

**DJAMEL BENAROUS
HAMOOD M ALENEZI
SAMAR AHMED ELRABBAT
RABEB EL HAMDI**

User experience, customer trust, and epurchase decisions: examining the mediating role of trust in a cybersecurity context in Saudi Arabia

Abstract

Research background and purpose: The rapid expansion of e-commerce in Saudi Arabia has transformed consumer behavior while simultaneously increasing concerns regarding cybersecurity, privacy, and online trust. In this context, user experience (UX) plays a critical role in shaping consumers' perceptions of security and influencing their purchasing behavior. This study aims to examine how cybersecurity awareness and cybersecurity practices affect e-purchase decisions, with particular emphasis on the mediating roles of user experience and customer trust.

Design/methodology/approach: A quantitative design was used, based on a survey of 718 Saudi consumers. SEM and path analysis were conducted to assess direct, indirect, and mediating effects.

Findings: The results indicate that cybersecurity practices have a strong positive effect on both customer trust and e-purchase decisions, while user experience significantly mediates the relationship between security practices and trust. Cybersecurity awareness contributes positively to trust, although its direct impact on purchasing behavior remains relatively limited. The findings highlight the central role of trust as a key mechanism linking cybersecurity and consumer decision-making. No statistically significant gender differences were observed.

Value added and limitations: This study contributes to the literature by providing an integrated framework that links cybersecurity, user experience, and customer trust within an emerging digital market context. It extends prior research by emphasizing the mediating role of UX and trust in shaping e-purchase decisions. However, the study is limited by its cross-sectional design and focus on a single country. Future research could adopt longitudinal approaches, incorporate additional moderating variables, and explore cross-cultural comparisons.

Keywords: *cybersecurity, user experience, customer trust, online purchasing, consumer behavior*

JEL

Classification: C80; D83; L81; M15

Received: 2026-04-04; **Revised:** 2026-05-21; **Accepted:** 2026-06-01

1. Introduction

Recent advancements in digital technologies have significantly reshaped consumer purchasing behavior, leading to an increasing reliance on e-commerce platforms. E-commerce is widely recognized as one of the most transformative developments in the history of commerce, enabling buyers and sellers to conduct transactions without direct physical interaction (Sekar et al., 2022). This digital shift offers numerous advantages, including convenience, accessibility, and efficiency for both consumers and businesses (Rahman & Firdaus, 2024). Despite these benefits, many consumers remain hesitant to engage in online purchasing due to persistent concerns related to cybersecurity, data protection, and privacy risks (Lima & Rezende, 2024; Pilakaew et al., 2024).

Online purchasing is often perceived as a complex activity characterized by uncertainty and risk. In such environments, prior transaction experience and perceived system reliability play an essential role in reducing ambiguity and building consumer confidence. User experience (UX) has therefore emerged as a critical determinant of online purchase decisions (Putri et al., 2024). Beyond its traditional focus on usability and interface design, UX increasingly reflects a broader customer experience (CX) perspective, encompassing emotional, cognitive, and security-related perceptions during online interactions. In the context of e-commerce, UX extends beyond technical usability and human-computer interaction to include service quality, website environment, perceived security, trust, and behavioral intention (Kim & Yum, 2024; Lee et al., 2022). A positive user experience has been shown to enhance purchase intentions, reduce perceived risks, and improve overall satisfaction with online platforms (Lee et al., 2022).

Customer trust represents another fundamental pillar of e-commerce success, particularly given the absence of face-to-face interaction between buyers and sellers. Previous research has identified trust as a key mechanism through which consumers evaluate online vendors and make purchasing decisions (Soleimani, 2022). Trust is influenced by several factors, including website design, reputation, perceived security, and previous experiences. Importantly, trust is not formed in isolation but is strongly shaped by users' experiences with digital interfaces and their perceptions of cybersecurity practices embedded within these environments. In markets where cybersecurity threats are increasingly visible, trust becomes even more critical in shaping consumer behavior.

Saudi Arabia provides a particularly relevant context for examining these relationships. The country has witnessed rapid growth in e-commerce adoption, especially following the COVID-19 pandemic, supported by national digital transformation initiatives. While this expansion has created new opportunities for consumers and businesses, it has also intensified cybersecurity concerns due to the rising incidence of online fraud and data breaches. Examples such as phishing attacks, fake e-commerce websites, and payment interception (e.g. man-in-the-middle attacks) have increased users'

sensitivity to security cues and influenced their online decision-making processes. As a result, Saudi consumers have become increasingly cautious, making it essential to understand how UX and trust influence their online purchasing decisions. Research suggests that user-friendly interfaces and secure digital environments can enhance purchase intentions and alleviate cybersecurity-related concerns (Guo & Cai, 2024; Xue & Jo, 2024).

Despite the growing body of literature on e-commerce, several gaps remain. Existing studies often examine user experience, cybersecurity, or trust in isolation, without fully integrating these constructs into a unified analytical framework. Moreover, limited attention has been given to understanding how cybersecurity awareness and cybersecurity practices jointly influence purchasing behavior through UX and trust, particularly in emerging digital markets such as Saudi Arabia. In addition, prior research has not sufficiently clarified the mechanisms through which UX dimensions—such as ease of use, enjoyment, and perceived security—translate into trust formation and risk reduction. The role of gender in shaping cybersecurity perceptions and online purchasing behavior also remains inconclusive, with prior studies reporting mixed findings across different cultural contexts (Costello et al., n.d.; Nurdiansyah et al., 2023; Pratiwi & Azhar, 2025).

At a time of rapid digital transformation, organizations increasingly rely on online platforms to engage with consumers, making the relationship between cybersecurity, UX, and trust more complex and strategically important. As consumers become more aware of cybersecurity threats, understanding how design features, ease of use, and perceived risk influence trust becomes essential for building sustainable customer relationships (Al-Kfairy et al., 2023). Accordingly, this study adopts an integrated perspective that aligns UX with broader customer experience (CX) considerations while explicitly incorporating cybersecurity dynamics into the analysis. Examining these relationships within the Saudi Arabian context is particularly important, given the country's advanced cybersecurity initiatives and its position as a leading digital economy in the region.

Accordingly, this study addresses the following research question: *How do user experience and customer trust mediate the relationship between cybersecurity awareness, cybersecurity practices, and e-purchase decisions in Saudi Arabia, and does gender moderate these relationships?*

By addressing this gap, the study contributes to both theory and practice by offering an integrated model that explains how cybersecurity-related factors interact with UX and trust to shape consumer purchasing decisions. The findings are expected to provide valuable insights for researchers, e-commerce managers, and policymakers seeking to enhance secure, trustworthy, and user-friendly digital marketplaces.

2. Literature review

In today's digital shopping environment, understanding how user experience, customer trust, and gender interact is essential for explaining online purchasing behavior, particularly in relation to cybersecurity. The rapid expansion of e-commerce in Saudi Arabia—driven by digital disruption and societal transformation—highlights the need for a coherent framework that captures how these factors jointly influence consumer decisions. Research consistently demonstrates that improving UX enhances engagement, loyalty, and trust, especially amid growing cybersecurity concerns. A positive UX, characterized by intuitive design, smooth navigation, and personalized services, significantly boosts trust and purchase intentions (Saoula et al., 2023; Endarwati et al., 2024; Wang & Emurian, 2005). From a broader perspective, these effects align with Customer Experience (CX) frameworks, where UX represents a key touchpoint shaping consumers' overall journey, including perceptions of security and reliability. Furthermore, gender-based differences in online behavior and security perception reveal diverse patterns of trust and risk evaluation (Kanwal et al., 2022; Midha, 2012).

Current literature shows that UX design elements play a crucial role in influencing perceived cybersecurity. Visual design, navigation clarity, and overall usability strongly shape users' feelings of safety and platform credibility. Gender-specific responses also emerge, as men and women may differ in risk sensitivity and security awareness (Kanwal et al., 2022; Garbarino & Strahilevitz, 2004). In addition, specific UX components such as ease of use, perceived enjoyment, and interface transparency contribute directly to reducing perceived risk and enhancing trust formation in digital environments. Despite these insights, considerable gaps remain regarding how these elements interact within the Saudi context. Much existing research is based on Western settings, which do not fully reflect the cultural and social dynamics of Saudi Arabia. There is therefore a need for region-specific studies examining how gender norms and cultural expectations shape trust and online shopping behavior. Additionally, international increases in cybersecurity breaches highlight the need for integrated analyses combining UX and cybersecurity within regional e-commerce. Addressing these gaps is essential for developing UX strategies that support gender-sensitive trust and promote secure.

Cybersecurity awareness plays a central role in shaping online purchase decisions by influencing customer confidence. Awareness of information security—especially regarding digital certificates—significantly contributes to trust and purchasing behavior (Sari & Prasetyo, 2018; Iskanto & Gunawan, 2023). Trust, alongside perceived benefits and brand image, has a strong positive impact on purchase intentions and decisions (Komalasari et al., 2021; Rita & Guinardi, 2023). Greater awareness enhances comfort in virtual environments, fostering electronic trust

essential for successful e-commerce (Najafi, 2012; Rahman & Firdaus, 2024). Website trust, shaped by reputation and consumer familiarity, also plays a direct role in influencing purchase intentions (Yoon, 2002; Midha, 2012). Prior satisfaction and experience similarly strengthen trust (Garbarino & Strahilevitz, 2004; Hsiao et al., 2010).

Moreover, cybersecurity awareness helps users recognize potential threats such as phishing attempts, fake e-commerce websites, and insecure payment environments, which in turn influences their perception of risk and their willingness to engage in online transactions. This awareness indirectly supports purchasing decisions by reinforcing trust in platforms that demonstrate credible security signals.

H1. The level of cybersecurity awareness positively influences the purchase decision through customer confidence.

User interface (UI) and UX design significantly influence perceived security and purchase decisions. Effective UI elements-such as functional links, demos, and intuitive navigation-enhance perceived safety and increase trust (Kamoun & Halaweh, 2012). Visual presentation strongly predicts perceived security, with purchasing willingness closely linked to perceived safety (Turner, 2002; Halaweh, 2012). Empirical evidence shows UI affects purchase decisions more strongly (58.6%) than UX (41.4%) (Sawal, 2023). Nevertheless, UX components such as visual clarity, navigation comfort, and security cues also shape customer perceptions (Davidavičienė et al., 2020; Stângaciu et al., 2024). Importantly, cybersecurity practices-such as secure authentication mechanisms, encryption, and safe browsing behaviors-enhance user experience by reducing uncertainty and providing a sense of control and safety during online interactions. These practices contribute to smoother user journeys, which are central to both UX and overall customer experience (CX).

H2. Cybersecurity practices positively impact purchase decisions through user experience.

UX plays a critical role in strengthening customer trust. Although UX may not hinder the adoption of mobile cybersecurity applications (Williams, 2022; Shin, 2013), positive UX-through enjoyment, control, and ease of use-significantly enhances trust (Koufaris, 2002; Hampton-Sosa & Koufaris, 2005). Integrating security systems with CRM can further enhance trust by reducing risk (Kim, 2010). Increased cybersecurity knowledge also lowers perceived risks and improves user behavior (El Haddad et al., 2018; Saoula et al., 2023). In particular, UX dimensions such as perceived ease of use and enjoyment influence cognitive and emotional responses, which subsequently shape trust formation by reducing perceived uncertainty and enhancing confidence in the platform.

H3: User experience mediates the relationship between cybersecurity practices and customer trust.

Customer trust is a well-established mediator in online purchasing behavior. Trust mediates the impact of website security, convenience, and design on purchasing outcomes (Hayuningtyas & Widiyanto, 2015). Online customer reviews and ratings influence trust and thereby affect purchase decisions (Novela et al., 2023). Ease of use, information quality, and perceived security also shape trust, which subsequently increases purchase intentions (Utami & Usman, 2021). Trust plays a particularly strong role in e-marketplaces such as food and snack platforms (Novela et al., 2023). However, prior research also indicates that trust can be fragile and highly sensitive to negative cybersecurity incidents, such as data breaches or fraudulent transactions, which may rapidly erode previously established confidence. This highlights the importance of considering both positive and negative scenarios in understanding trust dynamics.

H4: Customer trust mediates the relationship between cybersecurity practices and purchase decisions.

Security behavior among males (McGill & Thompson, 2018; Ifinedo, 2018; Alotaibi & Alshehri, 2020), whereas others show females exhibiting higher awareness (Daengsi et al., 2022). Gender also moderates elements such as security self-efficacy, technological experience, and learning preferences (Anwar et al., 2017). These findings suggest tailoring cybersecurity education to different gender needs (McGill & Thompson, 2018). Notably, age did not significantly affect awareness in some contexts (Daengsi et al., 2022). However, within integrated UX and CX frameworks, gender differences are often embedded within user profiles or personas, suggesting that their influence may be indirect and context-dependent rather than structurally central to the model.

H5: Cybersecurity awareness effects on trust vary by gender.

H6: Cybersecurity practices effects on trust vary by gender.

3. Materials and methods

This study follows a quantitative analytical design that aims to explore the impact of cybersecurity awareness and security practices on the e-purchase decision in e-commerce. Through user experience and customer trust, this design focuses on analyzing the relationship between different variables to understand how they affect the purchase decision, in addition to knowing the existence of differences in the

variables through the gender variable. More specifically, the proposed research model examines both direct and indirect relationships between cybersecurity-related factors (awareness and practices) and e-purchase decisions, while explicitly incorporating user experience (UEX) and customer trust (CTR) as mediating mechanisms that explain how these effects occur. To find out, a study model was designed to clarify the relationship between the variables, the terms of which were abbreviated as follows (Figure 1): cybersecurity awareness (AOC), cybersecurity practices (SPC), user experience (UEX), customer trust (CTR), gender (GDR), and electronic purchase decision (E-PD).

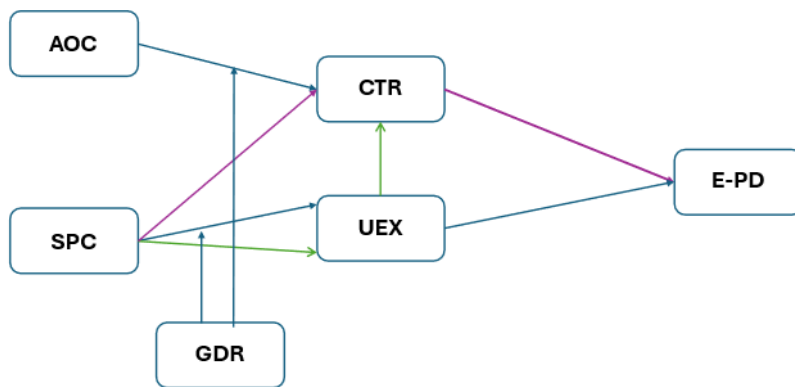


Figure 1. Study structure design

Source: prepared by reseachers

In this model, cybersecurity practices are expected to directly influence both user experience and customer trust, while user experience further contributes to building trust, which ultimately drives e-purchase decisions. This structure reflects an integrated UX–trust pathway consistent with customer experience (CX) perspectives.

Gender (GDR) was included as a grouping variable to examine potential differences between male and female respondents in cybersecurity perceptions and behaviors, rather than as a core structural component influencing the causal relationships.

Sampling plays a fundamental role in ensuring reliable and generalizable research outcomes. In this study, a total of 718 Saudi consumers participated, selected through a random sampling technique to enhance representativeness and reduce sampling bias, in line with methodological recommendations (Thompson, 2012; Creswell & Creswell, 2017). The sample size was calculated using standard social-science formulas based on a 95% confidence level and a 5% margin of error, ensuring robust statistical

significance (Fowler, 2013; Israel, 1992). This relatively large sample size also strengthens the robustness of SEM analysis and allows for reliable examination of mediation effects across the proposed model.

Data were collected using a structured electronic questionnaire consisting of 28 items measured on a five-point Likert scale. The instrument captured the main constructs of the study: AOC, SPC, UEX, CTR, GDR, and E-PD. Questionnaire development followed systematic methodological steps, beginning with an extensive review of prior research to identify relevant constructs, including studies addressing cybersecurity, trust, and online purchasing behaviors (Cerdeira, 2021; Carreón Guillén et al., 2015). Each construct was operationalized through multiple indicators reflecting its underlying dimensions; for example, user experience (UEX) includes aspects such as ease of use, navigation clarity, and perceived enjoyment, while customer trust (CTR) reflects perceptions of reliability, security, and confidence in the platform.

To ensure clarity and content validity, the questionnaire was reviewed by subject-matter experts. A pilot test on a small participant group provided additional feedback for refinement. Reliability testing using Cronbach's alpha yielded a value of 0.937, indicating excellent internal consistency and surpassing the commonly accepted threshold of 0.70 (Kiliç, 2016). The questionnaire was distributed via email and social media platforms, allowing broad and diverse participation across demographic groups.

Structural Equation Modeling (SEM) was employed to test the hypothesized direct and indirect relationships. SEM was applied to evaluate the measurement model, verify construct validity, and explore the causal structure among latent variables. Path analysis provided insight into the strength and direction of specific relationships, particularly those involving mediation mechanisms. These methods are particularly suitable for examining complex relationships involving mediating variables such as user experience and trust within a unified analytical framework.

Several limitations should be acknowledged. First, cultural factors specific to Saudi Arabia may influence participant responses, which may limit the generalizability of the findings to other regions. Second, reliance on self-reported data introduces the possibility of response bias. Third, while the model captures key relationships between cybersecurity, UX, and trust, it does not fully account for potential external disruptions such as major cybersecurity incidents or platform failures, which may significantly alter user trust and behavior. Despite these limitations, the study offers meaningful insights into cybersecurity-related consumer behavior within the rapidly evolving Saudi e-commerce context.

4. Data analysis and results

4.1. Descriptive statistics

The Table 1 presents the ratios and frequencies of gender among the respondents in the study, with a total sample size of 718 individuals. Among these, 409 respondents identified as male, which represents approximately 57% of the total sample. Conversely, 309 respondents identified as female, accounting for about 43%. This distribution may reflect the gender gap in Internet and e-commerce usage in Saudi Arabia. However, it should be noted that this percentage may be affected by other factors such as the nature of the study or the method of data collection.

Table 1. Ratios and frequencies

Variable	Level	Counts	Total	Proportion
gender	male	409	718	0.570
	female	309	718	0.430

Source: JASP outputs

Table 2 presents the descriptive statistics for the study variables and reflects generally positive perceptions among Saudi consumers regarding cybersecurity, user experience, trust, and online purchasing. Mean values were relatively high across constructs-AOC (3.885), SPC (4.196), UEX (4.377), CTR (4.312), and E-PD (4.300)-indicating strong awareness of online risks, active adoption of secure practices, and favorable experiences with e-commerce platforms. The relatively low standard deviations suggest consistent responses among participants, reinforcing the importance of these variables in shaping e-purchase decisions.

Table 2. Descriptive statistics

	AOC	SPC	UEX	CTR	EDP
Valid	718	718	718	718	718
Missing	617	617	617	617	617
Mean	3.885	4.196	4.377	4.312	4.300
Std. Deviation	0.793	0.727	0.774	0.690	0.772
Minimum	1.000	1.000	1.750	1.000	1.000
Maximum	5.000	5.000	5.000	5.000	5.000

Source: JASP outputs

4.2. Confirmatory factor analysis

Table 3 reports the factor loadings for all indicators associated with the five latent constructs: AOC, SPC, UEX, CTR, and E-PD. All indicators loaded strongly and significantly ($p < .001$) onto their corresponding constructs, confirming the adequacy of the measurement model. The loadings across constructs demonstrate high convergent validity, indicating that each set of indicators reliably captures its intended dimension. These results affirm the structural soundness of the model and support proceeding with further SEM analysis. Each indicator represents a specific aspect of its corresponding latent construct. For instance, cybersecurity awareness (AOC) items reflect users' knowledge of online risks and their ability to recognize secure digital environments. Cybersecurity practices (SPC) indicators capture actual user behaviors such as adopting secure passwords, verifying website authenticity, and using safe payment methods.

User experience (UEX) indicators correspond to perceived ease of use, navigation clarity, and overall interaction enjoyment, which are essential components influencing consumer perceptions during online transactions. Customer trust (CTR) indicators measure users' confidence in the platform's reliability, security, and integrity, while e-purchase decision (E-PD) items reflect the likelihood and intention of completing online purchases.

The clear and consistent loadings of these indicators confirm that the measurement model adequately reflects the theoretical relationships between cybersecurity, user experience, trust, and purchasing behavior.

For cybersecurity awareness (AOC), the indicators (A1–A6) reflect users' ability to recognize online risks and identify secure environments. The higher loadings for A2, A3, and A4 indicate that risk recognition is the most dominant aspect of awareness among respondents.

For cybersecurity practices (SPC), the indicators (B1–B7) capture actual protective behaviors such as password security and verification of websites. The consistently strong loadings show that respondents actively adopt secure practices, with B4, B6, and B7 having slightly stronger influence.

For user experience (UEX), the indicators (C1–C4) represent ease of use and navigation quality. The higher loadings of C2 and C3 suggest that usability and smooth interaction are the most influential components of user experience.

Customer trust (CTR), measured by indicators (D1–D6), reflects confidence in platform reliability and security. The strong and consistent loadings indicate that trust is mainly driven by perceived credibility, with D3 and D6 showing relatively stronger effects.

Finally, e-purchase decision (EPD) indicators (W1–W5) represent consumers' intention to complete online transactions. The consistent loadings across these indicators confirm

that purchasing behavior is well captured, with W2 and W3 contributing slightly more strongly.

Overall, these results confirm that each construct is well represented by its indicators, reinforcing the validity and strength of the measurement model.

Table 3. **Factor loadings**

Factor	Indicator	Estimate	Std. error	z-value	p	95% Confidence interval	
						Lower	Upper
AOC	A1	1.000	0.000			1.000	1.000
	A2	1.467	0.140	10.505	< .001	1.193	1.740
	A3	1.662	0.185	10.615	< .001	1.600	2.324
	A4	1.709	0.159	10.773	< .001	1.398	2.020
	A5	1.384	0.145	9.558	< .001	1.100	1.667
	A6	1.117	0.119	9.417	< .001	0.885	1.349
SPC	B1	1.000	0.000			1.000	1.000
	B2	1.135	0.089	12.812	< .001	0.962	1.309
	B3	1.066	0.075	14.305	< .001	0.920	1.212
	B4	1.175	0.077	15.254	< .001	1.024	1.326
	B5	1.112	0.091	12.215	< .001	0.934	1.291
	B6	1.190	0.085	14.024	< .001	1.024	1.357
	B7	1.173	0.080	14.635	< .001	1.016	1.331
UEX	C1	1.000	0.000			1.000	1.000
	C2	1.300	0.083	15.674	< .001	1.138	1.463
	C3	1.157	0.068	17.039	< .001	1.024	1.290
	C4	0.994	0.059	16.738	< .001	0.878	1.111

CTR	D1	1.000	0.000			1.000	1.000
	D2	0.994	0.063	15.704	< .001	0.870	1.118
	D3	1.158	0.065	17.702	< .001	1.030	1.286
	D4	1.123	0.066	16.999	< .001	0.994	1.253
	D5	0.976	0.058	16.959	< .001	0.863	1.089
	D6	1.203	0.085	14.145	< .001	1.037	1.370
EPD	W1	1.000	0.000			1.000	1.000
	W2	1.042	0.043	24.001	< .001	0.957	1.127
	W3	1.072	0.046	23.468	< .001	0.982	1.161
	W4	0.972	0.041	23.630	< .001	0.891	1.052
	W5	0.886	0.047	18.737	< .001	0.793	0.978

Source: JASP outputs

To visually illustrate the measurement model, Figure 1 presents the confirmatory factor analysis structure generated using JASP.

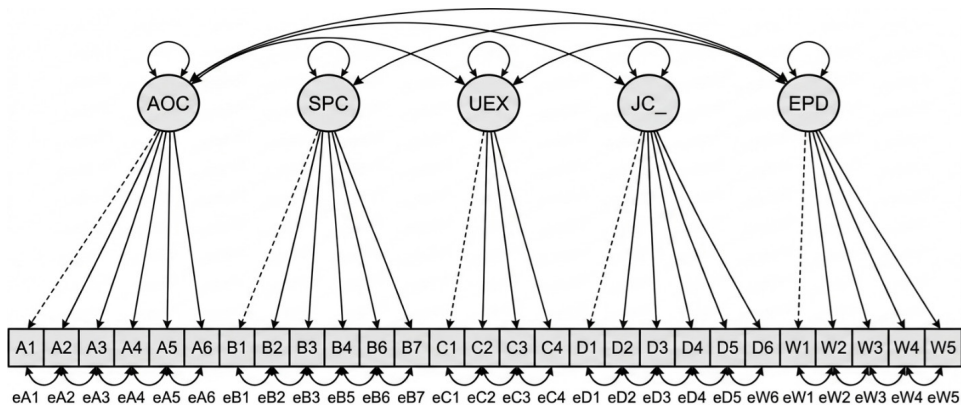


Figure 2: Model plot-factor analysis confirmatory

Source: JASP outputs

4.3. Testing mediation hypotheses H1, H2, H3, H4

Table 4 presents the covariances among the latent constructs of the study. All relationships were positive and statistically significant ($p < .001$), indicating strong interconnections between the variables. The covariance between AOC and SPC reflects a moderate positive association, while the covariance between SPC and UEX (0.290) and between SPC and CTR (0.272) demonstrates the central role of security practices in shaping both user experience and trust. The strongest covariance was observed between CTR and E-PD (0.361), highlighting trust as a key driver of purchasing decisions. These consistent correlations support the theoretical assumptions underlying the structural model and justify proceeding to path analysis.

Table 4. **Factor covariances**

			Estimate	Std. error	z-value	p	95% Confidence interval	
							Lower	Upper
AOC	—	SPC	0.173	0.022	7.729	< .001	0.129	0.217
AOC	—	UEX	0.146	0.020	7.177	< .001	0.106	0.185
AOC	—	CTR	0.153	0.020	7.637	< .001	0.114	0.192
AOC	—	EPD	0.161	0.022	7.320	< .001	0.118	0.204
SPC	—	UEX	0.290	0.029	10.060	< .001	0.233	0.346
SPC	—	CTR	0.272	0.026	10.320	< .001	0.221	0.324
SPC	—	EPD	0.348	0.031	11.053	< .001	0.286	0.410
UEX	—	CTR	0.327	0.029	11.158	< .001	0.270	0.384
UEX	—	EPD	0.289	0.028	10.400	< .001	0.235	0.344
CTR	—	EPD	0.361	0.030	12.131	< .001	0.303	0.419

Source: JASP outputs

To supplement these results, Figure 2 illustrates the covariance structure of the measurement model as generated by JASP.

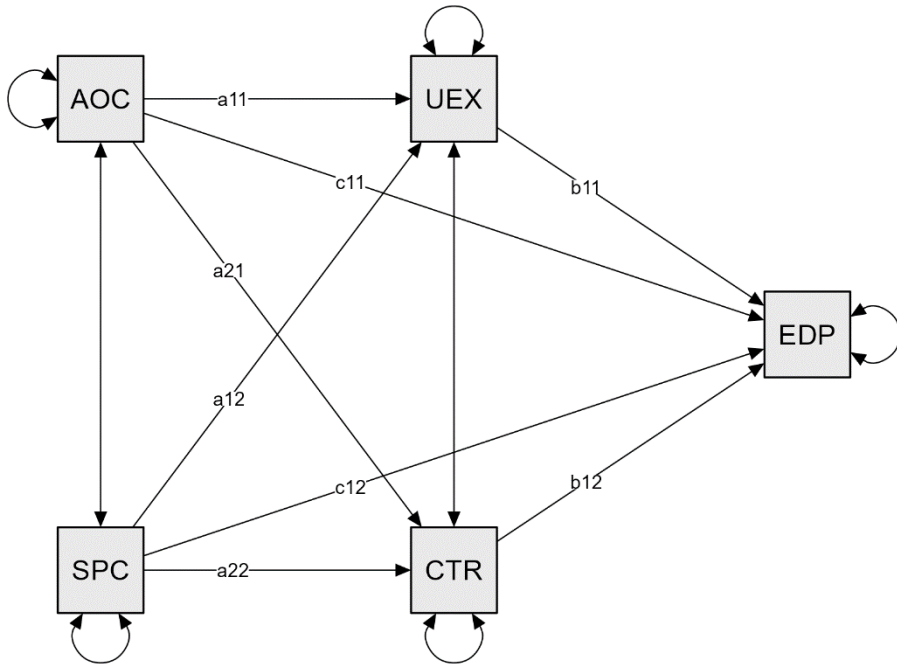


Figure 3. **Model plot-path analysis**

Source: JASP outputs

Table 5 presents the standardized direct effects among the study variables. The results show that cybersecurity awareness (AOC) has a positive but modest direct effect on e-purchase decisions (E-PD), indicating that awareness contributes to purchasing behavior, although its influence remains limited compared to other constructs.

This finding suggests that while awareness of cybersecurity risks is important, it does not necessarily translate directly into purchasing behavior unless it is supported by stronger experiential or trust-related factors. In contrast, cybersecurity practices (SPC) demonstrate a stronger and highly significant effect on both E-PD and customer trust (CTR), confirming their central role in shaping secure and confident online behavior. SPC also shows a particularly notable direct impact on CTR, reinforcing the importance of visible and reliable security measures in developing trust. This result highlights that actual protective behaviors—such as using secure payment methods or verifying platform credibility—play a more influential role in shaping consumer decisions than awareness alone. These direct relationships provide foundational support for the subsequent mediation analysis. Overall, the findings indicate that

cybersecurity practices represent a key operational driver of both trust and purchasing decisions within the proposed model.

Table 5. **Direct effects**

			Std. estimate	Std. error	z-value	p	95% Confidence interval	
							Lower	Upper
AOC	→	EDP	0.263	0.237	1.701	< .001	0.135	0.210
SPC	→	EDP	0.370	0.089	4.158	< .001	0.193	0.530
SPC	→	CTR	0.410	0.042	9.664	< .001	0.327	0.493

Source: JASP outputs

Table 6 presents the standardized path coefficients that clarify the direct effects between the latent variables in the structural model. The results indicate that customer trust (CTR) exerts the strongest direct influence on e-purchase decisions (E-PD), confirming its essential role in guiding consumers' final purchasing behavior. Trust appears to function as the central mechanism through which users evaluate platform reliability and decide whether to proceed with online transactions. This strong effect highlights that trust represents the most critical determinant in the decision-making process, acting as the final gateway between user perceptions and actual purchasing behavior.

Table 6. **Path coefficients**

			Std. estimate	Std. error	z-value	p	95% Confidence interval	
							Lower	Upper
UEX	→	EDP	0.102	0.048	2.118	0.024	0.002	0.193
CTR	→	EDP	0.589	0.054	10.878	< .001	0.477	0.691
AOC	→	EDP	0.063	0.037	1.701	< .001	0.010	0.135
SPC	→	EDP	0.370	0.089	4.158	< .001	0.193	0.530
AOC	→	UEX	0.084	0.059	1.418	< .001	0.028	0.204
SPC	→	UEX	0.558	0.061	9.127	< .001	0.442	0.680
AOC	→	CTR	0.146	0.049	2.992	0.003	0.050	0.244
SPC	→	CTR	0.604	0.048	12.650	< .001	0.515	0.692
UEX	→	CTR	0.461	0.037	12.590	< .001	0.394	0.531

Source: JASP outputs

Furthermore, cybersecurity practices (SPC) demonstrate consistently strong and significant effects on both user experience (UEX) and customer trust (CTR). These findings highlight that visible and well-structured security practices-such as secure login processes, reliable payment systems, and transparent data-handling procedures-substantially enhance how users perceive the platform and how confidently they interact with it. SPC also contributes directly to E-PD, reinforcing that secure environment help reduce hesitation and increase consumers' willingness to complete online purchases. These results suggest that cybersecurity practices not only influence trust directly but also shape the experiential dimension of online interaction, which further strengthens trust formation.

In comparison, cybersecurity awareness (AOC) shows smaller yet meaningful positive effects on UEX, CTR, and E-PD. Although its direct influence on purchase decisions is less pronounced than that of SPC, awareness still plays a role by shaping consumers' understanding of risks and contributing indirectly to trust and perceived system quality. This indicates that awareness alone is insufficient to drive behavior but becomes more effective when translated into actual security practices and positive user experiences.

Overall, the path coefficients illustrate that a combination of strong cybersecurity practices, positive user experiences, and high customer trust forms the most influential pathway driving e-purchase decisions. In particular, the sequential relationship (SPC → UEX → CTR → E-PD) reflects a coherent process where secure practices enhance user experience, which in turn builds trust and ultimately leads to purchasing decisions.

Table 7 presents the main model fit indices, including the Comparative Fit Index (CFI) and the Root Mean Square Error of Approximation (RMSEA). The results indicate that the model demonstrates a strong overall fit. The CFI value of 0.947 exceeds the commonly accepted threshold for good model fit, while the RMSEA value of 0.036 falls well within the range indicating a close and acceptable fit. Together, these indices confirm that the proposed measurement and structural model adequately represent the observed data and support proceeding with the analysis of indirect effects and mediation pathways.

Table 7. T-size fit indices

	CFI	RMSEA
Estimate	0.947	0.036
Poor-fair limit	0.893	0.058
Fair-close limit	0.938	0.055

Note: T-size statistics are computed for $\alpha = 0.05$.

Source: JASP outputs

Figure 4 presents the structural equation model illustrating the final configuration of the relationships among the study's latent variables (AOC, SPC, UEX, CTR, and E-PD). The diagram shows the strength and direction of the standardized paths, highlighting the prominent influence of cybersecurity practices on both user experience and customer trust, as well as the central role of trust in predicting e-purchase decisions. The SEM structure visually confirms the empirical results reported in the path coefficient tables and demonstrates the coherence and adequacy of the proposed theoretical model.

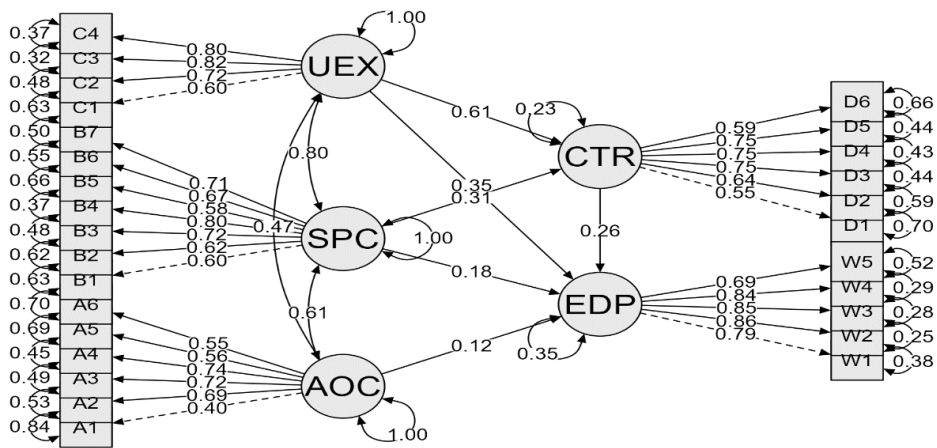


Figure 4. Model plot-structural equation modeling

Source: JASP outputs

Table 8 presents the indirect effects in the model, showing each hypothesis as the indirect effects:

H1: AOC → CTR → EDP (the effect of cybersecurity awareness on e-purchase decisions through customer trust): The standardized indirect effect is 0.086, which is statistically significant ($p < .001$). This supports H1, which means that cybersecurity awareness (AOC) has a positive indirect effect on e-purchase decisions (EDP) through increased customer trust (CTR). In simpler terms, increased cybersecurity awareness makes consumers trust online sellers more, which in turn makes them more likely to buy online.

- H2: $SPC \rightarrow UEX \rightarrow EDP$ (the effect of cybersecurity practices on e-purchase decisions through user experience): The standardized indirect effect is 0.057, which is statistically significant ($p < .001$). This supports H2, which means that cybersecurity practices (SPC) have a positive indirect effect on EDP through improved user experience (UEX). Consumers who engage in safer online practices tend to have a better experience, making them more likely to make online purchases.
- H3: $SPC \rightarrow UEX \rightarrow CTR$ (Cybersecurity practices influence customer trust through user experience): The standardized indirect effect is 0.280, which is statistically significant ($p < .001$). This supports H3, which means that cybersecurity practices (SPC) have a positive indirect effect on customer trust (CTR) through improved user experience (UEX). When consumers feel safe and have a good online experience (due to their security practices), they are more likely to trust online sellers.
- H4: $SPC \rightarrow CTR \rightarrow EDP$ (Cybersecurity practices influence online purchasing decisions through customer trust): The standardized indirect effect is 0.356, which is statistically significant ($p < .001$). This supports H4, which means that cybersecurity practices (SPC) have a positive indirect effect on EDP through increasing customer trust (CTR). Engaging in safe online practices builds trust, and trust, in turn, encourages online purchases.

All four hypothesized indirect effects are statistically significant, supporting the proposed mediating roles of user experience (UEX) and customer trust (CTR). The strongest indirect effect is between SPC and EDP through CTR (H4), indicating that the effect of safe online practices on purchasing decisions is largely mediated by trust. The indirect effect of SPC on CTR through UEX (H3) is also significant, highlighting the importance of user experience in building trust. The indirect effects of AOC and SPC on EDP through UEX and CTR, respectively (H1 and H2), are smaller but still statistically significant.

Table 8. Indirect effects

Hypothesis						Std. estimate	Std. error	z-value	p	95% Confidence interval	
										Lower	Upper decision
H1	AOC	$\rightarrow$	CTR	$\rightarrow$	EDP	0.086	0.026	3.368	< .001	0.033	0.133 Accepted
H2	SPC	$\rightarrow$	UEX	$\rightarrow$	EDP	0.057	0.026	2.224	< .001	0.105	0.203 Accepted
H3	SPC	$\rightarrow$	UEX	$\rightarrow$	CTR	0.280	0.022	12.576	< .001	0.241	0.043 Accepted
H4	SPC	$\rightarrow$	CTR	$\rightarrow$	EDP	0.356	0.054	6.543	< .001	0.261	0.467 Accepted

Source: JASP outputs

4.4. Testing hypotheses of differences by gender H5, H6

Table 9 presents the results of the independent samples t-tests conducted to examine potential gender differences in cybersecurity awareness (AOC) and cybersecurity practices (SPC). The findings show no statistically significant differences between males and females in either construct, as indicated by the high p-values associated with both variables. Effect sizes were also minimal, suggesting that even if minor differences existed, they would not be practically meaningful. These results imply that, within this sample, men and women exhibit comparable levels of cybersecurity awareness and similar engagement in secure online practices, reflecting a generally uniform pattern of cybersecurity behavior across genders.

Table 9. Independent samples T-Test

df	p	VS-MPR*	Cohen's d	SE Cohen's d
716	0.817	1.000	0.017	0.075
716	0.722	1.000	0.027	0.075

Source: JASP outputs

5. Discussions

This study investigated the relationships between cybersecurity awareness (AOC), cybersecurity practices (SPC), user experience (UEX), customer trust (CTR), and electronic purchasing decisions (EDP) among Saudi Arabian consumers, with a particular focus on the mediating roles of user experience and customer trust, and the moderating role of gender.

The purpose of this study was to examine the relationships between cybersecurity awareness (AOC), cybersecurity practices (SPC), user experience (UEX), customer trust (CTR), and electronic purchasing decisions (EDP) among Saudi Arabian consumers. The findings provide strong empirical support for the proposed model and highlight the central role of trust and user experience in shaping online purchasing behavior. The results confirm that cybersecurity awareness indirectly affects purchasing decisions through trust, consistent with previous evidence showing that online customer reviews and positive digital engagement significantly enhance trust and influence purchase intentions (Fadhilah et al., 2021; Fahrozi et al., 2022; Lathifah et al., 2024). Trust is a critical mediator in online shopping, and prior studies repeatedly emphasize its importance in translating online cues into behavioral outcomes (Alena & Hasanah, 2023; Lăzăroiu et

al., 2020; Tahir & Khan, 2020). The present findings align with this body of literature, supporting the notion that cybersecurity awareness enhances consumers' confidence, which subsequently increases their likelihood of purchasing online. However, the relatively weaker direct impact of cybersecurity awareness suggests that awareness alone may not be sufficient to drive actual purchasing behavior unless it is supported by positive experiences and strong trust in the platform.

In real-world digital environments, users may be aware of cybersecurity risks such as phishing attacks or fake e-commerce websites, yet still engage in online transactions based on their level of trust in a specific platform. This indicates that awareness contributes to cognitive risk evaluation, but trust remains the decisive factor translating perception into action.

The second hypothesis (H2) explored the indirect effect of cybersecurity practices (SPC) on e-purchase decisions (EDP) through user experience (UEX). The results confirmed that SPC has a significant indirect impact on purchasing behavior by improving user experience. This finding is consistent with prior studies showing that UX strongly shapes security perceptions, online behavior, and purchase intentions. For example, Furnell et al. (2019) demonstrated that guidance and supportive interface design enhance password selection and general security behavior, while El Haddad et al. (2018) found that cybersecurity knowledge reduces perceived online risks and improves shopping attitudes. Additionally, enhanced security features-such as end-to-end encryption and multi-factor authentication-have been shown to increase consumers' trust in digital platforms and subsequently improve overall UX (Sharma, 2024). Programs aimed at raising cybersecurity awareness also strengthen user compliance and interaction quality (Butler, 2014; Howell, 2021).

Collectively, these findings suggest that when users encounter secure, intuitive, and reliable digital environments, their experience improves, leading to greater confidence and a higher likelihood of completing online purchases. At the same time, cybersecurity practices contribute to reducing perceived uncertainty during online interactions, which enhances users' sense of control and comfort while navigating digital platforms. This reinforces the role of UX as a key experiential mechanism linking security practices to behavioral outcomes. However, the literature also cautions that overly complex security measures may create frustration and reduce ease of use, emphasizing the importance of balancing strong security with seamless UX. The current study supports this balanced approach, showing that SPC contributes to EDP primarily through its positive effect on UEX, thus confirming H2. This result highlights an important practical implication: effective cybersecurity should not only focus on technical robustness but also on usability, as poor design may undermine the positive effects of even the most advanced security systems.

The third hypothesis (H3) examined the mediating role of user experience (UEX) in the relationship between cybersecurity practices (SPC) and customer trust (CTR).

The results confirmed a strong and significant indirect effect, indicating that secure and well-designed digital environments foster positive user experiences, which in turn enhance trust. These findings are consistent with earlier research showing that intuitive and enjoyable website interactions contribute to higher trust levels by improving perceptions of usefulness, ease of use, and overall satisfaction (Koufaris, 2002; Hampton-Sosa & Koufaris, 2005).

Studies have also emphasized that integrating security mechanisms into customer relationship management (CRM) systems strengthens trust by reducing perceived risks and increasing transparency (Kim, 2010). Likewise, cybersecurity education and user knowledge significantly reduce perceived online risks, resulting in more confident and secure user behavior (El Haddad et al., 2018; Saoula et al., 2023). Collectively, this evidence highlights the importance of providing safe, predictable, and user-friendly digital experiences as a foundation for trust building.

Importantly, the results suggest that user experience acts as a psychological bridge between technical security practices and users' perceptions of trust. In other words, even highly secure systems may fail to build trust if users do not perceive them as intuitive or transparent.

This finding reinforces the idea that cybersecurity effectiveness is not purely technical but also experiential, as users evaluate security through their interactions with the interface rather than through technical knowledge alone.

Given these dynamics, the current study demonstrates that UX is not merely an interface factor but a central psychological bridge through which effective cybersecurity practices influence consumers' trust judgments. This strong mediation effect underscores the need for e-commerce platforms to integrate security practices seamlessly into user-centered design strategies to strengthen trust. Accordingly, the findings provide clear empirical support for H3.

The fourth hypothesis (H4) investigated the indirect effect of cybersecurity practices (SPC) on e-purchase decisions (EDP) through customer trust (CTR). The results demonstrated that this pathway represents the strongest mediation effect in the entire model, emphasizing the centrality of trust in digital purchasing behavior. This aligns with extensive empirical evidence highlighting trust as a key factor in e-commerce decision-making (Kim et al., 2008; Pavlou, 2003). Secure environmental cues-such as encryption, authentication mechanisms, and transparent data-handling processes-significantly enhance consumer perceptions of safety and consequently increase willingness to transact (Sharma, 2024).

Additionally, prior studies have shown that trust mediates the relationship between perceived security and customer loyalty, particularly in sensitive sectors such as digital banking (Febriawan et al., 2024). Perceived ease of use and platform convenience also strengthen trust and, in turn, influence repurchase intentions across various e-commerce platforms (Ruslim, 2024). Research further indicates that perceived security and trust

combined can account for a substantial proportion of consumer repurchase intention—often exceeding 50%—demonstrating the decisive role of these variables (Luthfiani & Susila, 2025).

However, scholars have noted that excessively complex security procedures may diminish user satisfaction by creating friction during the purchasing process. Although robust security is essential, platforms must strike a balance between protective measures and user-friendly design to avoid negatively impacting buying decisions. While the results confirm a strong positive relationship between trust and purchasing behavior, this relationship should not be interpreted as stable or guaranteed under all conditions. In real-world digital environments, trust remains highly fragile and can be rapidly undermined by negative cybersecurity incidents.

For instance, exposure to phishing attacks, fraudulent websites, or data breaches can significantly reduce users' willingness to engage in online transactions, even if they previously had positive experiences with a platform. A single critical incident may override accumulated positive experiences and lead to a sudden loss of trust.

This highlights that the relationship between trust and purchasing decisions is dynamic rather than linear, and it is strongly influenced by users' perceptions of risk at specific moments during the interaction process.

Therefore, while cybersecurity practices contribute to building trust, maintaining that trust requires continuous reinforcement through consistent security performance and clear communication of protective measures.

Overall, the findings of the present study provide strong empirical support for H4, confirming that customer trust is the primary mechanism through which cybersecurity practices influence electronic purchasing decisions.

The final hypotheses (H5 and H6) examined whether gender moderates the relationships between cybersecurity awareness (AOC), cybersecurity practices (SPC), and customer trust (CTR). The results showed no statistically significant gender differences in either AOC or SPC, indicating that male and female consumers within the Saudi sample exhibit comparable levels of cybersecurity awareness and similar engagement in protective online behaviors. These findings contrast with earlier studies reporting higher security behavior among males (McGill & Thompson, 2018; Ifinedo, 2018; Alotaibi & Alshehri, 2020) and those demonstrating higher cybersecurity awareness among females in other cultural contexts, such as Thailand (Daengsi et al., 2022).

Prior research also suggests that gender interacts with psychosocial determinants of cybersecurity behavior, including security self-efficacy, prior experience, and digital competencies (Anwar et al., 2017). Such differences have led scholars to recommend gender-sensitive approaches when designing cybersecurity education and awareness interventions (McGill & Thompson, 2018). However, the absence of significant gender differences in the present study may reflect the rapid digital transformation in Saudi

Arabia, where both males and females are increasingly exposed to similar technological environments and cybersecurity awareness initiatives.

This finding also supports the view that gender differences in digital behavior are becoming less pronounced in highly connected and technology-driven societies, particularly when access to digital services and education becomes more standardized.

From a modeling perspective, these results justify treating gender as a grouping variable rather than a structural determinant, as its influence appears to be context-dependent and not directly involved in shaping the core relationships between cybersecurity, user experience, and trust.

However, the lack of gender differences in the present study may reflect Saudi Arabia's rapid digital transformation and increasing technological exposure for both genders, reducing previously observed behavioral gaps.

Overall, the findings indicate that gender does not moderate the pathways linking cybersecurity awareness or practices to trust, providing no support for H5 or H6. This suggests that security-related behaviors and perceptions are becoming more uniform across genders within Saudi Arabia's digitally advancing society.

6. Conclusions

This study provides important insights into the factors shaping online purchasing decisions among Saudi Arabian consumers by analyzing the direct and indirect effects of cybersecurity awareness, cybersecurity practices, user experience, and customer trust. The findings confirm the central role of customer trust in e-commerce, consistent with established literature emphasizing trust as a key determinant of online behavior (Gefen et al., 2003; Pavlou, 2003). The results demonstrate that trust not only acts as a direct driver of electronic purchasing but also functions as a crucial mediator, linking both cybersecurity awareness and practices to consumers' final purchase decisions. These outcomes underscore the need to strengthen trust mechanisms within digital platforms to encourage secure and confident online transactions. More importantly, the study highlights that trust is not a static construct but a dynamic and context-dependent mechanism that can be strengthened or weakened depending on users' experiences and their exposure to cybersecurity risks.

The study employed a quantitative approach that effectively revealed the interconnectedness of cybersecurity perceptions, gender differences, and the mediating influence of user experience and trust. The implications of these findings contribute to academic understanding of gender-related dynamics in online shopping, while also offering practical guidance for e-commerce providers seeking to design user experiences that align with diverse customer expectations (Park & Kim, 2003). The importance of designing user-friendly interfaces that clearly communicate security features is

further highlighted, as such elements enhance trust and engagement in digital contexts (Nurdiansyah et al., 2023).

Moreover, the study emphasizes the substantial influence of cybersecurity practices on both user experience and customer trust. The positive link between secure online behavior and a satisfying user experience shows that when platforms prioritize robust security standards, users feel safer and more comfortable, resulting in stronger trust and higher purchase intention. This finding aligns with research emphasizing the role of secure environments in improving user perceptions (Howell, 2021; Matlala, 2023; Panditharathna et al., 2024). However, the findings also suggest that strong security mechanisms alone are not sufficient; their effectiveness depends on how they are experienced by users. Poorly designed or overly complex security processes may reduce usability and negatively influence purchasing behavior despite their technical strength. Notably, the strong indirect effect of cybersecurity practices on purchasing decisions through trust reinforces the idea that trust is the primary mechanism connecting platform security with consumer behavior.

Although cybersecurity awareness also contributes to trust formation, the findings suggest that actual security practices exert a more tangible influence on both trust and purchasing decisions. This indicates that awareness alone is insufficient; rather, consumers must actively engage in secure online behaviors to fully benefit from improved trust and positive user experiences. These insights hold significant implications for both consumers and online retailers, highlighting the importance of cybersecurity education and the promotion of practical safety behaviors in digital environments.

While this study offers meaningful contributions, several limitations should be noted. First, the cross-sectional design restricts the ability to establish causal relationships; future research should consider longitudinal methods to capture changes in consumer behavior over time. Second, although the sample size was relatively large, it may not fully represent all Saudi online consumers, especially given the rapidly evolving digital landscape. Future studies should incorporate more diverse sampling strategies across demographic groups and regions. Third, the study focuses primarily on general cybersecurity perceptions and behaviors and does not explicitly capture the impact of specific critical cybersecurity incidents, such as fraud cases, phishing attacks, or data breaches, which may significantly influence trust and purchasing behavior. Future research is encouraged to examine these high-risk scenarios in greater detail. Finally, the research is focused on the Saudi Arabian context, which has distinct cultural and socio-economic characteristics. Comparative studies across different countries are recommended to validate and generalize the proposed model. Additionally, future studies may explore other potential moderating variables—such as age, digital literacy, or prior online experience—to better understand variations in user experience and trust formation.

This study makes several important contributions to both academic research and managerial practice within the field of e-commerce and digital consumer behavior. Theoretically, the study offers an integrated framework that combines cybersecurity awareness, cybersecurity practices, user experience, customer trust, and gender differences-variables that are often examined separately in prior research. By incorporating these constructs into a unified model, the study advances understanding of how cybersecurity-related perceptions and behaviors shape online purchasing decisions in emerging digital markets.

Furthermore, the research adds value by situating these relationships within the Saudi Arabian context-a rapidly developing digital economy characterized by unique cultural, regulatory, and socio-economic dynamics. While much of the existing literature is grounded in Western or East Asian settings, this study provides empirical evidence from the Middle East, thereby enriching the global discourse on cybersecurity and consumer behavior. The findings highlight the strong mediating role of both user experience and customer trust, offering new insight into the psychological and experiential mechanisms through which security perceptions influence purchasing decisions.

From a practical standpoint, the study provides actionable implications for e-commerce firms. The results emphasize the importance of enhancing cybersecurity practices, improving user experience design, and communicating security cues clearly to build and maintain customer trust. These insights can guide digital businesses in designing safer, more transparent, and more user-friendly online environments that encourage customer engagement and increase purchase intentions. The findings further underscore the growing need for continuous cybersecurity education and user awareness programs to support safer digital behavior.

Finally, the study lays a foundation for future research by identifying promising avenues for further investigation. These include exploring additional mediators or moderators, examining cross-cultural differences, and applying longitudinal approaches to capture behavioral changes over time. By addressing both theoretical and practical gaps, this research contributes meaningfully to the ongoing development of secure and trust-enhancing digital commerce ecosystems.

Authors' contribution

B.D.: theoretical content of the article, research methods applied, data collection, draft manuscript preparation. **H.M.A.:** data collection, draft manuscript preparation. **S.A.E.:** theoretical content of the article, conducting the research, analysis and interpretation of results. **R.E.H.:** article conception, analysis and interpretation of results, draft manuscript preparation.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors did not use Generative AI and AI-assisted technologies in the writing process.

References

- Alena, V.N. & Hasanah, Y.N. (2023). Analysis of online customer review on purchase decisions with customer trust as intervening. *Jurnal Manajemen Dan Bisnis*, 7(2), 201–211.
- Al-Kfairy, M., Alomari, A., Al-Bashayreh, M., Alfandi, O., Altaee, M., & Tubishat, M. (2023). A review of the factors influencing users' perception of metaverse security and trust. In *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 1–6). IEEE. <https://doi.org/10.1109/SNAMS60348.2023.10375478>
- Alotaibi, F. & Alshehri, A. (2020). Gender differences in information security management. *Journal of Computer and Communications*, 8(3), 53–60. <https://doi.org/10.4236/jcc.2020.83006>
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. <https://doi.org/10.1016/j.chb.2016.12.040>
- Butler, M.J. (2014). Towards online security: Key drivers of poor user behaviour and recommendations for appropriate interventions. *South African Journal of Business Management*, 45(4), 21–32.
- Carreón Guillén, J., Hernández Valdés, J., Morales Flores, M. D. L., Rivera Varela, B. L., & García Lirios, C. (2015). Contraste de un modelo de ciberconsumo [Testing a cyber-consumption model]. *Xihmai*, 10(19), 38–51. <https://doi.org/10.37646/xihmai.v10i19.255>
- Cerdeira, J.P. (2021). Trustworthiness, security, and the decision to buy on electronic platforms: Validity studies of a scale. *Consumer Behavior Review*, 5(1), 31–44.
- Choudhury, M.M. (2003). *A study of the significant factors affecting trust in electronic commerce*. [Doctoral dissertation, Durham University].
- Creswell, J.W. & Creswell, J.D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.
- Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-021-10806-7>
- Davidavičienė, V., Markus, O. & Davidavičius, S. (2020). Identification of the opportunities to improve customer's experience in e-commerce. *Journal of Logistics, Informatics and Service Science*, 7(1), 42–57. <https://doi.org/10.33168/LISS.2020.0104>
- El Haddad, G., Shahab, A., & Aïmeur, E. (2018). Exploring user behavior and cybersecurity knowledge: An experimental study in online shopping. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1–10). IEEE. <https://doi.org/10.1109/PST.2018.8514190>
- Endarwati, E.T., Indriany, Y., Rusdianto, R., Suarniki, N.N. & Pratiwi, L. (2024). The effect of product personalization, user experience, and consumer trust on the level of e-commerce consumer satisfaction in Indonesia. *Jurnal Bisnisan: Riset Bisnis dan Manajemen*, 6(1), 163–179.

- Fadhilah, F., Putri Wenang, L.F. & Affifatusholihah, L. (2021). Factors affecting trust on purchase decisions through e-marketplace. *International Journal of Economics, Business and Accounting Research (IJEBAR)*, 5(4), 1120–1129.
- Fahrozi, R., Rahmawati, D., Muldani, V., & Saddam, M. (2022). The influence of online customer review on trust and its implications for purchasing decisions on the Tokopedia marketplace. *Jurnal Administrare: Jurnal Pemikiran Ilmiah Dan Pendidikan Administrasi Perkantoran*, 9(1), 217–228.
- Farooq, A., Isoaho, J., Virtanen, S. & Isoaho, J. (2015). Observations on genderwise differences among university students in information security awareness. *International Journal of Information Security and Privacy (IJISP)*, 9(2), 60–74. <https://doi.org/10.4018/IJISP.2015040104>
- Febriawan, M.V., Lakilaki, E., Ariefandri, D., Saputra, R.A., Wijaya, P. & Manikam, D. (2024). Asses the impact of cyber crime mitigation strategies on Islamic banks in Bandar Lampung City. *Jurnal Ekuilnomi*, 6(3), 441–450.
- Fowler, F.J., Jr. (2013). *Survey research methods*. Sage publications.
- Furnell, S. M., Alotaibi, F., & Esmael, R. (2019). Aligning security practice with policy: Guiding and nudging towards better behavior. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 5558–5567). University of Hawai`i at Mānoa. <https://doi.org/10.24251/HICSS.2019.676>
- Garbarino, E. & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, 57(7), 768–775. [https://doi.org/10.1016/S0148-2963\(02\)00363-6](https://doi.org/10.1016/S0148-2963(02)00363-6)
- Geetha, B. T., Usman, M., Randhawa, N., Pipliwal, L., Maheshwari, K., & Kapila, N. (2024). Revolutionizing the dynamics of digital marketing by including cybersecurity measures and safeguarding consumer data. In *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies* (pp. 1–5). IEEE. <https://doi.org/10.1109/TQCEBT59414.2024.10545098>
- Gefen, D., Karahanna, E. & Straub, D.W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90. <https://doi.org/10.2307/30036519>
- Glavee-Geo, R., Shaikh, A.A. & Karjaluoto, H. (2017). Mobile banking services adoption in Pakistan: Are there gender differences? *International Journal of Bank Marketing*, 35(7), 1090–1114. <https://doi.org/10.1108/IJBM-09-2015-0142>
- Guo, J., Wang, X. & Wu, Y. (2020). Positive emotion bias: Role of emotional content from online customer reviews in purchase decisions. *Journal of Retailing and Consumer Services*, 52, 101891. <https://doi.org/10.1016/j.jretconser.2019.101891>
- Halaweh, M. (2012). Modeling user perceptions of e-commerce security using partial least square. *Journal of Information Technology Management*, 23(1), 22–33.
- Hampton-Sosa, W. & Koufaris, M. (2005). The effect of web site perceptions on initial trust in the owner company. *International Journal of Electronic Commerce*, 10(1), 55–81. <https://doi.org/10.1080/10864415.2005.11043963>
- Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon*, 10(8), e29714.
- Hayuningtyas, W. H., & Widiyanto, I. (2015). Antecedent kepercayaan dan keputusan pembelian [Antecedents of trust and purchase decisions]. *Diponegoro Journal of Management*, 4(4), 639–749.
- Howell, C.J. (2021). *Self-protection in cyberspace: Assessing the processual relationship between thoughtfully reflective decision making, protection motivation theory, cyber hygiene, and victimization*. University of South Florida.

- Hsiao, K.L., Lin, J.C.-C., Wang, X.Y., Lu, H.P. & Yu, H. (2010). Antecedents and consequences of trust in online product recommendations: An empirical study in social shopping. *Online Information Review*, 34(6), 935–953. <https://doi.org/10.1108/14684521011099414>
- Ifinedo, P. (2018). Roles of perceived fit and perceived individual learning support in students' weblogs continuance usage intention. *International Journal of Educational Technology in Higher Education*, 15, 1–8. <https://doi.org/10.1186/s41239-018-0092-3>
- Iskamto, D. & Gunawan, R.I. (2023). Impulse purchase behaviour on the Shopee platform and the role of real-time commerce marketing. *Jurnal Manajemen Bisnis*, 10(2), 444–461. <https://doi.org/10.33096/jmb.v10i2.623>
- Israel, G.D. (1992). *Determining sample size*. University of Florida Cooperative Extension Service.
- Kamoun, F. & Halaweh, M. (2012). User interface design and e-commerce security perception: An empirical study. *International Journal of E-Business Research (IJEER)*, 8(2), 15–32.
- Kanwal, M., Burki, U., Ali, R. & Dahlstrom, R. (2022). Systematic review of gender differences and similarities in online consumers' shopping behavior. *Journal of Consumer Marketing*, 39(1), 29–43. <https://doi.org/10.1108/JCM-02-2021-4401>
- Karmelia, H. & Dahlan, K.S. (2024). The influence of user experience, e-service quality, and e-trust mediated by e-satisfaction on e-loyalty: Customers subscription video on demand (Svod). *Journal of Social Science (JoSS)*, 3(9), 1706–1725.
- Kedaton, N.R., Sadat, A.M. & Sari, D.A. (2024). The effect of e-trust, information quality, and user interface quality on e-customer loyalty through e-satisfaction as an intervening variable: Study on Tokopedia users in Jabodetabek. *International Journal of Education, Social Studies, and Management (IJESSM)*, 4(2), 720–733.
- Khare, A., Kautish, P. & Khare, A. (2023). The online flow and its influence on awe experience: An AI-enabled e-tail service exploration. *International Journal of Retail & Distribution Management*, 51(6), 713–735.
- Kiliç, S. (2016). Cronbach's alpha reliability coefficient. *Psychiatry and Behavioral Sciences*, 6(1), 47.
- Kim, D.J., Ferrin, D.L. & Rao, H.R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>
- Kim, S. (2010). Assessment on security risks of customer relationship management systems. *International Journal of Software Engineering and Knowledge Engineering*, 20(1), 103–109. <https://doi.org/10.1142/S0218194010004591>
- Komalasari, F., Christianto, A. & Ganiarto, E. (2021). Factors influencing purchase intention in affecting purchase decision: A study of e-commerce customer in Greater Jakarta. *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi Dan Organisasi*, 28(1), 1.
- Koufaris, M. (2002). *Customer trust online: Examining the role of the experience with the website*. Department of Statistics and Computer Information Systems Working Paper Series.
- Ladhari, R. & Leclerc, A. (2013). Building loyalty with online financial services customers: Is there a gender difference? *Journal of Retailing and Consumer Services*, 20(6), 560–569. <https://doi.org/10.1016/j.jretconser.2013.07.005>
- Lathifah, A., Hadita, H., & Komariah, N. S. (2024). Pengaruh online customer review dan electronic word of mouth terhadap keputusan pembelian melalui kepercayaan pelanggan: Studi kasus produk fashion pada platform Shopee di Teluk Pucung Kota Bekasi [The influence of online customer reviews and electronic word of mouth on purchase decisions through customer trust: A case study of fashion products on the Shopee platform in Teluk Pucung, Bekasi City]. *Jurnal*

- Penelitian Ekonomi Manajemen dan Bisnis, 3(2), 110–124. <https://doi.org/10.55606/jekombis.v3i2.3481>
- Lăzăroiu, G., Neguriță, O., Grecu, I., Grecu, G. & Mitran, P.C. (2020). Consumers' decision-making process on social commerce platforms: Online trust, perceived risk, and purchase intentions. *Frontiers in Psychology*, 11, 890. <https://doi.org/10.3389/fpsyg.2020.00890>
- Lee, V., Park, S. & Lee, D. (2022). The effect of e-commerce service quality factors on customer satisfaction, purchase intention, and actual purchase in Uzbekistan. *Global Business & Finance Review*, 27(3), 56.
- Lima, E. de S., & Rezende, P. I. da S. (2024). Os desafios da proteção do consumidor no comércio eletrônico [The challenges of consumer protection in electronic commerce]. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, 10(11), 726–738. <https://doi.org/10.51891/rease.v10i11.16525>
- Lohr, S.L. (2021). *Sampling: Design and analysis*. Chapman and Hall/CRC. <https://doi.org/10.1201/9780429298899>
- Luthfiani, D. A., & Susila, I. (2025). Analisis pengaruh security dan reliable payment system terhadap repurchase intention dimediasi oleh brand trust pada platform digital perjalanan Agoda [Analysis of the effect of security and reliable payment system on repurchase intention mediated by brand trust on the Agoda digital travel platform]. *Hirarki: Jurnal Ilmiah Manajemen dan Bisnis*, 7(1), 65–86. <https://doi.org/10.30606/9nx5s846>
- Matlala, N.P. (2023). Behavioural insights into cybersecurity practices among digital banking consumers in South Africa. *Indonesian Journal of Business Analytics*, 3(4), 1425–1442. <https://doi.org/10.55927/ijba.v3i4.5515>
- McGill, T., & Thompson, N. (2018). Gender differences in information security perceptions and behavior. In *Proceedings of the 29th Australasian Conference on Information Systems*. <https://espace.curtin.edu.au/handle/20.500.11937/75017>
- Midha, V. (2012). Impact of consumer empowerment on online trust: An examination across genders. *Decision Support Systems*, 54(1), 198–205. <https://doi.org/10.1016/j.dss.2012.05.005>
- Najafi, I. (2012). The role of e-commerce awareness on increasing electronic trust. *Life Science Journal*, 9(4), 1487–1494.
- Novela, S., Sihombing, Y. O., Hansopaheluwakan, S., & Aurellia, C. (2023). How online customer review and online customer rating influence customer purchase decision on e-marketplace with customer trust as a mediator. In *2023 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICTMOD59086.2023.10472906>
- Nurdiansyah, Y., Ardi, M.Z. & Hidayat, M.A. (2023). Decision-making system for selecting alternative product purchase stores in Tokopedia using a combination of SAW and TOPSIS. *Journal of Informatics Development*, 2(1), 16–22.
- Panditharathna, R., Liu, Y., de Macedo Bergamo, F.V., Appiah, D., Trim, P.R. & Lee, Y.I. (2024). How cyber security enhances trust and commitment to customer retention: The mediating role of robotic service quality. *Big Data and Cognitive Computing*, 8(11), 165. <https://doi.org/10.3390/bdcc8110165>
- Park, C.H. & Kim, Y.G. (2003). Identifying key factors affecting consumer purchase behavior in an online shopping context. *International Journal of Retail & Distribution Management*, 31(1), 16–29. <https://doi.org/10.1108/09590550310457818>

- Pavlou, P.A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Peña-García, N., Losada-Otálora, M., Auza, D.P. & Cruz, M.P. (2024). Reviews, trust, and customer experience in online marketplaces: The case of Mercado Libre Colombia. *Frontiers in Communication*, 9, 1460321.
- Pilakaew, T., Thanitbenjasith, P. & Kamkankaew, P. (2024). The impact of consumer perceptions of privacy and security risks on repurchasing intention for online shopping in Chiang Mai Province, Thailand. *International Journal of Sociologies and Anthropologies Science Reviews*, 4(6), 531–542. <https://doi.org/10.60027/ijssar.2024.5065>
- Putri, T., Guntara, R.G. & Prehanto, A. (2024). The influence of user experience on decisions PLN mobile user purchases. *Journal of Investment Development, Economics and Accounting*, 1(2), 230–242.
- Rahman, M. N., & Firdaus, R. (2024). E-commerce solusi jitu masalah perekonomian [E-commerce: The right solution to economic problems]. *Jurnal Intelek dan Cendekiawan Nusantara*, 1(3), 4298–4301.
- Rita, R. & Guinardi, D.N. (2023). The impact of flash sales and brand image on purchase intention and its impact on purchase decision. *Jurnal Mantik*, 7(1), 334–343.
- Ruslim, T.S. (2024). The effect of security and perceived ease of use on repurchase intention in online marketplace consumers with trust as mediation (Case: Marketplace “T” in Jakarta). *Prima-nomics: Jurnal Ekonomi & Bisnis*, 22(3), 243–254.
- Saoula, O., Shamim, A., Suki, N.M., Ahmad, M.J., Abid, M.F., Patwary, A.K. & Abbasi, A.Z. (2023). Building e-trust and e-retention in online shopping: The role of website design, reliability, and perceived ease of use. *Spanish Journal of Marketing-ESIC*, 27(2), 178–201. <https://doi.org/10.1108/SJME-07-2022-0159>
- Sari, P. K., & Prasetyo, A. (2018). Customer awareness towards digital certificate on e-commerce: Does it affect purchase decision? In *2018 Third International Conference on Informatics and Computing (ICIC)* (pp. 1–4). IEEE. <https://doi.org/10.1109/IAC.2018.8780519>
- Sawal, A. (2023). Influence of UI/UX on online purchase decisions in e-commerce. In *AIP Conference Proceedings*, 2828(1). AIP Publishing. <https://doi.org/10.1063/5.0165871>
- Sekar, S., Solayappan, A., Srimathi, J., Raja, S., Durga, S., Manoharan, P., Hamdi, M. & Tunze, G.B. (2022). Autonomous transaction model for e-commerce management using blockchain technology. *International Journal of Information Technology and Web Engineering (IJITWE)*, 17(1), 1–4. <https://doi.org/10.4018/IJITWE.30404>
- Sharma, B. P. (2024). *Role of advanced cybersecurity frameworks in safeguarding data integrity and consumer trust in digital commerce and enterprise systems* (Manuscript No. 11.01-5/VECTORAL.2024. PUB) [Preprint]. VECTORAL. <https://www.researchgate.net/publication/387949002>
- Shin, D.H. (2013). User experience in social commerce: In friends we trust. *Behaviour & Information Technology*, 32(1), 52–67. <https://doi.org/10.1080/0144929X.2012.692167>
- Soleimani, M. (2022). Buyers' trust and mistrust in e-commerce platforms: A synthesizing literature review. *Information Systems and e-Business Management*, 20(1), 57–78. <https://doi.org/10.1007/s10257-021-00545-0>
- Stângaciu, A., Țimiraș, L., Zaiț, L., Nichifor, B., Danu, M. & Harja, E. (2024). The EU e-commerce market in a pandemic context—linking demographic factors and territorial convergence. *Journal of Business Economics and Management*, 25(1), 21–46. <https://doi.org/10.3846/jbem.2024.20705>

- Sudirjo, F., Fajariana, D. E., Vandika, A. Y., & Sagena, U. (2024). The effect of digital transformation, user experience, and user interface on customer loyalty in technology startups in Bandung. *West Science Interdisciplinary Studies*, 2(9), 1850–1856. <https://doi.org/10.58812/wsis.v2i09.1305>
- Ta, V., Griffith, C., Boatfield, C., Wang, X., Civitello, M., Bader, H., DeCero, E. & Loggarakis, A. (2020). User experiences of social support from companion chatbots in everyday contexts: Thematic analysis. *Journal of Medical Internet Research*, 22(3), e16235.
- Tahir, M., & Khan, W. (2020). Online review and customer purchase intention in social e-commerce context: Role of trust as a mediator and source credibility as moderator. *KASBIT Business Journal*, 13(1). <https://kasbitoric.com/index.php/kbj/article/view/13>
- Thompson, S.K. (2012). *Sampling*. John Wiley & Sons.
- Turner, C.W. (2002). The online experience and consumers' perceptions of e-commerce security. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 46(14), 1246–1250. <https://doi.org/10.1177/154193120204601402>
- Utami, N. N., & Usman, O. (2021). *Effect of customer trust, use easy and information quality on purchase decisions on Lazada e-commerce*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3768293
- Wang, Y.D. & Emurian, H.H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1), 105–125. <https://doi.org/10.1016/j.chb.2003.11.008>
- Williams, S. D. (2022). Exploring the user experience design of commercially available cybersecurity products for personal mobile devices. In *2022 IEEE International Professional Communication Conference (ProComm)* (pp. 187–191). IEEE. <https://doi.org/10.1109/ProComm53155.2022.00037>
- Yapinski, J. J., Nursanti, T. D., & Scoth, J. (2024). Optimizing e-service quality and user experience to enhance customer loyalty via satisfaction. In *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCICT)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICCICT62134.2024.10701164>
- Yoon, S.J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, 16(2), 47–63. <https://doi.org/10.1002/dir.10008>
- Zhang, X., Prybutok, V.R., Ryan, S. & Pavur, R. (2009). A model of the relationship among consumer trust, web design, and user attributes. *Journal of Organizational and End User Computing (JOEUC)*, 21(2), 44–66.
- Zhao, Y., Wang, L., Tang, H. & Zhang, Y. (2020). Electronic word-of-mouth and consumer purchase intentions in social e-commerce. *Electronic Commerce Research and Applications*, 41, 100980. <https://doi.org/10.1016/j.elerap.2020.100980>