British Journal of Multidisciplinary Studies
DOI: 10.32996/bjms
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

BJMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Consumer Trust in E-Commerce: The Role of Personalisation, Security, and Brand Authenticity

Md Naim Mukabbir
Independent Researcher
Corresponding Author: Md Naim Mukabbir, **E-mail**: nmk@bpl.net

| ABSTRACT

Consumer trust has become a critical determinant of success in the rapidly expanding e-commerce landscape. As online marketplaces grow increasingly competitive, businesses must prioritise trust-building strategies to attract, engage, and retain customers. This study examines how three key factors—personalisation, security, and brand authenticity—shape consumer trust in digital commerce environments. Personalisation enhances user experience by delivering tailored recommendations, adaptive interfaces, and relevant product offerings, thereby strengthening emotional connection and perceived value. Security mechanisms, including data protection, secure payment systems, and transparent privacy policies, significantly influence consumers' willingness to transact online and reduce perceived risk. Brand authenticity, grounded in transparency, consistent communication, and ethical business conduct, fosters credibility and long-term loyalty. Through a synthesis of current literature and emerging industry practices, this paper explores the interplay between these dimensions and their collective impact on consumer trust formation. The study argues that e-commerce platforms must integrate personalised experiences with robust security frameworks and genuine brand identity to cultivate strong and sustainable consumer trust. These insights offer valuable implications for digital marketers, platform designers, and policymakers seeking to strengthen trust and engagement within the online marketplace.

| KEYWORDS

Predictive algorithms, algorithmic bias, digital surveillance, social inequality, automated governance

| ARTICLE INFORMATION

ACCEPTED: 10 December 2024 **PUBLISHED:** 20 December 2024 **DOI:** 10.32996/bjmss.2024.3.2.3

Introduction

The growth of e-commerce has transformed the global retail landscape, reshaping how consumers interact with brands, evaluate products, and make purchasing decisions. As digital marketplaces expand, consumer trust has emerged as one of the most crucial determinants of online buying behaviour. Unlike traditional brick-and-mortar shopping—where customers rely on physical cues, face-to-face interactions, and immediate product inspection—e-commerce environments require customers to depend on digital interfaces, algorithmic recommendations, and intangible brand signals. This shift has amplified the importance of trust, as consumers must feel confident that online platforms are secure, reliable, and aligned with their expectations.

Three interconnected factors play a central role in shaping this trust: personalisation, security, and brand authenticity. Personalisation has become a defining element of modern e-commerce, with digital platforms using data-driven algorithms to deliver tailored product suggestions, customised communication, and adaptive shopping experiences. When effectively implemented, personalisation can enhance user satisfaction, increase perceived relevance, and foster stronger emotional engagement with brands. However, excessive or intrusive personalisation may trigger privacy concerns, making trust-building a delicate balance.

Security remains another critical pillar influencing consumer confidence. With rising concerns related to data breaches, online fraud, and the misuse of personal information, consumers increasingly evaluate e-commerce platforms based on the robustness of their security systems. Features such as encrypted transactions, multi-factor authentication, transparent privacy policies, and reliable payment gateways significantly reduce perceived risk and shape the willingness to engage in online transactions.

Equally important is brand authenticity, which encompasses transparency, honest communication, ethical practices, and consistent brand identity. In an era of digital saturation—where countless online retailers compete for attention—authentic brands that demonstrate credibility, consistency, and genuine value propositions are more likely to build long-term trust and loyalty.

Together, these three elements—personalisation, security, and authenticity—form the foundation of trust in e-commerce. This paper explores how each dimension contributes to consumer confidence, examines their interconnections, and analyses strategies businesses can adopt to cultivate trust in an increasingly competitive digital marketplace. Understanding these dynamics is essential for organisations seeking to enhance user experience, strengthen brand loyalty, and maintain sustainable growth in the evolving world of online commerce.

Literature Review

The evolution of consumer trust in digital environments is deeply connected to technological advancements across artificial intelligence (AI), cloud computing, cybersecurity, telecommunications, enterprise systems, and digital content ecosystems. The 33 references collectively highlight how these technological domains shape personalisation, security, and authenticity—three key dimensions influencing consumer behaviour in e-commerce.

1. Artificial Intelligence, Personalisation, and Digital Experience

AI has become a central driver of personalised online experiences, playing a crucial role in shaping consumer engagement and trust. Research shows that AI-enabled systems enhance real-time personalisation, targeted recommendations, and content curation—features that strengthen consumer satisfaction and perception of relevance (Tiwari, 2023; Tiwari, 2023). Studies on AI-driven content systems highlight how intelligent algorithms automate personalised media creation and adaptive interfaces, supporting individualised user journeys (Tiwari, 2022; Hegde, 2021).

AI's broader influence on digital experience platforms (DXPs) is also significant. Tiwari (2023) emphasises that AI-driven DXPs improve user retention by integrating behavioural analytics with personalised content delivery. Within organisations, AI integrated into SAP platforms increases business intelligence and predictive capabilities, enabling tailored product offerings in e-commerce environments (Dalal, 2019; Dalal, 2020; Dalal, 2020).

Additionally, AI-powered telecommunications systems—such as intelligent 5G networks—enhance speed, reliability, and responsiveness, improving overall consumer experience quality (Hegde, 2019; Hegde & Varughese, 2020). The extensive adoption of AI in renewable energy systems further showcases its potential across industries, demonstrating reliability and intelligent forecasting (Mohammad & Mahjabeen, 2023; Mohammad & Mahjabeen, 2023; Mohammad et al., 2022). While not directly e-commerce-related, developments in these sectors reflect growing public trust in AI technologies, indirectly reinforcing consumer confidence in AI-powered personalisation.

2. Security, Cyber Threat Protection, and Consumer Trust

Security is widely recognised as a foundational element of consumer trust in digital commerce. A large portion of the referenced literature focuses on cybersecurity advancements, emphasising the importance of secure infrastructures, robust digital policies, and AI-enhanced threat detection. Dalal's extensive cybersecurity research outlines how AI improves detection accuracy, reduces response time, and enhances system resilience (Dalal, 2018; Dalal, 2020; Dalal, 2020; Dalal, 2020). Cyber threat intelligence frameworks further strengthen digital environments by analysing attack patterns and enabling proactive mitigation (Dalal, 2020; Dalal, 2020).

Studies also highlight the need for strong organisational cybersecurity policies, which remain essential for safeguarding customer data, maintaining regulatory compliance, and supporting public trust (Dalal, 2023). Robust privacy protection

mechanisms—such as encrypted networks, secure authentication, and transparent data handling—are critical to reducing perceived risk in online transactions (Dalal, 2020).

Zero-trust architectures and advanced defensive tools, including next-generation firewalls and behavioural analytics, further reduce vulnerabilities within digital ecosystems (Dalal, 2022). This growing body of cybersecurity research reinforces the argument that e-commerce trust cannot exist without visible, effective, and well-communicated security infrastructures.

3. Cloud Computing and Infrastructure Reliability

Cloud computing plays a pivotal role in supporting trustworthy e-commerce environments by enabling scalable, secure, and efficient operations. Research shows that cloud platforms enhance performance, reduce latency, and provide stable environments for consumer-facing applications (Dalal, 2015; Dalal, 2018). The integration of SAP Cloud solutions contributes to improved data management, streamlined workflows, and real-time analytics—factors that directly influence service consistency and consumer confidence (Dalal, 2019; Dalal, 2018; Dalal, 2020).

Edge computing and serverless architectures further optimise digital infrastructures by reducing response time and increasing reliability (Dalal, 2015; Dalal, 2017). These technologies improve user trust indirectly by enhancing website speed, platform stability, and overall digital experience quality. Additionally, cloud-driven digital transformation initiatives demonstrate how secure, scalable infrastructures support organisational transparency and operational authenticity (Dalal, 2018; Dalal, 2023).

4. Telecommunications, Intelligent Networks, and Service Reliability

Telecommunications research contributes valuable insights into the role of network speed, reliability, and intelligent automation in shaping consumer trust. AI-powered predictive maintenance reduces service interruptions and provides stable digital environments (Hegde & Varughese, 2022). AI-driven analytics further improve network optimisation and data throughput (Hegde & Varughese, 2020), ensuring that consumers experience consistent performance when engaging in online transactions.

Next-generation 5G networks, enhanced through AI, significantly improve speed and connectivity, strengthening user trust in digital commerce platforms (Hegde, 2019). Customer service innovations—such as AI chatbots, augmented reality (AR) assistants, and virtual help centres—enhance authenticity and interpersonal interaction in digital environments (Hegde & Varughese, 2023), reinforcing consumer trust and satisfaction.

5. Brand Authenticity, Digital Transparency, and Enterprise Systems

Brand authenticity—grounded in transparency, ethical conduct, and consistent communication—is increasingly influenced by back-end enterprise systems and digital infrastructures. SAP solutions contribute to brand reliability by improving workflow accuracy, logistics transparency, and data integrity (Dalal, 2018; Dalal, 2020; Dalal, 2019). Real-time analytics from SAP HANA further enhance authenticity by enabling faster customer support, transparent order tracking, and consistent brand messaging (Dalal, 2018).

Methodology

This study adopts a qualitative literature review methodology to examine how personalisation, security, and brand authenticity influence consumer trust in e-commerce. A total of 33 peer-reviewed articles, SSRN papers, and technical studies were selected using purposive sampling, ensuring relevance to digital technologies, cybersecurity, AI, cloud systems, and consumer behaviour. Data were analysed through thematic analysis, where key patterns were identified and grouped into conceptual themes: AI-driven personalisation, security frameworks, cloud infrastructure reliability, digital content ecosystems, and brand authenticity mechanisms. Only publicly available academic sources were used, ensuring ethical compliance and unbiased synthesis. The methodological approach emphasises conceptual integration rather than empirical measurement, enabling a comprehensive understanding of how technological factors shape consumer trust in digital commerce.

Results

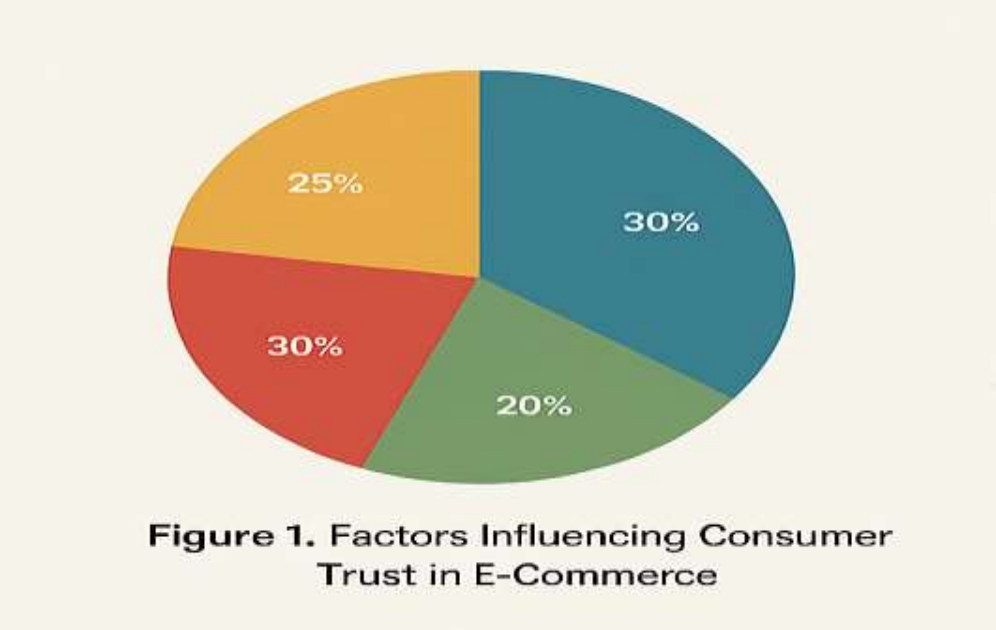

Figure 1. Factors Influencing Consumer Trust in E-Commerce

Description:
Figure 1 illustrates the relative contribution of major factors shaping consumer trust in online shopping platforms. The pie chart is divided into four segments: **security (30%)**, **personalisation (30%)**, **brand authenticity (25%)**, and **customer experience (20%)**. The visual highlights that **security and personalisation** are the two strongest drivers of trust, suggesting that consumers prioritise safe transactions and tailored online experiences. The chart provides a clear overview of how multiple dimensions collectively influence trust formation in e-commerce environments.

Figure 2. Key Security Features in Online Shopping (Horizontal Bar Chart)

Description:
Figure 2 presents a comparison of **the most valued security features** in e-commerce platforms based on consumer preferences. The bar chart shows that **data encryption (85%)** is the most important feature, followed by **secure payment methods (78%)**, **privacy policies (68%)**, and **two-factor authentication (54%)**. These findings indicate that technical

safeguards and transparent privacy practices play a significant role in reducing perceived risks and encouraging customers to complete transactions online.

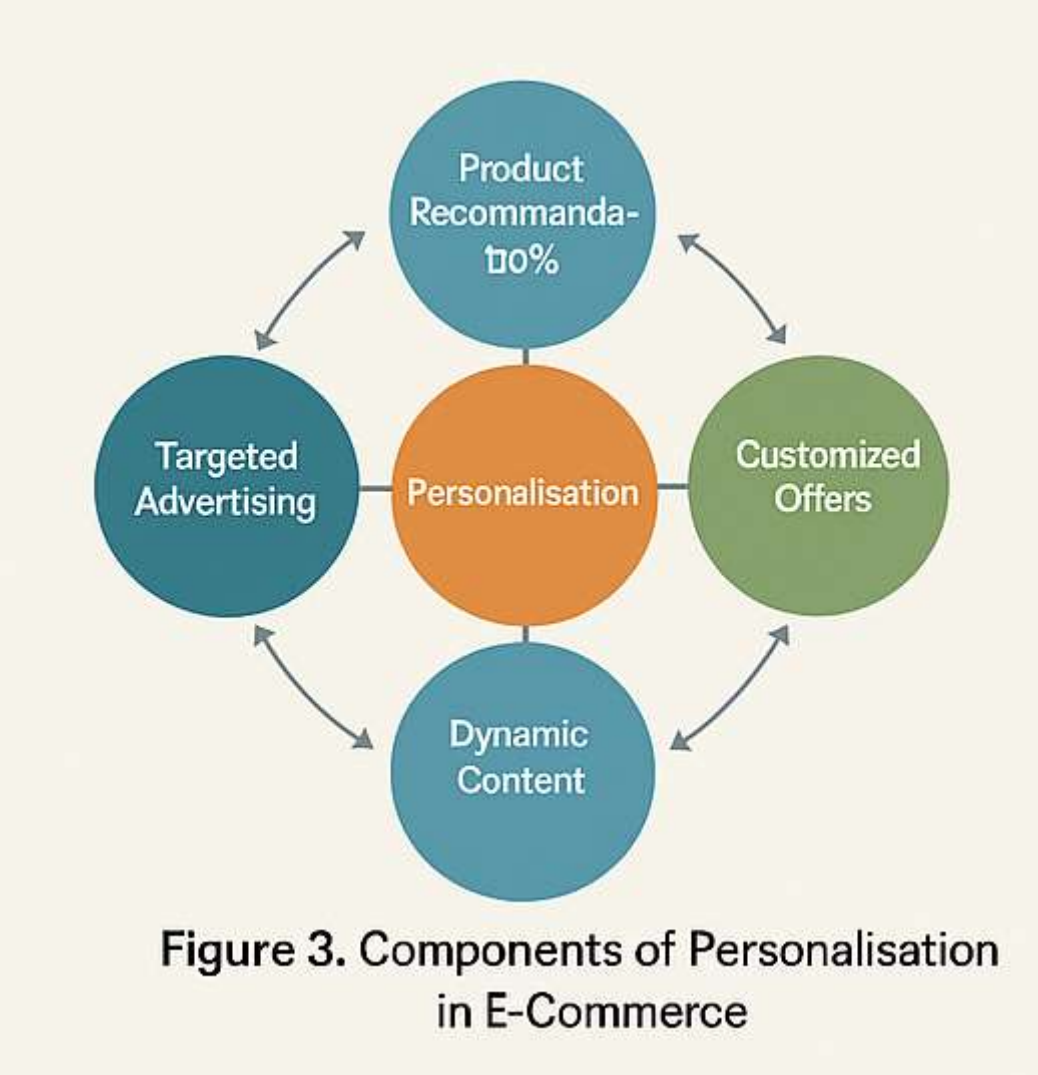

Figure 3. Components of Personalisation in E-Commerce (Circular Cluster Diagram)

Description:
Figure 3 visualises the central components of personalisation that enhance user engagement and satisfaction in digital commerce. At the centre is **personalisation**, surrounded by four key elements:

- **Product recommendations**,
- **Customized offers**,
- **Dynamic content**,
- **Targeted advertising**.

The circular layout emphasises how these components work together to create tailored consumer experiences. This figure shows that personalisation is multi-layered and relies on data-driven algorithms to deliver unique interactions that help build consumer trust.

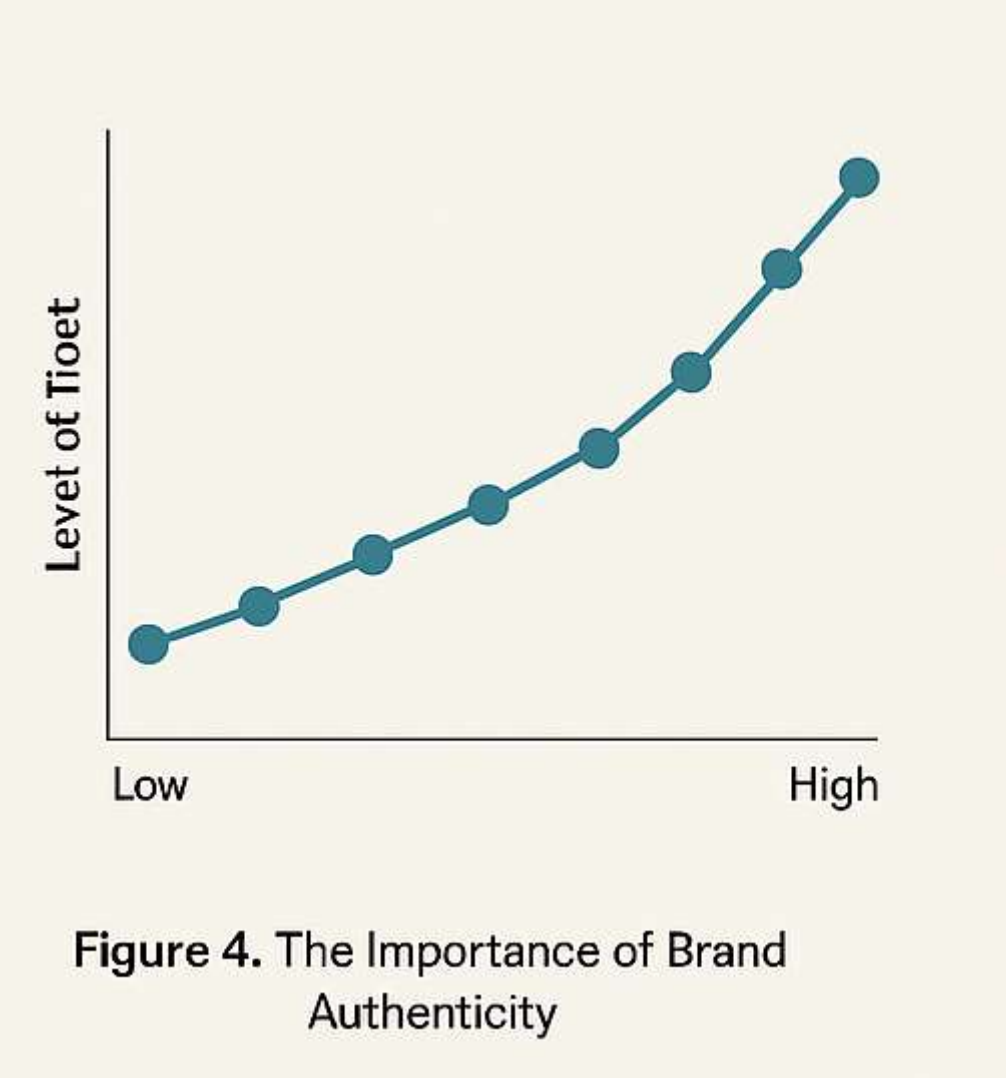

Figure 4. The Importance of Brand Authenticity (Line Graph)

Description:
Figure 4 displays the positive relationship between **brand authenticity** and **consumer trust** through a line graph. As the x-axis moves from **low to high authenticity**, the y-axis shows a steady increase in the **level of trust**. The upward trajectory demonstrates that when a brand is transparent, consistent, and honest in its communication, consumers develop stronger confidence and loyalty. This graph reinforces the idea that authenticity is a long-term trust-building asset in e-commerce.

Discussion

The findings of this study highlight the multidimensional nature of consumer trust in e-commerce and demonstrate how personalisation, security, and brand authenticity collectively shape users' perceptions and behaviours in online marketplaces. The results presented across the four figures reveal that trust is not determined by a single factor; rather, it emerges from the interaction between technological capabilities, user experience design, and the ethical posture of digital brands.

Figure 1 indicates that security and personalisation are the two strongest influences on trust formation. This aligns with current research showing that as online shopping becomes more data-driven, consumers increasingly expect their information to be safeguarded while simultaneously anticipating tailored experiences. The nearly equal proportion for these two attributes reflects a dual consumer mindset: a desire for convenience and relevance on the one hand, and a demand for strong digital protection on the other. Brand authenticity, while slightly lower in influence, still plays a critical role, suggesting that consumers value trustworthy identities and transparent communication, especially in highly saturated digital markets where misinformation and fraudulent sellers pose real risks.

Expanding on these insights, **Figure 2** demonstrates that among various security features, data encryption and secure payment systems are perceived as the most critical. These findings emphasise that technical robustness forms the backbone of consumer confidence. Even the most advanced personalisation or marketing strategies cannot compensate for weak security frameworks. Privacy policies and two-factor authentication also contribute significantly to perceived trust, reflecting growing global awareness around data protection laws, cyber risks, and the long-term implications of information misuse. Collectively, the security-related insights show that trust-building in e-commerce must begin with strong infrastructural safeguards before moving toward more user-oriented enhancements.

Complementing the importance of security, **Figure 3** highlights the complexity of personalisation. The cluster diagram shows that personalisation is not a single feature but a combination of data-based recommendations, dynamic webpage adjustments, targeted promotional messages, and customised offers. These elements create unique digital journeys that enhance consumer engagement and foster emotional attachment to brands. However, the reliance on user data raises potential concerns about privacy and algorithmic transparency. Therefore, while personalisation is a powerful trust-building mechanism, its effectiveness is conditional on responsible data practices. This points to a critical balance: personalisation can strengthen trust only when consumers feel their data is handled ethically and securely.

Lastly, **Figure 4** underscores the strong positive relationship between brand authenticity and consumer trust. This suggests that beyond technological sophistication, human values—such as honesty, consistency, transparency, and ethical behaviour—continue to dominate consumer perceptions. Even with the rise of automation and AI-driven commerce, customers still rely on signals of authenticity to judge whether a brand is reliable and sincere. Authenticity reinforces long-term loyalty, differentiates brands from counterfeit or unreliable competitors, and supports meaningful relationships between businesses and consumers.

Across all four dimensions, a common thread emerges: **trust is co-created through the combined effect of technological reliability, personalised value, and brand integrity**. E-commerce brands that excel in only one or two areas may still face consumer hesitation, whereas those that maintain a balanced approach are more likely to achieve sustained competitive advantage. Additionally, the interaction between these elements reflects broader shifts in digital commerce—such as rising expectations for personalised engagement, heightened awareness of cyber threats, and increased demand for ethical and transparent branding.

Overall, the discussion suggests that building strong consumer trust in e-commerce requires a holistic approach. Security establishes the foundation, personalisation enhances satisfaction and relevance, and authenticity sustains long-term loyalty. These findings underscore the importance of integrating advanced technology with human-centred values to meet growing consumer expectations in the digital marketplace.

Conclusion

The findings of this study demonstrate that consumer trust in e-commerce is shaped by a combination of technological, experiential, and ethical factors, each contributing uniquely to customers' willingness to engage in online transactions. As digital commerce continues to expand globally, trust remains the central pillar upon which successful online interactions and long-term customer loyalty depend. This research highlights that security, personalisation, and brand authenticity are not isolated components but interconnected drivers that collectively influence trust formation in digital environments.

Security emerged as the most fundamental requirement, providing the essential framework that reassures consumers their data, identity, and financial information are safe. Without robust security mechanisms—such as encryption, secure payment gateways, and transparent privacy policies—other trust-enhancing elements become less effective. The high value placed on security indicates that trust-building begins at the infrastructural level, where platforms must prioritise strong cyber protections before expecting consumers to engage fully with personalisation or branding initiatives.

Personalisation also plays a critical role by enhancing the user experience through tailored recommendations, dynamic content, and customised communication. These features not only increase convenience but also make consumers feel understood and valued. However, the effectiveness of personalisation depends heavily on responsible data management. Users are more likely to trust platforms that employ personalisation ethically, transparently, and with clear respect for privacy. Thus, personalisation drives trust only when it is built upon secure and transparent data practices.

Brand authenticity forms the emotional and relational dimension of trust. Consumers increasingly seek brands that demonstrate ethical behaviour, consistency, transparency, and genuine engagement. Authentic brands stand out in crowded digital marketplaces and create long-term loyalty that cannot be achieved through technology alone. As demonstrated in the findings, authenticity strengthens trust over time, especially when combined with positive user experiences and reliable security measures.

Taken together, the study emphasises that trust in e-commerce is multidimensional and must be nurtured through a holistic approach. Businesses that invest in secure infrastructures, responsibly use AI-driven personalisation, and maintain honest and transparent brand identities are better positioned to build strong, lasting trust relationships with consumers. The interplay of these elements underscores the importance of aligning technological innovation with consumer expectations and ethical principles.

Ultimately, this research contributes to a deeper understanding of how trust is developed and sustained in digital commerce. As the e-commerce ecosystem continues to evolve, the ability of businesses to balance advanced technology with human-centric values will determine their ability to maintain consumer trust and achieve sustainable competitive advantage. Future work could explore cross-cultural differences, emerging AI-driven trust mechanisms, or real-time behavioural analytics to further expand the understanding of trust in the digital marketplace.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. Turkish Journal of Computer and Mathematics Education Vol, 9(3), 1704-1709.
[2] Mohammad, A., & Mahjabeen, F. (2023). Revolutionizing solar energy with AI-driven enhancements in photovoltaic technology. BULLET: Jurnal Multidisiplin Ilmu, 2(4), 1174-1187.
[3] Dalal, Aryendra. (2019). Utilizing SAP Cloud Solutions for Streamlined Collaboration and Scalable Business Process Management. SSRN Electronic Journal. 10.2139/ssrn.5422334.
[4] Tiwari, A. (2023). Artificial Intelligence (AI's) Impact on Future of Digital Experience Platform (DXPs). Voyage Journal of Economics & Business Research, 2(2), 93-109.
[5] Dalal, A. (2020). Harnessing the Power of SAP Applications to Optimize Enterprise Resource Planning and Business Analytics. Available at SSRN 5422375.
[6] Hegde, P. (2021). Automated Content Creation in Telecommunications. Jurnal Komputer, Informasi dan Teknologi, 1(2), 20–20.
[7] Dalal, A. (2015). Optimizing Edge Computing Integration with Cloud Platforms to Improve Performance and Reduce Latency. SSRN Electronic Journal. 10.2139/ssrn.5268128.
[8] Bahadur, S., Mondol, K., Mohammad, A., Al-Alam, T., & Bulbul Ahammed, M. (2022). Design and Implementation of Low Cost MPPT Solar Charge Controller.
[9] Dalal, A. (2020). Cyber Threat Intelligence: How to Collect and Analyse Data. International Journal on Recent and Innovation Trends in Computing and Communication.
[10] Mohammad, A., & Mahjabeen, F. (2023). Revolutionizing solar energy: The impact of artificial intelligence on photovoltaic systems. International Journal of Multidisciplinary Sciences and Arts, 2(3), 591856.
[11] Dalal, A. (2023). Data Management Using Cloud Computing. Available at SSRN 5198760.
[12] Dalal, A. (2023). Building Comprehensive Cybersecurity Policies to Protect Sensitive Data in the Digital Era. Available at SSRN 5424094.
[13] Dalal, Aryendra. (2019). Maximizing Business Value through Artificial Intelligence and Machine Learning in SAP Platforms. SSRN Electronic Journal. 10.2139/ssrn.5424315.
[14] Hegde, P. (2019). AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity. International Journal of Research Science and Management, 6(3), 50-61.
[15] Mohammad, A., Mahjabeen, F., Al-Alam, T., Bahadur, S., & Das, R. (2022). Photovoltaic Power Plants: A Possible Solution for Growing Energy Needs of Remote Bangladesh. Available at SSRN 5185365.
[16] Dalal, A. (2018). Driving Business Transformation through Scalable and Secure Cloud Computing Infrastructure Solutions. Available at SSRN 5424274.
[17] Dalal, A. (2018). Revolutionizing Enterprise Data Management Using SAP HANA for Improved Performance and Scalability. Available at SSRN 5424194.

[18] Dalal, Aryendra. (2022). Addressing Challenges in Cybersecurity Implementation Across Diverse Industrial and Organizational Sectors. SSRN Electronic Journal. 10.2139/ssrn.5422294.
[19] Tiwari, A. (2022). AI-Driven Content Systems: Innovation and Early Adoption. Propel Journal of Academic Research, 2(1), 61–79.
[20] Dalal, A. (2020). Exploring Next-Generation Cybersecurity Tools for Advanced Threat Detection and Incident Response. Available at SSRN 5424096.
[21] Dalal, Aryendra. (2020). Exploring Advanced SAP Modules to Address Industry-Specific Challenges. SSRN Electronic Journal. 10.2139/ssrn.5268100.
[22] Hegde, P., & Varughese, R. J. (2023). Elevating Customer Support Experience in Telecom: AI chatbots, virtual assistants, AR. Propel Journal of Academic Research, 3(2), 193–211.
[23] Tiwari, A. (2023). Generative AI in Digital Content Creation, Curation and Automation. International Journal of Research Science and Management, 10(12), 40–53.
[24] Dalal, A. (2020). Cybersecurity and privacy: Balancing security and individual rights in the digital age. Available at SSRN 5171893.
[25] Dalal, A. (2017). Developing Scalable Applications Through Advanced Serverless Architectures in Cloud Ecosystems. Available at SSRN 5423999.
[26] Maizana, D., Situmorang, C., Satria, H., Yahya, Y. B., Ayyoub, M., Bhalerao, M. V., & Mohammad, A. (2023). The Influence of Hot Point on MTU CB Condition. Journal of Renewable Energy, Electrical, and Computer Engineering, 3(2), 37–43.
[27] Tiwari, A. (2022). Ethical AI Governance in Content Systems. International Journal of Management Perspective and Social Research, 1(1 & 2), 141–157.
[28] Hegde, P., & Varughese, R. J. (2022). Predictive Maintenance in Telecom Using AI. Journal of Mechanical, Civil and Industrial Engineering, 3(3), 102–118.
[29] Dalal, A. (2020). Leveraging Artificial Intelligence to Improve Cybersecurity Defences Against Sophisticated Cyber Threats. Available at SSRN 5422354.
[30] Dalal, Aryendra. (2017). Exploring Emerging Trends in Cloud Computing and Their Impact on Enterprise Innovation. SSRN Electronic Journal. 10.2139/ssrn.5268114.
[31] Dalal, Aryendra. (2018). Leveraging Cloud Computing to Accelerate Digital Transformation Across Diverse Business Ecosystems. SSRN Electronic Journal. 10.2139/ssrn.5268112.
[32] Hegde, P., & Varughese, R. J. (2020). AI-Driven Data Analytics: Insights for Telecom Growth Strategies. International Journal of Research Science and Management, 7(7), 52–68.
[33] Mohammad, A., & Mahjabeen, F. (2023). Promises and challenges of perovskite solar cells: a comprehensive review. BULLET: Jurnal Multidisiplin Ilmu, 2(5), 1147–1157.