SUSTAINABILITY, SOCIAL INNOVATIONS AND
DIDGITAL TRANSFORMATION 1(1), 2025

DOI: 10.2478/ssidt-2025-0003

INFLUENCE OF CYBERSECURITY MEASURES ON CONSUMER TRUST AND LOYALTY IN DIGITAL MARKETING IN INDIA

Sneha Ganeshram[1], Jevgenija Dehtjare[2]

[1]EKA University of Applied Sciences, Riga, Latvia, snehaganeshram23@gmail.com

[2]EKA University of Applied Sciences, Riga, Latvia, jevgenija.dehtjare@eka.edu.lv ORCID: https://orcid.org/0000-0002-6859-2327

Received 26 August 2025; accepted 14 November 2025

Abstract

Research purpose. In India's rapidly growing digital economy, cybersecurity has become a key factor shaping consumer perception and behaviour on digital marketing platforms. Rising data breaches and privacy concerns have elevated the importance of user trust. Cybersecurity is now seen not only as a technical safeguard but also as a strategic element for retaining consumers. Despite its growing significance, there is limited research on how cybersecurity directly influences consumer trust and loyalty in the Indian context. This study addresses that gap. The purpose of the research is to analyse the impact of cybersecurity measures on consumer trust and loyalty toward digital marketing platforms in India. To achieve that, such factors as data protection, privacy practices, and incident response, and their influence on consumer trust, engagement, and long-term loyalty to digital marketing platforms are assessed. The visibility of cybersecurity practices and their meaning to consumers are also analysed, as well as the translation of such perceptions into repeat purchasing behaviour and brand advocacy. By achieving that, the paper not only contributes to the scientific purpose but also provides actionable guidance for practitioners. The research analyses how trust serves as a mediating factor between cybersecurity measures and loyalty outcomes.

Design / Methodology / Approach. A mixed-methods approach is used. Quantitative data from a structured online survey (50 participants across India) is combined with qualitative insights from an interview with a digital marketing professional. Analytical methods include regression, factor analysis, and thematic evaluation.

Findings. Results show a strong positive link between effective cybersecurity and consumer trust, which significantly affects loyalty. Transparent data protection policies and visible cybersecurity efforts enhance consumer confidence and repeat usage. The study provides practical recommendations for strengthening user trust via improved cybersecurity. The findings are also intended to support digital platforms in designing security strategies that strengthen consumer confidence and create sustainable competitive advantage.

Originality / Value / Practical implications. This research is one of the few studies that empirically examines how cybersecurity measures directly influence consumer trust and loyalty in the Indian digital marketing context. Its originality lies in combining consumer perception analysis with expert insights to reveal that visible and transparent cybersecurity practices are more influential than technical certifications. The findings provide practical guidance for digital platforms on how to build consumer trust and loyalty by integrating cybersecurity as a core element of brand strategy.

Keywords: cybersecurity; consumer trust; digital marketing; loyalty; India.

JEL codes: M31; M15

Introduction

As the digital economy continues to expand, trust has become a crucial element in shaping consumer relationships with online platforms. Digital marketing platforms play a central role in customer outreach and data-driven engagement, which places them under increasing scrutiny regarding how they manage user information. According to Da Silva Wegner et al. (2023), if a company wants to correctly reach the target audience, it can use digital marketing as a factor influencing competitiveness and the performance of marketing actions.

The topicality of the research is related to the fact that the growing number of cyber threats and incidents involving data misuse has led consumers to become more aware of and sensitive to online security issues. Consequently, cybersecurity is no longer viewed as merely a technical requirement; it is now a strategic tool that affects consumer trust and loyalty. When digital platforms prioritise robust security protocols and transparent data practices, users are more likely to develop confidence in their services. This trust is essential in fostering customer loyalty, which encompasses ongoing usage, repeat interactions, and a greater willingness to recommend the platform to others.

This article focuses on digital marketing platforms in India and explores how cybersecurity measures influence consumer trust and loyalty. The subject of this study revolves around the relationship between cybersecurity strategies and consumer behaviour in the digital space. The primary aim is to analyse the impact of cybersecurity measures on consumer trust and loyalty toward digital marketing platforms within the Indian context.

Correspondingly, the study sought to answer key research questions, such as how cybersecurity measures influence trust, what relationship exists between trust and loyalty, which cybersecurity strategies most effectively enhance loyalty, and how consumer perceptions of cybersecurity affect their online purchasing decisions.

To achieve this objective, a comprehensive literature review was conducted to understand the theoretical underpinnings of cybersecurity, trust, and loyalty in the digital environment. The study identifies and categorises key cybersecurity strategies adopted by Indian digital marketing platforms, such as certifications, encryption protocols, privacy policies, and user data handling practices. A structured consumer survey was designed and administered to capture perceptions of cybersecurity and levels of trust in various platforms, while also assessing loyalty indicators such as repeat usage, customer retention, and willingness to recommend.

In parallel, in-depth interviews with digital marketing professionals were conducted to gain insights into the strategic motivations behind cybersecurity implementation and its connection to customer engagement. The study also examined consumer purchasing decisions considering cybersecurity perceptions and compared loyalty levels across platforms with differing levels of cybersecurity transparency. These tasks enabled a thorough analysis of which practices most effectively influence consumer trust and loyalty.

The analysis revealed that specific cybersecurity perceptions significantly impact customer loyalty to digital marketing platforms. In particular, the presence of secure-looking websites such as HTTPS indicators and padlock symbols, clear and accessible privacy policies, and user sensitivity to insecure payment pages emerged as the most influential factors. These findings underscore the need for visible, transparent, and reassuring cybersecurity practices. While features like two-factor authentication and general feelings of safety were positively associated with loyalty, their lesser statistical significance suggests they play a more supportive role in influencing consumer behaviour.

Ultimately, this research provides actionable insights for digital marketing platforms in India. By aligning cybersecurity strategies with consumer expectations and communicating these measures effectively, platforms can enhance trust, strengthen brand loyalty, and maintain a competitive edge in India’s rapidly evolving digital landscape.

Literature Review

The digital transformation of global markets has fundamentally reshaped how businesses operate, communicate, and build relationships with consumers. As organisations increasingly rely on digital platforms for marketing and customer engagement, issues of security, privacy, and data protection have become central to sustaining consumer confidence. Cybersecurity, once viewed as a purely technical concern, now plays a strategic role in shaping consumer behaviour and influencing brand perception. Understanding how these technological and behavioural dimensions interact provides the foundation for examining the relationship between cybersecurity, trust, and loyalty in the digital marketing environment.

According to Carlsson (2004), the digital economy is more efficient in its dynamics, not static. It describes new activities and products, not higher productivity. Digital economy, therefore, can be described as a new form and level of connectivity among multiple heterogeneous ideas and actors, contributing to a rise of a vast new range of combinations, as it consists of a wide range of activities (Skvarciany & Jurevičienė, 2021). Productivity and efficiency also have some measurable effects, but the more important long-run effects in the digital economy are beyond measurement.

Huge global corporations, such as Google, Meta, Alibaba, and others, unheard of some twenty years ago, have now emerged as key players in the whole economic landscape. According to Kannan and Li (2016), the increase in their activity and market coverage explains how digital platforms are reshaping global business landscapes, creating new ways of interaction for companies and consumers. The evolution of the digital economy has brought about a paradigm shift in how businesses connect with consumers, particularly through digital marketing platforms. In India, where digital adoption has surged due to increased smartphone penetration and affordable internet access, digital marketing is not merely a promotional tool but a strategic interface through which brands communicate, collect data, and build consumer relationships. As a result, trust has emerged as a pivotal factor governing consumer interactions with such platforms, with cybersecurity now acting as a critical foundation of that trust.

Digital marketing, which encompasses techniques such as social media outreach, search engine optimisation, and personalised advertising, plays a vital role in influencing purchasing behaviour, especially in culturally diverse markets like India. This form of marketing integrates both traditional marketing goals, such as satisfying customer needs, and modern methods of reaching a technologically savvy population via platforms like WhatsApp, Instagram, and vernacular content channels (Jackson & Ahuja, 2016). With its dynamic nature and massive data dependency, digital marketing becomes particularly vulnerable to cybersecurity threats, thereby introducing risk factors that can affect how consumers perceive these platforms. Digital marketing, rooted in traditional marketing theory, is defined as the strategic process of creating, communicating, and delivering value to customers to satisfy their needs and build lasting relationships (Kotler & Keller, 2016).

According to Obitovich and Utkirovna (2024), cybersecurity becomes an even more pressing problem in the context of digital marketing; its influence on various business operations cannot be underestimated. The ability to ensure a high level of cybersecurity has advanced impressively during recent years, enabling an opportunity to keep up with the rapid changes that occur in cyberspace. With the help of cybersecurity, a country or an organisation is able to safeguard its products and information in cyberspace (Perwej et al., 2021). Cybersecurity, in this regard, refers to the suite of technologies, processes, and measures designed to protect digital information and infrastructure from unauthorised access and cyberattacks.

In India, the legal foundation of cybersecurity is established through the Information Technology Act of 2000 and is supplemented by additional compliance standards such as ISO/IEC 27001 and data protection frameworks proposed by CERT-In. Given that digital marketing relies heavily on user data for behavioural targeting and analytics, any compromise of this data through phishing, malware, or breaches can significantly damage a platform's credibility.

According to Nim et al. (2024), digital marketing ecosystems can provide global multinational players with greater multinational flexibility, enabling them to fit their international strategies to the increasing complexities of the global markets, especially of the emerging countries, where trends toward increased

protectionism and geopolitical disruptions exist. The Indian digital marketing ecosystem has expanded at an unprecedented rate, as reflected in studies that show a growing trend in online retail, influencer-driven campaigns, and real-time data analytics (Anurag & Kaur, 2021). However, this growth also amplifies the exposure to cyber threats. Bunnell (2025) points out that digital marketers face increasing attacks through fake URLs, malicious plugins, and bot traffic - all of which can jeopardise customer information. With platforms storing large volumes of user profiles, transaction histories, and preferences, any laxity in cybersecurity measures could erode user confidence and lead to reputational damage.

The regulatory response in India has been multifaceted, involving institutional mechanisms like the Indian Computer Emergency Response Team (CERT-In), which issues advisories and coordinates incident responses. The presence of guidelines for encryption standards, breach notifications, and regular security audits has become a non-negotiable aspect of digital marketing operations. Yet, regulation alone is insufficient to ensure consumer trust, where user perception becomes crucial.

Consumer trust in digital platforms has been widely studied, with research indicating that trust is influenced not only by the technical robustness of a platform but also by transparency in data handling and ethical behaviour (Thaw et al., 2009). In the Indian context, where consumer decisions are shaped by a mix of social influence, brand heritage, and online reviews, building and sustaining trust requires consistent and visible cybersecurity actions. Trust, in turn, acts as a gateway to long-term brand loyalty, making it essential for digital marketers to communicate their commitment to data protection.

According to Khamitov et al. (2024), trust is one of the most important concepts of consumer research; the strength of its antecedents, consequences, and moderators should be thoroughly analysed. Consumer trust is not a static metric; it evolves based on the brand's responsiveness to emerging threats, disclosure of data breaches, and implementation of consumer privacy rights. Moreover, Siddiqui and Gir (2015) argue that integrating reputation mechanisms with security policies enhances consumer faith in digital transactions. Consumer loyalty, meanwhile, is closely tied to trust and satisfaction. Nowadays, digital technologies deeply penetrate consumers` lives and become powerful means for data collection and use by companies (Quach et al., 2022). However, fresh privacy concerns emerge, as consumer loyalty is closely tied to trust and satisfaction. In India, loyalty is influenced not only by service quality but also by factors such as emotional connection, local cultural relevance, and user convenience (Bassano et al., 2018; Verma, 2017). Loyalty ecosystems built through mobile wallets and cashback platforms like Paytm or PhonePe further highlight how seamless, secure digital experiences drive continued engagement (Srivastava et al., 2023). As such, cybersecurity plays an indirect but crucial role in sustaining loyalty. When users feel protected, they are more inclined to repeatedly interact with a brand.

This interdependence between cybersecurity, trust, and loyalty means that platforms must go beyond compliance and adopt a more consumer-centric view of data protection (Celestin, 2024). Studies show that platforms employing strong encryption, multi-factor authentication, and fraud detection systems are viewed more favourably (Asthana, 2025). Furthermore, when platforms align their cybersecurity strategies with public expectations such as visible privacy policies, responsive customer service during incidents, and consistent updates, consumers respond with uninterrupted support and advocacy. However, satisfaction of these expectations is a challenging process. Cybersecurity managers often face various issues, such as complexity, tool overlap, etc. Blind spots arise, resulting from reliance on multiple vendors and fragmented solutions. In this regard, the consolidation of digital platforms' cybersecurity measures becomes essential as it simplifies security operations and strengthens risk posture. It also allows companies to meet consumer demands for transparency and reliability and builds trust in a more efficient and sustainable way (Ajish, 2024).

Indian consumers are also becoming more aware of their digital rights, with an increasing number expressing concern over how their personal data is used. Ravikumar et al. (2022) found that digital-savvy consumers in India expect brands to function as custodians of their data, and breaches of that trust can lead to immediate disengagement. Sun et al. (2018) explain that even one cybersecurity incident can lead to reduced purchase intentions and a shift to competing platforms perceived to be more secure.

The transparency of a platform's cybersecurity policies further affects user engagement. Platforms that openly communicate about their security posture, explain user data rights, and take swift action after incidents tend to inspire greater loyalty (Jimmy, 2023). In contrast, those that operate in opacity and fail to disclose incidents in a timely manner can suffer long-term reputational damage.

From a strategic perspective, companies are increasingly viewing cybersecurity not just as a defensive necessity but as a proactive brand-building tool. McKie (2025) highlighted that leading digital brands use cybersecurity as a differentiator, especially in competitive markets like India, where consumer trust is hard-earned and easily lost. Bhosle and Shinde (2025) noted that in the context of digital payments and marketing ecosystems, regulatory compliance also reduces financial and legal risks, making cybersecurity a strategic imperative for both brand sustainability and growth.

In conclusion, the reviewed literature underscores the inseparability of cybersecurity from consumer trust and loyalty in digital marketing. In a market like India, where the digital space is evolving rapidly, and user expectations are becoming more sophisticated, cybersecurity is not just an IT concern—it is a business priority and a core element of customer experience. As such, Indian digital marketing platforms must not only implement robust security measures but also communicate their efforts transparently and ethically to sustain consumer trust and foster long-term loyalty.

Research Methodology

This study employs a mixed-methods research design, integrating both quantitative and qualitative methodologies to explore the relationship between cybersecurity measures, consumer trust, and loyalty within the Indian digital marketing ecosystem.

The research was guided by several hypotheses: that a strong cybersecurity framework (e.g., ISO, PCI-DSS) positively influences consumer trust; that higher trust levels contribute to greater loyalty in India's digital marketing sector; that cybersecurity initiatives impact purchasing behaviour and long-term brand commitment; and that trust in cybersecurity plays a role in consumers' willingness to engage with digital marketing efforts.

Adopting a mixed-methods approach, the research integrated both quantitative and qualitative methodologies. Quantitative data were collected through an online survey distributed to participants representing diverse demographic backgrounds across India, using Google Forms as the data collection tool. The survey assessed consumer attitudes toward cybersecurity, perceived trust, and loyalty behaviours. Stratified random sampling was employed to ensure broad demographic representation. The qualitative component involved a semi-structured interview with an industry expert, providing depth to the understanding of practical cybersecurity applications.

Data were analysed using various methods: descriptive and frequency analysis, reliability analysis, correlation analysis, and thematic transcription analysis for qualitative insights. This combination enabled a robust understanding of consumer behaviour and platform strategies.

A combination of primary and secondary data was used to ensure both depth and breadth of understanding. Data for the quantitative phase were collected using a structured online survey distributed via Google Forms during the spring of 2025. The questionnaire included multiple Likert-scale items ranging from 1 to 5 to assess respondents' perceptions of cybersecurity effectiveness, their trust in digital marketing platforms, and their degree of loyalty. The survey targeted digital consumers across India, and responses were obtained from 50 participants. A stratified random sampling technique was employed to ensure demographic diversity across variables such as age, gender, income level, region, and occupation.

For the qualitative phase, a semi-structured in-depth interview was conducted with a digital marketing professional experienced in cybersecurity implementation. The objective was to gain practical insights into how businesses apply cybersecurity strategies and how these practices influence consumer perceptions and engagement. The industry expert was selected through purposive sampling to ensure relevant professional expertise.

Following data collection, descriptive and frequency analyses were conducted to summarise demographic variables and key survey responses. This helped identify basic trends related to shopping frequency, trust levels, cybersecurity awareness, and experiences of data breaches. Relationships between variables were examined using Pearson correlation analysis to evaluate the strength and direction of linear associations, such as between cybersecurity perception and trust, or between trust and loyalty.

Overall, the integration of stratified random sampling for the survey and purposive sampling for expert interviews ensured both representativeness and relevance. The chosen methodology effectively enabled the study to address its research questions while maintaining analytical rigour and practical relevance.

Research Results

This section presents and interprets the key findings of the study based on data collected from the online survey and the expert interview. The results are organised to highlight different aspects of consumer behaviour and perceptions related to cybersecurity, trust, and loyalty. The analysis begins with descriptive insights on participants' shopping frequency across demographic groups, followed by an examination of the relationship between cybersecurity measures and consumer trust, the link between trust and loyalty, and the impact of visible cybersecurity cues on online purchasing behaviour. Together, these findings provide an integrated view of how cybersecurity practices shape consumer attitudes and engagement with digital marketing platforms in India.

Shopping Frequency by Income Level

The data analysed in Figure 1 reveal how income levels influence shopping frequency in digital platforms.

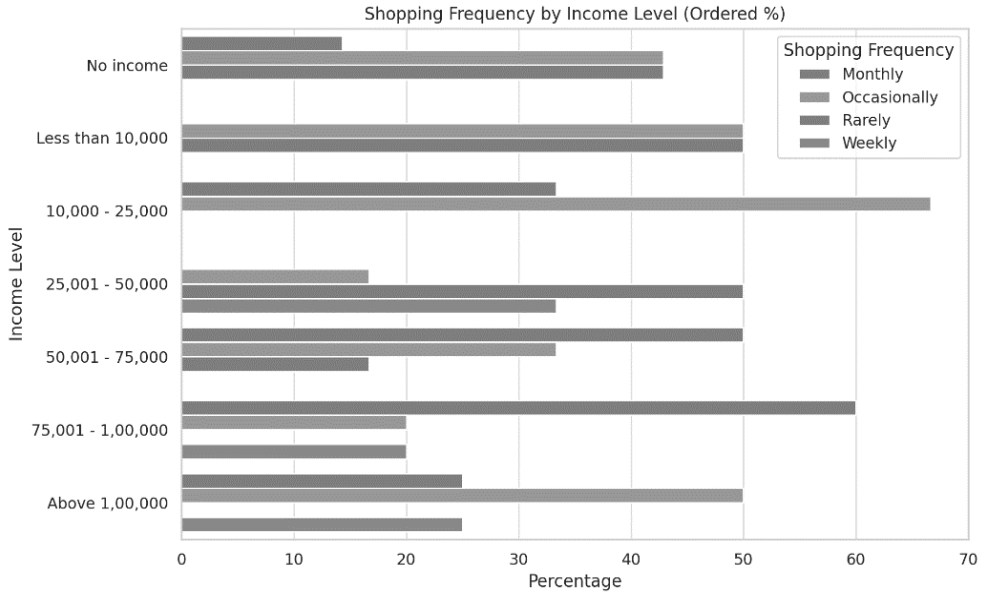

Fig. 1. Shopping frequency by income level (Source: made by author)

Based on the above chart on the Fig.1, there is a relative distribution of shopping behaviours within each income group. A larger share of higher-income groups shop monthly or occasionally. Lower-income segments show a broader spread, with some rarely or occasionally shopping.

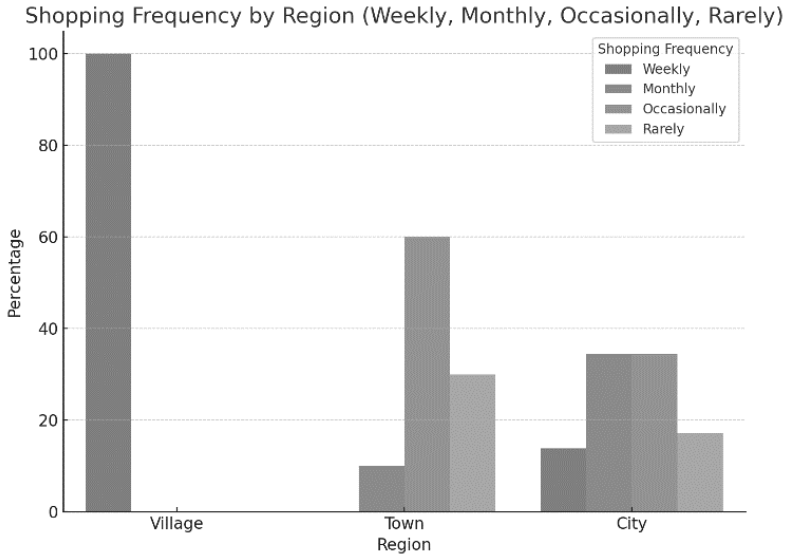

Fig. 2. Shopping frequency by region (Source: made by author)

Based on the survey results (Fig.2), there was a limitation in the number of responses from village users. Otherwise, we observe that city residents show mixed reviews of shopping frequency. Town residents mostly shop occasionally.

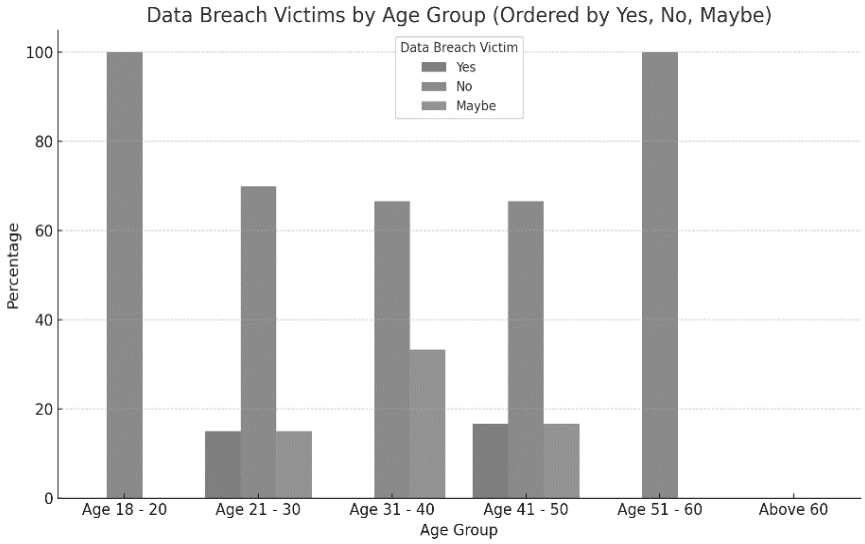

Fig. 3. Data Breach Victims by Age group (Source: made by author)

As per Fig.3, the age 21–30 and 41-50 group reports the highest 'Yes' responses, indicating higher exposure or awareness of online scams.

The Relation between Cybersecurity and Trust

Considering the survey and interview questions below (in order), a correlation and relation between Cybersecurity and Trust has been analysed.

- I believe Indian digital marketing platforms implement strong cybersecurity measures and certifications (such as ISO 27001 or PCI-DSS). [Referred to as A in the Table]
- I trust a platform more if it offers clear explanations of its data protection and privacy policies [Referred to as B in Table 1]

- Secure-looking websites (i.e., HTTPS sites that have a padlock option and no security warnings from the browser) and websites that mention they use data encryption make me feel more confident in sharing financial details. [Referred to as C in Table 1]
- I feel confident and safe sharing my personal information on digital marketing platforms in India [Referred to as D in Table 1]

Table 1. Correlation between Cybersecurity Measures and Consumer Trust (Source: made by author)

	A	**B**	**C**	**D**
A	1	0.26	0.12	0.57
B	0.26	1	0.56	0.13
C	0.12	0.56	1	-0.03
D	0.57	0.13	-0.03	1

The Relation between Trust and Loyalty

Dependent Variable: "I am more loyal to a digital platform that values my data security…"

From the survey and interview, three questions that represent the dimensions of trust were selected:

- I trust a platform more if it offers clear explanations of its data protection and privacy policies (Trust via policies).
- My trust in a platform influences my decision to make repeated purchases (Repeated purchase trust).
- I feel confident and safe sharing my personal information. (General confidence).

Table 2. Correlation between Trust and Loyalty (Source: made by author)

Predictor	**Coefficient**	**p-value**	**Interpretation**
Trust via policies	+0.44	0.0024	Positive and Significant
Repeated purchase trust	+0.45	0.0022	Positive and Significant
General confidence	+0.07	0.5081	Not significant

From Table 2, we can interpret that platforms that clearly explain policies and build repeat-purchase trust have a strong, proven effect on loyalty.

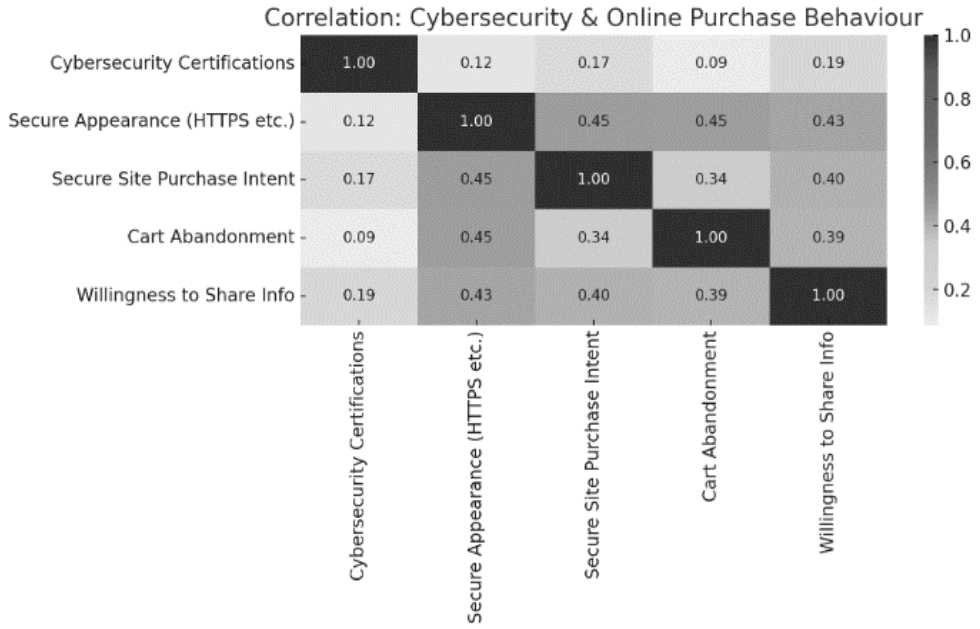

Fig. 4. Correlation between Cybersecurity and Online Purchase Behaviour (made by author)

Based on the results, we observe consumers react more to 'what they can see (HTTPS, padlocks, security badges)' than to technical compliance like ISO certifications.

Conclusions

In conclusion, this study demonstrates that cybersecurity plays a pivotal role in shaping consumer trust and loyalty toward digital marketing platforms in India. The main aim of this research was to analyse the impact of cybersecurity measures on consumer trust and loyalty toward digital marketing platforms in India. By focusing on how data protection practices, privacy transparency, and visible security cues influence user perceptions, the study sought to understand how trust mediates the relationship between cybersecurity and customer loyalty.

By adopting a mixed-methods approach, the research uncovered strong positive correlations between visible cybersecurity features such as secure websites, clear privacy policies, and responsive data protection practices and increased consumer trust. These trust elements, in turn, significantly influence consumer loyalty, particularly through repeat purchase behaviour and emotional confidence in the platform. While technical certifications like ISO 27001 (ISO/IEC 27001:2022, 2022) add value, consumers respond more strongly to easily visible and understandable security cues.

The findings reinforce the strategic importance of cybersecurity as more than a compliance necessity - it is a brand-building tool that can foster lasting consumer relationships. As digital adoption accelerates in India, platforms must align their cybersecurity efforts with consumer expectations by being transparent, proactive, and user-focused. Clear communication about data protection, user education on privacy rights, and visible commitment to secure online experiences can create a competitive advantage, enhancing both trust and loyalty in a crowded digital marketplace.

The results confirm that cybersecurity has a strong and positive influence on consumer trust, which in turn fosters greater loyalty toward digital marketing platforms. This finding aligns with previous research emphasising that transparent communication about data protection policies and visible security indicators enhances user confidence in online environments (Thaw et al., 2009). Similar to the conclusions of McKie (2025), this study also demonstrates that cybersecurity can serve as a strategic brand differentiator, reinforcing customer commitment and repeated engagement.

Furthermore, the finding that consumers respond more strongly to visible and easily understandable security cues rather than to technical certifications supports the observations of Wahab et al. (2023) and

Sun et al. (2018), who highlight the importance of perceived rather than purely technical security. These results suggest that user-oriented communication about cybersecurity is essential for building sustainable consumer trust.

In summary, the research contributes to the understanding that cybersecurity should not only be seen as a compliance requirement but as a strategic component of digital brand management. For practitioners, this means emphasising transparency, user education, and visible protective measures. For researchers, the study provides empirical evidence from the Indian context, supporting global findings that link security perception to customer loyalty in digital markets.

Disclosure statement

No potential conflict of interest was reported by the authors.

Declaration of generative AI in scientific writing

During the preparation of this work, the authors used Grammarly in order to improve grammar and ChatGPT to discuss the reviewer`s comments. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

Ajish, D. (2024). Streamlining cybersecurity: Unifying platforms for enhanced defense. *International Journal of Information Technology Research and Applications*, *3*(2), 48–57. https://doi.org/10.59461/ijitra.v3i2.106

Anurag, U., & Kaur, S. (2021). Systematic literature review on digital marketing in India: Present scenario. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3993539

Asthana, B. (2025, May 20). *Airtel launches fraud detection solution, a first in the world. Airtel*. https://www.airtel.in/press-release/05-2025/airtel-launches-fraud-detection-solution-a-first-in-the-world/

Bassano, C., Piciocchi, P., Spohrer, J. C., & Pietronudo, M. C. (2018). Managing value co-creation in consumer service systems within smart retail settings. *Journal of Retailing and Consumer Services*, *45*, 190–197. https://doi.org/10.1016/j.jretconser.2018.09.008

Bunnell, J. (2025, March 17). *6 cybersecurity threats of digital marketing*. *Spider AF*. https://spideraf.com/articles/6-common-cybersecurity-threats-in-digital-marketing

Carlsson, B. (2004). The digital economy: What is new and what is not? *Structural Change and Economic Dynamics*, *15*(3), 245–264. https://doi.org/10.1016/j.strueco.2004.02.001

Celestin, M. (2024). How emerging data protection laws are reshaping digital marketing and consumer privacy policies. *Brainae Journal of Business, Sciences and Technology. Available at SSRN*. https://doi.org/10.2139/ssrn.5188091

Da Silva Wegner, R., Da Silva, D. J. C., Da Veiga, C. P., De Fátima Barros Estivalete, V., Rossato, V. P., & Malheiros, M. B. (2023). Performance analysis of social media platforms: Evidence of digital marketing. *Journal of Marketing Analytics*, *12*(3), 599–610. https://doi.org/10.1057/s41270-023-00211-z

Bhosle, A., & Shinde, S. (2025, April 2). *The digital payments ecosystem of India: Planning security today for a resilient tomorrow. EY.* https://www.ey.com/en_in/insights/payments/the-digital-payments-ecosystem-of-india-planning-security-today-for-a-resilient-tomorrow

International Organization for Standardization (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. https://www.iso.org/standard/27001

Jackson, G., & Ahuja, V. (2016). Dawn of the digital age and the evolution of the marketing mix. *Journal of Direct Data and Digital Marketing Practice*, *17*(3), 170–186. https://doi.org/10.1057/dddmp.2016.3

Jimmy, F. (2023). Cloud security posture management: tools and techniques. *Journal of Knowledge Learning and Science Technology*, *2*(3), 614–622. https://doi.org/10.60087/jklst.vol2.n3.p622

Kannan, P., & Li, H. (2016). Digital marketing: A framework, review and research agenda. *International Journal of Research in Marketing*, *34*(1), 22–45. https://doi.org/10.1016/j.ijresmar.2016.11.006

Khamitov, M., Rajavi, K., Huang, D., & Hong, Y. (2024). Consumer Trust: Meta-Analysis of 50 years of Empirical research. *Journal of Consumer Research*, *51*(1), 7–18. https://doi.org/10.1093/jcr/ucad065

Kotler, P., & Keller, K. L. (2016). *Marketing management* (15th ed.). Pearson Education.

McKie, C. (2025, February 24). *Cybersecurity as a brand differentiator: Building consumer trust*. *Forbes*. https://www.forbes.com/councils/forbescommunicationscouncil/2025/02/24/cybersecurity-as-a-brand-differentiator-building-consumer-trust/

Nim, N., Pedada, K., & Hewett, K. (2024). Digital marketing ecosystems and global market expansion: Current state and future research agenda. *International Marketing Review*, *41*(5), 872–885. https://doi.org/10.1108/imr-04-2024-0108

Obitovich, K.M., Utkirovna, E.S. (2024). Quantifying the impact of cyber security risks on digital marketing ROI: A case study analysis. In Y. Koucheryavy, & A. Aziz (eds), *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. NEW2AN ruSMART 2023 2023. Lecture Notes in Computer Science (Vol 14542, (pp. 387–397). Springer. https://doi.org/10.1007/978-3-031-60994-7_33

Perwej, D., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A Systematic literature review on the cyber security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Ravikumar, T., Suresha, B., Prakash, N., Vazirani, K., & Krishna, T. (2022). Digital financial literacy among adults in India: Measurement and validation. *Cogent Economics & Finance*, *10*(1), 2132631. https://doi.org/10.1080/23322039.2022.2132631

Siddiqui, M. Y., & Gir, A. (2015). Integration of policy and reputation based trust mechanisms in e-commerce industry. *International Journal of Computer Applications*, *110*(8), 15–19. https://doi.org/10.5120/19337-0815

Skvarciany, V., & Jurevičienė, D. (2021). An approach to the measurement of the digital economy. *Forum Scientiae Oeconomia*, *9*(3), 89–102. https://doi.org/10.23762/fso_vol9_no3_6

Srivastava, R., Gupta, P., Kumar, H., & Tuli, N. (2023). Digital customer engagement: A systematic literature review and research agenda. *Australian Journal of Management*, *50*(1), 220–245. https://doi.org/10.1177/03128962231177096

Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1744–1772. https://doi.org/10.1109/COMST.2018.2885561

Thaw, Y. Y., Mahmood, A. K., & Dominic, P. D. D. (2009). A study on the factors that influence the consumers' trust on e-commerce adoption. *International Journal of Computer Science and Information Security*, *4*(1 & 2), 153–159. https://doi.org/10.48550/arxiv.0909.1145

Wahab, F., Khan, I., Kamontip, N., Hussain, T., & Amir, A. (2023). An investigation of cyber attack impact on consumers' intention to purchase online. *Decision Analytics Journal*, *8*, 100297. https://doi.org/10.1016/j.dajour.2023.100297

Verma, H. V. (2017). *Brand management: Text and cases*. Excel Books India