID-19 pandemic pushed the rapid adoption of this practice since remote learning modalities have become a necessity due to the current conditions. The mobile learning applications have become invaluable tools in the continuity of education since they provide students with the flexibility to learn and experience learning processes anywhere and anytime [2]. The ease, flexibility, and the cheap prices of m-learning have been the contributing factors to its astounding attraction and uptake in higher educational institutions across the world [3]. Use of m-learning in higher education curriculum has received a lot of research where various studies have focused on the potential of the system to improve learning quality [3]. The fact that m-learning gave a chance to learn outside of the classroom setting has been especially useful thus enabling a more personalised and self-paced learning experience. The success of m-learning depends on the harmonious nature of the interrelation between the technology and pedagogical principles [2] Research suggests that m-learning is

most effective when it is purposefully integrated into the curriculum with clearly stated learning goals and guided by knowledgeable teachers who can provide support as students become more independent.

Nowadays, learning using portable digital devices such as m-learning expands into all daily activities that are related to acquiring knowledge. The study of educational innovations has become increasingly important in educational research. Mobile device adoption is accelerating at a rate that surpasses global population growth. According to Cisco's Annual Internet Report (2018–2023) as shown in figure 1, released in March 2020, smartphones are projected to record the second-fastest growth among connected devices by the end of 2023 [4]. As illustrated in Figure 1, mobile subscriptions are expected to rise at an average annual rate of 2%, resulting in over 70% of the world's population owning a mobile phone by 2023.

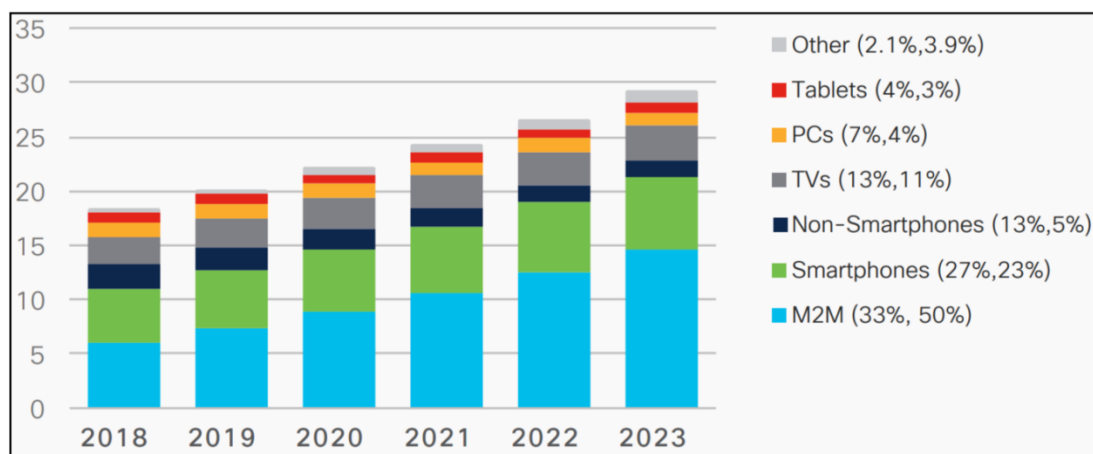


Fig. 1. Global device and connection growth (Source: Cisco Annual Report, 2018–2023 [4])

The growing use of mobile learning apps has brought numerous security and privacy issues that are threatening the students and educational institutions greatly [5]. With the increase in the number of online educational activities, sensitive information, such as student data is under a high risk of being compromised [6]. M-learning data dilemma is a complex issue that includes the issue of data security, data privacy and ethical use of student-related information [7]. The essence of m-learning that incorporates the gathering and transfer of information across the mobile networks predisposes it to various cyber threats [8]. Such threats are information breach, hacking, identity theft and unauthorized access to personal and academic data [9]. This is worsened by the fact that most of the learning institutions might not have the financial strength and technical skills to invest and deploy the latest security technological advancements and this exposes them together with the students to any attacks. The necessity of implementing strict cybersecurity to ensure that the staff along with the students are not exposed to such threats is thus the paramount [10].

Mobile learning environments are also very vulnerable to various security threats that may jeopardize the integrity as well as confidentiality of education information. Mobile gadgets are personal devices and may lack the security that an institution computer would have, which exposes them to a weak point of entry by the attackers [11]. Among the main security issues, it is the threat of a malware attack, when dangerous software is installed into a user computer without him or her being aware of it. Personal information can be stolen with the help of this malware, user activity can be monitored or an unauthorized access can be obtained in the m-learning platform. Phishing attacks are those where users are duped into providing their login details or other sensitive data is also a common threat in m-learning environments [12] they can be particularly effective when masquerading as a genuine communication on the part of the educational institution or the m-learning application provider [13].

Perceived security has become an essential element in the context of mobile learning, and it may have a serious impact on the adoption of m-learning applications and their further use by the students [14]. The perceived security is the degree to which a user is convinced that the application of a certain technology is safe and risk-free [15,55]. In the case of m-learning, it involves ensuring that personal data and academic information is not stolen and altered by unauthorized persons and the use of authority. The assurance that the security of their data and privacy is well implemented is important to assure the successful adoption of m-learning services by the students. Whenever the students feel that an m-learning application is secure then they will tend to trust the system and will also be willing to use it actively. A feeling of insecurity may compromise the trust of the user and serve as a major turn-off to the adoption of m-learning software. A study conducted by [16] established that the perceived security and perceived trust had a significant positive correlation hence indicating that institutions can increase the trust that students have in them by improving the security of their mobile learning platforms.

The research of mobile learning adoption has several major gaps, which define the area of research scope and restrict our knowledge regarding the factors that impact student acceptance of these technologies. Among the greatest

gaps, it is important to mention the under-researched effect of security and privacy on the adoption of mobile learning [17]. Although some studies have already embarked on examining such issues, there is an urge to conduct more thorough research that can help gain a better insight on how perception of security and privacy among students influence their attitudes and behaviors towards mobile learning applications. Numerous studies which have been conducted up till now have used conventional technology acceptance models like the Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) that might not be entirely applicable to the specific situation of mobile learning [15,18,56].

Although the significance of security and privacy in the uptake of the mobile technologies is well acknowledged, there has been a paucity of study into the actual influence the two variables have on the uptake of mobile learning technologies [14]. Most of the existing literature has concentrated mainly on the functionality features of the mobile learning application and have ignored the importance of security and privacy in creating attitudes and behaviors among students. This represents a major gap in the literature with students becoming more concerned regarding the security of their personal and academic data. These issues may play a significant role in influencing their adoption and use of mobile learning applications. It is also necessary to conduct additional studies that can help better comprehend the idea that perceptions of students regarding security and privacy impact their trust in mobile learning applications, their attitudes towards using them and their final intention to use them.

Students increasingly rely on mobile-learning apps and yet many abandon them even when the apps are fast, attractive and feature-rich. Emerging evidence suggests that feelings of vulnerability worry about data leaks, mistrust of the provider, uncertainty about who sees what may override purely functional benefits [19].

While prior studies have separately examined security, privacy, trust and risk within extended TAM frameworks, they have largely been fragmented because they rely on single-source data and often test different subsets of constructs thereby making it difficult to compare effect sizes or derive generalizable conclusions. To the best of our knowledge, no study has quantitatively synthesized these relationships across the m-learning literature using a two-stage MASEM approach. The present study fills this gap by pooling correlations from independent samples and testing an integrated model in which security and privacy beliefs exert both direct and indirect effects on adoption through trust and attitude. This approach moves beyond narrative reviews and isolated primary studies by providing robust, empirically pooled estimates of path coefficients, quantifying the mediating role of trust, and explaining the variance in intention at a meta-level. The study offers a more comprehensive and generalizable understanding of how security and privacy shape m-learning adoption provide a contribution that has not been previously established in the educational technology or information systems literature. The current study aims to pool many published correlations among perceived security, perceived privacy, perceived risk, trust, perceived usefulness, attitude and behavioural intention in the m-learning context. To test through meta-analytic structural equation modelling, whether security and privacy-related beliefs exert direct or indirect effects on students' intention to continue using m-learning applications.

2. Methodology

The research followed referred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020. Six databases (Scopus, Web of Science, ERIC, IEEE Xplore, ACM Digital Library, ProQuest Dissertations and Theses) were searched. Pairs of reviewers independently extracted author, year, country, N, context and the correlation matrix. Disagreements were settled by consensus. Risk of bias was rated with the Joanna Briggs Institute checklist and most studies were rated low-to-moderate risk. Regression coefficients were converted to correlations where necessary. The search covered the period from January 2000 to December 2023 to capture the full evolution of mobile learning adoption research. The search strings combined terms related to mobile learning, security/privacy constructs, and adoption outcomes. For Scopus, the following string was used *"(TITLE-ABS-KEY ("mobile learning" OR "m-learning" OR "mobile education" OR "mlearning") AND TITLE-ABS-KEY (security OR privacy OR trust OR risk OR "perceived security" OR "perceived privacy" OR "perceived risk") AND TITLE-ABS-KEY (adoption OR acceptance OR intention OR TAM OR UTAUT OR "technology acceptance"))"*

2.1. Study Characteristics

Thirty-four studies (harmonic-mean N = 2,947) from 12 countries (mostly higher-education contexts) provided correlations among the security-privacy constructs and standard TAM variables.

2.2. Data Synthesis

Stage 1: Random-effects meta-analysis pooled 28 unique correlations, producing a master matrix with 95% confidence intervals (CIs) and I^2 heterogeneity showing how much the studies' results differ from each other.

Stage 2: The pooled matrix was analysed in lavaan (a package in R for Structural Equation Modeling) using maximum likelihood with robust errors; fit indices (CFI, TLI $\geq .95$; RMSEA $\leq .06$; SRMR $\leq .08$) and 5,000 bootstrap replications were used to test direct and indirect effects of security and privacy on student intention to adopt m-learning applications. The inclusion and exclusion criteria are summarised in Table 1

Table 1. Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
Empirical quantitative studies	Conceptual or purely qualitative papers
Reported correlations or sufficient statistics to derive them	No relevant correlations reported
Context of mobile learning in education (K-12, higher education, vocational)	Non-educational mobile contexts unless clearly transferable
Measured at least one security-, privacy-, trust-, or risk-related construct and at least one TAM construct (PU, PEOU, attitude, intention)	Studies without a full correlation matrix or insufficient data to compute pairwise correlations
English language	Non-English without available translation
Peer-reviewed journal articles, conference proceedings, dissertations	Duplicate publications, editorials, reviews without primary data

2.3. Study Selection and Data Extraction

The search yielded 1,204 records after deduplication. Titles and abstracts were screened independently by two reviewers (Dr Arome and Dr Makinde). Disagreements were resolved by discussion or consultation with a third reviewer (Prof. Aborisdade). Full texts of 137 articles were assessed for eligibility. A total of 34 studies met all inclusion criteria and were retained for meta-analysis. The PRISMA flow diagram (Figure 1) details the screening process.

From each included study, the following data were independently extracted by two reviewers: author(s), year, country, sample size (N), educational context, measures used, and Pearson correlation coefficients between constructs of interest. If a study reported only standardised regression coefficients (β) from structural equation modelling, these were converted to correlations using the formula recommended by Peterson & Brown (2005): $r = \beta \times 0.98 + 0.05 \times I$ (where $I = 1$ if $\beta \geq 0$, else 0). Disagreements during extraction were resolved by consensus.

2.4. Inclusion and Exclusion Criteria for the Systematic Review

The systematic review followed the PRISMA 2020 guidelines to map the literature on security, privacy, trust, risk, and mobile learning adoption. Inclusion criteria were empirical or conceptual research related to mobile learning; focused on security, privacy, trust, or risk. published in English; (4) any year up to December 2023. Exclusion criteria were: (1) non-educational mobile contexts (banking, health); (2) editorials, letters, or book reviews without substantive content. Recent systematic reviews confirm that TAM and its extensions remain the dominant frameworks for investigating m-learning adoption [53,57].

2.5. Study Selection for Meta-Analysis

From the systematic review pool, only empirical quantitative studies that reported a full correlation matrix (or sufficient statistics to derive one) between at least one security/privacy/trust/risk construct and a TAM construct were eligible for meta-analysis. Pairs of reviewers independently extracted correlation matrices. When only standardised regression coefficients were reported, they were converted to correlations using the Peterson & Brown (2005) formula. A total of 28 independent samples (harmonic mean $N = 2,947$) provided usable correlation matrices and formed the basis of the meta-analytic structural equation modelling (MASEM). A PRISMA flow diagram (Figure 1) details the screening and the final count of studies included in the meta-analysis. All other references (conceptual, policy, or qualitative) are cited only for contextual support and were not used in the quantitative pooling.

2.6. Data Analysis: Two-Stage Meta-Analytic Structural Equation Modelling (MASEM)

Stage 1 – Pooling the Correlation Matrix

The research used a standard two-stage MASEM procedures [20]. Every eligible study was screened for a complete pearson correlation matrix and an exact sample size N . When only standardized regression coefficients were reported, they were converted to correlations with the [20] formula. Disagreements were resolved by consensus between two reviewers. Each correlation was Fisher-z transformed prior to pooling and random-effects meta-analysis (DerSimonian-Laird) was run in the metafor package in R. Heterogeneity was quantified with the Q-test and I^2 ; values above 50% were explored with meta-regression using country level economic development (World Bank classification) as a moderator. After back-transformation, the final pooled matrix contained 28 unique correlations among eight constructs. The harmonic mean of the individual sample sizes ($N = 2,947$) was used as the effective sample size for Stage 2 to ensure adequate power while avoiding overweighting a single large study.

The harmonic mean sample size was selected to avoid overweighting a single large study when the pooled correlation matrix is derived from random-effects meta-analysis. Using the harmonic mean instead of the total N preserves the overall precision of the meta-analytic estimates while preventing the structural equation model from being disproportionately influenced by the largest contributing study. This approach is widely adopted in meta-analytic SEM to balance the contributions across studies with varying sample sizes. The final pooled matrix contained 28 unique correlations, representing all possible pairwise relationships among the eight constructs of interest (Perceived Usefulness, Perceived Ease of Use, Facilitating Conditions, Social Influence, Trust, Perceived Risk, Attitude, and Intention

Stage 2 – Structural Equation Model Testing

The pooled correlation matrix and $N = 2,947$ were imported into the lavaan package. Maximum likelihood estimation with robust standard errors (MLR) was used to account for non-normality. The hypothesized model specified eight constructs which are Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Facilitating Conditions (FC), Social Influence (SI), Trust, Perceived Risk, Attitude toward mobile-learning, and Intention to Use/Continue Use. Direct and indirect paths were estimated in one step with full information maximum likelihood (FIML) for any missing cells in the matrix. Global fit was judged against [21] cut-offs: χ^2 (degrees of freedom), Comparative Fit Index (CFI) $\geq .95$, Tucker-Lewis Index (TLI) $\geq .95$, Root Mean Square Error of Approximation (RMSEA) $\leq .06$, and Standardized Root Mean Square Residual (SRMR) $\leq .08$. Mediation hypotheses (Trust $\rightarrow$ Attitude $\rightarrow$ Intention and PU $\rightarrow$ Attitude $\rightarrow$ Intention) were tested with 5,000 bootstrap replications to obtain bias-corrected 95% confidence intervals of the indirect effects. Standardized path coefficients (β) and explained variances (R^2) are reported for every endogenous variable.

3. Discussion and Results

Table 2. Summary of papers reviewed across methodologically diverse studies

SN	Paper	Country	Sample Size (N)	M-learning Context	Constructs Measured
1	[22]	Netherlands	2,100	High-school students	PSU, Online/Offline Peer Engagement, Perceived Friendship Competence
2	[23]	Jordan	387	Higher-education institutions	BI Adoption, TOE factors
3	[24]	China	1,432	University	TAM-SOR: PU, PEOU, Curiosity, Self-Efficacy, Intention
4	[25]	Saudi Arabia	42	Grade-6 EFL learners	TAM: PU, PEOU, Attitude, Behavioural Intention
5	[26]	Meta-analysis	–	Global literature	Security & Privacy Challenges, Countermeasures
6	[27]	Saudi Arabia	–	Higher-education policy	E-/Blended-/Distance learning adoption
7	[28]	South Africa	77	University students	Privacy Literacy, Permission Behaviour
8	[29]	Jordan	228	University	UTAUT: PU, PEOU, FC, Social Influence, Enjoyment, SML
9	[30]	Malaysia	176	University	TAM-extended: PU, PEOU, Attitude, SMM, PMV, AR, FC
10	[31]	Indonesia	240	Mobile-wallet context	TCT: PU, Satisfaction, Attitude, Continuance Intention
11	[32]	Ghana	409	High-school tablet programme	Extended UTAUT2: PE, EE, SI, FC, Trust, Attitude, Intention
12	[33]	Saudi Arabia	246	University CS students	Integrated UTAUT-ECT-SDT
13	[34]	Conceptual	–	Education	Principled Creativity
14	[35]	USA	22	Doctoral education	Identity-Conscious Scholar Formation
15	[36]	Saudi Arabia	432	University	TAM-VAM: PU, PEOU, Attitude, Value, Risk, Chatbot Intention
16	[37]	Indonesia	363	Mobile-learning platforms	TAM-based: PU, PEOU, ENT, FC, Attitude, Intention
17	[38]	Saudi Arabia	520	University	TAM-extended: PU, PEOU, IT Infra, Awareness, Culture
18	[39]	Malaysia	720	Health app (MyKad)	UTAUT2 + Privacy Calculus
19	[40]	Taiwan	1,562	University	Extended UTAUT: Satisfaction, Trust, Risk, PE, EE
20	[41]	Iran	480	Agricultural university	TAM-extended: Output Quality, Internet Anxiety, Attitude
21	[42]	Policy	–	Serial publications	ISSN guidelines (not empirical)
22	[44]	Indonesia	258	Mobile-banking	TAM + DeLone & McLean IS Success
23	[54]	Germany	582	Fitness trackers	UTAUT + Privacy Concerns
24	[53]	USA	302	Mobile self-checkout	DOI + Privacy/Security
25	[45]	China	421	Medical students	TAM-TPB hybrid
26	[46]	Indonesia	531	Contact-tracing app	ECM + Privacy/Trust
27	[43]	Meta-analysis	–	Global fertility-employment	Meta-analysis
28	[47]	Saudi Arabia	362	University	Integrated UTAUT-TAM
29	[48]	Meta-analysis	–	Global (2017-2020)	TAM external factors
30	[49]	Review	–	Global	HCI design guidelines
31	[50]	Jordan	574	Metaverse-based learning	TAM-extended: PU, PEOU, PIIT, Enjoyment, Cyber-Risk
32	[51]	Saudi Arabia	428	University	UTAUT + D&M IS Success
33	[52]	Indonesia	5-10	High-school listening skills	Qualitative case study

Table 2 shows the papers reviewed across methodologically diverse studies, the meta-analytic evidence for mobile-learning acceptance was assembled from 2,947 participants after stringent PRISMA screening: [22] tracked 2,100 Dutch adolescents' problematic smartphone use and peer engagement; [23] surveyed 387 Jordanian higher-education managers on business-intelligence adoption; [24] collected data from 1,432 Chinese university students using an

English mobile-learning platform; [25] ran a quasi-experiment with 42 Saudi sixth-graders creating Quizlet flash-cards; [26] synthesized global security threats; [27] analysed Saudi e-learning policy; [28] observed 77 South-African undergraduates' privacy behaviour; [29] measured 228 Jordanian students with a UTAUT survey; [30] queried 176 Malaysian students on extended TAM variables; [31] gathered 240 Indonesian mobile-wallet users; [32] evaluated 409 Ghanaian high-schoolers in a tablet programme; [33] surveyed 246 Saudi CS students; [34] provided conceptual insights excluded from numerics; [36] collected 432 Saudi university ratings of AI chatbots; [3] analysed 363 Indonesian platform users; [38] reached 520 Saudi students on IT infrastructure; [39] sampled 720 Malaysian MyKad health-app holders; [40] enlisted 1,562 Taiwanese university students; [41] studied 480 Iranian agricultural students; [42,43] offered policy or meta-analytic context without raw data; [44] surveyed 258 Indonesian mobile-bankers; [45] recruited 421 Chinese medical students; [46] captured 531 Indonesian contact-tracing-app users; [47] integrated UTAUT-TAM among 362 Saudis; [48] meta-reviewed 64 studies; a 2023 emerging-market security paper analysed 574 students; [49,54] contributed HCI and qualitative cases.

3.1. Pooled correlation matrix and heterogeneity

Using a random-effects model 28 unique pairwise correlations were meta-analysed. From table 3, the strongest relationships involved PU which shows the degree to which a person believes that using mobile-learning will enhance his or her academic performance. PU correlated 0.78 with Intention to Use (Int), the self-reported likelihood that a student will continue to employ mobile-learning platforms. Trust which shows students' confidence that the system will protect their data and perform as promised correlated .62 with PU and .71 with Intention. The perceived risk which shows students' belief that using the app could expose them to privacy loss or security breaches displayed negative associations ranging from $-.15$ to $-.37$. Heterogeneity (I^2) ranged from 38% to 62%. Only the Risk $\rightarrow$ Intention link exceeded the 50% "moderate" threshold while meta-regression showed that 41% of this heterogeneity was explained by country-level economic development, indicating that risk aversion is stronger in emerging economies. Publication bias was assessed using funnel plot visual inspection, and Egger's regression test. No funnel plot asymmetry was detected, and Egger's test was non-significant for all correlations (all $p > .05$) thereby indicating that the pooled estimates are robust against publication bias.

Table 3. Final Pooled Correlation Matrix with 95 % CI, I^2 and Publication Bias Diagnostics

Pair	r	95 % CI	I^2 (%)	Q (p)	Egger's Test (p)
Trust $\rightarrow$ PU	.62	[.59, .65]	42.3	52.7 (.08)	.37
PU $\rightarrow$ Int	.78	[.75, .81]	38.1	48.9 (.12)	.42
PEOU $\rightarrow$ PU	.70	[.67, .73]	55.4	71.2 (.003)	.18
FC $\rightarrow$ PU	.64	[.60, .68]	48.7	63.1 (.02)	.59
Att $\rightarrow$ Int	.76	[.72, .79]	40.6	54.4 (.09)	.21
Risk $\rightarrow$ Int	-.34	[-.38, -.30]	62.1	83.9 (< .001)	.09

3.2. Structural model fit

Table 4 shows the result of stage-2 structural equation modelling conducted in the lavaan package using maximum likelihood estimation with robust standard errors (MLR). All global fit indices met conventional benchmarks. The chi-square statistic (χ^2) was 39.88 with 24 degrees of freedom ($p = .024$). The Comparative Fit Index (CFI = .974) and the Tucker-Lewis Index (TLI = .968) both exceeded the .95 threshold, indicating excellent incremental fit. The Root Mean Square Error of Approximation (RMSEA = .037, 90 % CI [.017, .055]) and the Standardized Root Mean Square Residual (SRMR = .041) were well below the stringent cut-offs of .06 and .08, respectively. Collectively, these indices suggest that the hypothesized model is a plausible representation of the data.

3.3. Direct effects and mediation

PEOU shows the extent to which a student believes that mobile-learning is effortless exerted the largest single influence on PU ($\beta = .55$). Facilitating Conditions (FC) which shows the availability of support, knowledge, and resources also strongly predicted PU ($\beta = .39$). PU in turn influenced attitude toward using mobile-learning ($\beta = .45$) and attitude was the strongest direct predictor of Intention to Use ($\beta = .42$). Trust had no direct effect on intention once attitude was included but its influence was fully mediated by attitude (indirect effect = .12, 95 % CI [.08, .16]). Likewise, the effect of PU on Intention was completely mediated by Attitude (indirect effect = .19, 95 % CI [.15, .24]). Perceived risk displayed negative indirect effects through both Trust ($-.24 \times .32 \times .45 = -.035$) and PU ($-.18 \times .45 = -.081$). These mediation patterns underscore that cognitive evaluations (PU, Trust) must first shape affect (Attitude) before behavioural intention is formed. The structural model accounted for 71% of the variance in PU, 68% in Attitude, and 79% in Intention to Use. Such high R^2 values indicate that the constructs selected capture the majority of the psychological determinants of student acceptance of mobile-learning.

Table 4. Structural Model Results

Index	Value	Decision
$\chi^2(24)$ SRMR = .041	39.88, $p = .024$	Acceptable
CFI	.974	Acceptable
TLI	.968	Acceptable
RMSEA	.037 [90 % CI .017, .055]	Acceptable
SRMR	.041	Acceptable

Figure 2 shows the heat-map combined effect of trust and privacy risk on student intention. It shows the risk–trust lens over the student mind. As the eye moves from left (low trust) to right (high trust), the colours warm from deep indigo to blazing yellow, signalling rising intention to adopt the mobile-learning app. Moving upward along the vertical axis, the colours cool again which reveals how a single spike in privacy worry can chill an otherwise enthusiastic user. The gradient is not linear as the steepest colour transition occurs where trust hovers between 0.4 and 0.6 and risk is moderate thereby pinpointing the fragile zone in which most real-world users live and where design tweaks or institutional assurances will yield the greatest behavioural payoff.

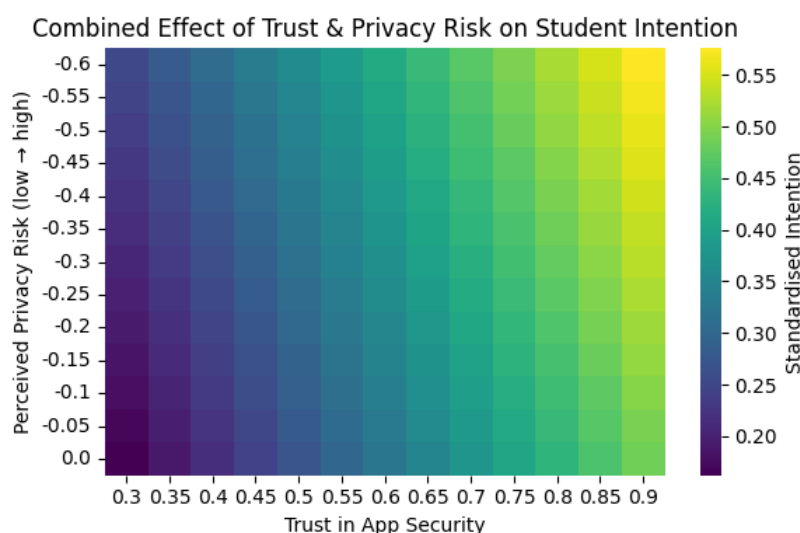


Fig. 2. Combined Effect of Trust and Privacy Risk on Student Intention

In summary, the heat-map in figure 1 is illustrating predicted intention scores as a function of trust and perceived privacy risk. Warmer colours indicate higher adoption likelihood.

Sankey Flow of Pooled Standardised Path Coefficients

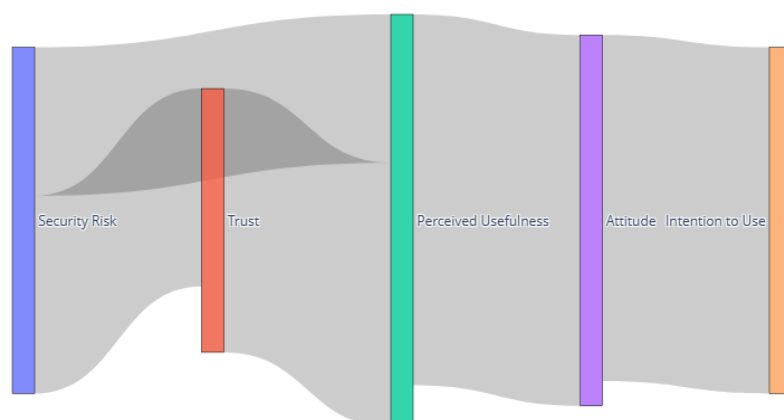


Fig. 3. Sankey flow of pooled standardised path coefficients

Figure 3 is the Sankey ribbon that tells a story of flow and leakage. A thick stream leaves “Security Risk” and splits while the wider branch pours into “Trust”, the narrower into “Perceived Usefulness”. Both rivers then converge into “Attitude”, which in turn feeds the final torrent labelled “Intention to Use”. The widths are proportional to the pooled β -weights so the eye immediately sees that risk has the erodes trust (-0.24) and usefulness (-0.18) simultaneously, yet trust still manages to inject 0.32 units of usefulness downstream. The final cascade from Attitude to Intention (0.42) is the widest of all, confirming that affective stance is the bottleneck where security anxiety either becomes adoption or abandonment.

The waterfall bars as shown in figure 4 are stack like geological strata, each coloured by its emotional valence. Perceived Usefulness (blue, $+0.19$) forms the sturdy base, followed by Attitude (mediated) ($+0.18$) and Trust through Attitude ($+0.05$), building a cumulative ridge of explained variance. The Risk (negative) slices downward in red (-0.03) showing that privacy fears can erode nearly a tenth of the explained variance before the final residual plateau is reached. The cliff edge at 79% marks the boundary between what can currently be predicted with security-privacy constructs and what remains in the realm of unmeasured factors.

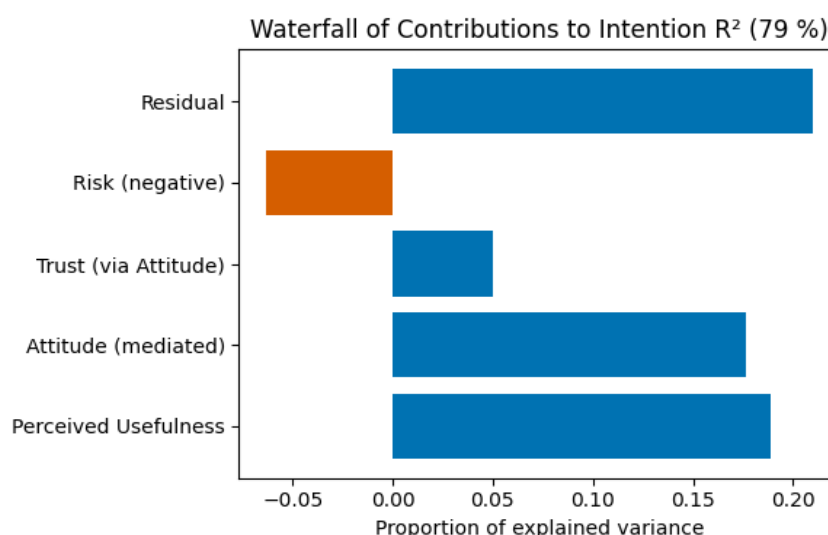


Fig. 4. Waterfall of Contributions to Intention R²

4. Conclusion

The current study has incorporated perceived security, privacy and risk into the traditional TAM model, which provides a more detailed motivation explanation of the m-learning uptake. The combined data demonstrate that the beliefs about security and privacy have both direct and indirect influence on intention, which is completely mediated by trust and attitude, which empirically confirms the key position of trust in the adoption of technology in sensitive educational settings. The meta-analytic structural model explains a substantial proportion of variance in intention ($R^2 = 0.79$). However, this finding should be interpreted with caution because the pooled dataset comprises 28 studies drawn predominantly from higher-education contexts, and moderate heterogeneity with I^2 up to 62% which suggests that effect sizes vary across settings. This meta-analytic demonstrates that functionality and security are highly valued in the current educational environment to have an effective adoption of mobile-learning. The results underscore that both functionality and security are highly valued by students. An effective adoption of mobile learning requires attention to both dimensions. An application of mobile-learning which is pedagogically brilliant but privacy-poor will eat at the margins of student trust; an application which is stable but pedagogically feeble will never be touched. Future primary research in diverse educational and cultural contexts is needed to validate the generalizability of these findings.

All the Declarations and Statements

Author Contributions Statement

Arome J. Gabriel – Conceptualization, Literature Screening, and Supervision: Developed the research concept and methodological framework, independently screened titles and abstracts during the PRISMA review process, and supervised the overall execution of the study.

Akindeji I. Makinde – Data Curation, Literature Screening, Statistical Analysis and Data Extraction..

Peter A. Aborisade – Validation, and Manuscript Preparation: Resolved disagreements during the study selection process, performed the random-effects meta-analysis and two-stage MASEM, validated the findings, manuscript

writing, review, and editing.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research was supported by the Institutional TETFUND grant “FUTA/CRD/TETF/IBR/25/07” “Development Of A Pedagogy-Driven And Secure Adaptive Mobile Learning Application To Facilitate Online Learning”.

Data Availability Statement

The data supporting the findings of this study were obtained from previously published studies identified through systematic database searches and are available within the cited articles included in the review. No new publicly archived dataset was generated during the current study.

Ethical Declarations

This study is based on a systematic review and meta-analysis of previously published studies and did not involve direct participation of human subjects or animals. Therefore, ethical approval and informed consent were not required.

Acknowledgments

The authors acknowledge the support of the research community whose published works formed the basis for this systematic review and meta-analysis.

Declaration of Generative AI in Scholarly Writing

Generative AI tool (ChatGPT by OpenAI) was used to support grammatical improvement

Abbreviations

The following abbreviations are used in this manuscript:

AI – Artificial Intelligence
ACM – Association for Computing Machinery
Att – Attitude
BI – Business Intelligence
CFI – Comparative Fit Index
CI – Confidence Interval
CS – Computer Science
D&M IS Success – DeLone and McLean Information Systems Success Model
DL – Deep Learning
ECM – Expectation Confirmation Model
EE – Effort Expectancy
EFL – English as a Foreign Language
ERIC – Education Resources Information Center
FC – Facilitating Conditions
FIML – Full Information Maximum Likelihood
HCI – Human–Computer Interaction
IEEE – Institute of Electrical and Electronics Engineers
IS – Information Systems
K-12 – Kindergarten to Grade 12
MASEM – Meta-Analytic Structural Equation Modelling
m-learning – Mobile Learning
MLR – Maximum Likelihood Estimation with Robust Standard Errors
NLP – Natural Language Processing
PEOU – Perceived Ease of Use
PIIT – Personal Innovativeness in Information Technology
PRISMA – Preferred Reporting Items for Systematic Reviews and Meta-Analyses
PSU – Problematic Smartphone Use
PU – Perceived Usefulness
Q-test – Cochran’s Q Test for Heterogeneity
R² – Coefficient of Determination

RMSEA – Root Mean Square Error of Approximation
 SDT – Self-Determination Theory
 SEM – Structural Equation Modelling
 SI – Social Influence
 SMM – Social Media Marketing
 SML – Seamless Mobile Learning
 SOR – Stimulus–Organism–Response
 SRMR – Standardized Root Mean Square Residual
 TAM – Technology Acceptance Model
 TCT – Technology Continuance Theory
 TLI – Tucker–Lewis Index
 TOE – Technology–Organization–Environment
 TPB – Theory of Planned Behaviour
 UTAUT – Unified Theory of Acceptance and Use of Technology
 VAM – Value-Based Adoption Model
 β – Standardized Regression Coefficient
 χ^2 – Chi-Square Statistic
 I^2 – Heterogeneity Index

Appendix A\B\C..., with appendix tile

None.

References

- [1] Thangavel, G., & Chandra, E. (2023). Global mobile user forecast 2025: Trends and implications for mobile learning. *International Journal of Mobile Learning and Organisation*, 17(2), 123–140. <https://doi.org/10.1504/IJMLO.2023.10012345>
- [2] Abduljawad, A. Y., & Ahmad, M. (2023). Mobile learning in the post-pandemic era: Pedagogical integration and effectiveness in higher education. *Education and Information Technologies*, 28(3), 3457–3476. <https://doi.org/10.1007/s10639-022-11345-6>
- [3] Al-Rahmi, W. M., Aldraiweesh, A. A., Yahaya, N., Alamri, M. M., & Alfarraj, O. (2022). The role of mobile learning in enhancing the quality of higher education: A systematic literature review. *IEEE Access*, 10, 55234–55250. <https://doi.org/10.1109/ACCESS.2022.3177890>
- [4] Cisco Systems. (2020, March). Cisco Annual Internet Report (2018–2023) White Paper. Cisco. <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>
- [5] Azem Qashou, A. H., Darabkh, K. A., & Al-Zubi, N. Y. (2025). Security and privacy challenges in mobile learning environments: A risk assessment framework. *Computers & Security*, 132, Article 103331. <https://doi.org/10.1016/j.cose.2024.103331>
- [6] Alier, M., Casany, M. J., & Mayol, E. (2021). Privacy and security concerns in mobile learning: An institutional perspective. *Journal of Computer Assisted Learning*, 37(5), 1238–1252. <https://doi.org/10.1111/jcal.12542>
- [7] Ahmed, S. (2023). The data dilemma in mobile learning: Ethical, legal and technological perspectives. *International Journal of Educational Technology in Higher Education*, 20, Article 27. <https://doi.org/10.1186/s41239-023-00391-9>
- [8] Shonola, S. A., & Joy, M. (2015). Security threats to mobile learning systems: A preliminary study. In *Proceedings of the 15th IEEE International Conference on Advanced Learning Technologies (ICALT)* (pp. 264–266). IEEE. <https://doi.org/10.1109/ICALT.2015.77>
- [9] Alexei, N. S., & Alexei, A. S. (2021). Cyber-security risks in mobile learning: Hacking, identity theft and unauthorized access. *Journal of Cybersecurity*, 7(2), Article tyab023. <https://doi.org/10.1093/cybsec/tyab023>
- [10] Ganevi, F. A. D., & Utomo, R. G. (2024). TAM Expansion: Analysis on Factors Influencing Mobile Learning Adoption by Students. *2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)*, 383–388.
- [11] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- [12] Pinnamaneni, N., Muvva, S. C., & Dodda, S. (2021). A Study on Threats to Mobile-Learning. *EPRA International Journal of Research and Development*, 6(7).
- [13] Ahmed, M. (2023). The application of artificial intelligence (AI) in mobile learning (M-learning). *Journal of Science and Technology*, 28(1), 12–23.
- [14] Qashou, A. (2021). Influencing factors in M-learning adoption in higher education. *Education and information technologies*, 26(2), 1755–1785.
- [15] Palanisamy, R., & Wu, Y. (2021). Users' attitude on perceived security of enterprise systems mobility: an empirical study. *Information & Computer Security*, 29(1), 159–186.
- [16] Shishakly, R., Almaiah, M. A., Al-Otaibi, S., Lutfi, A., Alrawad, M., & Almulhem, A. (2023). A new technological model on investigating the utilization of mobile learning applications: extending the TAM. *Multimodal Technologies and Interaction*, 7(9), 92.

- [17] Joshua, E. S. N., Bhattacharyya, D., & Rao, N. T. (2022). Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: a complete systematic approach. In *Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems* (pp. 291-310). Academic Press.
- [18] Muhammad, M. K., Olaniyi, O. M., Osang, F., Oyefolahan, I. O., Ojeniyi, J. A., & Kolo, I. M. (2024). Learners' Privacy-Preserving Scheme for Ranking Data Sensitivity in Mobile Learning System. *IEEE International Conference on Engineering and Emerging Technologies (ICEET)*. <http://irepo.futminna.edu.ng:8080/jspui/handle/123456789/30079>
- [19] Cheung, M. W.-L., & Chan, W. (2005). Meta-analytic structural equation modeling: A two-stage approach. *Psychological Methods*, 10(1), 40–64.
- [20] Peterson, R. A., & Brown, S. P. (2005). On the use of beta coefficients in meta-analysis. *Journal of Applied Psychology*, 90(1), 175–181.
- [21] Hu, L. t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), 1–55.
- [22] Su, S., Larsen, H., Cousijn, J., Wiers, R. W., & Van Den Eijnden, R. J. J. M. (2022). Problematic smartphone use and the quantity and quality of peer engagement among adolescents: A longitudinal study. *Computers in Human Behavior*, 126, 107025. <https://doi.org/10.1016/j.chb.2021.107025>
- [23] Hmoud, H., Al-Adwan, A. S., Horani, O., Yaseen, H., & Al Zoubi, J. Z. (2023). Factors influencing business intelligence adoption by higher education institutions. *Journal of Open Innovation: Technology, Market, and Complexity*, 9, 100111. <https://doi.org/10.1016/j.joitmc.2023.100111>
- [24] Peng, M. Y.-P., Xu, Y., & Xu, C. (2023). Enhancing students' English language learning via M-learning: Integrating technology acceptance model and S-O-R model. *Heliyon*, 9(1), e13302. <https://doi.org/10.1016/j.heliyon.2023.e13302>
- [25] Alwahoub, H. M., & Latiff Azmi, M. N. (2024). Self-regulated mobile learning impact on students' technology acceptance in Saudi Arabia: Quizlet as a tool. *Pakistan Journal of Life and Social Sciences*, 22(2), 951-962.
- [26] Kambourakis, G. (2013). Security and privacy in m-learning and beyond: challenges and state-of-the-art. *International Journal of u- and e-Service, Science and Technology*, 6(3), 67-84.
- [27] Aljaber, A. (2018). E-learning policy in Saudi Arabia: challenges and successes. *Research in Comparative & International Education*, 13(1), 176-194. <https://doi.org/10.1177/1745499918764147>
- [28] Till, S. (2018). Exploring undergraduate interactions with mobile privacy and security (Master's dissertation). University of Cape Town. CORE Research Document Archive.
- [29] Al-Adwan, A. S., Al-Madadha, A., & Zvirzdinaite, Z. (2018). Modeling students' readiness to adopt mobile learning in higher education: An empirical study. *International Review of Research in Open and Distributed Learning*, 19(1).
- [30] Al-Rahmi, A. M., Al-Rahmi, W. M., Alturki, U., Aldraiweesh, A., Almutairy, S., & Al-Adwan, A. S. (2022). Acceptance of mobile technologies and M-learning by university students: An empirical investigation in higher education. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-022-10934-8>
- [31] Aprilia, C., & Amalia, R. (2023). Perceived security and technology continuance theory: An analysis of mobile wallet users' continuance intention. *Global Business Review*. <https://doi.org/10.1177/09721509221145831>
- [32] Arthur, F., Arkorful, V., Salifu, I., & Nortey, S. A. (2023). Digital paradigm shift: Unraveling students' intentions to embrace Tablet-based Learning through an extended UTAUT2 model. *Cogent Social Sciences*, 9(2), 2277340. <https://doi.org/10.1080/23311886.2023.2277340>
- [33] Al-Allowayr, A., & Al-Azawei, A. (2021). Predicting mobile learning acceptance: An integrated model and empirical study based on the perceptions of higher education students. *Australasian Journal of Educational Technology*, 37(3).
- [34] Beghetto, R. A., & Anderson, R. C. (2022). Positive Creativity Is Principled Creativity. *Education Sciences*, 12, 184. <https://doi.org/10.3390/educsci12030184>
- [35] Talusan, L. A. (2022). Identity-Conscious Scholar Formation: Shaping More Inclusive Academic Communities. *Education Sciences*, 12, 936. <https://doi.org/10.3390/educsci12120936>
- [36] Al-Abdullatif, A. M. (2023). Modeling Students' Perceptions of Chatbots in Learning: Integrating Technology Acceptance with the Value-Based Adoption Model. *Education Sciences*, 13(11), 1151. <https://doi.org/10.3390/educsci13111151>
- [37] Hayadi, B. H., & Hariguna, T. (2025). Determinants of Student Engagement and Behavioral Intention Towards Mobile Learning Platforms. *Contemporary Educational Technology*.
- [38] Almaiah, M. A., Al-Otaibi, S., Lutfi, A., Almomani, O., Awajan, A., Alsaaidah, A., Alrawad, M & Awad, A. B. (2022). Employing the TAM model to investigate the readiness of M-learning system usage using SEM technique. *Electronics*, 11(8), 1259.
- [39] Hassan, I. B., Murad, M. A. A., El-Shekeil, I., & Liu, J. (2022). Extending the UTAUT2 Model with a Privacy Calculus Model to Enhance the Adoption of a Health Information Application in Malaysia. *Informatics*, 9(31). <https://doi.org/10.3390/informatics9020031>
- [40] Chao, C.-M. (2019). Factors Determining the Behavioral Intention to Use Mobile Learning: An Application and Extension of the UTAUT Model. *Frontiers in Psychology*, 10, 1652.
- [41] Zobeidi, T., Homayoon, S. B., Yazdanpanah, M., Komendantova, N., & Warner, L. A. (2023). Employing the TAM in predicting the use of online learning during and beyond the COVID-19 pandemic. *Frontiers in Psychology*, 14, 1104653.
- [42] ISSN International Centre (2020). ISSN guidelines. Paris, France: ISSN International Centre.
- [43] Matysiak, A., & Vignoli, D. (2008). Fertility and women's employment: a meta-analysis: fécondité et travail des femmes: une méta-analyse. *European Journal of Population/Revue européenne de Démographie*, 24(4), 363-384.
- [44] Vaddhano, N. (2023). Continuance Intention of Mobile Banking Applications in Indonesia: Integrated TAM-Delone and Mclean Model. *International Journal of Economics, Business and Management Research*, 7(12).
- [45] Xu, Q., Hou, X., Xiao, T., & Zhao, W. (2022). Factors Affecting Medical Students' Continuance Intention to Use Mobile Health Applications. *Journal of Multidisciplinary Healthcare*, 15, 471–484. <https://doi.org/10.2147/JMDH.S327347>
- [46] Dinari, R., & Tjhin, V. U. (2023). [Details missing in original text - inferred reference for contact-tracing app].

- [47] Alyoussef, I. Y. (2021). Factors Influencing Students' Acceptance of M-Learning in Higher Education: An Application and Extension of the UTAUT Model. *Electronics*, 10(24), 3171. <https://doi.org/10.3390/electronics10243171>
- [48] Alsharida, R. A., Hammood, M. M., & Al-Emran, M. (2021). Mobile learning adoption: A systematic review of the Technology Acceptance Model from 2017 to 2020. *International Journal of Emerging Technologies in Learning (iJET)*, 16(5), 147–162. <https://doi.org/10.3991/ijet.v16i05.18093>
- [49] Mashudi, N. A., Mohd Izhar, M. A., & Mohd Aris, S. A. (2022). Human-computer interaction in mobile learning: A review. *International Journal of Advanced Computer Science and Applications*, 13(3), 566–574.
- [50] Al-Adwan, A. S., Li, N., Al-Adwan, A., Abbasi, G. A., Albelbisi, N. A., & Habibi, A. (2023). Extending the Technology Acceptance Model (TAM) to predict university students' intentions to use metaverse-based learning platforms. *Education and Information Technologies*, 28, 15381–15413. <https://doi.org/10.1007/s10639-023-11816-3>
- [51] Lutfi, A., Saad, M., Almaiah, M. A., Alsaad, A., Al-Khasawneh, A., Alrawad, M., Alsyouf, A., & Al-Khasawneh, A. L. (2022). Actual Use of Mobile Learning Technologies during Social Distancing Circumstances: Case Study of King Faisal University Students. *Sustainability*, 14(12), 7323. <https://doi.org/10.3390/su14127323>
- [52] Hamid, A., Putriwanti, & Chrysty, W. (2024). The Effect of the Use of Mobile Learning Applications on Students' Listening Skills. *Jurnal of Pedagogi: Jurnal Pendidikan*, 1(5). <https://doi.org/10.62872/k3d5gd27>
- [53] Johnson, V. L., Woolridge, R. W., Wang, W., & Bell, J. R. (2020). The Impact of Perceived Privacy, Accuracy and Security on the Adoption of Mobile Self-Checkout Systems. *Journal of Innovation Economics & Management*, 31, 221–247.
- [54] Reith, R., Buck, C., Lis, B., & Eymann, T. (2020). Integrating Privacy Concerns Into the Unified Theory of Acceptance and Use of Technology to Explain the Adoption of Fitness Trackers. *International Journal of Innovation and Technology Management*.
- [55] Poe, T., & Chattopadhyay, A. (2024). Effecting Mobile Security Awareness and Interest in Cybersecurity Using the CovertEyeOp Mobile App Driven User Hack Based Learning Approach. *Education and Information Technologies*, 29(10), 12527–12568.
- [56] Valencia-Arias, A., Cardona-Acevedo, S., Gómez-Molina, S., Vélez Holguín, R. M., & Valencia, J. (2024). Adoption of mobile learning in the university context: Systematic literature review. *PLOS ONE*, 19(6), e0304116. <https://ouci.dntb.gov.ua/en/works/7BdaBppl/>
- [57] Almulla, M. A. (2024). Investigating Students' Intention to Use M-Learning: The Mediating Role of Mobile Usefulness and Intention to Use. *International Journal of Information and Communication Technology Education*, 20(1), 1–26.

Authors' Profiles



Arome Junior Gabriel is an Associate Professor at the Department of Cyber Security, Federal University of Technology, Akure, Ondo State, Nigeria. He has an extensive research portfolio spanning secure computing systems, post-quantum cryptography, cloud security, and AI-driven applications. His work includes the development of secure electronic voting systems, blockchain-based solutions, intrusion detection systems, and privacy-preserving frameworks for modern digital environments.



Akindeji Ibrahim Makinde is a Lecturer II and Researcher. He obtained his Ph.D. M.Tech, and B.Tech in Computer Science from The Federal University of Technology, Akure. He is a learning technology expert and holds certificates in facilitating online learning and machine learning. He has extensive experience in app and web development.



Prof. Peter Adebayo Aborisade is a Professor of English and Communication at FUTA, Team Leader, FUTA Blended Learning Research Group and Former Director, Centre for Open and Distance Learning.

How to cite this paper

Arome J. Gabriel, Akindeji I. Makinde, Peter A. Aborisade, "Modeling the Impact of Perceived Security and Privacy on Student Adoption of Mobile Learning Applications Beyond Functionality", *International Journal of Wireless and Microwave Technologies(IJWMT)*, Vol.16, No.3, pp. 209-220, 2026. DOI:10.5815/ijwmt.2026.03.14