Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-7 |July: 2026

Original Researcher Article

AI-Driven Trust in E-Commerce: Structural Pathways for Enhancing Consumer Confidence

Dnyaneshwaree Shrikant Jawale[1], Dr. Jyoti Singh[2], Dr. Nilesh R. Berad[3]

[1] Ph.D. Scholar, MET's Institute of Management (Affiliated to Savitribai Phule Pune University), Nashik, Maharashtra, India.
ORCID: 0009-0003-1567-9335

[2] GM – Academics & Training, Maharashtra State Faculty Development Academy, Pune, Maharashtra, India.
ORCID: 0009-0005-3882-574X

[3] Director, MET's Institute of Management (Affiliated to Savitribai Phule Pune University), Nashik, Maharashtra, India.
ORCID: 0009-0004-5510-7486

Corresponding Author:
Dnyaneshwaree Shrikant Jawale

ABSTRACT

Purpose: This study examines how Artificial Intelligence (AI) influences consumer trust (e-trust) in e-Commerce. It identifies key AI-driven factors, explores their interrelationships and develops a structural framework to explain how AI technologies enhance trust.

Methods: This study applies Interpretive Structural Modelling (ISM) to analyse nine AI-related variables: personalization, fraud detection, predictive analytics, transparency, recommendation accuracy, data privacy, customer support, reputation management and e-trust. Expert opinion was used to construct the VAXO matrix, followed by SSIM, reachability matrices, MICMAC analysis and a conceptual framework.

Results: The findings show that fraud detection, data privacy and predictive analytics are the strongest drivers of trust. Personalization, transparency and recommendation accuracy act as mediators, while E-trust emerges as the most dependent outcome variable. The structural model highlights how technical drivers combine with experiential factors to create consumer confidence on online shopping platforms.

Implications: This study makes both theoretical and practical contributions to the literature. For businesses, the framework offers actionable insights into building trust through transparent AI, robust fraud detection and ethical data practices. Policymakers emphasize the need for clear regulatory frameworks to protect consumer rights. It offers a foundation for future empirical studies across industries and geographies.

Originality: This study integrates multiple AI factors into a unified model of trust, providing a novel perspective on how AI strategically enhances consumer trust in e-Commerce.

Keywords: Artificial Intelligence, E-Commerce, E-trust, Interpretive Structural Modelling (ISM).

INTRODUCTION:

E-commerce platforms and E-commerce market are taking over the world. People regularly use commerce. The marketplace establishes and sustains itself by increasing consumer trust. E-trust is a critical challenge for commerce platforms, as very little is known about what gains customer E-trust. The growth of technologies has greatly affected mankind and computers and the world wide web have been the leaders of the knowledge revolution (Sang-Hyeak Yoon, 2025). The latest advancements in artificial intelligence (AI) have widened its range of use (Gillath et al., 2021). The increased use of Artificial Intelligence (AI) technologies in e-commerce platforms creates new possibilities, but also leads to several challenges in terms of how customers feel about privacy, dependability and security. AI's role is increasing in fraud detection, customer services and personalisation, yet thorough research is required to understand the capability of AI and the role it plays in the impact on E-trust.

This is the need of the hour and must be researched since if its role is not thoroughly researched companies are at risk of destroying customers' trust, which is a major obstacle in the retention and expansion of the customer base in this extremely competitive e-commerce landscape. In the wake of rapid e-commerce expansion, market competition has heightened significantly. Platforms must now prioritize strategies that both attract new customers and retain them. Customers represent the most valuable competitive asset. Success hinges not only on product quality but also on cultivating **customer stickiness** the likelihood that customers continually engage with a platform and remain loyal. This concept has gained strategic importance: loyal customers typically spend significantly more over time than new customers, contributing disproportionately to revenue enhancements.

Accordingly, e-commerce platforms face an urgent need to elevate the customer experience in ways that promote long-term engagement and strengthen customer loyalty. As the primary product discovery and consumption interface, e-commerce sites increasingly depend on personal recommendation services for fashion customer experiences (Song & Sun, 2019). Such recommendation services rely on advanced big data models using customers' past behavioral data to match product attributes with personal preferences and hence provide personalized recommendations (Barzegar Nozari et al., 2024). For example, Amazon the world-leading e-commerce site utilizes a personalized recommendation system that examines customers' purchases and search histories to present them with tailored shopping experiences. Such personalization helps customers find relevant products quickly hence, greatly enhances shopping convenience. (Cakmak et al., 2024) stated that such algorithmic recommendation mechanism might also limit customers' exposure to a wide variety of content and present them with a more restricted information space corresponding to their existing domain of interests. (Yan et al., 2025).

This research focuses on scientifically investigating how AI technologies aid in constructing and strengthening E-trust in the E-commerce industry. In particular, it aims to identify the mechanism by which AI-powered features, such as user-personalization, anti-fraud systems, predictive engines and transparency functions, engage with and affect consumer trust. With AI increasingly being integrated into online retail operations, it is essential to know which elements best promote trust, minimize perceived risk and enhances user satisfaction. This study intends to fill the gap between what is technologically possible and consumer perceptions by presenting an explicit model of how AI influences trust relationships in e-commerce.

Research Question:

How do AI-enabled mechanisms influence the formation of consumer trust in online retail platforms?

Which factors act as primary drivers, intermediaries, or outcomes in building consumer trust?

Can an ISM-based framework guide e-commerce platforms in prioritizing AI-enabled features to enhance trust effectively?

This study contributes to the existing body of knowledge by offering a comprehensive framework that captures the multifaceted impact of AI on E-Trust in e-commerce. Unlike previous studies that focused on isolated trust factors or generic digital trust, this study uniquely integrates AI capabilities within a structural model to reveal their collective influence. This highlights the pivotal role of AI in driving transparency, improving security and personalizing user experiences, thereby filling a gap in understanding how AI can strategically build consumer trust in online shopping environments.

The paper is organized into five sections, It starts with a review of the current literature on AI applications and trust in e-commerce, followed by the methodology outlining the interpretive structural modelling approach used to analyse variable interdependencies. The findings section presents the key AI factors influencing E-Trust, supported by matrix and digraph analyses. This is followed by a discussion of the theoretical and practical implications and the paper concludes with limitations and future research directions.

3. Key Enablers of AI-Driven E-Trust in E-Commerce

1. Personalization

AI-driven personalization customizes shopping according to consumer’s individual preferences, which can significantly boost consumer trust. Companies can provide accurate forecasts of customer requirements via machine learning algorithms that scan consumer information. (Sharma, 2023) found that personalization with AI enhances engagement and makes customers return to the platform, as they are made to feel heard and understood. (Singh, 2023) found that successful personalization also provokes a feeling of belonging to the platform, which is important for maintaining consumer loyalty.

2. Fraud Detection

AI-driven fraud detection builds consumer confidence by ensuring secure transactions, data protection and supporting the digital marketplaces. In addition, (N. Yildiz Z. O. ,. &. Beloff, 2020) suggest that AI-enhanced security features can positively impact trust and maintained transparency and accountability, making users feel protected and valued. Globally, fraud prevention has been studied for biometric authentication. In (Nguyen et al., 2021), whether convolutional neural networks in facial recognition-based payment authentication prevent identity fraud using facial biometric verification via AI and it was established that facial biometric verification via AI in payment authentication is better than conventional biometric methods of avoiding identity fraud (Zhang et al., 2023).

3. Predictive Analytics

Predictability is the reliability of a trustee's actions or performance over the long run by (Rheu et al., 2021). When the performance of an AI application is uniform over a long period and in different situations, it facilitates a more accurate prediction of the action of an application with some degree of confidence (Nordheim et al., 2019). Thus, predictability is connected with understandability, where users can predict the future actions of an AI if they can comprehend how it functions. This will prompt users to develop the common assumption that the new technology is reliable (i.e. reliability) (Sheridan, 2019). Accordingly, an increased level of predictability means that there is a decreased possibility of unforeseen effects that are unforeseen and potentially have adverse effects on society (Pringle et al., 2016). Belief is often regarded as the ultimate phase in trust development. Only after an AI application's performance is considered predictable and reliable will the user instil their trust and readiness to depend on technology when necessary (Rheu et al., 2021; Sheridan, 2019).

4. Transparency

Transparency in AI processes is critical to ensuring consumer trust. As consumers become more concerned with data privacy and using AI in their recommendations, transparent communication around the AI's role can reduce suspicion. (Schmidt et al., 2020) indicated that platforms based on transparent AI systems enable customers to know how their data are utilized, which decreases ambiguity and builds trust. This involves describing the rationale behind recommendation algorithms, which positively influences consumer trust by clarifying the advantages and disadvantage of AI systems clear (Teodorescu et al., 2023).

5. Recommendation Accuracy

AI- and machine-learning-based recommendation systems have been built to scan shopper behavior and make precise product recommendations (Fernandez-Garcıa et al., 2019). Studies also indicate that explanations in recommender systems can positively impact customers' buying intentions (Chen et al., 2019), with trust being an important mediator of these intentions (Gefen et al., 2003; Kim & Peterson, 2017). Therefore, recommendation precision is strongly linked to interpretability and transparency, both of which are critical for establishing consumer trust on an online shopping website.

6. Customer Support

AI-enabled customer support tools such as chatbots provide quick and consistent responses, increasing user satisfaction and trust in service reliability. Effective customer support increases interaction through positive psychological experiences, because users tend to engage and stick around when they are supported and cared for (Kosiba et al., 2020; Patterson et al., 2006). Over the long term, such support creates customer loyalty, as happy users tend to repurchase and develop long-term relationships with the platform and service providers (Griffin & Herres, 2002; D. Lee et al., 2015).

7. Reputation Management

Reputation management is critical in influencing consumer trust and the adoption of AI services, especially when users lack direct experience with new technologies. Consumers tend to generalize trust from a firm's established reputation to its new offerings by relying on previous experiences and brand image as cues for reliability (Eisingerich & Bell, 2008). Such evidence from online banking indicates that offline banks' trust significantly affect the adoption of their online services (E.-J. Lee et al., 2007) and in e-commerce, vendors' reputation trust positively affect repurchase intentions (Liu & Tang, 2018). A positive reputation therefore diminishes uncertainty, counters perceive risks and promotes consumer commitment, which supports commitment–trust theory (Morgan & Hunt, 1994). However reputation management is threatened when businesses launch high-autonomy AI services that are incompatible with their developed brand reputation since categorization theory posits that a negative fit between innovation and brand reputation has the potential to erode trust and lower the odds of adoption (Aaker & Keller, 1990; A. Y. Lee & Aaker, 2004).

8. Data Privacy

Data privacy is a critical ethical concern in AI-driven e-commerce. Because AI customizes shopping experiences using large volumes of data, extensive data gathering can impact consumer privacy. Consumers can be reluctant to interact with sites they perceive as too intrusive, particularly given the increased scrutiny of data practices. (N. Yildiz Z. O. ,. &. Beloff, 2020) point out that as consumers realize the personal data that are made available to AI systems, their trust in the latter declines, primarily if the usage of data should be communicated more transparently. (Chauhan & Keprate, 2022) point to stringent data governance rules underlining that "where there is no specific demarcation or consumer consent over data usage, there is a considerable risk that privacy rights might be violated on e-commerce platforms."

9. E-Trust

E-trust refers to customers' trust in internet shopping, which is the major basis for internet transactions. In such cases, consumers do not have to personally to encounter the seller. The notion of e-trust describes trust in the fulfillment of promises by service providers according to consumer expectations. E-trust not only acts as a platform for conducting transactions but also serves as an essential factor in building customer loyalty. Improved trust will boost customer satisfaction and move transactions into the future (Ltifi, 2023). Studies establish that the more e-trust consumers possess, the more satisfied they are following a transaction. This shows that e-trust has a positive effect on customer experiences when buying online. E-trust does not develop naturally; it needs be to developed through good interactions between consumers and providers. Providers' clear and correct information plays a significant role in establishing trust (Ltifi, 2023).

Research Methodology

This study used a qualitative approach grounded in Interpretive Structural Modelling (ISM) for the analysis of interdependencies between key AI-based factors and their influence on E-Trust in e-commerce. In developing the VAXO matrix, seven Artificial Intelligence, e-commerce and consumer behavior experts were sought for advice. These specialists provided their opinions about the relationships of nine key variables: "Personalization, Fraud Detection, Customer Support, Data Privacy, Reputation Management, Predictive Analytics, Transparency, Recommendation Accuracy and E-Trust." The collective opinions of the specialists were gathered and the most frequent opinion was used as the final opinion to build the VAXO matrix. "The matrix assisted in finding the direct and indirect effects between these variables, a robust explanation of the ways in which AI technologies support the development of trust in online shopping sites. Thereafter, a Structural Self-Interaction Matrix (SSIM) was formed along with the formation of reachability and digraph matrices to observe the hierarchical structure and the dependence between the factors. This approach allowed a realistic depiction of the way each variable impacts E-Trust and the way the factors that are powered by AI are linked in creating consumer trust in the web shopping situation." A VAXO matrix was created as shown in Table 1.

Table 1: VAXO Matrix

Factors	E-Trust	Recommen dation	Transparen cy	PA	Reputation Manageme	Data Privacy	CS	FD
AI Driven Personalization	V	X	O	O	O	O	O	O
AI Fraud Detection (FD)	V	O	O	O	O	X	O	
AI driven Customer Support (CS)	V	O	O	O	O	O		
AI Driven Data Privacy	V	O	V	O	O			
AI driven Reputation Management	V	O	O	O				
AI Predictive Analysis (PA)	V	V	V					
AI Transparency	V	V						
AI Recommendation Accuracy	V							
E-Trust	V							

Data Analysis and Interpretation:

Table 2: Structural Self-Interaction Matrix

Structural Self-Interaction Matrix (SSIM)

Variables	1	2	3	4	5	6	7	8	9
Personalization		O	O	O	O	O	O	X	V
Fraud Detection			O	X	O	O	O	O	V
Customer Support				O	O	O	O	O	V
Data Privacy					O	O	V	O	V
Reputation Management						O	O	O	V
Predictive Analytics							V	V	V
Transparency								V	V
Recommendation Accuracy									V
E-Trust									

In Interpretive Structural Modelling (ISM), the Structural Self-Interaction Matrix (SSIM) is a qualitative tool used to examine the interdependencies among various system variables, as presented in Table 2. In Interpretive Structural Modelling (ISM), the Structural Self-Interaction Matrix (SSIM) is a qualitative tool used to examine the interdependencies between various system variables. Four symbols are used to represent the direction and sign of relationships between two variables: 'V' indicates the column variable is influenced by the row variable, 'A' indicates the row variable influences the column variable, 'X' illustrates two-way influence between the two variables and 'O' represents no influence. The SSIM image captures the influences of nine variables: Personalization, Fraud Detection, Customer Support, Data Privacy, Reputation Management, Predictive Analytics, Transparency, Recommendation Accuracy and E-Trust. The most affected variable is E-Trust as it influenced by almost every other variable, which shows that it is a highly dependent outcome. Personalization is a driving influence because it affects multiple variables but itself is not affected, which shows its original role. Fraud Detection is a two-way process with Customer Support, which means high interdependence. Customer Support

Assists Data Privacy, Reputation Management and E-Trust and thus plays an important role as a connector. Data Privacy and Reputation Management both play supporting roles in influencing E-Trust. Predictive Analytics strongly influences Transparency, Recommendation Accuracy and E-Trust and thus is an important driver. On the other hand, Transparency and Recommendation Accuracy are intervening influencers that directly impact E-Trust. Typically, the matrix outlines a path from analytical and personalization-focused inputs to trust-building outcomes, which will prove helpful to systems that aim to enhance user trust and web reliability.

Table 3: Reachability Matrix

Variables	1	2	3	4	5	6	7	8	9	Driving Power
Personalization	1	0	0	0	0	0	0	1	1	3
Fraud Detection	0	1	0	1	0	0	0	0	1	3
Customer Support	0	0	1	0	0	0	0	0	1	2
Data Privacy	0	1	0	1	0	0	1	0	1	4
Reputation Management	0	0	0	0	1	0	0	0	1	2
Predictive Analytics	0	0	0	0	0	1	1	1	1	4
Transparency	0	0	0	0	0	0	1	1	1	3
Recommendation Accuracy	1	0	0	0	0	0	0	1	1	3
E-Trust	0	0	0	0	0	0	0	0	1	1
Dependence Power	2	2	1	2	1	1	3	4	9	

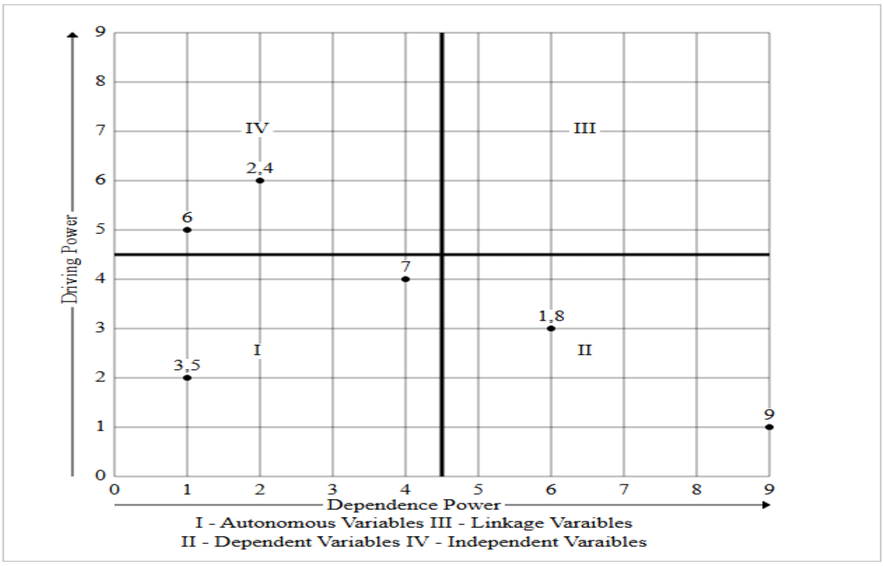
As shown in Table 3, the Reachability Matrix illustrates that the most dependent variable is E-Trust, which depends on all others with a power of 9. Data Privacy and Predictive Analytics hold the maximum driving power (4) meaning that they are significant drivers affecting other variables. Personalization, Fraud Detection, Transparency and Recommendation Accuracy were all moderately powerful, with a driving forces of 3. Customer Support and Reputation Management are the least powerful, indicating that they act as intermediate or support variables in the system. Overall, the matrix indicates how trust is established through the power of analytical, privacy and personalization-related factors.

Table 4: Final Reachability Matrix

Variables	1	2	3	4	5	6	7	8	9	Driving Power
Personalization	1	0	0	0	0	0	0	1	1	3
Fraud Detection	1*	1	0	1	0	0	1*	1*	1	6
Customer Support	0	0	1	0	0	0	0	0	1	2
Data Privacy	1*	1	0	1	0	0	1	1*	1	6
Reputation Management	0	0	0	0	1	0	0	0	1	2
Predictive Analytics	1*	0	0	0	0	1	1	1	1	5
Transparency	1*	0	0	0	0	0	1	1	1	4
Recommendation Accuracy	1	0	0	0	0	0	0	1	1	3
E-Trust	0	0	0	0	0	0	0	0	1	1
Dependence Power	6	2	1	2	1	1	4	6	9	

Table 4 presents that the Final Reachability Matrix (FRM) enhances the previous reachability matrix with the addition of transitive influences, represented by cells marked with an asterisk (*). These asterisks represent the indirect influences now covered, improving variable interaction accuracy. In this matrix, Fraud Detection and Data Privacy are the most dominant variables, both with the highest driving power of 6, suggesting they have a significant influence on many other factors within the system. Predictive Analytics closely trails behind a driving power of 5, indicating it too has an important role in influencing outcomes. Variables such as Transparency and Personalization have moderate driving powers of 4 and 3 respectively, while E-Trust continues to be the most dependent variable with a driving power of 1, i.e., it is affected by numerous others but affects none. The dependency power values indicate that all the variables impact E-Trust, further establishing its role as the most important output of the system. This matrix reflects the manner in which trust is ultimately developed through successive layers of interaction beginning from privacy, detection and analytics to personalization and transparency.

Figure 1: MICMAC Chart



The MICMAC (Matrix of Cross-Implication Multiplications Applied to Classification) chart is presented in Figure 1 that categorizes the nine variables according to their Driving Power (impact on other variables) and Dependence Power (how much they are impacted by). The graph is divided into four quadrants:

Quadrant I (Independent Variables): Low driving and low dependence power variables 3 (Customer Support) and 5 (Reputation Management) are somewhat detached from the system and exert little dependence or influence.

Quadrant II (Dependent Variables): Variables 1 (Personalization), 8 (Recommendation Accuracy) and 9 (E-Trust) have high dependence but low to moderate driving power, meaning that they are consequences with strong dependency on other variables but minimal influence themselves. Notably, E-Trust (9) had the highest dependence power with minimal driving power, marking it as the key dependent variable.

Quadrant III (Linkage Variables): No variables are plotted here, meaning that no variables are highly influential and highly dependent, indicating no complex feedback loops in the system.

Quadrant IV (Independent Variables): Variables 2 (Fraud Detection), 4 (Data Privacy) and 6 (Predictive Analytics) have high driving power but low dependence power, positioning them as key drivers or independent variables that influence many others without being heavily influenced themselves. Variable 7 (Transparency) lies just below the driving power threshold, serving a moderate driving role.

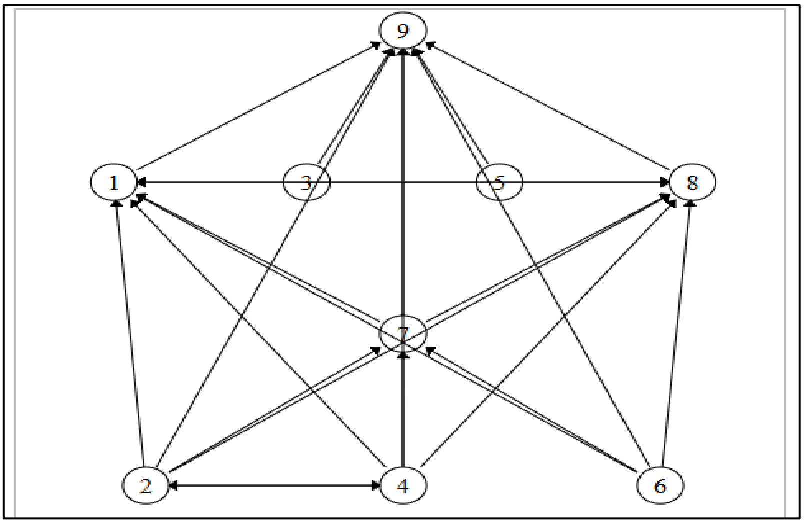
Fraud Detection, Data Privacy and Predictive Analytics are the main independent drivers shaping the system, whereas **E**-Trust, Personalization and Recommendation Accuracy are primarily dependent outcomes and Customer Support and Reputation Management are relatively autonomous with limited interaction.

Table 5: Level Partitioning

Elements(Mi)	Reachability Set R(Mi)	Antecedent Set A(Ni)	Intersection Set R(Mi)∩A(Ni)	Level
1	1, 8,	1, 2, 4, 6, 7, 8,	1, 8,	2
2	2, 4,	2, 4,	2, 4,	4
3	3,	3,	3,	2
4	2, 4,	2, 4,	2, 4,	4
5	5,	5,	5,	2
6	6,	6,	6,	4
7	7,	2, 4, 6, 7,	7,	3
8	1, 8,	1, 2, 4, 6, 7, 8,	1, 8,	2
9	9,	1, 2, 3, 4, 5, 6, 7, 8, 9,	9,	1

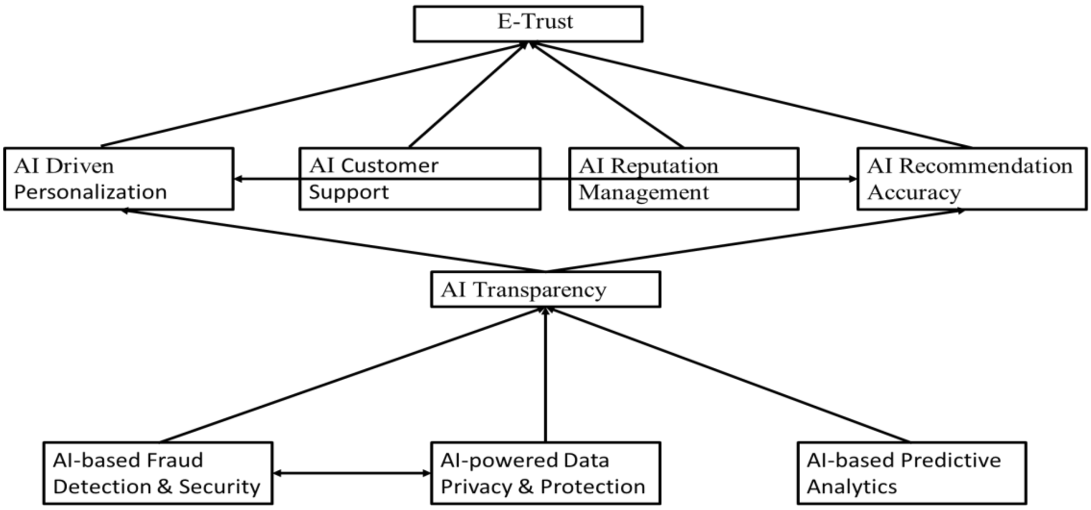
As illustrated in Table 5, Level Partitioning organizes variables into hierarchical levels based on their reachability and antecedent sets. Each variable's **Reachability Set** includes itself and the variables it influences, whereas the **Antecedent Set** lists the variables that influence it. The **Intersection Set** identifies the common variables in both sets and the assigned level corresponds to the variables where the reachability and intersection sets match. Here, **E-Trust (9)** is at Level 1, indicating that it is the ultimate outcome influenced by others but does not influence any variable itself. (1) Fraud detection (2), data privacy (4) and Predictive Analytics (6) are at Level 4 and are the core drivers with high control over the system. Middle variables such as Transparency (7) are at Level 3 and Personalization (1), Customer Support (3), Reputation Management (5) and Recommendation Accuracy (8) are at Level 2, acting as bridges between drivers and results. This hierarchical structuring aids in explaining the influence flow, indicating the way underlying factors propel middle-level factors that ultimately result in the outcome of E-Trust.

Figure 2: Digraph



As shown in Figure 2, the digraph graphically represents the directional relationships and influence among nine variables in the system. Each variable is defined by a node and the influence direction from one to another variable is represented by arrows. The graph illustrates the intricate web of influences, as seen that some variables, like nodes 2, 4 and 6, are influential drivers impinging on others, whereas nodes like 9 have the influence brought to them in the prime and therefore referred to as an outcome variable. The middle location of node 7 also indicates it plays a moderating or bridging function in the system. This diagrammatic representation is employed to explain the flow of influence and interdependencies and give a clear picture of how various factors are part of the dynamics of the system.

Figure 3: Conceptual Framework



The conceptual framework of this study is shown in Figure 3. Everything starts with three foundational elements: "Fraud Detection, Data Privacy and Predictive Analytics". These are the engines of the system. They can be seen as powerful and influences all the factors. However, they are largely self-contained. These core engines then power a critical set of operation functions: "Personalization, Customer Support, Reputation Management and Recommendation Accuracy". This is the point at which technical capabilities are translated into an actual user experience. This is achieved through transparency, which acts as a balancing factor to ensure accountability and openness. All of these factors then stream from the core elements, through operational functions, guided by transparency and finally create E-trust. This is the final measure of a user's confidence in e-commerce platforms. The above graphical representation is a blueprint of how AI technologies increase E-trust among of E-commerce users.

Discussion

Artificial intelligence technologies are significantly involved in the development of e-trust in e-commerce websites via several connected mechanisms such as personalization, fraud prevention, predictive analytics, transparency, recommendation precision, customer support, reputation management and data privacy. Personalization assists websites in making the online shopping experience consumer-specific to favor interests and enhances consumer engagement, loyalty and sense of belonging (Sharma, 2023; Singh, 2023). Fraud identification, particularly through biometric verification, promotes customer trust and transaction safety (Nguyen et al., 2021; Zhang et al., 2023). Predictive analytics enhances reliability and long-term trust by ensuring consistent and explainable AI performance (Rheu et al., 2021; Sheridan, 2019). Algorithmic explainability in data analysis and decision-making reduces uncertainty and promotes consumer trust (Schmidt et al., 2020; Teodorescu et al., 2023). Similarly, accurate recommendations promote higher user satisfaction and shopping intentions when complemented with interpretability (Chen et al., 2019; Kim & Peterson, 2017). Chatbots for AI-powered customer support establish trust and loyalty through responsive, stable and consistent support and effective conflict resolution (Kosiba et al., 2020; Verhagen & van Dolen, 2006). Reputation management also enhances trust by tapping into developed brand credibility, although highly autonomous AI technology can undermine this if viewed as divergent from brand personality (Aaker & Keller, 1990; Eisingerich & Bell, 2008). Third, privacy of data is an important driver of trust, since invasive or non-transparent practices will destroy customer faith and thus transparency and robust regulation are imperative (Chauhan & Keprate, 2022; Z. O. Yildiz & Beloff, 2020). Together, they influence consumers' trust, satisfaction and loyalty, making AI the foundation for developing safer, more trusted digital marketplaces.

Conflict of Interest: The authors declare no conflict of interest related to this research.

Conclusion

The findings of this study indicates that Artificial Intelligence (AI) significantly increases user trust (E-Trust) on e-commerce platforms. The key drivers of this confidence are the AI's ability to enhance fraud detection, ensure data privacy and power predictive analytics. This study highlights how the combined effect of these AI technologies fosters trust, with personalization and transparency acting as crucial mediators in this process. E-commerce companies can leverage AI to build trust by prioritizing transparent data practices, robust fraud prevention and user-friendly experiences. This AI-driven approach creates a safer and more reliable online shopping environment, ultimately promoting greater consumer well-being. The authors conclude that policymakers must understand these technologies to craft effective regulations. Ensuring that AI in e-commerce is transparent, secure and respectful of privacy is essential for maintaining public trust in digital marketplaces.

REFERENCES

Aaker, D. A., & Keller, K. L. (1990). Consumer Evaluations of Brand Extensions. Journal of Marketing, 54(1), 27–41. https://doi.org/10.1177/002224299005400102

2. Barzegar Nozari, R., Divsalar, M., Akbarzadeh Abkenar, S., Fadavi Amiri, M., & Divsalar, A. (2024). A Novel Behavior-Based Recommendation System for E-Commerce. arXiv Preprint arXiv:2403.18536. https://arxiv.org/abs/2403.18536

3. Cakmak, M. C., Agarwal, N., & Oni, R. (2024). The bias beneath: Analyzing drift in YouTube's algorithmic recommendations. Soc. Netw. Anal. Min, 14, 171. https://doi.org/10.1007/s13278-024-01343-5

4. Chauhan, S., & Keprate, A. (2022). Standards, Ethics, Legal Implications & Challenges of Artificial Intelligence. 2022 IEEE International Conference on Industrial Engineering and Engineering Management, ,1048-1052. https://doi.org/10.1109/IEEM55944.2022.9989614

5. Chen, X., Zhang, Y., & Qin, Z. (2019). Dynamic explainable recommendation based on neural attentive models". Proceedings of the AAAI Conference on Artificial Intelligence, 33, 53-60,. https://doi.org/10.1609/aaai.v33i01.330153.

6. Eisingerich, A. B., & Bell, S. J. (2008). Perceived Service Quality and Customer Trust: A Study of the Moderating Effect of Customer Loyalty. Journal of Service Research, 10(3), 256–268. https://doi.org/10.1177/1094670507310769

7. Fernandez-Garcıa, A. J., Iribarne, L., Corral, A., Criado, J., & Wang, J. Z. (2019). A recommender system for component-based applications using machine learning techniques". KnowledgeBased Systems, 164, 68-84,. https://doi.org/10.1016/j.knosys.2018.10.019.

8. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519

9. Gillath, O., Ai, T., Branicky, M. S., Keshmiri, S., Davison, R. B., & Spaulding, R. (2021). Attachment and trust in artificial intelligence. Computers in Human Behavior, 115.

10. Griffin, J., & Herres, R. T. (2002). Customer Loyalty: How to Earn it, how to Keep it. Jossey-Bass.

11. Kim, Y., & Peterson, R. A. (2017). A meta-analysis of online trust relationships in E-commerce. Journal of Interactive Marketing, 38, 44–54. https://doi.org/10.1016/j.intmar.2017.01.001

12. Kosiba, J. P., Boateng, H., Okoe, A. F., & Hinson, R. (2020). Trust and customer engagement in the banking sector in Ghana. Serv. Ind. J, 40, 960–973. https://doi.org/10.1080/02642069.2018.1520219

13. Lee, A. Y., & Aaker, J. L. (2004). The Impact of Sub-branding on Brand Loyalty: The Role of Perceived

Fit. Journal of Marketing, 68(1), 118–132. https://doi.org/10.1509/jmkg.68.1.118.24030

14. Lee, D., Moon, J., Kim, Y. J., & Mun, Y. Y. (2015). Antecedents and consequences of mobile phone usability: Linking simplicity and interactivity to satisfaction, trust and brand loyalty. Inf. Manage, 52, 295–304. https://doi.org/10.1016/j.im.

15. Lee, E.-J., Kwon, K., & Schumann, D. W. (2007). Segmenting the Non-Adopter Category in the Diffusion of Internet Banking. International Journal of Bank Marketing, 25(5), 332–352. https://doi.org/10.1108/02652320710772930

16. Liu, C.-C., & Tang, T. (2018). The impact of e-vendor reputation on repurchase intention in e-commerce: The mediating role of trust and satisfaction. Journal of Retailing and Consumer Services, 45, 92–103. https://doi.org/10.1016/j.jretconser.2018.08.005

17. Ltifi, M. (2023). Impact of the E-brand on the Consumer's E-trust, Reliance and Resistance Towards the Chatbot. In Communication Design and Branding: A Multidisciplinary Approach (pp. 267–292). Springer Nature Switzerland.

18. Morgan, R. M., & Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. Journal of Marketing, 58(3), 20–38. https://doi.org/10.1177/002224299405800302

19. Nguyen, L., Tran, H., & Pham, D. (2021). Enhancing fraud detection in online payments using deep learning-based biometric authentication. IEEE Access, 9, 105432–105445.

20. Nordheim, C. B., Følstad, A., & Bjørkli, C. A. (2019). An initial model of trust in chatbots for customer service-findings from a questionnaire study. Interacting with Computers, 31(3), 317–335. https://doi.org/10.1093/iwc/iwz022

21. Patterson, P., Yu, T., & Ruyter, K. (2006). Understanding customer engagement in services. Proceedings of the ANZMAC 2006 Conference: Advancing Theory, Maintaining Relevance, 4–6.

22. Pringle, R., Michael, K., & Michael, M. G. (2016). Unintended consequences of living with AI: The paradox of technological potential? IEEE Technology and Society Magazine, 35(4), 17–21. https://doi.org/10.1109/MTS.2016.2632978

23. Rheu, M., Shin, J. Y., Peng, W., & Huh-Yoo, J. (2021). Systematic review: Trust-building factors and implications for conversational agent design. International Journal of Human-Computer Interaction, 37(1), 81–96. https://doi.org/10.1080/10447318.2020.1807710

24. Sang-Hyeak Yoon, S.-H. Lee., Sung-Byung Yang. (2025). Comprehensive examination of the bright and dark sides of generative AI services: A mixed-methods approach, Electronic Commerce Research and Applications, Volume 70, 2025, 101491, ISSN 1567-4223, https://doi.org/10.1016/j.elerap.2025.101491. https://doi.org/10.1016/j.elerap.2025.101491.

25. Schmidt, P., Biessmann, F., & Teubner, T. (2020). Transparency and trust in artificial intelligence systems. Journal of Decision Systems, 29(3), 260–278. https://doi.org/10.1080/12460125.2020.1819094

26. Sharma, et al., S. (2023). Ethical Considerations in AI-Based Marketing: Balancing Profit and Consumer Trust. Tuijin Jishu/Journal of Propulsion Technology. Https://doi.org/10.52783/tjjpt.v44.i3.474. https://doi.org/10.52783/tjjpt.v44.i3.474

27. Sheridan, T. B. (2019). Individual differences in attributes of trust in automation: Measurement and application to system design. Frontiers in Psychology, 10, https://doi.org/1117. 10.3389/fpsyg.2019.01117. https://doi.org/10.3389/fpsyg.2019.01117

28. Singh, N. (2023). AI-Driven Personalization in eCommerce Advertising. International Journal for Research in Applied Science and Engineering Technology. Https://doi.org/10.22214/ijraset.2023.57695Yildiz,. https://doi.org/10.22214/ijraset.2023.57695Yildiz

29. Song, X., & Sun, H. (2019). Enhancing customer stickiness in e-commerce platforms: The role of information cocoon. Electronic Commerce Research and Applications, 36, 100861. https://doi.org/10.1016/j.elerap.2019.100861

30. Teodorescu, D., Aivaz, K., Vancea, D., Condrea, E., & Drăgan, C. (2023). Consumer trust in AI algorithms used in e-commerce: A case study of college students at a Romanian public university. https://doi.org/10.3390/su151511925.

31. Verhagen, T., & van Dolen, W. (2006). Explaining online purchase intentions: A trust-risk model. Proceedings of the 15th European Conference on Information Systems.

32. Yan, X., Wang, W., & Jiao, Y. (2025). Promoting or inhibiting? The impact of the information cocoon on customer stickiness in e-commerce platforms: The moderating role of decision-making style. Electronic Commerce Research and Applications, 71, 101505. https://doi.org/10.1016/j.elerap.2025.101505

33. Yildiz, N., Z. O. ,. &. Beloff. (2020). The Emerging AI Policy for e-commerce Industry. Proceedings of the 2020 5th International Conference on Intelligent Information Technology. Https://doi.org/10.1145/3385209.3385210. https://doi.org/10.1145/3385209.3385210

34. Yildiz, Z. O., & Beloff, N. (2020). The Emerging AI Policy for e-commerce Industry. Proceedings of the 2020 5th International Conference on Intelligent Information Technology. https://doi.org/10.1145/3385209.3385210

35. Zhang, Z., Gao, L., & Liu, Y. (2023). Explainable AI in financial fraud detection: A case research on deep learning interpretability. IEEE Transactions on Artificial Intelligence, 2(3), 289–300...