Journal of Risk Analysis and Crisis Response, 2026, 16(1), 19-42
https://jracr.com/
ISSN Print: 2210-8491
ISSN Online: 2210-8505

Article

Building Consumer Trust in Fintech: The Influence of Digital Risk, Technology Dependence, and Cybersecurity

Anggun Anggita Kinasih Sunowo Putri [1,*], Hafizh Fitrianna [2], Arif Siaha Widodo [3] and Fitriani [4]

[1] Department of Management, Faculty Business and Law, Universitas PGRI Yogyakarta, Yogyakarta (55182), Indonesia
[2] Department of Management, Faculty of Economics and Business, Universitas Negeri Yogyakarta, Yogyakarta (55281), Indonesia
* Correspondence: anggun.anggita@upy.ac.id

Received: June 30, 2025; Received in revised form: October 31, 2025; Accepted: March 21, 2026; Available online: March 31, 2026

Abstract: The growth of fintech services in emerging markets has accelerated financial inclusion while simultaneously introducing digital risks that may compromise consumer trust. This study investigates how perceived digital risks, technology dependence, and cybersecurity perceptions influence user trust in fintech platforms. Drawing from the Technology Acceptance Model (TAM) and Perceived Risk Theory, the research analyses responses from Indonesian fintech users using Structural Equation Modelling (SEM) via AMOS. The data were collected in May 2025 through an online survey. Out of 300 questionnaires distributed, 284 were returned and 250 were valid for analysis. The findings indicate that emerging risks and technology dependence significantly shape both cybersecurity perceptions and trust in digital financial platforms. Additionally, cybersecurity itself exerts a direct and statistically significant influence on consumer trust. Hypothesis testing results confirm that all proposed hypotheses (H1–H7) are supported, indicating that trust in fintech is simultaneously shaped by user perceptions of risk, technology dependence, and cybersecurity. These results suggest that trust in fintech is driven by both user perceptions of risk and the perceived strength of platform-level security systems. Practically, the study urges fintech providers to adopt transparent and user-centric security strategies, and encourages regulators to prioritize digital literacy and robust cybersecurity governance in the rapidly evolving fintech landscape.

Keywords: Emerging Digital Risk; Technology Dependence; Perceived Security Risk; Cybersecurity; Consumer Trust

1. Introduction

In recent years, the adoption of technology-based financial services (fintech) has grown rapidly in developing countries such as Indonesia. Platforms like GoPay, OVO, and DANA have facilitated daily financial transactions and management for the general population, while simultaneously promoting financial inclusion and the transition toward a cashless society [1]. However, this growth has also been accompanied by significant risks, including data breaches, identity theft, and cyberattacks, which threaten both consumer trust and the integrity of financial systems [2,3]. To mitigate these risks, solutions such as investments in cybersecurity infrastructure, cyber insurance, and a deeper understanding of user characteristics are essential for developing adaptive security

systems and maintaining consumer trust-an element vital to the long-term success of the fintech sector [1,2,4].

Consumer trust plays a critical role in driving the adoption and retention of digital services, as perceptions of security and service reliability directly influence user decision making [5]. In today's complex digital landscape, cybersecurity risks pose a major challenge that can erode trust particularly when consumers doubt the protection of their personal data [6]. Transparency in security policies and practices has been shown to alleviate consumer anxiety and strengthen confidence in digital platforms [2,5]. The implementation of advanced technologies such as blockchain has demonstrated considerable potential in enhancing data privacy and integrity [7], while a structured incident management approach contributes to a sense of safety and enhances the service provider's reputation [6,8]. Therefore, digital service providers must take strategic steps, including collaboration with cybersecurity experts and open communication about data protection practices, to foster trust and sustainably mitigate cyber risks [9,10].

Although numerous studies have highlighted the importance of consumer perceptions of data security, usage frequency, and digital risk awareness in shaping trust toward fintech services, there remains a significant gap in understanding the mediating mechanisms that bridge perceived risk and consumer trust. Most prior research has concentrated on the direct relationships between these variables, while relatively few have explored how specific cybersecurity practices such as data encryption, protocol transparency, and incident response systems function as critical mediators in trust formation. These technical aspects are often key benchmarks for consumers when assessing the credibility of fintech service providers, particularly among risk conscious users [11,12,13]. Furthermore, although frequent service usage is believed to foster familiarity and trust, direct experience without adequate security mechanisms may not suffice to generate sustained user loyalty. Therefore, there is an urgent need for research frameworks that explicitly integrate cybersecurity practices as mediating variables to better capture the dynamics of trust formation in the context of fintech adoption [6,14,15]. This gap presents a critical opportunity for empirical investigation that emphasizes the strategic role of cybersecurity as a foundational pillar of consumer trust in an increasingly complex digital era.

Building on this background, the present study aims to examine the influence of emerging risks, digital platform dependency, and data security perception on consumer trust, while analyzing the mediating role of cybersecurity in these relationships. The urgency of this investigation is particularly relevant in the context of Indonesia, a developing country experiencing rapid fintech adoption yet facing significant challenges in digital literacy and personal data protection. The absence of robust regulations and uneven consumer awareness regarding digital security further accentuate the critical need to strengthen cybersecurity as a foundation for consumer trust. To address these challenges, this study explores how digital risks, perceived security, and technology dependence influence consumer trust in fintech platforms, while highlighting the strategic importance of cybersecurity in trust formation. By applying the Technology Acceptance Model and Perceived Risk Theory in the context of Indonesia's emerging fintech landscape, this research contributes to a deeper understanding of how users perceive and respond to security-related threats in digital financial services. The study aims to provide empirical insights that support the development of trust-based strategies for fintech providers and regulators in developing economies.

While prior research has extensively examined the direct impact of perceived risk and technology usage on consumer trust, few have explored the strategic function of cybersecurity within these relationships. Unlike previous studies that treat cybersecurity merely as an external safeguard or control variable, this study uniquely positions it as a mediating construct that channels the effects of digital risk, security perception, and technology dependence toward consumer trust in fintech services. This theoretical positioning allows us to uncover indirect trust-building mechanisms embedded in user experiences with security systems. Moreover, by contextualizing the analysis within an emerging market, Indonesia, where regulatory frameworks and digital literacy remain uneven, this study contributes empirical insights into how cybersecurity mediates risk and trust in underexplored digital ecosystems. This dual contribution both conceptual and contextual marks a distinct advancement in the digital trust literature.

Despite extensive research on consumer trust in fintech adoption, limited attention has been paid to how perceived digital risk and technology dependence jointly shape perceptions of cybersecurity and, consequently, consumer trust. Prior studies have largely treated the Technology Acceptance Model (TAM) and the Perceived Risk Theory (PRT) as parallel frameworks, focusing separately on either technological determinants or risk-related inhibitors of trust [16,17]. This study advances the literature by integrating TAM and PRT through the mediating role of perceived cybersecurity, thereby explaining how risk cognition and technology dependence interact to build user trust in fintech services [18,19]. Unlike earlier work that treats cybersecurity merely as an external system attribute or technical safeguard, this research positions it as a central psychological mechanism that translates users' awareness of digital risks into trust formation [20]. Theoretically, this integration contributes a risk-embedded technology trust model applicable to emerging economies; practically, it offers actionable guidance for fintech providers and regulators to enhance consumer confidence through transparent, user-centric, and security-assured digital ecosystems.

2. Literature Review

In recent years, fintech services have expanded rapidly across developing economies, including Indonesia, improving financial inclusion while simultaneously increasing exposure to digital risks such as data breaches and cyberattacks [21,22]. These risks have heightened consumer awareness of security and privacy concerns, making trust a central factor in fintech adoption. To explain how users evaluate and adopt financial technologies under conditions of digital uncertainty, this study employs two complementary frameworks: the Technology Acceptance Model (TAM) and the Perceived Risk Theory (PRT).

To understand consumer behavior in adopting digital technologies, the Technology Acceptance Model (TAM) and Perceived Risk Theory provide two complementary theoretical frameworks. TAM posits that perceived usefulness and ease of use are strong determinants of individuals' intention to adopt technology. When trust in the system is high, these factors further encourage the adoption of digital financial services [23]. Conversely, Perceived Risk Theory explains that heightened risk perception can diminish behavioral intention, necessitating strategies to mitigate such perceptions in the adoption process [24]. In this context, cybersecurity plays a vital role in reducing perceived risk, as security assurances have been shown to enhance trust and strengthen consumer commitment to digital platforms [25]. Consumer trust itself acts as a mediator that reinforces the relationship between perceived usefulness, security, and adoption intention. This finding is consistent with studies in other

domains such as vehicle infotainment systems where data security perceptions emerge as a primary determinant of usage intention [24]. Furthermore, comprehensive cybersecurity design can serve as a crucial mechanism for fostering trust and reducing perceived risks, as emphasized by [26]. External factors also contribute technology adoption. For example, corporate responsibility (CSR) initiatives have been found to positively influence adoption by enhancing consumer trust [27]. Taken together, these findings suggest that trust shaped by both security perceptions and social values serves as a foundational driver of digital technology adoption in today's increasingly complex environment.

Recent empirical studies confirm that consumer trust is a key factor in the adoption of fintech services because it directly influences users' intentions and decisions to use digital financial technology [28,29]. This trust is multifaceted, encompassing dimensions of security, transparency, cultural acceptance, and provider credibility [30].Technical aspects such as security and transparency have been shown to be foundational to building trust and driving competitiveness [28], while trust has a significant influence on users' behavioral intentions in using digital payment systems [29]. The integration of trust into technology adoption models also directly contributes to fintech adoption decisions [30]. Cultural factors also influence consumer trust, so adoption strategies need to align with societal norms [31,32]. Furthermore, company size and reputation can increase trust levels, although this is not universally true [33].The COVID-19 pandemic has further emphasized the importance of trust, as consumers have become more aware of digital risks and the need for comprehensive protection, which ultimately determines their level of engagement with fintech innovations [34,35].

2.1. Integration of TAM and Perceived Risk Theory

While the Technology Acceptance Model (TAM) emphasizes rational and cognitive factors such as perceived usefulness and ease of use, the Perceived Risk Theory (PRT) focuses on affective responses to uncertainty and potential loss. In fintech adoption, these two perspectives are complementary rather than competing. Consumers' acceptance of digital finance depends not only on the functional benefits of the technology but also on how secure and trustworthy they perceive the system to be [36,37].

This study integrates TAM and PRT through the mediating role of cybersecurity perception, which functions as a bridge connecting risk appraisal and technology-based trust. Specifically, perceived digital risks and technology dependence shape users' evaluations of cybersecurity strength representing their confidence in the system's reliability, transparency, and protection mechanisms [38,39,40]. This, in turn, reinforces consumer trust, aligning with TAM's postulate that perceived system quality drives behavioral intention.

Hence, the integration presented here does not require structural alteration of the TAM model but extends its explanatory scope by embedding risk-based cognition and cybersecurity assurance. The resulting conceptual framework termed a *risk-embedded technology trust model* captures how digital risk perception interacts with technology dependence to influence consumer trust in fintech services.

2.2. Emerging Risks in Relation to Cybersecurity and Consumer Trust

The growing threats within the digital landscape, such as phishing, malware, and data theft underscore the urgent need for information system protection in the digital financial ecosystem,

particularly within the fintech sector, which is highly susceptible to both technical vulnerabilities and users' psychological concerns. As users become increasingly aware of digital risks that may jeopardize their personal data and financial transactions, expectations for robust security infrastructures also rise. Consequently, risk perception emerges as a primary driver of demand for enhanced security measures [41,42]. In this context, the interaction between consumer trust and perceived risk becomes especially critical, as trust in financial services is strongly influenced by perceptions of data security and privacy policies [22,23].

Perceptions of digital threats play a crucial role in how users evaluate the effectiveness of cybersecurity systems implemented by digital platforms. A study indicates that increased user concern over digital attacks can positively influence their perception of security systems[43], particularly when those systems are perceived as active and transparent. In the context of fintech services, research in the United Arab Emirates confirms that perceived risk leads users to place greater value on the cybersecurity features provided by service platforms [44]. These findings suggest a positive relationship between risk perception and the evaluation of security feature quality and effectiveness. Moreover, involving users in open and transparent risk management processes enhances their positive perception of the platform. Thus, perceived risk serves as a key driver of user responsiveness, whereby higher perceived risks increase user demand for effective and credible cybersecurity systems.

From the perspective of consumer trust, perceptions of digital risk also have significant implications for the level of trust in digital services themselves. It has been demonstrated that without adequate mitigation measures, users' trust in a platform may decline sharply, subsequently affecting their intention and decision to continue using the service [45]. Although this effect may diminish among more experienced users or platforms with established reputations [46], perceived risk remains a psychological factor that cannot be overlooked. In this regard, a robust and demonstrably effective security system in managing and communicating risks can serve as a critical bridge for building user trust. It also emphasizes that in the context of Islamic banking, effective risk management in fintech is vital for maintaining user trust amid emerging digital threats [44]. Therefore, the combination of clearly defined security features and transparency in operational practices constitutes a crucial strategy for reducing perceived risk and reinforcing consumer trust in digital services.

These insights indicate that digital risks do not only generate concern but also stimulate users' awareness toward security mechanisms, highlighting their indirect contribution to trust formation through cybersecurity perception.

Based on the theoretical foundation and consistent empirical findings, the following hypotheses are proposed:

Hypothesis 1: *Emerging risks have a positive and significant effect on cybersecurity.*

Hypothesis 2: *Emerging risks have a positive and significant effect on consumer trust.*

2.3. Perceived Security Risk in Relation to Cybersecurity and Consumer Trust

Perceived security risk refers to an individual's subjective assessment of potential losses or threats to personal data during digital interactions. This concept plays a vital role in shaping user behavior, including their willingness to share information online. Studies have shown that high levels of perceived risk can inhibit the adoption of technologies such as virtual shopping, electronic medical records, and cloud computing [47,48,49]. Therefore, enhancing transparency and information

security is crucial for building trust and encouraging participation in the continuously evolving digital ecosystem.

Users perceived security risk is a key factor in shaping their perception of the effectiveness of cybersecurity systems on digital platforms. When individuals become aware of potential threats such as data breaches and cyberattacks, they tend to be more critical in evaluating the security features offered, including multi-factor authentication, encryption protocols, and transparent privacy policies [50,51]. Interestingly, this perceived security risk does not necessarily lead to negative outcomes; on the contrary, it can foster greater appreciation for robust and responsive security infrastructures. Systems that are perceived as resilient in managing cyber threats contribute to more favorable perceptions of a platform's readiness to handle digital vulnerabilities, ultimately enhancing the technical legitimacy and credibility of service providers [52,53]. Therefore, higher perceived risk increases user demand and expectation for effective cybersecurity, directly shaping how digital security systems are evaluated.

In addition, perceived security risk also plays a vital role in shaping and reinforcing users' trust in digital services. When users believe that a service provider has adequate and trustworthy data protection mechanisms in place, they are more likely to adopt a positive attitude and maintain sustained usage of the service [41]. This trust is further strengthened by users' perceptions of the provider's commitment to safeguarding information privacy and offering transparent communication regarding security policies. Clear and consistent explanations about data management practices help alleviate user fears and foster stronger confidence in the integrity of digital services [24,46]. For instance, transparency in communicating security policies coupled with active user participation in protecting personal information can create a strong reciprocal relationship that enhances trust and reduces concerns over cyber risks [51,54] Thus, a risk management strategy that addresses not only technical aspects but also emphasizes communication and user engagement is essential for building long term trust in today's increasingly complex digital landscape [55].

Therefore, perceived security risk acts as a cognitive lens that connects users' assessment of data protection to the formation of trust in fintech services.

Based on the theoretical arguments and consistent empirical support, the following hypotheses are proposed:

Hypothesis 3: *Perceived security risk has a positive and significant effect on cybersecurity.*

Hypothesis 4: *Perceived security risk has a positive and significant effect on consumer trust.*

2.4. Technology Dependence in Relation to Cybersecurity and Consumer Trust

Technology dependence refers to the increasing duration and intensity of individual interactions with technology-based services, particularly fintech applications. In this context, it is argued within the framework of the Unified Theory of Acceptance and Use of Technology (UTAUT), argues that such dependence is closely linked to perceived usefulness, performance expectations, and repeated positive user experiences [56]. This indicates that the presence of fintech services not only facilitates financial transactions but also becomes an integral part of individuals' daily routines, as practicality and ease of access serve as key drivers behind continued usage [57].

Technology dependence, particularly in the context of fintech applications, significantly increases user expectations regarding cybersecurity. As usage frequency rises, users become more sensitive to data protection infrastructure and potential cyber risks. It has been found that users with

frequent interactions and a better understanding of data security tend to perceive fintech systems as more secure, thereby enhancing their security perception in parallel with their engagement with the platform [23]. In line with this, it is asserted heightened awareness of potential cyber threats leads consumers to value the protection systems provided, reinforcing positive perceptions of the platform's preparedness to counter digital threats [12]. Thus, greater dependence on digital platforms increases user expectations and positive perceptions of cybersecurity effectiveness. This relationship becomes a critical factor in the development of sustainable protection systems by service providers.

On the other hand, technology dependence also plays a crucial role in shaping users' trust in fintech services. When users consistently experience relevant and tangible benefits from using an application, they tend to perceive the platform as possessing a high level of integrity and professionalism [58]. Repeated interactions foster positive experiences that reinforce trust in the reliability and quality of services, even in the presence of ongoing digital risks. Although there are concerns that excessive digital usage may lead to fatigue, within the fintech sector closely tied to users' economic and financial needs, the relationship between usage and trust remains largely positive and productive. Moreover, cybersecurity awareness further strengthens this trust; when users are aware that a platform actively manages digital threats, they are more likely to develop greater loyalty and long-term commitment [12]. Therefore, dependence on digital services not only enhances users' perceptions of security but also directly contributes to building trust and deeper engagement within the fintech ecosystem.

Accordingly, technology dependence strengthens the link between user experience and trust, emphasizing the mediating role of cybersecurity in this process.

Based on the conceptual foundation and empirical evidence, the following hypotheses are proposed:

Hypothesis 5: *Technology dependence has a positive and significant effect on cybersecurity.*

Hypothesis 6: *Technology dependence has a positive and significant effect on consumer trust.*

2.5. The Effect of Cybersecurity on Consumer Trust

Cybersecurity encompasses technical measures, policies, and training designed to protect systems and data from digital threats [50,59]. In digital sectors such as fintech, the effectiveness and transparency of security mechanisms play a critical role in shaping user trust [12]. Trust is fostered when users perceive their data to be secure and when companies are proactive and transparent in addressing risks [52]. Therefore, investing in security infrastructure and user education is not only essential for protecting data but also serves as a fundamental pillar in building trust and ensuring the long-term sustainability of digital services.

User trust in digital services is strongly influenced by perceptions of information security, with cybersecurity functioning as a key determinant of this confidence. It is demonstrated that data security not only drives the intention to adopt fintech services but also strengthens user trust, particularly when service providers communicate security measures transparently [23]. This finding highlights that cybersecurity is not merely a technical component but also a reflection of a company's commitment to consumer protection. Furthermore, it is emphasized that regardless of varying levels of digital literacy, effective and trustworthy security systems form the core foundation for building long-term trust [60]. More broadly, proactive monitoring of transactions and prompt incident response are critical in enhancing perceptions of reliability. It is also highlighted that a company's

commitment to security particularly when reinforced through corporate social responsibility (CSR) initiatives can further bolster user loyalty and trust in digital platforms [61]. Based on these insights, the following hypothesis is proposed:

Hypothesis 7: *Cybersecurity has a positive and significant effect on consumer trust.*

Building upon the theoretical integration of TAM and Perceived Risk Theory (PRT), this study conceptualizes a sequential causal chain linking digital risk, technology dependence, cybersecurity, and consumer trust. Digital risk and technology dependence represent antecedent variables that shape users' perceptions of cybersecurity, as individuals who face higher levels of perceived digital threats or who are more reliant on fintech technologies are likely to pay greater attention to data protection and system transparency [12,23,42,44]. Cybersecurity, in turn, functions as a mediating construct that translates these antecedent perceptions into trust-related outcomes [6,23,50]. This mechanism aligns with TAM's cognitive pathway, where perceived system quality influences behavioral intention [16,62] and extends it with PRT's emphasis on emotional assurance [24,17]. Consequently, consumer trust emerges as the final behavioral and psychological outcome of users' risk evaluation and confidence in cybersecurity mechanisms [12,23,45,60]. This theoretical chain clarifies the directional logic of the model, positioning cybersecurity as the bridge that connects risk cognition, technology interaction, and trust formation in the fintech context.

While the proposed relationships are theorized as positive and linear for analytical clarity, prior studies acknowledge that these associations may not always manifest uniformly across contexts. For instance, heightened exposure to digital risk can initially increase awareness and demand for cybersecurity but may also generate anxiety or distrust when risk perceptions exceed users' tolerance thresholds [12,23,45]. Similarly, excessive technology dependence can lead to cognitive fatigue or privacy concerns, thereby diminishing trust beyond a certain point [42,60]. These potential non-linear and conditional dynamics suggest that the current model represents an idealized structure aimed at isolating primary effects, while acknowledging the possibility of more complex behavioral responses that future research could further investigate.

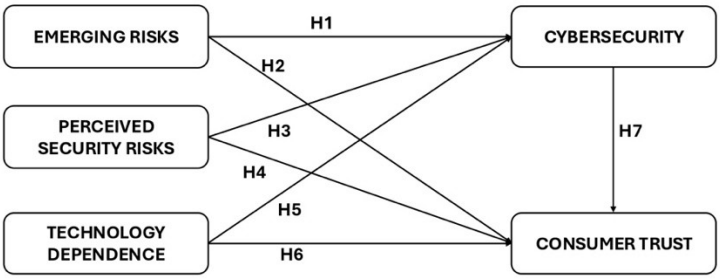

Figure 1. Conceptual Model (Source: Authors' work).

3. Research Methodology

This study employed a quantitative approach, utilizing data collected through an online questionnaire distributed via Google Forms. The survey link was voluntarily distributed via WhatsApp. Respondents were selected using non-probability purposive sampling, which targeted individuals meeting specific criteria to ensure that participants have relevant experience with the use of fintech services. In this study, the selected respondents were individuals who had used fintech services such as digital wallets, online lending platforms, and investment applications for a minimum

period of three months. This criterion was established to ensure that all respondents had sufficient experience to provide accurate evaluations of the variables examined in the study [11,63].

3.1. Measurement of Variables and Indicators

The measurement of variables in this study was conducted using indicators adapted from prior literature and empirically validated in previous research (Table A1). The Emerging Risks variable was measured using six indicators covering perceptions of digital vulnerability, uncertainty, potential financial loss, concerns over personal data breaches, exposure to cyber fraud, and perceived insecurity during digital transactions [17,19]. The Technology Dependence variable was measured using six indicators covering service usage frequency, dependence on the platform, digital habits, preference for digital over manual services, integration into daily activities, and perceived necessity of the platform, based on previous research [62]. The Perceived Security Risk variable was measured using seven indicators encompassing trust in encryption systems, authentication protocols, data access controls, information sharing with third parties, compliance with privacy regulations, transparency in data management, and user control over consent, adapted from previous studies [20,64]. The Cybersecurity variable was measured using six indicators including the effectiveness of security infrastructure, detection response mechanisms, antifraud systems, protection against malware, incident transparency, and digital system resilience, adapted from previous research [65]. In this study, cybersecurity is conceptualized as a perceptual construct rather than a technical system outcome. It reflects respondents' cognitive and affective evaluations of how effectively fintech platforms protect their personal and financial data. Accordingly, cybersecurity is modelled as being influenced by emerging risks and technology dependence, reflecting how perceived digital threats and usage intensity heighten users' attention to data protection. In turn, perceived cybersecurity functions as a mediating variable that channels these antecedent perceptions into consumer trust. This conceptualization distinguishes between technical cybersecurity (system-level protection) and psychological cybersecurity (user perception of safety), ensuring theoretical clarity and preventing circularity between mediator and outcome constructs. Lastly, the Consumer Trust variable was assessed using six indicators covering perceptions of platform reliability, provider integrity, goodwill, service consistency with expectations, reputation, and users' past experiences, based on previous studies [66,67,16].

All indicators were measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree), to obtain consistent and accurate responses from participants. The quality of the measurement instrument was assessed through tests of reliability, convergent validity, and discriminant validity. Reliability was examined using Cronbach's Alpha and Composite Reliability (CR), with all constructs exceeding the threshold of 0.70 (CR values ranging from 0.83 to 0.93), indicating high internal consistency. Convergent validity was confirmed through factor loadings (all significant at $p < 0.001$) and Average Variance Extracted (AVE) values above 0.50, demonstrating that the variance among indicators was adequately captured by their respective constructs.

3.2. Data Analysis

This study employed Structural Equation Modelling (SEM) with AMOS software. AMOS was selected due to its strength in confirmatory factor analysis and its ability to test complex models involving multiple latent variables and observed indicators. The measurement model was evaluated

based on three main criteria: (1) internal reliability, measured using Cronbach's Alpha and Composite Reliability (CR) with thresholds of ≥ 0.70; (2) convergent validity, assessed through standardized factor loadings (≥ 0.70) and Average Variance Extracted (AVE > 0.50); and (3) model fit, determined using indices such as Chi-square/df, Root Mean Square Error of Approximation (RMSEA ≤ 0.08), Comparative Fit Index (CFI ≥ 0.90), and Tucker-Lewis Index (TLI ≥ 0.90) to ensure the adequacy of the proposed model.

4. Results

Data for this research were collected in May 2025 through an online survey involving 250 respondents who were users of digital financial services in Indonesia. The demographic analysis showed that the majority of participants were female (58.4%), while males accounted for 41.6%, indicating that women play an important role in fintech adoption. In terms of age, most respondents were between 26 and 35 years old (40.0%), followed by those aged 36–45 (27.6%), 18–25 (20.4%), and over 45 years (12.0%), showing that the survey primarily captured productive-age individuals who are typically active digital platform users.

From an educational perspective, the majority of respondents held a bachelor's degree (46.8%), followed by diploma holders (25.2%), high school graduates (19.2%), and those with a master's degree or higher (8.8%). This educational profile supports the view that digital and financial literacy are important prerequisites for fintech adoption. Regarding occupation, respondents were predominantly private-sector employees (40.4%), followed by entrepreneurs (28.0%), university students (13.6%), civil servants (10.0%), and a smaller proportion of freelancers or individuals without permanent employment. These trends reflect an economically active user base likely to integrate fintech solutions into daily routines.

In terms of income, the majority reported monthly earnings between IDR 3,000,000 and IDR 5,000,000 (35.2%), followed by IDR 1,500,000–3,000,000 (31.2%), above IDR 5,000,000 (21.6%), and below IDR 1,500,000. Fintech usage was high, with 94.8% of respondents reporting the use of at least one digital financial service. Digital wallets such as OVO, GoPay, Dana, and ShopeePay were the most frequently used (83.2%), followed by digital investment platforms like Bibit and Ajaib (46.0%) and online lending services (31.6%). These figures highlight the widespread adoption of fintech services across diverse demographic groups and emphasize the importance of examining how security and trust influence user engagement.

The results of the validity test conducted using AMOS are summarized in Table 1.

Based on Table 1, the validity test results involving 250 respondents and a total of 31 questionnaire items indicate that all items achieved a factor loading greater than 0.50.

Therefore, it can be concluded that all items in the questionnaire are valid and appropriate for further analysis.

Table 1. Validity test.

Variable	Indicator	Loading Factor	Limit	Description
Emerging Risks	ER1	0.801	> 0.5	Valid
Emerging Risks	ER2	0.765	> 0.5	Valid
Emerging Risks	ER3	0.746	> 0.5	Valid
Emerging Risks	ER4	0.719	> 0.5	Valid

Variable	Indicator	Loading Factor	Limit	Description
Emerging Risks	ER5	0.765	> 0.5	Valid
Emerging Risks	ER6	0.726	> 0.5	Valid
Perceived Security Risk	PSR1	0.913	> 0.5	Valid
Perceived Security Risk	PSR2	0.856	> 0.5	Valid
Perceived Security Risk	PSR3	0.629	> 0.5	Valid
Perceived Security Risk	PSR4	0.948	> 0.5	Valid
Perceived Security Risk	PSR5	0.916	> 0.5	Valid
Perceived Security Risk	PSR6	0.876	> 0.5	Valid
Perceived Security Risk	PSR7	0.862	> 0.5	Valid
Technology Dependence	TD1	0.876	> 0.5	Valid
Technology Dependence	TD2	0.806	> 0.5	Valid
Technology Dependence	TD3	0.825	> 0.5	Valid
Technology Dependence	TD4	0.787	> 0.5	Valid
Technology Dependence	TD5	0.831	> 0.5	Valid
Technology Dependence	TD6	0.768	> 0.5	Valid
Cybersecurity	CS1	0.852	> 0.5	Valid
Cybersecurity	CS2	0.868	> 0.5	Valid
Cybersecurity	CS3	0.882	> 0.5	Valid
Cybersecurity	CS4	0.874	> 0.5	Valid
Cybersecurity	CS5	0.894	> 0.5	Valid
Cybersecurity	CS6	0.884	> 0.5	Valid
Consumer Trust	CT1	0.849	> 0.5	Valid
Consumer Trust	CT2	0.766	> 0.5	Valid
Consumer Trust	CT3	0.845	> 0.5	Valid
Consumer Trust	CT4	0.732	> 0.5	Valid
Consumer Trust	CT5	0.769	> 0.5	Valid
Consumer Trust	CT6	0.792	> 0.5	Valid

Table 2. Reliability test results.

Variable	CR	Limit	VE	Limit	Description
Emerging Risks	0.888	> 0.7	0.569	> 0.5	Reliable
Perceived Security Risk	0.953	> 0.7	0.744	> 0.5	Reliable
Technology Dependence	0.923	> 0.7	0.666	> 0.5	Reliable
Cybersecurity	0.952	> 0.7	0.767	> 0.5	Reliable
Consumer Trust	0.910	> 0.7	0.629	> 0.5	Reliable

Based on Tables 1 and 2, all questionnaire items are confirmed to be both valid and reliable. The next stage involves conducting a comprehensive analysis of the research model to test the proposed hypotheses. The results of the hypothesis testing are presented in Figure 2 and Table 3.

The corresponding structural relationships can be expressed as:

$$CS = \beta_1 ER + \beta_2 TD + \beta_3 PSR + \varepsilon_1$$

$$CT = \beta_4 ER + \beta_5 TD + \beta_6 PSR + \beta_7 CS + \varepsilon_2$$

where:

ER = Emerging Risks, TD = Technology Dependence, PSR = Perceived Security Risk, CS = Cybersecurity, CT = Consumer Trust, and ε denotes the residual terms.

The model demonstrated good fit indices (χ^2/df = 1.873, RMSEA = 0.047, CFI = 0.947, TLI = 0.932), meeting the recommended thresholds.

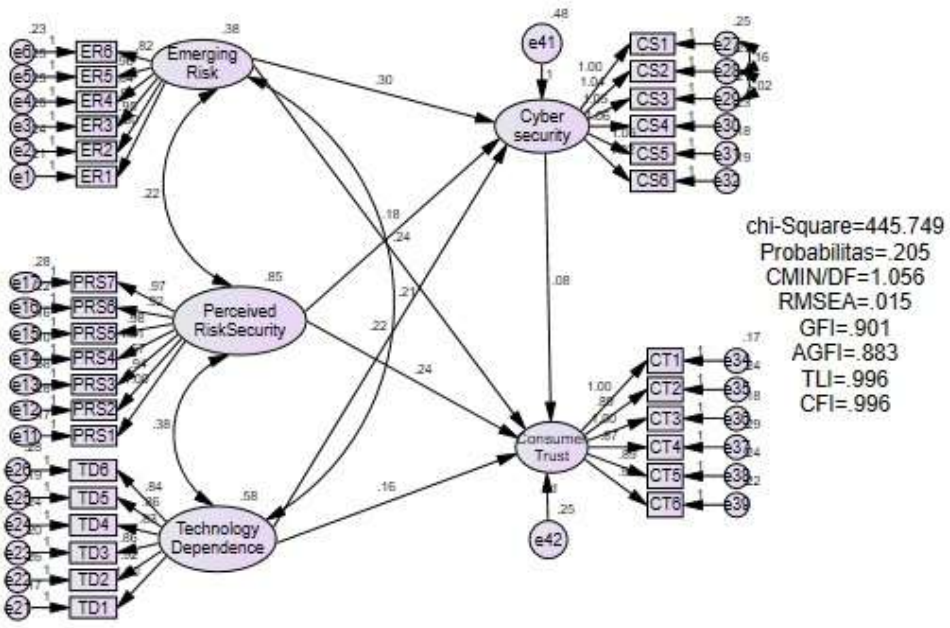

Figure 2. Full model analysis (Source: Authors' work).

Hypothesis testing was performed using t-statistic and p-value to determine whether the relationships between variables were positive and statistically significant. A relationship was considered positive and significant when the t-statistic exceeds 1.96 and the p-value was below 0.05 [48]. In the direct path analysis, all hypotheses from H1 to H7 showed p-values below 0.05 and t-statistics above 1.96, indicating that each path achieved statistical significance. Accordingly, the findings of this study confirm all the proposed hypotheses.

In addition to statistical significance, the practical implications were examined by analyzing the effect of each relationship. Hypothesis 1 (*Emerging Risks → Cybersecurity***)** showed an estimated effect size of 0.297, indicating a moderate effect and suggesting that perceived digital risks increase user attention to cybersecurity. This finding implies that heightened awareness of emerging risks activates users' vigilance toward protection mechanisms, aligning with Perceived Risk Theory, which posits that risk perception can motivate adaptive security behaviors rather than deterrence [44,45]. Hypothesis 2 (*Emerging Risks → Consumer Trust*) produced an estimate of 0.238, indicating that higher perceived risk strengthens consumer trust in digital platforms. This relationship reflects a cognitive transformation process in which users channel risk awareness into reliance on institutional safeguards, interpreting visible security assurances as evidence of system integrity and reliability [23,60]. Hypothesis 3 (*Perceived Security Risk → Cybersecurity***)** yielded an effect size of 0.181, showing that positive perception of data security significantly influences evaluations of cybersecurity system strength. This suggests that users who feel confident in data protection measures perceive stronger cybersecurity performance overall, consistent with the Technology Acceptance Model's emphasis on

perceived system usefulness and reliability [50,51]. Hypothesis 4 (*Perceived Security Risk → Consumer Trust*) recorded an effect size of 0.238, confirming that perceived data security also serves as a crucial foundation in building trust. From the lens of Perceived Risk Theory, this indicates that transparency and responsiveness in security communication help convert uncertainty into assurance, reinforcing emotional confidence in fintech platforms [24,46,54].

Table 3. Hypothesis Test Results.

No.	Hypothesis	Estimate	S.E.	C.R.	P	Result
H1	Emerging Risks → Cybersecurity	0.297	0.094	3.162	0.002	Supported
H2	Emerging Risks → Consumer Trust	0.238	0.073	3.252	0.001	Supported
H3	Perceived Security Risk → Cybersecurity	0.181	0.064	2.831	0.005	Supported
H4	Perceived Security Risk → Consumer Trust	0.238	0.050	4.744	0.000	Supported
H5	Technology Dependence → Cybersecurity	0.219	0.082	2.675	0.007	Supported
H6	Technology Dependence → Consumer Trust	0.161	0.063	2.539	0.011	Supported
H7	Cybersecurity → Consumer Trust	0.114	0.051	2.210	0.027	Supported

Hypothesis 5 (*Technology Dependence → Cybersecurity*) demonstrated an effect size of 0.219 indicating that frequent digital platform use contributes to higher demand for cybersecurity protection. This finding implies that greater interaction with fintech applications enhances user familiarity with protection systems, thereby strengthening their perception of cybersecurity reliability and preparedness [23,42,57]. Hypothesis 6 (Technology Dependence → Consumer Trust) yielded an effect size of 0.161, suggesting that repeated use of digital platforms enhances consumer trust, provided that adequate security is maintained. This outcome reflects a reinforcement loop in which repeated positive experiences with secure platforms develop habitual confidence, consistent with TAM's notion that consistent performance and perceived usefulness evolve into affective trust [12,58]. Finally, Hypothesis 7 (*Cybersecurity → Consumer Trust*) reported the smallest effect size at 0.114. While modest, this relationship was statistically significant, indicating that perceptions of cybersecurity still play a meaningful role in directly reinforcing consumer trust. This supports the argument that visible cybersecurity practices act as psychological assurance cues, transforming users' rational evaluation of safety into emotional commitment to continued usage [16,23,60].

Overall, the results of this study confirm that all the hypothesized relationships in this research model are mutually reinforcing both statistically and in practical terms. For digital service providers and policymakers, these findings underscore the importance of developing robust cybersecurity systems and fostering positive perception of data protection practices.

5. Discussion

The results indicate that emerging digital risks have a positive and significant impact on cybersecurity, reinforcing prior research on the importance of adaptive responses to cyber threats. The rising intensity of attacks such as phishing and malware has encouraged organizations to develop more resilient and proactive protection systems [68,69]. However, such risks are not inherently effective in driving cybersecurity improvements without sufficient user awareness. Low levels of digital literacy can undermine system effectiveness, as individuals often fail to recognize threats accurately [2,70]. Accordingly, digital risks should not be viewed solely as threats but also as strategic drivers of cybersecurity innovation. Previous studies further support this view, showing that risk awareness fosters favourable perceptions of data protection [71]and stimulates the development of sustainable security policies [72]. A responsive and integrated risk management approach is therefore essential for navigating the increasing complexity of the digital ecosystem [73].

The findings also confirm that perceived security risk significantly influences cybersecurity, consistent with studies emphasizing the importance of risk perception in shaping individual behaviour toward information security [74,75]. As digitalization intensifies, systems become increasingly vulnerable to attacks, making security perception a critical factor in both user and organizational responses. It has been found that trust in systems encourages openness in information sharing, although psychological factors still influence user caution [76]. Proactive strategies such as Engineering Chaos Security [77] and strengthening security culture through training, have also proven effective in enhancing resilience [78,79]. These findings reinforce the conclusion that perception-based and educational security strategies are essential to building adaptive and trustworthy systems capable of confronting evolving digital threats.

In addition, the study shows that perceived security risk plays a significant role in shaping consumer trust in digital platforms. This result align with prior research indicating that when users believe their data is securely managed and compliant with regulations, they perceive security measures as both effective and credible [80]. In a landscape marked by rising concerns over data breaches and cyberattacks, ensuring information security becomes increasingly important [81,82]. Negative experiences, such as data leaks or inadequate provider responses, can undermine trust and hinder engagement [68]. These findings highlight the need to cultivated positive security perceptions through robust protection policies and transparent communication, both of which are critical in fostering trust and sustaining adoption [13,83].

The study further reveals that technology dependence strongly influence perceptions of cybersecurity. Higher frequency and intensity of digital service elevate user expectations for reliable security systems. Consistent with prior studies, the result show that increased interaction within the digital ecosystem enhances sensitivity to potential security disruptions and strengthens awareness of data protection [36,42]. Intensive engagement fosters a psychological attachment to service providers, creating a demand for sustained commitment to system integrity. Without adequate safeguards, however, high dependence can erode trust and damage reputation [45,84]. Conversely, consistent positive experiences build trust in service reliability [2,85], while negative experiences may prompt users to switch to alternative platforms perceived as more secure [36]. Therefore, providers must actively maintain service quality and proactively enhance security systems with transparency to preserve trust amid today's complex challenges [71,86,87,88].

This study also demonstrates that cybersecurity significantly impact on consumer trust, functioning not only as a technical safeguard but also as a reflection of ethical responsibility and

corporate accountability. This consistent with research showing that perceptions of data security contribute directly to loyalty and engagement [11,89]. When consumers believe their data is managed securely and transparently, trust increases, strengthening intentions to continue and recommended service use [90,91]. Moreover, corporate reputation and alignment with CSR principles further reinforce the emotional bond between consumers and providers [92]. Hence, cybersecurity should be regarded not merely as a technical requirement but as a strategic foundation for building long-term trust, satisfaction, and consumer engagement.

This study conceptualizes cybersecurity not as a technical outcome, but as a perceptual construct that reflects users' cognitive and affective evaluation of digital protection mechanisms. While cybersecurity was modelled as being influenced by perceived risks and technology dependence, its mediating role pertains to how these antecedent perceptions are internalized by users and subsequently translated into trust-related judgments. Hence, there is no circular causality, as the construct represents a psychological bridge rather than a technical endpoint. This distinction aligns with prior research emphasizing that users perceived cybersecurity rather than objective system performance shapes behavioural intentions and trust in digital finance [23,66,67]. By clarifying this conceptual boundary, the model preserves structural rigor and avoids endogeneity between mediator and outcome variables.

Overall, the findings affirm the theoretical framework and show that the combination of emerging digital risks, technology dependence, security perceptions, and cybersecurity effectiveness collectively shape consumer trust. Trust is influenced by technical safeguards, psychological perceptions, interactive experiences, and the extent to which users feel engaged and protected. Therefore, providers must adopt a holistic approach that integrates technical systems, transparent communication, and user security literacy to foster user loyalty and sustain engagement in a competitive digital environment.

Beyond practical insight, the study contributes both theoretically and contextual. Theoretically, it extends the Technology Acceptance Model (TAM) by positioning cybersecurity not as an external control factor but as a strategic mediating construct that channels the effect of digital risk, perceived security, and technology dependence into consumer trust. While TAM traditionally emphasizes perceived usefulness and ease of use, this study broadens its scope by integrating risk-based cognitive evaluations and security awareness, factors especially salient in fragile trust environments. By combining TAM with Perceived Risk Theory, the research proposes a hybrid framework for analysing trust formation that accounts for both rational adoption and emotional perception of risk. Contextually, the focus on Indonesia provides novel empirical insights into digital trust dynamics in emerging markets characterized by rapid fintech adoption but uneven cybersecurity literacy and regulatory enforcement. These findings suggest that in such settings, trust is shaped not only by technical performance but also by user perceptions of exposure and security assurance. Practically, the results emphasize the need for fintech providers to adopt user-centric cybersecurity strategies that are transparent, proactive, and responsive to evolving expectations. For policymakers, the findings highlight cybersecurity as a public trust infrastructure, requiring coordinated regulation, consumer protection standards, and national digital literacy initiatives. Such efforts are essential to sustaining trust and building resilient financial ecosystems in developing markets.

In the Indonesian context, cybersecurity and digital trust are governed by overlapping mandates from the Financial Services Authority (Otoritas Jasa Keuangan, OJK) and the Ministry of

Communication and Information Technology (Kementerian Komunikasi dan Informatika, Kominfo). Financial institutions and fintech providers are required to establish comprehensive cybersecurity frameworks, perform regular system audits, and report incidents transparently as part of information technology risk management [93]. Additionally, a national legal foundation for data privacy and user protection is enforced through personal data protection regulations [94]. It also promotes nationwide digital literacy through programs such as Siberkreasi and the Digital Talent Scholarship, aimed at enhancing public awareness of cybersecurity practices.

Despite these regulatory advancements, Indonesia's digital landscape remains heterogeneous. Urban centres such as Jakarta and Surabaya enjoy robust digital infrastructure and institutional readiness, whereas rural and eastern regions continue to experience limited connectivity and low cybersecurity literacy. This persistent digital divide constrains the consistent adoption of data protection standards and leads to uneven trust formation across regions. Bridging this divide requires targeted capacity-building, region-specific digital literacy initiatives, and harmonized regulatory enforcement between OJK and Kominfo [95]. Therefore, recommendations such as strengthening cybersecurity and improving digital literacy should be operationalized through localized interventions that promote equitable inclusion and sustainable digital trust across Indonesia.

Finally, the findings hold cross-national relevance for other developing economies facing similar challenges, such as India, Brazil, and Nigeria. Building consumer trust in digital finance is not a purely local concern but a global one. Accordingly, the proposed model can be adapted to analyse user behaviour and risk mitigation strategies in comparable jurisdictions. By emphasizing the mediating role of cybersecurity in trust formation, this framework offers significant potential for comparative studies and policy efforts aimed at strengthening resilience in the global fintech ecosystem.

The findings of this study empirically confirm that the integration of the Technology Acceptance Model (TAM) and Perceived Risk Theory (PRT) provides a comprehensive explanation for consumer trust in fintech services. Within this framework, TAM accounts for users' cognitive evaluations of technology how they perceive fintech as useful and reliable while PRT captures the affective dimension, reflecting users' concerns and risk perceptions toward digital transactions. The significant effects of emerging risks, perceived security risk, and technology dependence on both cybersecurity and trust demonstrate that consumers' acceptance of fintech is shaped by a dual process: rational evaluation of technological utility and emotional assessment of digital safety. Thus, the combined theoretical perspective elucidates that trust formation in fintech is not only driven by system quality and performance (as TAM predicts) but also moderated by perceptions of vulnerability and assurance (as PRT posits).

This synthesis between TAM and PRT enriches the understanding of fintech trust dynamics by positioning cybersecurity perception as the bridge between these two domains. When users perceive that fintech platforms manage risks transparently and maintain strong protection mechanisms, their risk-related anxiety diminishes, allowing cognitive trust to strengthen. Consequently, the joint explanatory power of TAM and PRT highlights that fostering consumer trust requires not only technological excellence but also consistent communication and risk-mitigation strategies that address users' psychological needs for safety and control.

6. Conclusion

This study offers new insights into the determinants of consumer trust in fintech services, particularly within emerging markets such as Indonesia. By integrating the Technology Acceptance Model (TAM) and Perceived Risk Theory, the findings reveal that perceived digital risk, technology dependence, and perceptions of cybersecurity each play significant roles in shaping consumer trust. These results confirm that trust in digital financial platforms is influenced not only by system performance and usability, but also by users' psychological responses to security-related risks. From a practical standpoint, the study underscores the importance for fintech providers to adopt transparent, proactive, and user-centric cybersecurity strategies that reinforce safety and reliability. In an environment where digital threats continue to evolve, strong cybersecurity practices can serve as a competitive advantage by fostering user loyalty and engagement. Moreover, the study highlights the role of regulators particularly OJK and Kominfo in strengthening cybersecurity as a national trust infrastructure through the enforcement of POJK IT risk management regulations, implementation of the Personal Data Protection Law (Law No. 27 of 2022), and expansion of inclusive digital literacy initiatives across diverse regions.

Despite these contributions, the study has several limitations. First, the use of cross-sectional data may not capture the dynamic nature of trust over time. Second, the sample was dominated by digital literate users, which may limit generalizability among less experienced populations. Third, the study did not distinguish between specific types of fintech services, even though consumer perceptions may vary across digital wallets, online lending, or investment platforms. Future research should therefore adopt longitudinal designs to track shifts in trust following security incidents, and incorporate qualitative approaches such as in-depth interviews or focus groups to better understand consumer motivations. Cross-country studies would also provide comparative insights into how cultural and regulatory contexts shape cybersecurity and digital trust.

From a practical perspective, the findings offer concrete implications for fintech providers, regulators, and consumers. Fintech companies must not only implement robust cybersecurity systems but also communicate data protection policies transparently to users. Security education, digital literacy, and heightened risk awareness should be integrated into a comprehensive risk management strategy. By consistently maintaining service quality and reinforcing ethical commitments to data protection, companies can build long-term consumer loyalty and engagement. For regulators particularly the Financial Services Authority (OJK) and the Ministry of Communication and Information Technology (Kominfo) the results highlight the urgency of strengthening data protection regulations, enforcing minimum cybersecurity standards, and launching nationwide digital literacy campaigns. Such coordinated efforts are vital for sustaining public trust and ensuring the resilience of Indonesia's digital financial ecosystem.

The findings of this study have several practical policy implications. To raise public awareness of digital and financial threats, regulators, particularly the Financial Services Authority (OJK) and the Ministry of Communication and Information Technology (Kominfo), must strengthen regulations related to data protection. Furthermore, they should establish minimum cybersecurity standards for all fintech service providers and conduct a national digital literacy campaign. Fintech providers should implement stricter security practices such as the use of multi-factor authentication, transparent user data management, and proactive communication with customers in the event of a security incident. Fintech providers can also incorporate digital security education features into their applications to increase customer risk awareness. Consumers should become more informed about

digital finance, including digital threats like phishing and identity theft, and adopt secure practices such as using strong passwords and regularly updating their applications.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: The authors sincerely appreciate the institutional support, academic environment, and invaluable guidance that contributed to this research.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Measurement items.

Emerging Risks [17,19]		
	ER1	I feel that fintech platforms are vulnerable to digital threats (e.g., hacking).
	ER2	Using fintech services involves uncertainty about the safety of my transactions.
	ER3	I am concerned about potential financial losses when using fintech services.
	ER4	I worry about personal data breaches when using fintech platforms.
	ER5	I feel exposed to cyber fraud when using fintech services.
	ER6	I feel insecure during digital transactions on fintech platforms.
Perceived Security Risk [20,64]		
	PSR1	I trust that fintech platforms use strong encryption systems to protect my data.
	PSR2	I believe fintech platforms have reliable authentication protocols (e.g., OTP, biometrics).
	PSR3	I feel confident that fintech platforms have strict data access controls.
	PSR4	I am comfortable with how fintech platforms share my data with third parties.
	PSR5	I believe fintech platforms comply with privacy regulations.
	PSR6	Fintech platforms are transparent about how they manage my data.
	PSR7	I feel I have control over my consent regarding data usage on fintech platforms.
Technology Dependence [62]		
	TD1	I frequently use fintech services for my financial transactions.
	TD2	I depend on fintech platforms to manage my daily financial needs.
	TD3	Using fintech services has become a habit in my daily life.
	TD4	I prefer using fintech services over traditional manual financial services.
	TD5	Fintech services are well-integrated into my daily activities.
	TD6	I feel that fintech services are a necessary part of my financial management.
Cybersecurity [65]		
	CS1	Fintech platforms have effective security infrastructure to protect my data.
	CS2	Fintech platforms have reliable detection and response mechanisms for cyber threats.
	CS3	Fintech platforms have strong anti-fraud systems in place.
	CS4	Fintech platforms effectively protect against malware and other cyber threats.
	CS5	Fintech platforms are transparent about how they handle security incidents.
	CS6	The digital systems of fintech platforms are resilient against cyber threats.
Consumer Trust [16,66,67]		

CT1	I believe fintech platforms are reliable for my financial transactions.
CT2	I trust the integrity of fintech service providers.
CT3	I feel that fintech platforms act with goodwill toward their users.
CT4	Fintech services consistently meet my expectations.
CT5	Fintech platforms have a good reputation in my opinion.
CT6	My past experiences with fintech platforms have been positive.

References

[1] Urus, S., Kurniasari, F., Nazri, S. N. F., Utomo, P., Othman, I., So, J., & Hamid, N. (2022). A comparative study of fintech payment services adoption among Malaysian and Indonesian fresh graduates: Through the lens of UTAUT theory. Eastern-European Journal of Enterprise Technologies, 5(1), 73–88. https://doi.org/10.15587/1729-4061.2022.265662

[2] Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: Surviving online threats. Journal of Business Strategy, 44(1), 3-12. https://doi.org/10.1108/JBS-08-2021-0146

[3] Boonen, T., Feng, Y., & Tong, Z. (2025). Cybersecurity investments and cyber insurance purchases in a non-cooperative game. ASTIN Bulletin, 55(1), 1–23. https://doi.org/10.1017/asb.2024.40

[4] Li, J., Wu, L., Qi, J., Zhang, Y., Wu, Z., & Hu, S. (2023). Determinants affecting consumer trust in communication with AI chatbots: the moderating effect of privacy concerns. Journal of Organizational and End User Computing, 35(1), 1–24. https://doi.org/10.4018/JOEUC.328089

[5] Atlas, F., Khan, K., & Khan, F. (2024). Intertwining between online retailer's trustworthiness attributes and consumer's purchase intentions: a knowledge management perspective in response to covid -19. Knowledge and Process Management, 32(1), 28–41. https://doi.org/10.1002/kpm.1794

[6] Onwubiko, C., & Ouazzane, K. (2020). SOTER: A playbook for cybersecurity incident management. IEEE Transactions on Engineering Management, 67(4), 1–21. https://doi.org/10.1109/TEM.2020.2979832

[7] Gou, C., & Deng, X. (2023). A Blockchain-based security model for cloud accounting data. International Journal of Ambient Computing and Intelligence, 14(1), 1–16. https://doi.org/10.4018/IJACI.332860

[8] Rao, S., & Jain, A. (2024). Advances in malware analysis and detection in cloud computing environments: A review. International Journal of Safety and Security Engineering, 14(1), 225–230. https://doi.org/10.18280/ijsse.140122

[9] Aarland, M. (2024). Cybersecurity in digital supply chains in the procurement process: introducing the digital supply chain management framework. Information and Computer Security, 33(1), 5–24. https://doi.org/10.1108/ICS-10-2023-0198

[10] Patil, R., & Gottumukkala, H. (2023). Improved association rule mining-based data sanitization for privacy preservation model in cloud. Journal of Telecommunications and Information Technology, 1, 51-59. https://doi.org/10.26636/jtit.2023.166922

[11] Nguyen, Y. T. H., Tapanainen, T., & Nguyen, H. T. T. (2022). Reputation and its consequences in fintech services: the case of mobile banking. International Journal of Bank Marketing, 40(7), 1364–1397. https://doi.org/10.1108/IJBM-08-2021-0371

[12] Bajwa, I., Ahmad, S., Mahmud, M., & Bajwa, F. (2023). The impact of cyberattacks awareness on customers' trust and commitment: Empirical evidence from the Pakistani banking sector. Information & Computer Security, 31(4), 1–15. https://doi.org/10.1108/ICS-11-2022-0179

[13] Sasikumar, K., & Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. IEEE Access, 12, 52325-52351. https://doi.org/10.1109/ACCESS.2024.3385449

[14] Gao, S., Li, G., Feng, L., Chen, Y., & Chen, Y. (2023). A secure data sharing system for 6G networks. IEEE Access, 11, 133281-133293. https://doi.org/10.1109/ACCESS.2023.3336399

[15] Tritto, A., He, Y., & Junaedi, V. (2020). Governing the gold rush into emerging markets: a case study of Indonesia's regulatory responses to the expansion of Chinese-backed online P2P lending. Journal of Financial Innovation, 6(1), 1–24. https://doi.org/10.1186/s40854-020-00202-4

[16] 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

[17] 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

[18] Nguyen, T., Pham, H., Dick, M., & Richardson, J. (2021). Trust types and mediating effect of consumer trust in m-payment adoption: An empirical examination of Vietnamese consumers. Australasian Journal of Information Systems, 25. https://doi.org/10.3127/ajis.v25i0.3043

[19] Zhou, T. (2011). An empirical examination of initial trust in mobile payment. Internet Research, 21(5), 527–540. https://doi.org/10.1108/10662241111176353

[20] Bélanger, F. (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

[21] Білявський, В., Білявська, Ю., Уманців, Ю., Шестак, Я., Журба, О., & Хаванов, А. (2024). Digital technologies in the financial sector of the economy. Financial and credit activity problems of theory and practice, 4(57), 171-183. https://doi.org/10.55643/fcaptp.4.57.2024.4444

[22] Căciulescu, A., Rughinis, R., Țurcanu, D., & Radovici, A. (2024). Mapping cyber-financial risk profiles: implications for European cybersecurity and financial literacy. Risks, 12(12), 200. https://doi.org/10.3390/risks12120200

[23] Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data security, customer trust and intention for adoption of fintech services: an empirical analysis from commercial bank users in Pakistan. SAGE Open, 13(3), 21582440231181388. https://doi.org/10.1177/21582440231181388

[24] Yu, Z., & Cai, K. (2022). Perceived risks toward in-vehicle infotainment data services on intelligent connected vehicles. Systems, 10(5), 162. https://doi.org/10.3390/systems10050162

[25] Gauch, K., & Quick, R. (2025). Assure or Insure Cyber Risk? Nonprofessional Investors' Willingness to Invest. Accounting Perspectives, 24(2), 517-552. https://doi.org/10.1111/1911-3838.12389

[26] Farzin, M., Ghaffari, R., & Fattahi, M. (2022). The influence of social network characteristics on the purchase intention. Business Perspectives and Research, 10(2), 267-285. https://doi.org/10.1177/22785337211009661

[27] Ali, I., Naushad, M., & Alasmri, H. (2023). Effect of CSR activities on customers' purchase intention: The mediating role of trust. Innovative Marketing, 19(2), 155–169. https://doi.org/10.21511/im.19(2).2023.13

[28] Al-hazimeh, A., Al-Smadi, R., & Al-Smadi, A. (2024). Future trends in fintech and sustainability: empirical study. Investment Management and Financial Innovations, 21(3), 51-63. https://doi.org/10.21511/imfi.21(3).2024.05

[29] Alamoudi, H., Glavee-Geo, R., Alharthi, M., Doszhan, R., & Suyunchaliyeva, M. (2025). Exploring trust and outcome expectancy in fintech digital payments: insights from the stimulus-organism-response model. International Journal of Bank Marketing, 43(5), 897–919. https://doi.org/10.1108/IJBM-04-2024-0252

[30] Amnas, M. B., Selvam, M., Raja, M., Santhoshkumar, S., & Parayitam, S. (2023). Understanding the determinants of fintech adoption: Integrating UTAUT2 with trust theoretic model. Journal of Risk and Financial Management, 16(12), 505. https://doi.org/10.3390/jrfm16120505

[31] Alsmadi, A., & Al-Okaily, M. (2025). Future front of finance: the role of fintech strategies, competitiveness dynamics and sustainable solutions. Competitiveness Review: An International Business Journal. https://doi.org/10.1108/CR-11-2023-0298

[32] Budiyanto, A., Lubis, I., Pamungkas, I. B., & Maulana, A. E. (2025). Technology acceptance model, trust, and financial behavior in shaping consumer well-being: Insights from fintech adoption in urban Indonesia. Innovative Marketing, 21(2), 197–210. https://doi.org/10.21511/im.21(2).2025.16

[33] Zhao, H., Khaliq, N., Li, C., Rehman, F. U., & Popp, J. (2024). Exploring trust determinants influencing the intention to use fintech via SEM approach: Evidence from Pakistan. Heliyon, 10(8), e29716. https://doi.org/10.1016/j.heliyon.2024.e29716

[34] Chawla, U., Mohnot, R., Singh, H., & Banerjee, A. (2023). The mediating effect of perceived trust in the adoption of cutting-edge financial technology among digital natives in the post-covid-19 era. Economies. 11(12), 286. https://doi.org/10.3390/economies11120286

[35] Jha, S., & Dangwal, R. (2025). Actual adoption of fintech services among micro-entrepreneurs of urban slum area of Uttarakhand. Journal of Science and Technology Policy Management, 17(2), 457-491. https://doi.org/10.1108/JSTPM-08-2023-0144

[36] Jamil, H., Zia, T., Nayeem, T., Whitty, M., & D'Alessandro, S. (2025). Human-centric cyber security: applying protection motivation theory to analyse micro business owners' security behaviours. Information & Computer Security, 33(4), 1–15. https://doi.org/10.1108/ICS-10-2023-0176

[37] Sasidharan, A., & Venkatakrishnan, S. (2024). Intention to use mobile banking: An integration of theory of planned behaviour (TPB) and technology acceptance model (TAM). KSII Transactions on Internet and Information Systems, 18(4), 1–20. https://doi.org/10.3837/tiis.2024.04.013

[38] Schrank, J. (2025). Factors deterring the use of mobile payment among Generation Z. Family and Consumer Sciences Research Journal, 53(4), 1–15. https://doi.org/10.1111/fcsr.70016

[39] Al-Husamiyah, A., & Al-Bashayreh, M. (2022). A comprehensive acceptance model for smart home services. International Journal of Data and Network Science, 6(1), 45–58. https://doi.org/10.5267/j.ijdns.2021.10.005

[40] Wongyai, P., Ngo, T., Wu, H., & Tsui, K. (2025). Passengers' acceptance of biometric check-in kiosks: the case of Thai airports. Tourism and Hospitality Research, 14673584251385493. https://doi.org/10.1177/14673584251385493

[41] Mutambik, I., Almuqrin, A., Zhang, J., & Alharbi, Z. H. (2024). Trust in cryptocurrency payments. Journal of Organizational and End User Computing, 36(1), 1–36. https://doi.org/10.4018/JOEUC.353910

[42] Stewart, K., Perren, R., Chambers, C., & Zulauf, R. (2024). In tech we rely: how technology dependence fuels consumer vulnerability. Journal of Consumer Affairs, 58(3), 905–945. https://doi.org/10.1111/joca.12610

[43] Jones, K., Lodinger, N., Widlus, B., Siami Namin, A., Maw, E., & Armstrong, M. (2022). How do non experts think about cyber-attack consequences? Information & Computer Security, 30(4), 473–489. https://doi.org/10.1108/ICS-11-2020-0184

[44] Al Hammadi, M., Jimber-Del Río, J. A., Ochoa-Rico, M. S., Montero, O. A., & Vergara-Romero, A. (2024). Risk management in Islamic banking: the impact of financial technologies through empirical insights from the UAE. Risks, 12(2), 17. https://doi.org/10.3390/risks12020017

[45] Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2023). Rushing for security: a document analysis on the sources and effects of time pressure on organizational cybersecurity. Information and Computer Security, 31(4), 504–526. https://doi.org/10.1108/ICS-01-2021-0013

[46] Gafni, R., & Levy, Y. (2023). Experts' feedback on the cybersecurity footprint elements: in pursuit of a quantifiable measure of SMBs' cybersecurity posture. Information & Computer Security, 31(4), 1–15. https://doi.org/10.1108/ICS-05-2023-0083

[47] Jahn, S., Langer, A.-C., Elshiewy, O., & Boztug, Y. (2020). How perceived security risk influences acceptance of virtual shopping walls. Marketing ZFP, 42(4), 35–42. https://doi.org/10.15358/0344-1369-2020-4

[48] Liu, G., Xie, H., Wang, W., & Huang, H. (2024). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. Journal of Cloud Computing, 13, Article 608. https://doi.org/10.1186/s13677-024-00608-w

[49] Razzaq, M. A., Ahmad, M., Almansour, F., Ul Haq, I., Jhanjhi, N. Z., Zaib, M., & Masud, M. (2022). Security and privacy aspects of cloud computing: a smart campus case study. Intelligent Automation and Soft Computing, 31(1), 117–128. https://doi.org/10.32604/iasc.2022.016597

[50] Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., & Vasilyeva, T. (2023). Company cybersecurity system: Assessment, risks and expectations. Production Engineering Archives, 29(3), 379–392. https://doi.org/10.30657/pea.2023.29.43

[51] Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. Information & Computer Security, 32(4), 1–15. https://doi.org/10.1108/ICS-07-2023-0116

[52] Hasani, T., O'Reilly, N., Dehghantanha, A. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5), 97. https://doi.org/10.1007/s43546-023-00477-6

[53] Mathieu, R., & Turovlin, A. (2023). Lost in the middle – A pragmatic approach for ERP managers to prioritize known vulnerabilities by applying classification and regression trees (CART). Information & Computer Security, 31(4), 1–15. https://doi.org/10.1108/ICS-02-2023-0027

[54] Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R., & Cavallo, A. (2022). A quantification mechanism for assessing adherence to information security governance guidelines. Information & Computer Security, 30(4), 517-548. https://doi.org/10.1108/ICS-08-2021-0112

[55] Raza, B., St-Onge, S., & Ali, M. (2023). Frontline employees' performance in the financial services industry: The significance of trust, empathy and consumer orientation. International Journal of Bank Marketing, 41(3), 527–549. https://doi.org/10.1108/IJBM-06-2022-0237

[56] Joshi, R. (2024). A mixed methods UTAUT2-based approach to understanding unified payments interface adoption among low-income users. Banks and Bank Systems, 19(1), 58–73. https://doi.org/10.21511/bbs.19(1).2024.06

[57] Al Karim, R., Rabiul, M. K., Taskia, A., & Jarumaneerat, T. (2023). Millennial customer engagement with fintech services: the mediating role of trust. Business Perspectives and Research, 22785337231183275. https://doi.org/10.1177/22785337231183275

[58] Pedersen, S., Zhang, T., Zhou, Y., Aschemann-Witzel, J., & Thøgersen, J. (2023). Consumer attitudes towards imported organic food in China and Germany: the key importance of trust. Journal of Macromarketing, 43(2), 233-254. https://doi.org/10.1177/02761467221077079

[59] Dalal, R., Howard, D., Bennett, R., Posey, C., & Zaccaro, S. (2022). Organizational science and cybersecurity: Abundant opportunities for research at the interface. Journal of Business and Psychology, 37(1), 1–29. https://doi.org/10.1007/s10869-021-09732-9

[60] Hasan, R., Shams, R., & Rahman, M. (2021). Consumer trust and perceived risk for voice-controlled artificial intelligence: The case of Siri. Journal of Business Research, 131, 1–12. https://doi.org/10.1016/j.jbusres.2020.12.012.

[61] Thomas, S., Patel, R., & Bhatt, V. (2023). Private-label grocery buyers donation intentions and trust in CRM campaigns: An empirical analysis by employing social identity theory. Society and Business Review, 18(1), 1–15. https://doi.org/10.1108/SBR-12-2021-0247.

[62] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157–178. https://doi.org/10.2307/41410412

[63] Alshurideh, M. T., Al Kurdi, B., Masa'deh, R. E., & Salloum, S. A. (2021). The moderation effect of gender on accepting electronic payment technology: a study on United Arab Emirates consumers. Review of International Business and Strategy, 31(3), 375-396. https://doi.org/10.1108/RIBS-08-2020-0102

[64] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080

[65] Susanto, H., & Almunawar, M. N. (2012). Information security awareness within business environment: an IT review. arXiv preprint arXiv:1206.2597. https://doi.org/10.2139/ssrn.2161716

[66] 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

[67] Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. Industrial Management & Data Systems, 106(5), 601–620. https://doi.org/10.1108/02635570610666403

[68] Awiszus, K., Bell, Y., Lüttringhaus, J., Svindland, G., Voß, A., & Weber, S. (2024). Building resilience in cybersecurity: An artificial lab approach. Journal of Risk and Insurance, 91(3), 753-800. https://doi.org/10.1111/jori.12450

[69] Schreiber, A., & Schreiber, I. (2024). Bridging the knowledge gap: the contribution of employees' awareness of AI cyber risks comprehensive programs to reducing emerging AI digital threats. Information & Computer Security, 32(4), 1–15. https://doi.org/10.1108/ICS-10-2023-0199

[70] White, G. R., Allen, R. A., Samuel, A., Abdullah, A., & Thomas, R. J. (2020). Antecedents of cybersecurity implementation: a study of the cyber-preparedness of UK social enterprises. IEEE Transactions on Engineering Management, 69(6), 3826-3837. https://doi.org/10.1109/TEM.2020.2994981

[71] Gupta, S., Shahriar, K., Alqahtani, H., Alsalman, D., & Sarker, I. H. (2024). Modeling hybrid feature-based phishing websites detection using machine learning techniques. Annals of Data Science, 11(2), 217–242. https://doi.org/10.1007/s40745-022-00379-8

[72] Kumar, S., & Mallipeddi, R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. Production and Operations Management, 31(10), 3890–3912. https://doi.org/10.1111/poms.13859

[73] He, Y., Zamani, E., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): improving the incident response process in healthcare. International Journal of Information Management, *62*, 102435. https://doi.org/10.1016/j.ijinfomgt.2021.102435

[74] Veiga, A. (2023). A model for information security culture with creativity and innovation as enablers-refined with an expert panel. Information & Computer Security, 31(4), 1–15. https://doi.org/10.1108/ICS-11-2022-0178

[75] Maurer, F., & Fritzsche, A. (2023). Layered structures of robustness and resilience: evidence from cybersecurity projects for critical infrastructures in Central Europe. Strategic Change, 32(6), 1–15. https://doi.org/10.1002/jsc.2559

[76] Ravichandran, S., Osakwe, C., Elgammal, I., Abbasi, G., & Cheah, J.H. (2024). Feeding trust: exploring key drivers, moderators and consequences related to food app usage. Journal of Services Marketing, 38(5), 1–15. https://doi.org/10.1108/JSM-11-2023-0437

[77] Palacios Chavarro, S., Nespoli, P., Díaz-López, D., & Niño Roa, Y. (2023). On the way to automatic exploitation of vulnerabilities and validation of systems security through security chaos engineering. Big Data and Cognitive Computing, 7(1), 1. https://doi.org/10.3390/bdcc7010001

[78] Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the technical and vocational training corporation. Big Data and Cognitive Computing, 7(2), 73. https://doi.org/10.3390/bdcc7020073

[79] Kariuki, P., Ofusori, L., & Subramaniam, P. R. (2024). Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. Security Journal, 37(1), 1–20. https://doi.org/10.1057/s41284-023-00378-1

[80] Akhter, A., Karim, M., Jannat, S., & Islam, K. M. A. (2022). Determining factors of intention to adopt internet banking services: A study on commercial bank users in Bangladesh. Banks and Bank Systems, 17(1), 1–15. https://doi.org/10.21511/bbs.17(1).2022.11

[81] Agalit, M., Chakir, E. M., Taqafi, I., & Khamlichi, Y. (2023). A review of cybersecurity management standards applied in higher education institutions. International Journal of Safety and Security Engineering, 13(6), 1109–1116. https://doi.org/10.18280/ijsse.130614

[82] Agarwal, S., Ghosh, P., Ruan, T., & Zhang, Y. (2024). Transient customer response to data breaches of their information. Management Science, 70(2), 1–18. https://doi.org/10.1287/mnsc.2021.01335

[83] Eti, S., Yüksel, S., Pamucar, D., Dinçer, H., Deveci, M., & Gökalp, Y. (2024). Markov chain and RATGOS-driven fuzzy decision-making for prioritizing cybersecurity measures in microgrid systems. OPSEARCH, 1-27. https://doi.org/10.1007/s12597-024-00897-4

[84] Tanriverdi, H., Kwon, J., & Im, G. (2024). Taming complexity in cybersecurity of multihospital systems: The role of enterprise-wide data analytics platforms. MIS Quarterly, 49(1), 1–28. https://doi.org/10.25300/MISQ/2024/17752

[85] Berg, L., Slettemeås, D., Kjørstad, I., & Rosenberg, T. (2020). Trust and the don't-want-to-complain bias in peer-to-peer platform markets. International Journal of Consumer Studies, 44(3), 220–231. https://doi.org/10.1111/ijcs.12561

[86] Suzuki, Y., & Monroy, S. (2022). Prevention and mitigation measures against phishing emails: A sequential schema model. Security Journal, 35(4), 1162–1182. https://doi.org/10.1057/s41284-021-00318-x

[87] Lyon, G. (2024). Informational inequality: The role of resources and attributes in information security awareness. Information & Computer Security, 32(3), 1–15. https://doi.org/10.1108/ICS-04-2023-0063

[88] Saleem, J., Islam, R., & Islam, M. Z. (2024). Darknet traffic analysis: A systematic literature review. IEEE Access, 12, 42423-42452. https://doi.org/10.1109/ACCESS.2024.3373769

[89] Dexe, J., Franke, U., & Rad, A. (2021). Transparency and insurance professionals: a study of Swedish insurance practice attitudes and future development. The Geneva Papers on Risk and Insurance – Issues and Practice, 46(1), 1–26. https://doi.org/10.1057/s41288-021-00207-9

[90] Mohammad, V. M. (2020). Consumer trust towards content marketing of food & beverage businesses on Instagram: empirical analysis of Taiwanese and Singaporean consumers. International Journal of Business, 6(2), 73-85. https://doi.org/10.20469/ijbas.6.10002-2

[91] Yusuf, M. S., Dirie, K. A., Alam, M. M., & Salisu, I. (2024). Corporate social responsibility activities, consumers' trust and gender: An analysis of Islamic banks in Somalia. Social Responsibility Journal, 20(7), 1256–1283. https://doi.org/10.1108/SRJ-02-2023-0076

[92] Feng, N., Zhang, A., Van Klinken, R., & Cui, L. (2021). An integrative model to understand consumers' trust and willingness to buy imported fresh fruit in urban China. British Food Journal, 123(6), 2216-2234. https://doi.org/10.1108/BFJ-07-2020-0575

[93] Financial Services Authority of Indonesia (OJK). (2021). Regulation of the financial services authority No. 4/POJK.03/2021 concerning the implementation of risk management in the use of information technology by commercial banks. Jakarta: Financial Services Authority of the Republic of Indonesia. https://www.ojk.go.id

[94] Government of the Republic of Indonesia. (2022). Law of the Republic of Indonesia No. 27 of 2022 on personal data protection. Jakarta: Ministry of State Secretariat of the Republic of Indonesia. Retrieved from https://jdih.setneg.go.id

[95] World Bank. (2023). Bridging Indonesia's digital divide: Strengthening connectivity and inclusion. Washington, DC: World Bank Group. https://documents.worldbank.org

(Executive Editor: Qun Niu)