

Digital Trust in e-Commerce: A Netnographic Study of Risk, Security and Knowledge-sharing

Wafeequa Ben

University of Johannesburg, South Africa

wdinath@uj.ac.za

Abstract: Consumer trust remains a crucial determinant in e-commerce environments, yet it continues to be undermined by concerns surrounding digital risk, transaction security and platform reliability. While existing research has predominantly focused on technological and system-based determinants of trust, limited attention has been given to the role of informal knowledge sharing in shaping consumer perceptions and behaviour. This study adopts a knowledge management perspective to examine how digital consumers construct, negotiate and share knowledge about risk, security and trust within online communities. The research integrates a systematic literature review of studies published between 2021 and 2025 with a netnographic analysis of user generated discussions across digital platforms. The literature review synthesizes existing theoretical and empirical insights on digital literacy, trust and e-commerce security while the netnographic component captures naturally occurring peer interactions and experiential knowledge exchange. Thematic analysis reveals that online communities function as decentralised knowledge ecosystems where trust is collectively constructed through peer-led learning, emotional responses to risk and the use of cognitive heuristics in evaluating digital threats. These interactions transform individual experiences into shared knowledge that informs consumer decision making and risk perception. The findings contribute to knowledge management theory by conceptualising trust as a socially constructed knowledge-based asset emerging from informal digital interactions. This study further highlights the strategic importance of community-driven knowledge sharing processes in digital environments. Practical implications are offered for e-commerce platforms and policy makers seeking to leverage peer-based knowledge processes to improve user confidence and security engagement.

Keywords: Digital trust, Knowledge-sharing, e-Commerce, Netnography, Online consumer behaviour, Digital literacy, Informal learning, Knowledge management

1. Introduction

The rapid expansion of e-commerce has fundamentally transformed how consumers engage with markets enabling convenience, borderless and instantaneous transactions. However, alongside these advancements, persistent concerns regarding transaction security, privacy breaches and digital fraud continue to undermine consumer trust in online platforms. Despite significant technological progress in cybersecurity mechanisms, such as encryption protocols, secure payment gateways and artificial intelligence (AI) driven fraud detection, consumer trust remains uneven and, in many contexts, fragile. Existing research has predominantly approached trust in e-commerce from a technological and system-centric perspective, emphasizing platform security features, interface design and institutional assurances. While these dimensions are undeniably significant, such approaches often assume that trust is primarily an outcome of system reliability and technical robustness. This perspective overlooks a critical dimension of digital environments: the role of users as active participants in the creation, interpretation and dissemination of knowledge about online risks.

In parallel, the increasing prevalence of digital communities such as discussion forums, social media platforms and peer-to-peer networks has given rise to new forms of informal knowledge exchange. Within these spaces, consumers routinely share experiences, warnings, advice and evaluations of online shopping practices. These interactions extend beyond individual decision-making processes contributing to a collective understanding of risk, security and platform trustworthiness. From a Knowledge Management (KM) perspective, such environments can be conceptualised as decentralised knowledge ecosystems where experiential knowledge is continuously generated, negotiated and transferred among users. Despite the growing recognition of knowledge sharing as a central component of digital engagement, limited scholarly attention has been given to how these informal community driven processes shape trust in e-commerce contexts. There remains a lack of empirically grounded research that examines how consumers construct trust through real-time interactions and shared narratives within digital communities. This gap is particularly significant given the increasing complexity of online threats, where formal institutional communication may be insufficient to guide user behaviour effectively. Accordingly, this study adopts a KM perspective to examine how trust in e-commerce is constructed through the interaction between digital literacy and informal knowledge sharing within online communities. By integrating insights from both formal literature and real-world digital interactions, this study seeks to provide a more comprehensive understanding of trust as a socially constructed knowledge-based phenomenon.

This study is guided by the following research questions:

- How do consumers construct and share knowledge about risk and security in e-commerce environments?
- How is trust negotiated and developed within online consumer communities?
- What role does informal knowledge sharing play in shaping consumer trust and behavior in digital marketplaces?

2. Literature Review

This section reviews key literature on digital trust in e-commerce and the factors influencing consumer perceptions of risk and security.

2.1 Digital Trust in e-Commerce

The rapid digitalisation of commerce has enhanced consumer access to goods and services, offering convenience and expanded choices. However, despite these benefits, many consumers experience persistent concerns about the security of e-commerce platforms. Incidents such as unauthorised access, fraud, and data breaches continue to undermine trust in digital financial systems (Jayathilaka & Udara, 2024). These concerns highlight the central role of trust in shaping consumer engagement in digital marketplaces. Digital payment fraud not only erodes consumer confidence but also threatens broader financial stability (Khan *et al.*, 2024). Existing research has predominantly focused on technological and system-based aspects of e-commerce, including payment systems, platform design and security measures. While these elements are essential, they do not fully explain how trust is formed and maintained in practice. Importantly, trust is not solely a technical outcome but also a perceptual and interpretive process shaped by user understanding and experience. This suggests that technological reliability alone is insufficient and that consumer knowledge plays a crucial role in determining trust in digital environments.

2.2 Digital Literacy and Risk Perception

Perceptions of risk and trust in e-commerce are shaped by individual capabilities, particularly digital literacy. Digital literacy can be defined as an individual's ability to access, interpret, and critically assess digital information (Aslan *et al.*, 2024). Digital literacy enables consumers to recognise threats, understand platform security features, and make informed decisions. While technological interventions such as secure payment systems and robust authentication protocols constitute critical components of online transaction security, their effectiveness is limited when users lack the digital literacy required to engage with these systems effectively (Jayathilaka & Udara, 2024; Dai & Guo, 2022). As a result, consumers with lower levels of digital literacy may misinterpret risks, either overestimating threats or underestimating vulnerabilities. Conversely, individuals with higher levels of digital literacy demonstrate greater confidence in navigating digital environments and are more likely to adopt secure behaviours. This highlights the role of digital literacy as a mediating factor between technological systems and consumer trust reinforcing its importance in shaping e-commerce engagement.

2.3 Knowledge Sharing in Digital Environments

Despite the significance of digital literacy, consumers do not develop knowledge about online risks in isolation. Digital environments increasingly enable users to share experiences, advice and evaluations through online communities, social media platforms and peer-to-peer networks. These interactions facilitate informal knowledge exchange where individuals learn from the experience of others. From a KM perspective, these spaces can be understood as dynamic knowledge ecosystems that supports the creation, transfer and application of experiential knowledge. Through peer interactions, users collectively interpret risks, validate information and develop shared understandings of trust and security (Vo *et al.*, 2022). These processes extend beyond simple information exchange, involving social interaction, emotional expression and collective sensemaking. As such, knowledge sharing plays a crucial role in shaping how consumers perceive and respond to digital risks, positioning online communities as key sites of informal learning and trust formation.

2.4 Research Gap

Although existing literature has established the significance of digital literacy, trust and security in e-commerce, these elements have largely been examined in isolation. Current research tends to emphasize technological solutions and individual competencies with limited attention given to the social processes through which trust is constructed. There is a lack of empirically grounded research explaining how consumers

develop and negotiate trust through informal knowledge sharing within online communities. The gap is especially significant given the increasing complexity of digital risks and the growing reliance on peer-generated information in shaping consumer behaviour. Addressing this gap requires an integrated approach that considers both individual capabilities and collective knowledge processes. This study addresses this gap by examining how trust is constructed through the interaction between digital literacy and informal knowledge sharing within online communities. Figure 1 illustrates the conceptual framework underpinning this study, highlighting the relationships between digital literacy, risk perception, knowledge sharing and trust in e-commerce environments.

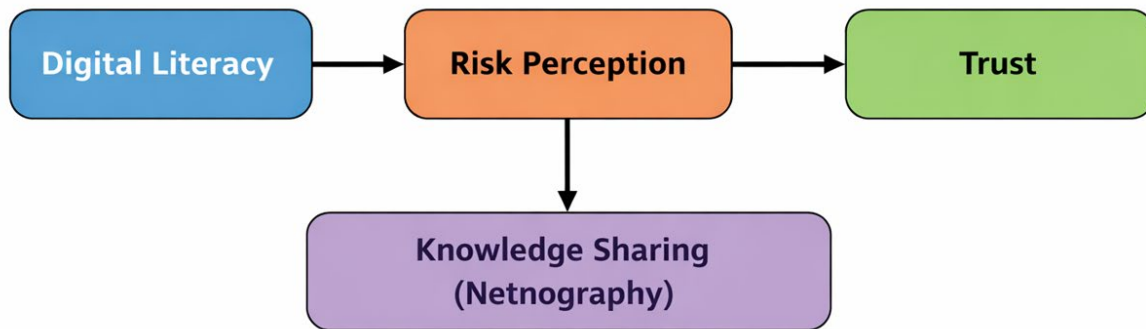


Figure 1: Conceptual Framework of Digital Trust in E-Commerce (Source: Author's Own, 2026)

3. Research Design and Methodology

This study adopts a mixed-method research design, integrating a systematic literature review (SLR) with netnographic analysis to investigate how trust in e-commerce is constructed through both formal knowledge and informal digital interactions. The mixed-method approach enables the integration of established academic insights with real-world user experiences, thereby providing a more comprehensive understanding of the research problem.

3.1 Systematic Literature Review

The SLR was conducted to establish a theoretical foundation on digital literacy, trust and e-commerce security (Shin & Lee, 2021:418). The review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines to ensure transparency and methodological rigour (Aslan et al., 2024:9). Peer-reviewed open access journal articles published between 2021 and 2024 were retrieved from the Clarivate Web of Science database using the search string “**digital literacy**” AND “**online security**” OR “**transaction security**”. Inclusion and exclusion were applied to ensure the relevance and quality of selected studies as summarised in Table 1.

Table 1: Inclusion and Exclusion Criteria (Source: Author's Own, 2026)

Criteria	Inclusion	Exclusion
Publication Years	2021, 2022, 2023, 2024, 2025	Publications outside the 2021–2025 range
Document Type	Peer-reviewed journal articles	Book chapters, theses, reports, non-peer-reviewed sources
Language	English	Non-English publications
Access Type	Open Access	Subscription-only or restricted-access content
Subject Scope	Digital literacy in e-commerce, online security, transaction security, consumers' perceptions, trust	Studies unrelated to digital literacy, security, online shopping or e-commerce
Data Source	Indexed in Clarivate Web of Science database	Grey literature, blogs, news articles, and unindexed sources

Table 1 outlines the criteria used to ensure that only relevant and high-quality studies were included in the review. A total of 26 articles were selected following a structured screening process. The study selection process followed PRISMA guidelines as illustrated in Figure 2. Data extraction was conducted using Microsoft

Excel, capturing key variables such as study focus, theoretical framework, and findings related to trust and risk perception (Falloon, 2023:11). The analysis employed thematic synthesis to identify recurring patterns and relationships across the literature. VOSviewer was used to support keyword co-occurrence analysis and thematic clustering.

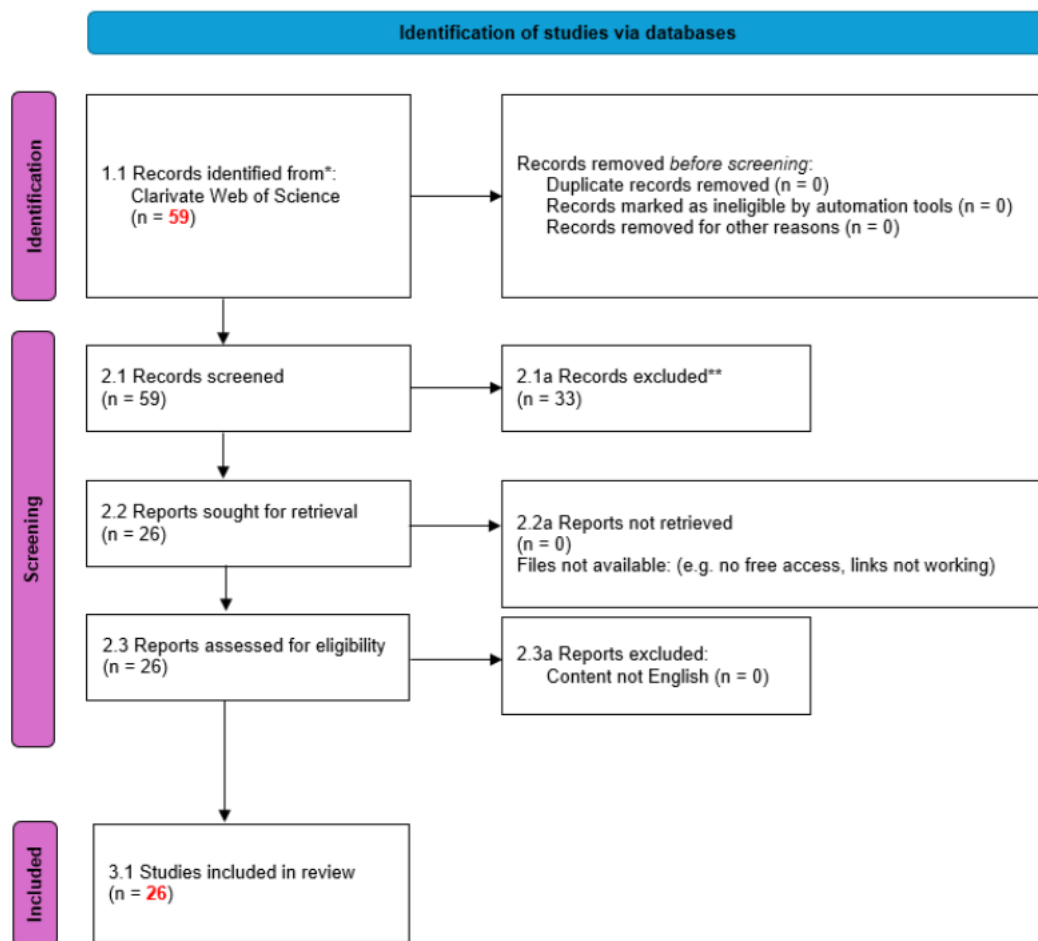


Figure 2: PRISMA Flow Diagram of Study Selection Process (Source, Author's Own, 2025)

3.2 Netnographic Approach

To complement the literature review, this study employed netnography as a qualitative research method to examine user-generated content within online communities. Netnography enables the study of digital cultures and communities through the observation of naturally occurring interactions. Data was collected from publicly accessible platforms including online discussion forums and social media communities where users engage in conversations related to e-commerce experience, digital risks and transaction security. Platform selection was based on relevant to e-commerce discussions, level of user interaction and accessibility of public content. A non-participatory observational approach was adopted, where posts, comment threads and discussions were systematically reviewed and documented. No direct interaction with participants was conducted.

3.3 Data Analysis

The netnographic data was analysed using thematic analysis involving the identification, coding and categorisation of recurring patterns in user discussions. Key analytical themes included peer-led knowledge sharing, emotional responses to risk, trust evaluation mechanisms and informal learning practices. The findings from the netnographic analysis were then compared with insights from the SLR to identify areas of convergence and divergence. This integrative approach embedded a deeper understanding of how theoretical insights align with real-world consumer behaviour.

3.4 Ethical Considerations

This study utilised only publicly available data and did not involve direct interaction with participants. All data were anonymised and no personally identifiable information was collected. The research adhered to ethical standards for digital research, ensuring respect for use privacy and data integrity. Ethical clearance for this was obtained from the University of Johannesburg ensuring compliance with institutional guideline for research involving digital data.

4. Findings

This section presents the findings of the study, beginning with insights derived from the SLR followed by the netnographic analysis.

4.1 Findings from Systematic Literature Review

Numerous key findings regarding how different levels of digital literacy affect consumers' risk, security and trust during online transactions are revealed by the SLR of 26 academic articles published between 2021 and 2025. The findings are presented thematically across key dimensions of trust, risk and digital literacy.

4.1.1 *Consumer perceptions of security and risk in e-Commerce*

Security refers to the extent to which users perceive digital transactions as safe and reliable. Perceived security is associated with the belief that unauthorised parties will not utilise a customer's confidential information. Trust and security are key determinants influencing the adoption of digital payment systems (Tsai, Chen, & Shih, 2022; Yu, Chen, Liu, Xu, & Lin 2024). There is significant risk factors associated with e-commerce transactions including financial and privacy related risks. Perceived financial and privacy risks significantly influence consumers' willingness to engage in online transactions.

4.1.2 *Digital literacy and risk perception*

Digital literacy refers to the ability to locate, evaluate and use information through digital technologies (Aslan et al., 2024). Consumers' perceptions of threat in e-commerce settings are correlated with their level of digital literacy, according to an analysis of the involved studies. Higher levels of digital literacy are associated with more accurate and nuanced risk assessments (Jayathilaka & Udara, 2024). Empirical studies indicate that digitally literate consumers are better able to distinguish between perceived and actual security threats, leading to more informed decision making (Bednarz et al., 2024). Conversely, lower levels of digital literacy are associated with misinterpretation of risks, including both overestimation and underestimation of threats.

4.1.3 *Consumer privacy concerns*

Online privacy refers to an individual's ability to manage and control personal information in digital environments. Studies indicate that while internet shoppers feel at ease sharing broad, vague details about their own preferences and alternatives, they are uncomfortable sharing specific identity and credit card information, which are regarded as highly sensitive information. Privacy concerns remain a significant barrier to participation in e-commerce activities (Jayathilaka & Udara, 2024).

4.1.4 *Digital payments and fraud*

Despite advances in fraud detection systems, vulnerabilities remain in identifying emerging threats (Yu, Wang, Liu, An, Yuan, & Panneerselvam, 2024). Digital payment methods have grown popular due to their efficiency and convenience; however, they introduce significant fraud risks. Most individuals began utilising internet access and internet services extensively during the lockdown since most retail transactions were limited to online, necessitating the widespread use of digital payment methods in addition to cash. The rising popularity of e-commerce purchases was also linked to the expanding use of digital payments. Trust and security are crucial when making transactions online (Bednarz et al., 2024). Digital payment methods have grown popular due to their efficiency and convenience features; however, they raise significant fraud issues. Protecting consumer data remains a persistent challenge in digital environments (Btoush, Zhou, Gururajan, Chan, & Alsodi, 2025). Fraud involving digital payments undermines user confidence and security in online shopping and threatens the stability of the financial system (Khan et al., 2024).

4.1.5 *Society's acceptance of e-Commerce*

Society's acceptance of technology is significantly predicted by their level of trust in technology and security while utilising it. An individual's preparedness for adopting mobile payment services is influenced by their

perception of trust. In the field of digital transactions, perceived trust refers to an attitude of confident anticipation that an individual's susceptibility will not be abused in an online risk scenario. As compared to conventional cash payment approaches, mobile payments can lead to further security issues, such as potential that unauthorised users could monitor personal financial information (Boufounou, Mavroudi, Toudas, & Georgakopoulos, 2022). Trust and perceived security significantly influence the adoption of e-commerce technologies. In contexts characterised by lower levels of digital literacy, consumers demonstrate reduces trust and a preference from traditional transaction methods. This highlights the significance of socio-economic and contextual factors shaping digital trust and technology adoption (Jayathilaka & Udara, 2024). A keyword co-occurrence analysis further confirmed the prominence of security, trust, risk and digital payments as dominant themes within the literature, these findings reinforce the central role of security and trust as foundational components in e-commerce adoption and risk perception.

4.2 Netnographic Findings

The netnographic analysis provided complementary insights into how consumers create and share knowledge about e-commerce risks within online communities. Unlike the structured findings of the SLR, the netnographic data revealed dynamic real-time interactions that reflect how trust is negotiated in everyday digital environment. Four dominant themes emerged from the analysis.

4.2.1 Peer-led knowledge sharing

Online communities function as informal knowledge-sharing environments where users actively guide and educate one another through experience-based insights. This shows that knowledge about e-commerce security is continuously co-created through interaction rather than solely derived from formal sources. Consumers often share personal experiences related to online scams, platform reliability and transaction failures. These experiences are often used to warn others, validate or challenge perceptions of trust or recommend safer practices. This peer-led exchange shows that knowledge about e-commerce security is not solely derived from formal sources but instead continuously co-created through interaction. Users rely heavily on community feedback when assessing unfamiliar platforms, highlighting the role of collective knowledge in shaping trust.

4.2.2 Emotional responses to digital risk

The analysis revealed that emotional responses play a critical role in how consumers interpret and communicate risk. Fear, scepticism and frustration were commonly expressed in discussions related to fraud and security breaches. These emotional narratives often amplified perceived risks, influencing how other users assess similar situations. Conversely, positive experiences contributed to reassurance and trust-building especially when users shared successful transactions and effective security practices. This indicates that trust is not purely rational but rather shaped by emotional and experiential factors embedded in shared narratives.

4.2.3 Cognitive shortcuts in trust evaluations

Consumers often employed cognitive shortcuts, or heuristics when assessing the trustworthiness of online platforms. These included relying on visible indicators such as website design, brand familiarity, user reviews and perceived legitimacy of payment systems. Rather than conducting detailed technical assessments, users simplified complex security considerations into easily interpretable cues. These shortcuts were often reinforced through community discussions where users collectively endorsed and challenged specific trust signals. These heuristics simplify complex security evaluations into accessible cues, often reinforced through community interactions.

4.2.4 Informal learning and collective sensemaking

The findings further show that online communities serve as spaces for informal learning, where users develop practical knowledge through observation and participation. Through continuous discussions, individuals refine their understanding of digital risks and appropriate security behaviours. This process reflects collective sensemaking because individuals' experiences are transformed into shared knowledge that informs group behaviour. As a result, trust emerges not only as an individual judgment but more of a socially constructed outcome that is shaped by continuous interaction within digital communities.

5. Discussion

This study demonstrates that digital literacy significantly shapes consumer perceptions of security, trust, and risk in e-commerce. Higher digital literacy enables more accurate risk assessment, while lower levels increase hesitation and perceived vulnerability. Trust and perceived security emerge as key drivers in adopting digital payment systems. A key limitation of the SLR is that relatively few studies explicitly examine how digital literacy influences consumer perceptions in real-world digital transactions. In addition, the findings of this study indicate that trust in e-commerce environments is shaped not only by technological infrastructure and individual digital literacy but also by social and interactive processes that occur within online communities. While the SLR emphasized the role of digital literacy in enabling accurate risk assessment and informed decision-making, the netnographic findings demonstrate how these understandings are actively constructed, negotiated and reinforced through peer interactions. The literature consistently highlights that higher levels of digital literacy are associated with improved risk evaluation and increased trust in secure systems.

However, the netnographic analysis extends this understanding by illustrating that knowledge about security and risk is not developed in isolation. Instead, it emerges through ongoing engagement with other users, where experiences, advice and warnings shared and collectively interpreted. This suggests that trust should be reconceptualised as a socially constructed, knowledge-based phenomenon rather than solely as a function of system reliability. Online communities act as decentralised knowledge ecosystems where informal learning processes enable users to navigate complex digital environments. These findings align with KM perspectives that emphasize the importance of knowledge sharing and collective learning in shaping behaviour. The interaction between knowledge sharing, emotional expression and heuristic decision-making contributes to both the amplification and mitigation of perceived risk, ultimately shaping consumer trust and engagement in e-commerce. From a practical perspective, the findings suggest that e-commerce platforms and policymakers should move beyond purely technical solutions and consider social dimensions of trust. Facilitating transparent communication supporting community engagement and leveraging peer-based knowledge sharing mechanisms may enhance user confidence and promote safer online behaviour.

While this study provides valuable insights into the relationship between digital literacy and e-commerce security perceptions, several research gaps present opportunities for future investigation. Future research should explore how cultural and socio-economic factors intersect with digital literacy to shape consumer behaviour across different contexts. Additionally, the long-term effects of digital literacy interventions on consumer trust and purchasing patterns warrant longitudinal study. Emerging areas such as the psychological impact of AI-driven security features on consumer confidence, the role of generational differences in technology adoption, and the effectiveness of various educational approaches such as gamification versus traditional training remain underexplored. Furthermore, comparative studies between developed and developing economies could yield important insights for tailoring inclusive digital commerce strategies. These gaps present rich opportunities for researchers to develop more nuanced understandings of how to bridge the digital divide while enhancing e-commerce security for diverse populations. Future studies should also examine the ethical dimensions of security technologies and their accessibility implications for vulnerable consumer groups.

6. Conclusion

The study examined how trust in e-commerce environments is constructed through the interplay of digital literacy, risk perception and informal knowledge sharing. By integrating a systematic literature review with netnographic analysis, this research provides a comprehensive understanding of both formal academic perspectives and real-world consumer interactions. The findings demonstrate that digital literacy plays a crucial role in shaping how consumers interpret and respond to online risks. Individuals with higher levels of digital competence exhibit more accurate risk assessment and greater confidence in engaging with secure systems. However, the study extends beyond this individual level perspective by revealing that trust is not formed in isolation. Instead, it emerges through social processes within online communities, where users share experiences, exchange advice and collectively make sense of digital threats. The netnographic insights highlight the importance of peer-led knowledge sharing, emotional narratives, and cognitive shortcuts in influencing how consumers assess risk and trust. These findings position online communities as decentralised knowledge ecosystems that allow for informal learning and collective sensemaking. In this context, trust can be understood as a socially constructed, knowledge-based asset that is shaped through continuous interaction rather than solely technological assurance.

From a theoretical perspective, the study contributes to knowledge management by extending the understanding of knowledge sharing and informal learning into digital consumer environments. It emphasises the role of community driven knowledge processes in shaping behaviour and highlights the need to integrate social dynamics into models of digital trust. From a practical perspective, the findings suggest that e-commerce platforms and policymakers should move beyond technical solutions and recognise the value of facilitating knowledge sharing among users. Enhancing transparency, supporting community engagement, and designing user-centred communication strategies may strengthen consumer trust and promote safer participation in digital marketplaces. Despite its contributions, this study is not without limitations. The reliance on publicly available online data may not fully capture private or platform restricted interactions and the scope of the literature review was limited to selected databases and time frames. Future research could explore cross-cultural variations, longitudinal changes in trust formation and the impact of emerging technologies such as AI on consumer perceptions of security. In conclusion, this study shows that trust in e-commerce is not merely a product of technological systems but a dynamic outcome of knowledge sharing, social interaction, and collective learning. Addressing digital literacy gaps while leveraging community-based knowledge processes will be essential for fostering resilient and inclusive digital marketplaces.

AI Declaration: No AI tools were used in the development of the paper. All work, including the analysis, interpretation and writing was conducted solely by the author.

Ethics Declaration: This study utilised publicly available online data and did not involve direct interaction with participants. All data was anonymised and no personally identifiable information was collected. Ethical clearance for this study was obtained from the University of Johannesburg ensuring that all research procedures complied with institutional ethical standards for research involving digital data. Ethical clearance number: 2025SciiS008.

References

- Aslan, A., Mold, F., Van Marwijk, H. & Armes, J. (2024). What are the determinants of older people adopting communicative e-health services: a meta-ethnography. *BMC health services research*, 24(1). Available from: <https://doi.org/10.1186/s12913-023-10372-3>
- Bednarz, J., Markiewicz, M. & Szmelter-Jarosz, A. (2024). Digital payments during the COVID-19 pandemic in Poland: An initial insight on the consumer perception of security and convenience. *Argumenta Oeconomica*, 1(52). Available from: <https://doi.org/10.15611/aoe.2024.1.07>
- Boufounou, P., Mavroudi, M., Toudas, K. & Georgakopoulos, G. (2022). Digital transformation of the Greek banking sector in the COVID era. *Sustainability*, 14(19). Available from: <https://doi.org/10.3390/su141911855>
- Btoush, E., Zhou, X., Gururajan, R., Chan, K.C. & Alsodi, O. (2025). Achieving excellence in cyber fraud detection: A hybrid ML+ DL ensemble approach for credit cards. *Applied Sciences*, 15(3). Available from: <https://doi.org/10.3390/app15031081>
- Dai, Z. & Guo, X. (2022). Investigation of E-Commerce Security and Data Platform Based on the Era of Big Data of the Internet of Things. *Mobile Information Systems*, 2022(1). Available from: <http://doi.org/10.1155/2022/3023298>
- Elciyar, K. & Satılmış, N. (2025). Development & Validation of a Blockchain Literacy Scale. *Acta Informatica Pragensia*, 14(1). Available from: <http://doi.org/10.18267/i.aip.251>
- Falloon, G., 2023, February. Twelve years of iPads and apps in schools: What conditions support effective practices in K-6 classrooms?. In *Frontiers in Education* 8(). Available from: <https://doi.org/10.3389/feduc.2023.1122522>
- Harnaningrum, L.N., Ashari, A. & Putra, A.E. (2022). Mobile payment transaction model with robust security in the NFC-HCE ecosystem with secure elements on smartphones. *International Journal of Advanced Computer Science and Applications*, 13(8). Available from: <http://doi.org/10.14569/IJACSA.2022.0130819>
- Jayathilaka, R. & Udara, I. (2024). Security matters: Empowering e-commerce in Sri Lanka through customer insights. *Humanities & Social Sciences Communications*, 11(1). Available from: <http://doi.org/10.1057/s41599-024-03585-2>
- Khan, A.R., Khan, S., Iqbal, S., Naqvi, R.A. & Alharby, M. (2024). FinSafeNet: Securing digital transactions using optimized deep learning and multi-kernel PCA (MKPCA) with Nyström approximation. *Scientific Reports*, 14(1). Available from: <http://doi.org/10.1038/s41598-024-76214-2>
- Khan, H.U., Alshurideh, M.T., Al Kurdi, B. & Al-Dmour, R. (2023). Role of authentication factors in fintech mobile transaction security. *Journal of Big Data*, 10(1). Available from: <http://doi.org/10.1186/s40537-023-00807-3>
- Rybina, L. (2021). Factors affecting usage of mobile payments by youth in Kazakhstan. *Innovative Marketing*, 17(4). Available from: [http://dx.doi.org/10.21511/im.17\(4\).2021.09](http://dx.doi.org/10.21511/im.17(4).2021.09)
- Sathupadi, K., Wijetunge, D., Perera, K. & Silva, D. (2025). BankNet: Real-time big data analytics for secure internet banking. *Big Data and Cognitive Computing*, 9(2). Available from: <https://doi.org/10.3390/bdcc9020024>
- Shin, S., & Lee, W. J. (2021). Factors affecting user acceptance for NFC mobile wallets in the U.S. and Korea. *Innovation & Management Review*, 18(4). Available from: <https://doi.org/10.1108/INMR-02-2020-0018>

- Sui, X.C. & Geng, X.H. (2021). Continuous usage intention to e-transaction cards in wholesale markets of agriproducts: Empirical evidence from China. *Future Business Journal*, 7(1). Available from: <http://doi.org/10.1186/s43093-021-00056-x>
- Tabirca, A.I., Dumitrescu, C. & Radu, V. (2025). Enhancing banking transaction security with fractal-based image steganography using Fibonacci sequences and discrete wavelet transform. *Fractal and Fractional*, 9(2). Available from: <https://doi.org/10.3390/fractalfract9020095>
- Tang, X.F., Liu, Y., Zhou, Q. & Chen, H. (2023). Regulating sharing platforms in lateral exchange markets: The role of power and trust. *European Journal of Marketing*, 57(4). Available from: <https://doi.org/10.1108/EJM-06-2021-0432>
- Tsai, S.C., Chen, C.H. & Shih, K.C. (2022). Exploring transaction security on consumers' willingness to use mobile payment by using the technology acceptance model. *Applied System Innovation*, 5(6). Available from: <https://doi.org/10.3390/asi5060113>
- Vo, T.H.G., Bui, D.H., Le, N.H. & Nguyen, T.V. (2022). Establishing customer behavior through e-commerce websites in newly emerging market. *Marketing and Management of Innovations*, (4). Available from: <https://doi.org/10.21272/mmi.2022.4-09>
- Yu, W.Y., Chen, H., Liu, H., Xu, J. & Lin, Z. (2024). A multiperspective fraud detection method for multiparticipant e-commerce transactions. *IEEE Transactions on Computational Social Systems*, 11(2). Available from: <http://doi.org/10.1109/TCSS.2022.3232619>