International Journal of Safety and Security Engineering
Vol. 15, No. 8, August, 2025, pp. 1681-1689
Journal homepage: http://iieta.org/journals/ijsse

Cybersecurity Strategies and Service Quality in Mobile Payments: The Moderating Role of Fintech Literacy in Building Customer Trust

Syed Khusro Chishty[1*], Sarah Al Qahtani[2,3], Sonia Sayari[1], Shahid Alam[2], Ahmad Murtaza Alvi[2]

[1] Department of Business Administration, College of Administrative and Financial Sciences, Saudi Electronic University, Jeddah 23442, Saudi Arabia
[2] Department of Business Administration, College of Administrative and Financial Sciences, Saudi Electronic University, Riyadh 93499, Saudi Arabia
[3] Awqaf, The pioneering Digital City, Riyadh 93499, Saudi Arabia

Corresponding Author Email: s.chishty@seu.edu.sa

https://doi.org/10.18280/ijsse.150813

Received: 7 July 2025
Revised: 8 August 2025
Accepted: 18 August 2025
Available online: 31 August 2025

Keywords:
cybersecurity strategies, customer trust, service quality, moderating role of digital literacy, fintech, Structural Equation Modeling, STC Pay, Saudi Arabia

ABSTRACT

This study investigates how cybersecurity strategies influence perceived service quality through customer trust in the context of STC Pay, a prominent mobile payment platform in Saudi Arabia. Drawing on the Information Systems Success Model and trust-based theories, the research develops and tests a structural model incorporating cybersecurity strategies (technical, procedural, and behavioural), customer trust, and digital literacy. Survey data from 370 active users were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings reveal that cybersecurity strategies significantly enhance customer trust, which in turn improves perceived service quality. Customer trust also partially mediates the relationship between cybersecurity and service quality, supporting the role of trust as a key psychological conduit. Furthermore, digital literacy positively moderates the cybersecurity–trust relationship, indicating that trust-building effects are stronger among users with higher digital competence. These results confirm all hypothesized paths and explain substantial variance in both trust ($R^2 = 0.43$) and perceived service quality ($R^2 = 0.51$). The study contributes to both theory and practice by empirically validating the trust-mediated pathway from cybersecurity to service quality and by highlighting the importance of user-level competencies in shaping cybersecurity effectiveness in fintech environments.

1. INTRODUCTION

The global financial sector is undergoing a significant digital transformation, driven by rapid advancements in information technology, the proliferation of smartphones, and increasing internet accessibility. Saudi Arabia, under its Vision 2030 initiative, has prioritized the growth of a cashless economy and digital financial inclusion through regulatory support and institutional modernization [1, 2]. Within this context, STC Pay has emerged as one of the Kingdom's leading mobile wallet platforms, licensed by the Saudi Central Bank (SAMA) and positioned at the forefront of fintech innovation [3, 4]. As digital payment platforms become integral to daily financial transactions, the demand for secure, reliable, and high-quality digital experiences has escalated, making cybersecurity a cornerstone of customer satisfaction and trust [5]. The increasing sophistication of cyber threats—ranging from phishing attacks to data breaches—has heightened consumer concerns about the security of their digital financial transactions [2, 6]. In response, fintech providers have adopted comprehensive cybersecurity strategies that encompass technical safeguards, procedural controls, and user-focused measures such as awareness campaigns and multi-factor authentication [7]. However, while these strategies are operationally necessary, their effectiveness in shaping users' subjective experience—particularly their trust in the platform and perceived service quality—remains underexplored in the empirical literature [4].

Trust has long been recognized as a pivotal factor in the acceptance of electronic services [8], and service quality is central to user satisfaction and continued use [9]. Yet, few studies integrate cybersecurity strategy as an antecedent of trust and service quality, especially in the fintech sector of developing economies like Saudi Arabia. The existing body of knowledge also lacks a nuanced understanding of how user characteristics—particularly digital literacy—influence the efficacy of cybersecurity communication and implementation. Digital literacy encompasses the skills required to access, evaluate, and use digital tools safely and effectively [1]. Users with higher digital literacy may be better equipped to recognize cybersecurity efforts, thereby strengthening their trust in the platform. Conversely, users with lower literacy may fail to appreciate these efforts, undermining the intended effect. This potential moderating role of digital literacy is rarely addressed in the cybersecurity–trust literature, despite its importance in user-centered technology design and digital inclusion policies. The purpose of this study is to examine how cybersecurity strategies adopted by STC Pay influence customer trust and, subsequently, perceived service quality. Moreover, the study investigates whether customer trust acts as a mediating variable in this relationship and whether digital literacy moderates the link between cybersecurity strategies and trust. In doing so, the study draws upon established theoretical models such as the trust-based models of online behaviour [8] and Information Systems Success Model [9], extending them into a cybersecurity context within the fintech domain of the Global South. To address these issues, the study is guided by the following research questions:

1. How do cybersecurity strategies impact customer trust in STC Pay?
2. How does customer trust influence perceived service quality?
3. Does customer trust mediate the relationship between cybersecurity strategies and perceived service quality?
4. Does digital literacy moderate the effect of cybersecurity strategies on customer trust?

This study holds substantial relevance for multiple stakeholders. For fintech practitioners and platform designers, it offers actionable insights into how cybersecurity investments can translate into improved customer experience, particularly in trust-sensitive contexts such as digital finance [6]. For regulators like SAMA, the findings may inform policy frameworks that not only enforce security compliance but also enhance consumer trust and service quality. Academically, the study contributes to the service quality and information systems literature by proposing and empirically testing an integrated model that links cybersecurity strategies with trust-based evaluations of digital service performance [5, 9].

The remainder of the paper is structured as follows: the next section reviews the extant literature on cybersecurity, trust, digital literacy, and service quality in fintech, and develops hypotheses based on theoretical reasoning. This is followed by the methodology section, which outlines the research design, sampling, and data collection procedures. The results section presents the empirical findings from structural equation modelling. Finally, the discussion and conclusion elaborate on the study's theoretical contributions, practical implications, limitations, and directions for future research.

2. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1 Cybersecurity strategies in fintech

Cybersecurity strategies in fintech refer to a set of organizational and technical measures designed to ensure the confidentiality, integrity, and availability of data across digital financial infrastructures [10]. These strategies are typically classified into three core domains: technical, procedural, and behavioural [11]. Technical strategies encompass encryption protocols, firewalls, intrusion detection systems, and multi-factor authentication, serving as the backbone of information security systems [12]. Procedural strategies involve regulatory compliance, risk assessments, and internal audits aligned with standards such as ISO/IEC 27001, thereby institutionalizing secure practices [13]. Behavioural strategies include employee training, user awareness campaigns, and the promotion of a security-first culture, which are critical to reducing human-related vulnerabilities [14]. Cybersecurity in fintech has evolved beyond risk mitigation into a value-creating mechanism that enhances customer confidence and platform reputation [15, 16]. Particularly in mobile-based financial services like STC Pay, where users rely heavily on seamless and secure interactions, robust cybersecurity strategies are perceived as essential components of value delivery [12]. Research has shown that when users perceive a platform as safe, they are more likely to engage in transactions and form favourable impressions of service reliability [17]. Thus, the strategic deployment of cybersecurity measures not only prevents breaches but also contributes to perceived safety and assurance—factors foundational to user trust [18].

H1: Cybersecurity strategies positively influence customer trust in STC Pay.

2.2 Customer trust in digital financial services

Trust is a cornerstone of user behaviour in digital financial environments, where service interactions lack physical cues and are characterized by uncertainty [8]. Defined as the willingness of a party to be vulnerable to another based on positive expectations of behaviour [19], trust in fintech contexts is formed through perceptions of ability, benevolence, and integrity [20]. In the case of mobile wallets like STC Pay, trust is shaped by users' belief that the system will perform as promised and that their personal and financial data will be handled securely [21]. System assurance—rooted in visible security features such as authentication procedures, transaction transparency, and data encryption—plays a critical role in trust formation [17]. When cybersecurity strategies are well-communicated and effectively implemented, they serve as trust cues that signal organizational reliability and user respect [22]. Trust not only facilitates initial adoption but also fosters sustained usage and positive word-of-mouth [23]. In this regard, customer trust acts as a psychological bridge between the abstract implementation of cybersecurity and users' concrete evaluations of service performance.

H2: Customer trust positively influences the perceived service quality of STC Pay.

H3: Customer trust mediates the relationship between cybersecurity strategies and perceived service quality.

2.3 Perceived service quality

Perceived service quality refers to the customer's evaluation of the overall excellence or superiority of a service offering [24]. In the fintech context, service quality is often assessed across adapted SERVQUAL dimensions such as reliability (ability to perform dependably), responsiveness (promptness in service delivery), and assurance (confidence instilled through security and competence) [25]. As digital interfaces become the primary mode of user engagement, quality perceptions are increasingly influenced by the seamless integration of security features into the service experience [24]. Customer trust is instrumental in shaping these quality perceptions, as it reduces user anxiety and strengthens confidence in system performance [9]. The trust serves as an affective filter through which users interpret service outcomes. If users trust the platform, they are more likely to attribute positive meanings to their experiences, even amidst technical imperfections [26]. Therefore, cybersecurity strategies that build trust indirectly elevate perceptions of service quality by shaping user attitudes toward platform reliability and professionalism [1, 2].

2.4 Digital literacy as a moderator

Digital literacy, defined as the ability to effectively access, understand, evaluate, and use digital technologies [27], plays a critical role in shaping how users interpret cybersecurity signals. From a cognitive processing standpoint, digital literacy enhances users' ability to detect, decode, and evaluate system cues related to safety and reliability—factors central to the formation of trust in online platforms [28]. Digitally literate users can better interpret security features such as encryption indicators, two-factor authentication, or phishing warnings, thus forming more accurate risk assessments and trust judgments [29]. In contrast, users with limited digital skills may overlook or misunderstand these cues, thereby reducing the perceived credibility of the platform's security mechanisms, even if they are objectively robust [30].

Furthermore, trust formation in digital environments is not purely affective but is influenced by a user's perceived competence in interacting with the system [8]. Digital literacy enhances this perceived competence, leading to a more favorable interpretation of organizational intentions and technical safeguards. As such, the relationship between cybersecurity strategies and customer trust is likely to be contingent on the user's digital literacy level: high-literate users are more likely to appreciate and respond positively to security investments, while low-literate users may fail to internalize these efforts. This perspective aligns with the cognitive-affective model of trust, which highlights the role of individual cognitive filters in trust development [22]. Thus, we hypothesize that digital literacy moderates the cybersecurity–trust relationship, amplifying the positive effect of cybersecurity strategies on trust among more digitally competent users, as shown in Figure 1.

H4: Digital literacy positively moderates the relationship between cybersecurity strategies and customer trust, such that the relationship is stronger among users with higher digital literacy.

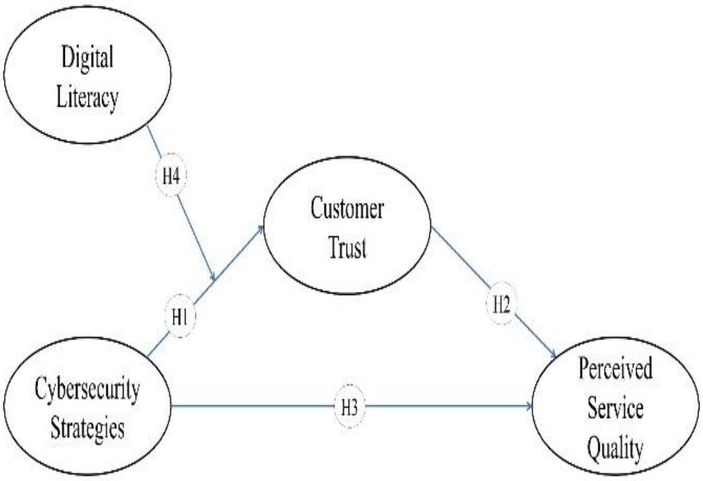

Figure 1. Conceptual framework

3. METHODOLOGY

This study employs a quantitative, cross-sectional research design to investigate the relationships among cybersecurity strategies, customer trust, perceived service quality, and digital literacy in the context of STC Pay, a leading mobile wallet platform in Saudi Arabia. Quantitative research is particularly suited for hypothesis testing and theory validation through empirical evidence [31, 32]. It enables the measurement of latent constructs using structured instruments and the evaluation of structural relationships via statistical modelling [33]. Anchored in the positivist paradigm, the study assumes that reality is measurable and generalizable, especially when the constructs are operationalized using validated tools [34]. The population for this study consists of active STC Pay users across Saudi Arabia, particularly from urban centres such as Riyadh, Jeddah, and Dammam. Participants were required to have completed at least one transaction using STC Pay in the past three months, ensuring familiarity with the platform's security features and service interface. A purposive sampling method was used to recruit respondents who met these eligibility criteria. This technique is appropriate in fintech adoption research where respondents need to have direct experience with the digital platform under investigation [4]. Data were collected through an online questionnaire hosted on Qualtrics, which was distributed via email and social media platforms. A total of 420 responses were received, and after eliminating incomplete or inconsistent responses, 370 valid observations were retained, satisfying the sample size recommendation for Partial Least Squares Structural Equation Modeling (PLS-SEM) [33].

Data collection was conducted entirely online, allowing for efficient access to digitally literate participants while ensuring respondent anonymity and confidentiality. An introductory section in the survey described the research purpose, ensured voluntary participation, and included informed consent following ethical research practices [35, 36]. Online surveys are particularly well-suited for studies in the fintech domain, given their reach and alignment with the digital nature of the platform being studied [37]. To ensure validity and reliability, all constructs were measured using established, multi-item instruments adapted from prior research. Cybersecurity strategies were measured using a 9-item scale from Dutta and McCrohan [11], encompassing technical (e.g., two-factor authentication), procedural (e.g., formal data protection policies), and behavioural (e.g., user training initiatives) security elements. Sample items included: "STC Pay uses secure authentication protocols" and "The platform regularly updates its security features." These items were designed to assess the user's perception of the comprehensiveness and visibility of cybersecurity mechanisms [17]. Customer trust was assessed using a 7-item scale developed by McKnight et al. [38], capturing the subdimensions of competence, integrity, and benevolence. Example statements included: "I believe STC Pay is competent in handling transactions securely" and "STC Pay acts in the best interest of its users." This scale is well-established in digital trust literature and aligns with the context of secure financial services [8].

Perceived service quality was measured using six items adapted from Yang and Fang [25], based on the SERVQUAL model. The three retained dimensions—reliability, responsiveness, and assurance—were tailored to fintech service delivery. Items included: "STC Pay provides consistent and error-free transactions" and "Customer service is quick to resolve transaction issues." This construct was evaluated from a user-centred lens to reflect actual perceptions of service excellence in a digital environment [9]. Digital literacy was measured using a 7-item scale adapted from Ng [20], which captures users' ability to access, evaluate, and respond to digital information, especially in security-sensitive contexts. Sample items were: "I can assess the safety of websites and apps before using them" and "I understand how digital systems protect my data." This construct functions as a moderator in the model and reflects the cognitive capability required to process security-related cues in online platforms [30]. All measurement items were scored using a 7-point Likert scale ranging from 1 ("strongly disagree") to 7 ("strongly agree"). Pretesting with 25 STC Pay users led to minor modifications for clarity and contextual appropriateness. The reliability of each construct was assessed using Cronbach's alpha, with all values exceeding the acceptable threshold of 0.70, indicating internal consistency [39].

Data analysis was conducted using PLS-SEM via SmartPLS 4.0. This method is particularly appropriate for exploratory models, small to medium sample sizes, and for examining models that include mediation and moderation effects [40]. The analysis proceeded in two stages. First, the measurement model was evaluated for indicator reliability (outer loadings ≥ 0.70), convergent validity (average variance extracted (AVE) ≥ 0.50), and discriminant validity using the Fornell–Larcker criterion and Heterotrait–Monotrait (HTMT) ratios. Second, the structural model was assessed to test the hypothesized relationships using bootstrapping with 5,000 samples, which enabled the estimation of standard errors and significance levels for each path coefficient [41]. To test mediation (H3), the indirect effect of cybersecurity strategies on perceived service quality through customer trust was assessed. The significance of the mediating pathway was determined by examining bias-corrected confidence intervals. Moderation analysis (H4) involved creating an interaction term between cybersecurity strategies and digital literacy and entering it into the model to assess its effect on customer trust. The significance and strength of this interaction were evaluated using t-values derived from bootstrapping [42]. Collinearity among constructs was examined through variance inflation factor (VIF) scores, which remained below the recommended threshold of 3.3, suggesting no multicollinearity bias [43]. Overall, the adopted methodology ensures analytical rigour and construct validity, allowing for robust testing of the conceptual framework. This approach aligns well with the methodological expectations of contemporary information systems and marketing research. To minimize potential biases in the questionnaire design, several methodological precautions were undertaken. First, all measurement items were adapted from well-validated scales in prior literature, which increases construct validity. Second, a pretest was conducted with 25 STC Pay users to assess item clarity, contextual appropriateness, and ease of comprehension; minor modifications were made accordingly. Third, to mitigate acquiescence bias and response patterning, the questionnaire included reverse-coded items and was balanced across positive and neutral phrasings. Fourth, expert review was sought from two domain scholars and one fintech practitioner to validate content relevance and reduce item ambiguity. Finally, anonymity and confidentiality were assured to minimize social desirability bias in self-reports. These strategies collectively enhanced the reliability, validity, and internal consistency of the instrument.

4. RESULTS

4.1 Descriptive statistics

The final dataset comprised 370 valid responses from active users of STC Pay across Saudi Arabia. As indicated in Table 1, the sample was gender-balanced (53% male and 47% female), with a majority of participants aged between 18 and 27 (57%), followed by 28–37 (31%), and 38–47 (12%). These data reflect a digitally native population likely to engage with mobile fintech services. Descriptive statistics for the latent variables showed acceptable mean scores ranging from 4.91 to 5.62, with standard deviations between 0.83 and 1.14, indicating moderate dispersion. These results suggest that participants had sufficiently diverse evaluations of the cybersecurity, trust, literacy, and service quality constructs to allow for meaningful structural modelling [33].

Table 1. Sample demographics

Variable	Percentage
Gender	
Male	47%
Female	53%
Age	
18-27	57%
28-37	31%
38-47	12%

4.2 Measurement model: Reliability and validity

The reliability and validity of the constructs were assessed using the two-step approach recommended by Hair et al. [40], as shown in Table 2. Cronbach's alpha values for all four latent variables were above the recommended threshold of 0.70: cybersecurity strategies (α = 0.84), customer trust (α = 0.86), perceived service quality (α = 0.85), and digital literacy (α = 0.82). These values confirm internal consistency reliability [39]. Convergent validity was demonstrated by factor loadings exceeding 0.79 and AVE values greater than 0.50 for each construct [44]. This confirms that items adequately represent their respective constructs. Discriminant validity was evaluated using the Fornell–Larcker criterion and HTMT ratios. In each case, the square root of the AVE for a construct exceeded the inter-construct correlations, meeting Fornell–Larcker criteria. Additionally, all HTMT values were below the threshold of 0.85, confirming discriminant validity [42]. No item cross-loadings exceeded their respective primary loadings, ensuring item-level discriminant clarity.

4.3 Structural model and hypothesis testing

Structural equation modelling was conducted using SmartPLS 4.0, applying 5,000-sample bootstrapping to test the significance of path coefficients. The model showed strong explanatory power, with $R^2 = 0.43$ for customer trust and $R^2 = 0.51$ for perceived service quality—indicating moderate to substantial predictive accuracy [45]. All four hypotheses (H1–H4) were supported, as summarized in Table 3. Cybersecurity strategies were found to influence customer trust significantly ($\beta = 0.48$, SE = 0.06, CR = 8.00, $p < .001$), supporting H1. This finding aligns with prior research suggesting that visible and reliable security protocols foster user confidence in digital platforms [17, 36]. Customer trust significantly predicted perceived service quality ($\beta = 0.52$, SE = 0.05, CR = 10.40, $p < .001$), validating H2 and confirming that trust acts as a central affective filter in shaping service evaluations [8].

Table 2. Constructs, items, and factor loadings

Construct	Source	Measurement Items	Factor Loadings	Cronbach's Alpha
Cybersecurity Strategies	Dutta and McCrohan [11]; Bélanger et al. [17]	1. STC Pay uses secure authentication protocols. 2. STC Pay regularly updates its security features. 3. The platform educates users about safe digital practices.	0.82 0.85 0.81	0.84
Customer Trust	Gefen et al. [8]; McKnight et al. [38]	1. I trust STC Pay to protect my personal and financial data. 2. STC Pay is competent in handling transactions. 3. STC Pay acts in my best interest.	0.86 0.83 0.85	0.86
Perceived Service Quality	DeLone and McLean [9]; Yang and Fang [25]	1. STC Pay provides consistent and error-free transactions. 2. STC Pay resolves issues promptly. 3. I feel safe using STC Pay.	0.84 0.81 0.87	0.85
Digital Literacy	Ng [20]; van Deursen and van Dijk [46]	1. I can assess the safety of apps before using them. 2. I understand how STC Pay secures data. 3. I can detect suspicious digital behaviour.	0.80 0.83 0.79	0.82

Table 3. SEM results for hypotheses testing

Hypothesis	Path	Standardized Estimate (β)	Standard Error (SE)	Critical Ratio (CR)	P-Value	Result
H1	Cybersecurity Strategies → Customer Trust	0.48	0.06	8.00	< .001	Supported
H2	Customer Trust → Perceived Service Quality	0.52	0.05	10.40	< .001	Supported
H3	Cybersecurity Strategies → Customer Trust → Perceived Service Quality (Mediation)	0.25	0.04	6.25	< .001	Supported (Mediation)
H4	Cybersecurity Strategies × Digital Literacy → Customer Trust (Moderation)	0.18	0.07	2.57	0.010	Supported (Moderation)

4.4 Mediation and moderation analysis

To examine H3, the mediating role of customer trust between cybersecurity strategies and perceived service quality was assessed using the bootstrapping method with bias-corrected confidence intervals. The indirect path was statistically significant ($\beta = 0.25$, SE = 0.04, CR = 6.25, $p < .001$), supporting partial mediation. This suggests that cybersecurity strategies enhance service quality not only directly but also indirectly by fostering greater trust—a result consistent with DeLone and McLean's information systems [9] success model and Pavlou's trust-centered e-commerce framework [21]. For H4, a product indicator approach was used to test the moderating effect of digital literacy on the relationship between cybersecurity strategies and customer trust. The interaction term was significant ($\beta = 0.18$, SE = 0.07, CR = 2.57, $p = .010$), confirming that the strength of the cybersecurity–trust relationship is contingent upon the user's level of digital literacy. This supports the findings by Ng [20] and van Deursen and van Dijk [46], who argue that higher digital literacy enables more effective evaluation and appreciation of security cues in online environments. Together, these findings confirm the robustness of the proposed conceptual model and highlight the pivotal role of trust and user competence in translating cybersecurity investments into perceived service quality.

5. DISCUSSION

The findings of this study reveal that cybersecurity strategies significantly enhance customer trust, which in turn improves users' perceptions of service quality on digital payment platforms like STC Pay. This supports the conceptual assertion that security functions as more than a technical requirement—it is a strategic asset that contributes directly to user trust and indirectly to service quality perceptions [17]. The strong standardized path coefficient between cybersecurity strategies and customer trust (β = 0.48, p < .001) indicates that users interpret visible security mechanisms—such as two-factor authentication and privacy safeguards—as indicators of organizational competence and commitment to user protection [11]. These perceptions of security translate into trust, which has long been considered central to customer engagement in electronic environments [8]. In line with prior research, the study confirms that customer trust is a significant predictor of perceived service quality in digital finance settings (β = 0.52, p < .001), corroborating the foundational role of trust in online service evaluations [9, 21]. Trust acts as a cognitive shortcut that reduces users' uncertainty, enhances their comfort, and positively biases their assessment of service reliability, responsiveness, and assurance [26]. This finding aligns with Yang and Fang's observation [25] that perceived security and trustworthiness are embedded within users' broader judgment of e-service quality. The mediation analysis further reveals that trust partially mediates the relationship between cybersecurity strategies and perceived service quality (β = 0.25, p < .001), thereby highlighting trust as a critical psychological conduit through which security investments are transformed into service quality gains.

Importantly, the moderating role of digital literacy (β = 0.18, p = .010) extends the current understanding of how individual differences shape the efficacy of organizational cybersecurity strategies. Users with higher digital literacy are better equipped to decode, appreciate, and evaluate security-related cues embedded in digital interfaces, leading to stronger trust formation [30, 39]. This supports the cognitive-affective model of trust development, which posits that user competence enhances the salience of risk-reducing mechanisms [22]. The inclusion of digital literacy as a moderator addresses a frequently overlooked dimension in IS research, which often assumes homogeneity in user perceptions of technical safeguards [30]. This study makes several theoretical contributions. First, it extends DeLone and McLean's IS Success Model [9] by integrating cybersecurity as a system characteristic that indirectly contributes to service quality through trust, thereby introducing a novel antecedent within the model's framework. Second, it bridges two important streams of literature—cybersecurity management and service quality—by showing that strategic security implementation contributes to user experience outcomes, not merely risk mitigation. Third, it enhances trust literature by empirically validating the mediating role of trust and by showing that its development is not solely based on transactional history but is also shaped by perceived system integrity [20]. Lastly, the inclusion of digital literacy as a moderator offers a contextual refinement to trust formation models, reflecting the growing complexity of user heterogeneity in fintech ecosystems [39]. The mediating role of customer trust (H3) underscores its position as a central conduit through which cybersecurity strategies influence user evaluations. This partial mediation indicates that while cybersecurity features may directly enhance perceptions of service quality, a significant portion of their impact is transmitted psychologically through trust. This aligns with the Information Systems Success Model [9], which posits that system characteristics must translate into user beliefs before affecting service evaluations. From a behavioral standpoint, cybersecurity measures reduce perceived vulnerability and signal organizational integrity, which are key antecedents of trust [38]. This suggests that platforms should not only implement robust security protocols but also actively communicate them to foster trust and, by extension, service quality.

The moderating effect of digital literacy (H4) further strengthens the model's explanatory power by highlighting user heterogeneity in trust formation. The significance of this interaction indicates that cybersecurity strategies are more effective in building trust among digitally literate users. This supports prior work suggesting that literate users possess better cognitive schemas to evaluate technological cues [20, 46]. These users are more likely to recognize the relevance of multi-factor authentication, data protection policies, and real-time alerts, interpreting them as credible signals of platform reliability. In contrast, less digitally literate users may overlook or misinterpret these features, dampening their trust response. This insight has profound implications for user segmentation and interface design: fintech firms may need to tailor security communication differently for users with varying digital proficiencies to ensure that trust-enhancing mechanisms are uniformly effective.

From a practical standpoint, the findings emphasize the need for fintech providers like STC Pay to treat cybersecurity as a user-facing quality attribute, not just a backend compliance requirement. Communicating security protocols clearly and making security features visible can significantly enhance customer trust, especially among digitally literate users. Service design teams should integrate security cues—such as padlock symbols, biometric options, and real-time alerts—into the user interface to reinforce perceptions of safety [17]. Furthermore, digital literacy should be treated as a strategic capability. Firms and regulators alike must invest in user education campaigns that empower individuals to understand and interpret digital security protocols, thereby amplifying the impact of organizational cybersecurity investments [30]. At the policy level, these insights support initiatives by SAMA and other financial regulators to make digital trust and security a pillar of fintech governance. Policies that mandate transparent security disclosures, user education programs, and interface-level protections can enhance not only compliance but also customer loyalty and service satisfaction [3]. As Saudi Arabia transitions toward a digital-first financial ecosystem, ensuring that security protocols resonate with users' perceptions will be essential to maintaining public trust and long-term platform engagement.

6. CONCLUSIONS

This study set out to examine the influence of cybersecurity strategies on perceived service quality in a digital payment context, using STC Pay in Saudi Arabia as a case example. The findings reveal that cybersecurity strategies have a significant direct effect on customer trust (β = 0.48, p < .001), confirming the central role of security perceptions in shaping user confidence in digital platforms [17]. In turn, customer trust was found to influence perceived service quality positively (β = 0.52, p < .001), underscoring the mediating role of trust as a psychological mechanism linking system features to service evaluations [9]. Additionally, digital literacy was shown to moderate the relationship between cybersecurity strategies and trust, suggesting that the impact of security cues is contingent on users' ability to interpret and evaluate digital risk [30, 39]. These findings collectively support the hypothesized framework and validate the integration of cybersecurity and trust models in the context of financial technology services. The study makes several important contributions to theory and practice. Theoretically, it extends the DeLone and McLean [9] Information Systems Success Model by introducing cybersecurity strategies as a critical antecedent of service quality, mediated by trust. This supports the growing recognition of security as a value-generating mechanism, not merely a technical function [11]. Furthermore, by incorporating digital literacy as a moderator, the study responds to recent calls in IS research for more nuanced models that capture user heterogeneity and its impact on technology perception [8]. Practically, the study provides fintech providers and regulators with evidence-based insights into how cybersecurity investments can be leveraged to enhance user experience, platform credibility, and service evaluations—particularly in digitally evolving economies like Saudi Arabia [3]. Despite its contributions, the study has certain limitations that should be acknowledged.

First, the use of a cross-sectional survey design limits the ability to infer causality. While SEM provides a robust framework for testing directional relationships, future studies may benefit from longitudinal designs to capture dynamic changes in trust and service perceptions over time [40]. Second, although the sample of 370 participants provided adequate statistical power, the study focused exclusively on STC Pay users in urban Saudi Arabia, potentially limiting the generalizability of findings to other platforms or less digitally literate populations [4]. Third, while the study relied on validated measurement instruments, all data were self-reported, which may introduce common method variance [47]. Building on these limitations, there are several future research directions. Researchers could explore comparative studies across different fintech platforms or regions to assess whether the effects of cybersecurity on trust and service quality are culturally or technologically contingent.

Additionally, qualitative methods such as interviews or focus groups could be used to delve deeper into users lived experiences and interpretations of cybersecurity features, thereby complementing the survey-based approach adopted here [32, 48]. Future models could also include additional moderating variables such as privacy concerns, perceived risk, or regulatory awareness to enrich the understanding of user evaluations in fintech ecosystems [21, 30, 48]. Lastly, as the fintech landscape continues to evolve, researchers may investigate how emerging technologies such as blockchain, biometric authentication, or AI-driven fraud detection influence the cybersecurity-trust-quality nexus [49].

7. LIMITATIONS AND FUTURE RESEARCH

Despite its contributions, this study is not without limitations. First, its cross-sectional design constrains the ability to establish causal relationships over time. Longitudinal research would be valuable to track how customer trust and perceptions of service quality evolve in response to cybersecurity improvements. Second, the exclusive focus on STC Pay limits the generalizability of findings across different fintech platforms or regions with varying regulatory environments. Comparative studies involving multiple service providers or cross-country settings could enrich the understanding of contextual influences. Third, the reliance on self-reported data introduces the potential for common method variance, despite efforts to ensure anonymity and item clarity. Future research may benefit from using mixed-method approaches, such as incorporating qualitative interviews to uncover nuanced user interpretations of cybersecurity cues. Additionally, exploring other moderating variables—such as privacy concerns, regulatory awareness, or cultural dimensions—can provide a more granular view of trust formation mechanisms in digital financial ecosystems [2, 50]. As technologies like blockchain and AI continue to reshape fintech infrastructures, examining their trust-building capabilities through cybersecurity-enhanced interfaces offers an exciting avenue for continued investigation. Lastly, researchers can consider deploying review methods (e.g., systematic reviews, critical reviews) to come up with meaningful insights via synthesis of the domain [51-53].

REFERENCES

[1] Al-Emran, M., Mezhuyev, V., Kamaludin, A. (2020). Technology Acceptance Model in M-learning context: A systematic review. Computers & Education, 125: 389-412. https://doi.org/10.1016/j.compedu.2018.06.008

[2] Tian, H., Siddik, A.B., Pertheban, T.R., Rahman, M.N. (2023). Does fintech innovation and green transformational leadership improve green innovation and corporate environmental performance? A hybrid SEM–ANN approach. Journal of Innovation & Knowledge, 8(3): 100396. https://doi.org/10.1016/j.jik.2023.100396

[3] Thottoli, M.M. (2024). The tactician role of FinTech in the accounting and auditing field: A bibliometric analysis. Qualitative Research in Financial Markets, 16(2): 213-238. https://doi.org/10.1108/QRFM-11-2021-0196

[4] Baabdullah, A.M., Alalwan, A.A., Rana, N.P., Kizgin, H., Patil, P. (2019). Consumer use of mobile banking (M-Banking) in Saudi Arabia: Towards an integrated model. International Journal of Information Management, 44: 38-52. https://doi.org/10.1016/j.ijinfomgt.2018.09.002

[5] Kocher, M.G., Sutter, M. (2006). Time is money—Time pressure, incentives, and the quality of decision-making. Journal of Economic Behavior & Organization, 61(3): 375-392. https://doi.org/10.1016/j.jebo.2004.11.013

[6] Shin, D.H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers, 22(5): 428-438. https://doi.org/10.1016/j.intcom.2010.05.001

[7] Papadopoulou, P., Andreou, A., Kanellis, P., Martakos, D. (2001) Trust and relationship building in electronic commerce. Internet Research, 11(4), 322-332. https://doi.org/10.1108/10662240110402777

[8] 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

[9] DeLone, W.H., McLean, E.R. (2003). The DeLone and McLean model of information systems success: A ten-year update. Journal of Management Information Systems, 19(4): 9-30.

https://doi.org/10.1080/07421222.2003.11045748

[10] Tallon, P.P. (2008). Inside the adaptive enterprise: An information technology capabilities perspective on business process agility. Information Technology and Management, 9(1): 21-36. https://doi.org/10.1007/s10799-007-0024-8

[11] Dutta, A., McCrohan, K.F. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1): 67-87. https://doi.org/10.2307/41166154

[12] Straub, D.W., Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(4): 441-469. https://doi.org/10.2307/249551

[13] Siponen, M., Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5): 267-270. https://doi.org/10.1016/j.im.2008.12.007

[14] Workman, M., Bommer, W.H., Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6): 2799-2816. https://doi.org/10.1016/j.chb.2008.04.005

[15] Teo, T.S.H., Srivastava, S.C., Jiang, L. (2008) Trust and electronic government success: An empirical study. Journal of Management Information Systems, 25(3): 99-132. https://doi.org/10.2753/MIS0742-1222250303

[16] Riggins, F.J., Rhee, H.S. (1998). Toward a unified view of electronic commerce. Communications of the ACM, 41(10): 88-95. https://dl.acm.org/doi/pdf/10.1145/286238.286252.

[17] Bélanger, F., Hiller, J.S., Smith, W.J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. The Journal of Strategic Information Systems, 11(3-4): 245-270. https://doi.org/10.1016/s0963-8687(02)00018-5

[18] Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1): 70-104. https://doi.org/10.1080/10864415.2004.11044320

[19] Mayer, R.C., Davis, J.H., Schoorman, F.D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3): 709-734. https://doi.org/10.5465/amr.1995.9508080335

[20] Ng, W. (2012). Can we teach digital natives digital literacy? Computers & Education, 59(3): 1065-1078. https://doi.org/10.1016/j.compedu.2012.04.016

[21] 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

[22] Chen, S.C., Dhillon, G.S. (2003). Interpreting dimensions of consumer trust in e-commerce. Information Technology and Management, 4(2): 303-318. https://doi.org/10.1023/A:1022962631249

[23] Jarvenpaa, S.L., Tractinsky, N., Vitale, M. (2000). Consumer trust in an Internet store. Information Technology and Management, 1(1-2): 45-71. https://doi.org/10.1023/A:1019104520776

[24] Zeithaml, V.A., Parasuraman, A., Malhotra, A. (2002). Service quality delivery through web sites: A critical review of extant knowledge. Journal of the Academy of Marketing Science, 30(4): 362-375. https://doi.org/10.1177/009207002236911

[25] Yang, Z., Fang, X. (2004). Online service quality dimensions and their relationships with satisfaction: A content analysis of customer reviews of securities brokerage services. International Journal of Service Industry Management, 15(3): 302-326. https://doi.org/10.1108/09564230410540953

[26] Chiu, C.M., Hsu, M.H., Wang, E.T.G. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. Decision Support Systems, 42(3): 1872-1888. https://doi.org/10.1016/j.dss.2006.04.001

[27] Eshet, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. Journal of Educational Multimedia and Hypermedia, 13(1): 93-106. https://www.learntechlib.org/primary/p/4793/.

[28] Flavián, C., Guinalíu, M., Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. Information & Management, 43(1): 1-14. https://doi.org/10.1016/j.im.2005.01.002

[29] Kim, D.J., Ferrin, D.L., Rao, H.R. (2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. Information Systems Research, 20(2): 237-257. https://doi.org/10.1287/isre.1080.0188

[30] Warkentin, M., Gefen, D., Pavlou, P.A., Rose, G.M. (2002). Encouraging citizen adoption of e-government by building trust. Electronic Markets, 12(3): 157-162. https://doi.org/10.1080/101967802320245929

[31] Churchill, G.A., Iacobucci, D. (2006). Marketing Research: Methodological Foundations (9th ed.). Thomson South-Western.

[32] Creswell, J.W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

[33] Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. (2022). Multivariate Data Analysis (8th ed.). Cengage Learning.

[34] Saunders, M., Lewis, P., Thornhill, A. (2019). Research Methods for Business Students (8th ed.). Pearson.

[35] Dillman, D.A., Smyth, J.D., Christian, L.M. (2014). Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method (4th ed.). John Wiley & Sons.

[36] Bryman, A., Bell, E. (2015). Business Research Methods (4th ed.). Oxford University Press.

[37] Wright, K.B. (2005). Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. Journal of Computer-Mediated Communication, 10(3): JCMC1034. https://doi.org/10.1111/j.1083-6101.2005.tb00259.x

[38] McKnight, D.H., Choudhury, V., Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3): 334-359. https://doi.org/10.1287/isre.13.3.334.81

[39] Nunnally, J.C., Bernstein, I.H. (1994). Psychometric Theory (3rd ed.). McGraw-Hill, New York.

[40] Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M. (2021). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (3rd ed.). SAGE

Publications.

[41] Preacher, K.J., Hayes, A.F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behavior Research Methods, 40(3): 879-891. https://doi.org/10.3758/BRM.40.3.879

[42] Henseler, J., Ringle, C.M., Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1): 115-135. https://doi.org/10.1007/s11747-014-0403-8

[43] Kock, N., Lynn, G.S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. Journal of the Association for Information Systems, 13(7): 546-580. https://doi.org/10.17705/1jais.00302

[44] Fornell, C., Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1): 39-50. https://doi.org/10.2307/3151312

[45] Chin, W.W. (1998). The partial least squares approach to structural equation modeling. In Modern Methods for Business Research, pp. 295-336. Psychology Press.

[46] van Deursen, A.J.A.M., van Dijk, J.A.G.M. (2014). The digital divide shifts to differences in usage. New Media & Society, 16(3): 507-526. https://doi.org/10.1177/1461444813487959

[47] Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5): 879-903. https://doi.org/10.1037/0021-9010.88.5.879

[48] Büyüközkan, G., Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. Technological Forecasting and Social Change, 213: 123996. https://doi.org/10.1016/j.techfore.2025.123996

[49] Luu, T.J., Samuel, B.M., Jones, M., Barnes, J.C. (2025). Exploring how the Dark Triad shapes cybercrime responses. Personality and Individual Differences, 244: 113250. https://doi.org/10.1016/j.paid.2025.113250

[50] Lallmahomed, M.Z.I., Lallmahomed, N., Lallmahomed, G.M. (2017). Factors influencing the adoption of e-Government services in Mauritius. Telematics and Informatics, 34(4): 57-72. https://doi.org/10.1016/j.tele.2017.01.003

[51] Bhaskar, R., Li, P., Bansal, S., Kumar, S. (2023). A new insight on CEO characteristics and corporate social responsibility (CSR): A meta-analytical review. International Review of Financial Analysis, 89: 102815. https://doi.org/10.1016/j.irfa.2023.102815

[52] Khan, F.M., Rasul T., Ahmed S.S., Ladeira, W.J., et al. (2025). Cultural values in consumer-centric research: A hybrid review exploring trends, structure, and future research trajectories. Global Business and Organizational Excellence. https://doi.org/10.1002/joe.70012

[53] Akbar, H., Pillai, M., Khan, F.M., Anas, M. (2025). Talent management: A review and research agenda. Global Business and Organizational Excellence, 45(1): 125-135. https://doi.org/10.1002/joe.70008