BenchCouncil Transactions on Benchmarks, Standards and Evaluations 5 (2025) 100247

Contents lists available at ScienceDirect

BenchCouncil Transactions on Benchmarks, Standards and Evaluations

journal homepage: www.keaipublishing.com/en/journals/benchcouncil-transactions-onbenchmarks-standards-and-evaluations/

Full Length Article

Evaluating barriers to establish digital trust in industry 4.0 for supply chain resilience in the Indian manufacturing industry

Vaibhav Sharma [a], Rajeev Agrawal [a,*], Anbesh Jamwal [b], Vijaya Kumar Manupati [c], Vikas Kumar [d]

[a] Department of Mechanical Engineering, Malaviya National Institute of Technology Jaipur Rajasthan 302017, India
[b] Operations and Decision Sciences, Jaipuria Institute of Management, Jaipur, India
[c] Operations & Supply Chain Management, Indian Institute of Management Mumbai, Mumbai, India
[d] University of Portsmouth, Winston Churchill Avenue, Portsmouth, Hampshire PO1 2UP, United Kingdom

ARTICLE INFO

Keywords:
Digital trust
Supply chain 4.0
Resiliency
Information-sharing
Digital transformation

ABSTRACT

Recent developments in Industry 4.0 technologies have led the manufacturing industry to implement them in its supply chains. The current state of lack of trust in digital systems has made organizations eager to build resilient systems to cope with uncertain circumstances. However, the challenges with handling stakeholder data with transparency, visibility, and accountability still persist. This transition demands the establishment of digital trust for secure information sharing and mitigating risks related to cybersecurity, data privacy, and potential misuse. Through a systematic literature review, this study identifies 17 barriers to establishing digital trust and applies exploratory factor analysis to group them into key dimensions. Further, a case-based analysis in the emerging Indian manufacturing economy's context employing Pythagorean Fuzzy Analytic Hierarchy Process-Decision-Making Trial and Evaluation Laboratory is conducted to prioritize these barriers and explore their interrelationships. The findings reveal that 'Top management commitment' and 'Cybersecurity' are the most influential barriers to be taken care of to promote collaboration and responsiveness in a digitally enabled supply chain environment. The study contributes by guiding practitioners and researchers working on the digital transformations for supply chains, highlighting digital trust as a foundational capability for achieving resiliency in Supply Chain 4.0. Being less explored in the field of supply chain digitalization, this study is a first step forward to explore digital trust in the Supply Chain 4.0 for resilience.

1. Introduction

Rising supply chain (SC) disruptions from disasters, instability, technological advancements, and shifting customer expectations exude the need for a resilient SC to cope with uncertainties, prevent delivery-supply delays, unmet demand, revenue loss, and business goodwill [1,2]. In the current era of digital transformation, resiliency can be built through digital trust (DT) in Industry 4.0 (I4.0), with a specific focus on transparency, legitimacy, and effectiveness for digital enterprise[1] The integration of I4.0 technologies, such as Artificial Intelligence (AI), Internet of Things (IoT), Big Data analytics, and blockchain (BC), has an impact on the resilience of different SCs [3–7]. These technologies enhance decision-making, responsiveness, and agility across the SC [8,9]. SC integrated with I4.0 can enhance flexibility through real-time asset tracking, enabling inventory, transportation, and distribution management [2]. Even leading consulting firms suggest that both data analytics and DT are important in business1.

It is well discussed in the literature that I4.0 potential is non-differentiable to transform and reshape SC practices, organizations, and their individual [10,11], which puts pressure on organizations to shift from traditional SC to Supply Chain 4.0 (SC4.0) [12]. Traditional SC refers to the flow of physical items and information through physical distribution channels, which consist of suppliers, warehouses, manufacturers, distributors, and customers [13]. However, the traditional SC

Peer review under the responsibility of The International Open Benchmark Council.
* Corresponding author.
E-mail addresses: vaib.me81@gmail.com (V. Sharma), ragrawal.mech@mnit.ac.in (R. Agrawal), anbesh.jamwal@jaipuria.ac.in (A. Jamwal), manupativijay@iimmumbai.ac.in (V.K. Manupati), vikas.kumar@port.ac.uk (V. Kumar).
[1] https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

https://doi.org/10.1016/j.tbench.2025.100247

Available online 3 December 2025

lacks real-time information flow, which lacks visibility, transparency, and integration, leading to inefficiencies in coordination, duty delays, and collaborative decision-making [9]. To address modern business challenges, the adoption of I4.0 technologies [14], leading transition toward SC4.0 or smart SCs [12]. In SC4.0 operations, there is a need to build a more efficient, flexible, and resilient system as it works on real-time data exchanges and process automation. This results in improved forecasting, reduced stockouts, and overproduction, and enables stronger collaboration and coordination among SC partners, with increased intelligent decision-making capabilities [15–17]. With the availability of these advantages, SC4.0 is still confronted with challenges of data integrity, cybersecurity, and trust in the I4.0 technologies' operations [18,19]. This underscores the need to explore DT in SC4.0.

In the cxtant literature, DT has been discussed as the confidence of stakeholders in an organization's ethical practices for the security, reliability in handling their sensitive and market-competitive information [20]. This lack of confidence can create a sense of hesitation among participants, particularly for organizations that operate or want to scale advanced digital technologies. This is evident in the report by James [21] that discusses eight recent cyberattacks on manufacturing, including data breaches at Volswagon's (April 2024), Nexperia's, Duvel Moortgat's, and Hoya Corporation's (March 2024), highlighting the vulnerability of interconnected systems. These incidents disrupt the end-to-end digital operations. Also, damaging the stakeholders' confidence and calling for an urgency to explore trust in digital transformation, making cybersecurity an SC risk, not a mere IT concern [18]. Further, in a global survey by PricewaterhouseCoopers [22] it is revealed that 58 % manufacturers anticipate software-level incidents in their devices, and 63 % of them foresaw a rise in third-party related cyber-threats. This necessitates that organizations revise policies and contracts with high-risk vendors and extend cybersecurity support through the DT framework and governance under unified compliance.

In an emerging economy like India, where government-led initiatives like 'Digital India' and 'Make in India' are creating a sense of motivation and pressure on firms to transform their traditional SC operations to SC4.0 operations to remain competitive [23,24]. However, many firms, being in their nascent stages, struggle to cope with digital transformation [25]. Although organizations may be aware of the cybersecurity risks and the importance of being resilient in the current uncertain environment, the aspect of DT is less explored [26]. This motivates us to explore the barriers to DT as a prerequisite for a resilient SC4.0

SC4.0 takes advantage of I4.0 technologies to act in uncertain and cyber-attack vulnerable environments [4]. This can instigate organizations to achieve resiliency in SC4.0 operations through transparency in real-time information exchange, which can enable swift recovery [6,7]. For instance, I4.0 technologies such as digital twin can capture dynamic demand patterns through real-time information sharing to forecast and predict inventory levels through analytics, thereby improving flexibility and resilience [3,27]. As visibility in SC 4.0 relies on information sharing about the product, location, and identity of upstream and downstream suppliers [5]. AI improves predictive maintenance, and BC ensures transaction transparency [28], and cloud platforms support seamless data sharing [29]. The confidence of SC stakeholders depends on the security of these platforms and the asset tracking mechanisms [30]. The extant literature has depicted the potential of I4.0 technologies in SC to build a resilient system. However, the effective security of information shared through these technologies relies on the building of DT among stakeholders in the digital ecosystem utilized by the organizations. This fear lies underneath due to risks of data breaches, identity theft, and unauthorized access to confidential business data [31]. Because integrity, security, and reliability of digital systems are the central column to build DT [32,33].

Despite the growing concerns over the security of data, DT has remained less explored, particularly in the fastly emerging economies like India. Most studies are focused on covering the technological and implementation aspects of SC4.0, subtly discussing DT in manufacturing SC of an emerging economy. For instance, Strazzullo [20] has explored DT as an internal phenomenon within manufacturing companies, highlighting the roles of both the individual and the organization. This study has given a specific focus on examining SC4.0 through the lens of DT for resiliency through the empirical validation of barriers to DT. Moreover, integrated multi-method approaches to capture priority and interdependence of barriers through industry perspectives in the horizontal value chain are still less explored. Therefore, this study aims to fill this gap by exploring, validating, and analyzing the DT barriers for resilient SC4.0 and pursues the following objectives:

- To identify and empirically validate the DT barriers.
- To prioritize and determine the causal relationship among the selected barriers.

To fulfill these objectives, the barriers were identified from literature and validated via an industry survey followed by Exploratory Factor Analysis (EFA) to uncover underlying dimensions. Further, a case study in an emerging economy's manufacturing organization used expert inputs analyzed using Pythagorean Fuzzy (PF) sets integrated with the Analytic Hierarchy Process (AHP) for prioritization, and the Decision-Making Trial and Evaluation Laboratory (DEMATEL) technique was applied to determine causal relationships among the barriers.

The study is composed of six sections. Section 2 presents a discussion of the background literature. Section 3 discusses the Methodology and its application. Section 4 presents discussions. Section 5 provides the implications. Section 6 discusses the conclusion and future research with practical limitations.

2. Background literature

This section develops the context and theoretical background of the study through the available literature on SC 4.0, DT, and their relationship to resiliency.

2.1. Supply chain 4.0 for resiliency

SC4.0 synchronizes operations with suppliers and customers [34] through collaborative actions and real-time information sharing [35], for the common perceived benefits such as inventory optimization, reduced delivery lead times, and enhanced SC agility and responsiveness [36,37]. In the horizontal value chain, integrating digital technologies enhances decision-making, risk management, visibility, transparency, and accountability throughout the SC [8,38,39]. Recently, the above issues have been highlighted by Patil, Srivastava [40] on digital twins for SC transparency, and suggested that DT can increase sustainable organizational performance. These digital transformations allow SC to reconfigure sustainability practices at the structural, process, and plant levels [41]. I4.0 technologies can provide greater flexibility and end-to-end visibility with a stakeholder-focused objective through real-time data exchanges as an organization's commitment to enhance its SC capabilities [42]. These commitments can be in terms of taking actions to build a robust cyber-secured infrastructure, data integrity measures for improving SC performance [43]. These measures are crucial to motivating organizations to establish a digitally trusted ecosystem for all SC stakeholders, fostering innovation and flexibility in the product value creation process [10]. In this regard, a cloud-based platform facilitates collaboration across the SC by enabling the sharing of data and information [44]. Therefore, I4.0 enables data-driven decision-making through collaboration, promoting transparency and addressing issues of disruptions, such as cyberattacks [10,38].

2.2. Theoretical background

Trust is regarded as a foundational concept in relational exchanges, building cooperation and reducing uncertainty in both traditional and

digital environments. According to the Trust Theory by McAllister [45], trust is conceptualised as one party's confidence in the reliability and integrity of another party. Process-based trust, in this context, reflects collecting detailed information to enhance interpersonal trust, whether between individuals or organizations. Rather than forming instantaneously, such trust evolves progressively across multiple interactions, wherein stakeholders actively evaluate available evidence to assess the credibility and dependability of their counterparts [46]. In the specific focus of SC, whereby the trustor's trust in one target transfers to another associated target, which implies that trust in SC practices corresponds to institutional trust, and its consequences can be transferred to particular products (interpersonal trust), thereby instilling the catalyst effect in operating on digital technologies [47]. Long established in the social sciences, Trust theory frames trust as a multi-dimensional construct encompassing cognitive, emotional, and moral components, and anchored perceptions of vulnerability, competence, and reliability between parties [48,49]. The traditional frameworks differentiate competence-based, integrity-based, relational, institutional, and system-based trust, which incubate cooperation and mitigate opportunism in complex organizational environments [50]. System-based trust corresponds to the confidence derived from institutional (organizational) management and arrangements to put regulations into action to reduce uncertainty in exchanges. The rational evaluations of competence and reliability based on available evidence put forth the cognition-based trust. Affect-based trust precludes emotional perceptions of the product and its information which correspond to the goodwill that goes beyond purely rational assessments. Institutional trust provides a broader spectrum consisting of societal norms, laws, and certifications that signal the legitimacy and compliance with international standards and frameworks [51]. Extending this view Lin and Lin [52] has utilised Commitment–Trust Theory in the purview of cloud SC adoption and outlined that a trusted relationship exists not only between people but also between people and computing systems, encompassing persistent trust in infrastructures, dynamic trust in specific situations, and persistent social-based trust that bridges social and technological confidence. Morgan and Hunt [53] extended this view through Commitment–Trust Theory (CTT) and reinforced that trust, coupled with commitment, is central to sustaining long-term relationships, a principle increasingly critical in digital ecosystems. In the SC4.0 environment, DT is built on the system's security, reliability, and stability, as well as the provider's credibility. These foundations serve as catalysts for commitment, which in turn strengthens long-term relational trust. This corresponds to the delicate nature of trust, which, although dynamic and evolving in context, interactions, and perceived risks, can deteriorate rapidly when breaches occur [54].

Extending the notion of trust to digital ecosystems, as depicted in Fig. 1, the trust in I4.0 is referred to as DT [55] can be understood as the willingness of stakeholders to rely on I4.0 technologies and platforms [56] under conditions of uncertainty, where confidence in data integrity, safety, system reliability, transparency, and institutional safeguards substitutes for traditional professional assurances. While DT is grounded in the same theoretical foundations as conventional trust, it is operationalized through mechanisms such as cybersecurity, regulatory compliance, and governance frameworks that ensure safety resiliency, transparency, interoperability, and ethical alignment in technologically mediated relationships [51]. System-based Trust in the digital ecosystem is expressed through cybersecurity protocols, BC verification, and governance structures that provide the robust structural assurance needed for secure information exchange and transaction integrity in SC4.0. Cognition-based Trust corresponds to confidence built on algorithmic transparency, data accuracy, and demonstrable technological competence of AI, IoT, and analytics systems for informed SC4.0 decision-making. Affect-based trust reflects user perception of fairness, ethical alignment, and confidence in digital platforms and automated systems. Institutional Trust in I4.0 context is anchored in adherence to international standards, regulatory frameworks, and certifications (e.g., ISO (International Organization for Standardization), GDPR (General Data Protection Regulation), NIST (National Institute of Standards and Technology)), which reassure compliance, accountability, and ethical practices across SC4.0.

2.3. Digital trust

DT has been the topic of discussion since the 90 s. However, there has

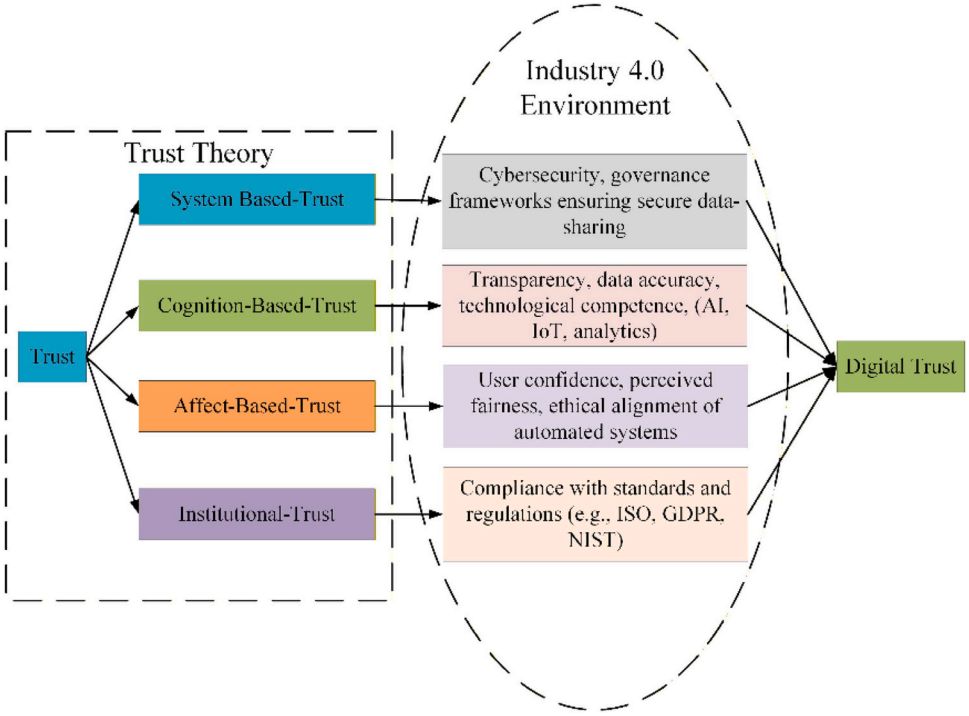

Fig. 1. Trust and Digital Trust.

been substantive discussion since 2016. It is characterized by a trustor, a trustee, trust in online merchants, vulnerability to trust violations by organizations, characteristics of an individual, and organizational responsibility [33].

DT is well-defined by Pietrzak and Takala [33] as:

"Digital trust is the measure of confidence that workers, consumers/ buyers, partners, and other stakeholders have in an organization's ability to protect data and the privacy of individuals."

According to the World Economic Forum [57]

"Digital trust is individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values."

Within the purview of the above definition, the literature also explains DT, which encompasses security, identifiability, traceability, and reliability [33]. DT is the stakeholders' confidence in maintaining the integrity of relationships, interactions, and transactions among the participants of the digital ecosystem [58]. The security and legitimacy of connected devices in the I4.0 environment are the pertinent requirements for DT [59]. So that the stakeholders can confidently engage in online transactions. At the same time, their data and information are secured [60]. A survey within the emerging economy's business landscape by Sivarama Krishnan [61] highlights that leaders' major focus is on cybersecurity. With these cybersecurity threats, an attack could result in a loss of customer data. User satisfaction with using digital technologies indirectly influences DT based on its perception [62].

2.4. Digital trust and supply chain 4.0

DT in SC4.0 lies much in altering the exchange and processing of information and fostering formal or informal business relations [55,63]. I4.0 technologies can help with transparency, better decision-making, asset utilization, and lower SC risks with reduced warehouse, transportation, and inventory costs [12]. The coupling of I4.0 technologies in the SCs opens up ways for information sharing as a key aspect among SC stakeholders, which is based on a trust mechanism [64]. This enables SC4.0 to access the stakeholders' real-time information sharing with full data transparency across the multi-tier as well [65]. However, the data protection of stakeholders in an SC4.0 environment depends on data integrity, privacy, and compliance management [66]. Furthermore, the issues of security, transparency, privacy, integrity, and reliability can be addressed by a robust digital ecosystem, enabling an efficient, resilient, and stakeholder-centric SC [67]. This generates an interest in exploring DT in SC4.0 for resiliency.

2.4.1. Digital trust and supply chain resiliency

The current digital environment creates a lacuna of trust among SC stakeholders, making them resistant to collaboration and agreement on specific data sharing, such as inventory and demand forecast policies [68]. For effective SC operations with I4.0, information sharing among partners is required, where trust between suppliers, distributors, and logistics providers is essential [69]. SC resilience corresponds to identifying flexibility, collaboration, agility, and trust within the network, building capabilities and enhanced risk management with reduced disruptions for trustworthy collaborations. I4.0 technology, such as the BC, enhances SC resilience by increasing SC trust with increased operational efficiency, cybersecurity, and order fulfilment with secured information sharing resistant to cyberattacks, enabling trusted transactions with reduced risk [14,70]. The more resilient the SC, the more trust in the organization handling data through BC [71]. However, the role of trust in addressing resiliency issues is not only related to the BC, but also trust in I4.0, as the umbrella is still to be addressed for SC resiliency. This study aims to fill this gap by identifying barriers to DT in SC4.0 for resiliency.

2.5. Research gaps

The extant literature within the context of the I4.0 environment for SC requires further exploration from the perspective of DT for resilient SC4.0. DT foundational requirements include security, identifiability, traceability, accountability, and fairness, which are well-articulated by [33,59,60]. Also, digital transformations have been linked to the sustainability of SC4.0 [41]. Lastly, stakeholder-centric initiatives by organizations with limited insights, aligning with DT, have been presented, where diverse stakeholders' expectations are critical to addressing cybersecurity challenges [58–60,62]. Despite studies highlighting challenges in adopting I4.0 technologies [12,34]. Similarly, the trade-offs between real-time information transparency and privacy concern the stakeholders' trust in the digital SC [10,17,65]. The role of digital systems and collaborative platforms in enhancing DT among the stakeholders is under-researched, with limited empirical investigations [10,44]. However, there is also a lack of exploration of a comprehensive assessment of the barriers to DT for SC 4.0 in the dynamic and emerging economies. Furthermore, the specific interplay of barriers to DT for resilient SC 4.0 remains less explored. Addressing these gaps is essential to advancing theoretical and practical knowledge of DT in SC 4.0, enabling robust, secure, and resilient SC 4.0.

3. Methodology

The strategic approach to analyzing the barriers to DT in SC4.0 in the emerging economy context is outlined through the methodology presented in Fig. 2. This approach extends the foundations led by previous studies (Table 1), which have demonstrated the effectiveness of mixed-method analysis designs in capturing complex I4.0 and SC problems. For instance Yadav and Singh [72] employed a three-phased methodology incorporating a literature review to identify 39 variables, Principal Component Analysis for reducing them into 12 factors, and fuzzy DEMATEL to examine cause-effect relationships. Similarly, Shayganmehr, Gupta [73] have utilized a two-module hybrid methodology combining EFA to categorize 29 critical success factors into five smaller constructs with a Hierarchical Fuzzy Expert System to assess the readiness of "swift trust" and "coordination" and to prescribe the most appropriate I4.0 tools through a case study. Other studies have utilised PF-AHP-DEMATEL for evaluating barriers to circular SC implementation [74], and EFA with AHP to evaluate challenges associated with I4.0 initiatives in the context of sustainable SC in emerging economies [75]. These applications reinforce the robustness of EFA, fuzzy logic, and case-based techniques in identifying and analyzing barriers. Guided by the literature, sixteen barriers were identified from the available literature and the consultation of area experts (demographics in Table 2) with rich experience in the fields of manufacturing, sustainability, I4.0, and SC management and their interrelations. Then, the industry experts were contacted through email, followed by discussions to understand the issues of DT in SC4.0. The identified barriers were shared with the experts, and mutual sharing of thoughts and experiences took place over the telephone and in person, resulting in the experts adding 'User Experience and Usability for Technology' as one more barrier and finalizing a total of seventeen barriers, as shown in Table 3 for empirical investigations.

3.1. Barriers to digital trust in supply chain 4.0 for resiliency

Through a three-step literature review, PRISMA is shown in Fig. 3. First, a search in the Scopus and Web of Science databases with keywords related to 'Supply Chain resiliency', 'Supply Chain', 'Trust', and 'Industry 4.0' was conducted. The articles were funneled down based on duplicity, research context, and studies focusing on the SC4.0 scenario. The study identified articles relevant to collecting key barriers to DT in SC4.0 for resiliency, resulting in sixteen barriers. Finally, the expert panel examined these barriers for confirmation, adding one more,

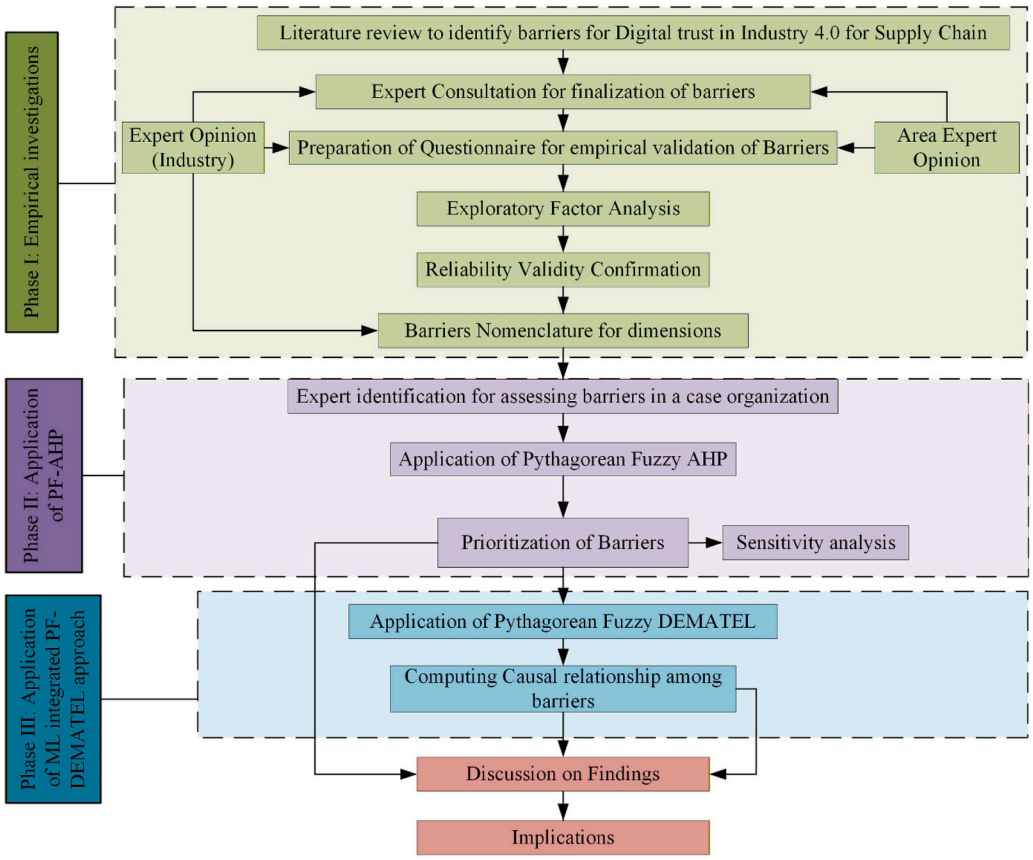

Fig. 2. Research Methodology.

resulting in a total of seventeen barriers, as shown in Table 3.

SC4.0 brings significant benefits of advanced digital technologies to enhance operational efficiency, responsiveness, and decision-making [16]. It enables real-time monitoring and enhances agility by making SCs more adaptable to disruptions caused by external factors such as global crises. It provides better visibility and traceability across different stages, leading to improved demand forecasting and reduced likelihood of stockouts or overproduction [9,44]. Despite the clear benefits, the operation of SC4.0 depends on information sharing, which is hindered by significant barriers to DT to achieve its full potential. One barrier is the perceived risk of cyberattacks and data breaches, which has grown with the increasing reliance on interconnected systems [76]. Additionally, the lack of standardized data security and privacy protocols across global SCs exacerbates these concerns, making it difficult for stakeholders to establish mutual trust [12,16]. The complexity of integrating disparate digital systems from various vendors introduces compatibility issues [77]. Trust in digital platforms is also undermined by the opacity of decision-making processes, where stakeholders may find it difficult to verify and validate algorithmic decisions, raising concerns about fairness and accountability [8,78,79]. Organizational and cultural resistance to change, particularly in industries with low digital literacy, represents a non-technical barrier to DT, slowing the digital transformation to SC4.0 [35,75].

Previous studies have focussed on identifying barriers to the digitalization of SC [16,32,75,78,79] with some studies [35,80–82] specifically focusing on BC implementing barriers while Yadav and Kumar [83], Khan, Haleem [84] analyzed barriers related to BC implementation in the emerging economy's manufacturing SC. However, the discussion and analysis of DT in adopting I4.0 for the SC present a significant gap.

3.2. Significance testing of barriers

This study is part of a broader investigation comprising barriers and enablers of DT in I4.0 for SCs in the emerging economy's manufacturing sector to establish DT and provide suggestions. Conducted between February and June 2024, this study analyzes barriers faced by manufacturing organizations. Professionals from 971 manufacturing firms with experience in SC and digital technologies were contacted via email and LinkedIn, with a brief explanation of the study's objectives. Using a five-point Likert scale, as used in previous studies [75,90], respondents rated the significance of various barriers with a questionnaire presented in Appendix A in the supplementary material. Initially, only 50 responses were received; however, after weekly reminders, 171 valid responses were collected, with 12 discarded due to biases or incomplete data, resulting in a 19.14 % response rate. This response rate is acceptable compared to similar studies [75,91]. The respondents' demographics are shown in Table 4. The mean and descriptive statistics of the identified barriers are detailed in Table 5.

3.3. Exploratory factor analysis

Exploratory Factor Analysis is a statistical method used for data reduction and analysis [92]. The reliability and validity testing of the factor was conducted using statistical software, SPSS, to validate the barriers. As per Table 5, the 'Kaiser-Meyer-Olkin' (KMO) value obtained was 0.873, i.e., higher than the minimum recommended range, i.e., 0.6. Bartlett's sphericity test is also found significant ($p < 0.01$). This suggests that the barriers collected for exploratory factor analysis are relevant. Further, the eigenvalues of discontinuity for the barriers are greater than 1.0, factor loadings are greater than 0.5, which suggests the collected data has convergent validity, and Cronbach's alpha is >0.7 as per the available literature by Nunnally [93]. Table 5 shows the results of the EFA after performing the dimension reduction. Four key dimensional

Table 1
Comparison of related works.

Reference	Problem addressed	Methodology	Technique
Yadav and Singh [72]	Traditional SC issues transparency, traceability, and data security. Factors such as human errors, fraud, delays, and documentation inefficiencies affect sustainability. Blockchain adoption to make a sustainable SC. Framework for critical factors of blockchain success.	Expert survey. Reduction of 39 blockchain variables to key factors. Identify cause–and–effect relationships among 12 key factors.	Principal Component Analysis and Fuzzy DEMATEL.
Shayganmehr, Gupta [73]	Investigated the humanitarian SC struggling with poor coordination, low information quality, and a lack of swift trust. Disaster events like pandemics require collaboration and smooth information exchange for effective relief operations.	Reduction of 29 critical success factors into 5 meaningful constructs: Logistics, Learning, Transparency, Information Quality, and Infrastructure. 3 Iranian Case-study.	Principal Component Analysis with Varimax rotation, Hierarchical Fuzzy Expert System (fuzzification, inference engine, defuzzification).
Lahane and Kant [74]	Circular SC adoption by evaluating multiple operational, economic, technological, and policy barriers. in the emerging economy context (India).	Expert evaluation through linguistic terms. PF sets. Sensitivity analysis for model robustness.	PF-AHP and PF-DEMATEL.
Luthra and Mangla [75]	I4.0 adoption barriers in manufacturing firms for sustainable SC development.	Categorized 18 challenges into 4 major groups. Prioritization of challenges.	Systematic Literature Review (SLR), Exploratory Factor Analysis and Analytic Hierarchy Process.

Table 2
Demographics of area experts.

Expert	Experience (Years)	Area of Expertise
Expert 1	23	Experience in research in SC design and sustainability, leveraging I4.0 technologies to manage SC operations.
Expert 2	10	Experience in research in intelligent manufacturing, with specific interests in Cyber-Physical systems and sustainable, resilient SCs.
Expert 3	8	Experience in research in SC management with a specific focus on SC collaborations

components were extracted: Stakeholder's intent (B1), Organizational (B2), Technical (B3), and Regulatory (B4) based on the experts' input for the nomenclature, which covers around 70.339 percent of the total variance. The nomenclature is discussed below:

Table 3
Barriers to Digital Trust in Supply Chain 4.0 for resiliency.

S. No.	Barrier Name	Description	References
1	Cybersecurity risks	Risks such as breaches, disruptions, and unauthorized access to sensitive data and systems hamper cargo, plant operations, and product specifications, undermining stakeholder confidence and integrity.	[76,77,81, 83–85]
2	Understanding the importance of trust in collaborative action	The real-time trust-based collaboration through data sharing between suppliers and organizations ensures product quality, innovation, and consistency for flexible decision-making and long-term partnerships.	[8,28]
3	Data Ownership, Quality, and Value	Data governance is data quality and value, which depends on the transparency of data ownership, enabling reliable decision-making, operational efficiency, and transparency among stakeholders.	[64,72,86]
4	Risk of information security and privacy	The potential loss of confidential and sensitive SC partners' information and the misuse of the private information for any of the data holder's benefit.	[8,32,82, 87]
5	Lack in the implementation of interactive digital communications	The limited adoption of real-time, transparent tools for seamless SC stakeholder collaboration. reduces transparency, delaying decision-making, and increasing the risks of misinformation.	[35,82,88]
6	Lack of information asymmetry over the shared platforms	Accurate, timely, and high-quality information over shared platforms enhances SC integration and decision-making and fosters DT.	[29,77]
7	Lack of digital culture	The organization's openness to acceptance is based on trust in utilizing digital technologies among its employees, reflecting its beliefs and confidence in utilizing these technologies.	[8,35,75,78, 79]
8	Distributed digital identity of supply chain entities	Verified SC entities (farmer, customer, grocer, warehouse) promote a smooth, secure, transparent operation; a lacuna creates an information gap.	[86]
9	Unwillingness to share information among SC partners	Insecurity for information sharing of the trading partners in the SC due to competitive disadvantage, which provides a de-collaborated environment, resulting in a loss of DT.	[78,79]
10	Lack of real-time information sharing	Lack of confidence in security and privacy makes digital SC participants hesitant to share real-time information, causing congestion and supply delays.	[35,78,84]
11	Interoperability and scalability, and issues	Interoperability is the ability of an information system to connect and exchange information among different SC entities. Scalability is the	[35,78, 80–82,85, 89]

(continued on next page)

Table 3 (*continued*)

S. No.	Barrier Name	Description	References
		ability of the digital system to be expanded without undue loss of performance.	
12	High investment cost of digital technologies	Capital investment in digital infrastructure for digitizing the SC ecosystem with perceived benefits of technology adoption enhances DT, customer retention, and competitive differentiation.	[78,79,84]
13	Unclear organizational objectives	Organizations assessing suppliers with digital technologies often lack data management policies, leading to reduced employee performance and customer loss due to diminished DT.	[78,79]
14	Lack of top management support	Management leadership commitment and support to instill confidence among the SC stakeholders to understand the value of digital technologies for enhanced SC performance	[8,78,79]
15	Low understanding of Industry 4.0 implications	SC participants' low comprehension of the benefits of I4.0 technologies in the SC, which include transparency, accuracy, collaboration, and agility for improved decision-making.	[8,75,78]
16	Lack of digital infrastructure	The absence of a secure and robust digital infrastructure helps to build DT, creating a sense of negligence toward adopting and practising digital technologies by the SC stakeholders.	[8,78,79]
17	User Experience and Usability for Technology	It is characterized by complex interfaces, a lack of transparency, security, and integration challenges, which prevent the user from working on SC4.0.	Expert input

- **Stakeholders' intent (B1)**: This component includes five barriers. The Total Variance Explained for this component is 21.925 %. This component consists of the barriers to implementing I4.0 for SC operations due to the stakeholder's perceived intent for enhancing resiliency through technology trust.
- **Organizational (B2):** This dimension includes six barriers with 17.589 % of explained variance. These barriers correspond to the organizational hurdles to implementing digital technologies for SC4.0 to address the disruption through a resilient system.
- **Technological (B3):** This component consists of four barriers, which account for 17.440 % of the total variance. These correspond to the technological factors preventing stakeholders from having DT in I4.0 technologies for the resilient SC.
- **Regulatory (B4):** The regulatory component consists of three factors related to the regulations the stakeholders follow to utilize the stakeholders' data safely and properly and build digitally resilient SC. It accounts for 13.385 % of the Total Variance Explained.

The identified components of the validated barriers are then further utilized to determine the barriers' priorities and their causal interrelationship to develop the framework. The priorities have been evaluated by implementing the PF-AHP to understand the hurdles for DT in SC4.0 to achieve resiliency. The implementation of PF-AHP is discussed in the next sub-sections.

3.4. Multicriteria analysis in the case organization

The identified barriers were then tested in a case organization. The case organization is a pioneering Robotics manufacturing organization working to develop cutting-edge solutions for various sectors, including Fire-Fighting Robots, Defence Robots, Humanoid Robots, and Manhole Cleaning Robots. The company is expected to have a turnover of over Rs. 5 billion. It is also ranked among the 100 top competitors in India. The company aims to integrate I4.0 technologies into its SC. However, trust issues in using these technologies are still a concern due to the infrastructural, employee, supplier, and customer concerns over the security of their data on the digital platforms utilized by organizations. The identified barriers were consulted with a questionnaire in Appendix B in the supplementary material, with a panel of five experts with experience in managing manufacturing SCs with I4.0 technologies. The demographic of the Expert panel is shown in Table 6. The PF-AHP is applied to compute the weights of the validated barriers. The top ten of the seventeen barriers are further analyzed to get the causal relationship through PF-DEMATEL [74].

3.5. Pythagorean fuzzy AHP

AHP was developed by Prof. Thomas L. Saaty in 1980 [94]. However, the implementation of AHP can generate inconsistencies in decision-making. Different studies [95,96] have employed fuzzy sets. This study employs PF sets to eliminate vagueness and inconsistencies. The following steps implement PF-AHP:

Step 1: The initial linguistic pairwise comparison matrix (P_k) as shown in Eq. (1) is generated for each expert, comparing the criteria i over j where $i, j = 1, 2, \ldots, m$ and based on the linguistic scale in Table C.1.

$$P_k = \begin{bmatrix} p_{11}^1 & \cdots & p_{1m}^k \\ \vdots & \ddots & \vdots \\ p_{m1}^k & \cdots & p_{mm}^k \end{bmatrix} \tag{1}$$

The linguistic scale inputs are converted into PF numbers based on Table C.1. Therefore $p_{ij}^k = \left\langle \left(\mu_{ijL}^k, \mu_{ijU}^k\right), \left(\nu_{ijL}^k, \nu_{ijU}^k\right) \right\rangle$ represents the numerical transformation of linguistic inputs.

Step 2: All expert inputs are aggregated using Eq. (2).

$$\left(\breve{X}_1, \ldots, \breve{X}_d\right) = \left\langle \left[\prod_{k=1}^d \mu_{k,L}^{w_k}, \prod_{k=1}^d \mu_{k,U}^{w_k}\right], \left[\left(1 - \prod_{k=1}^d \left(1 - \nu_{k,L}^2\right)^{w_k}\right)^{0.5}, \left(1 - \prod_{k=1}^d \left(1 - \nu_{k,U}^2\right)^{w_k}\right)^{0.5}\right] \right\rangle \tag{2}$$

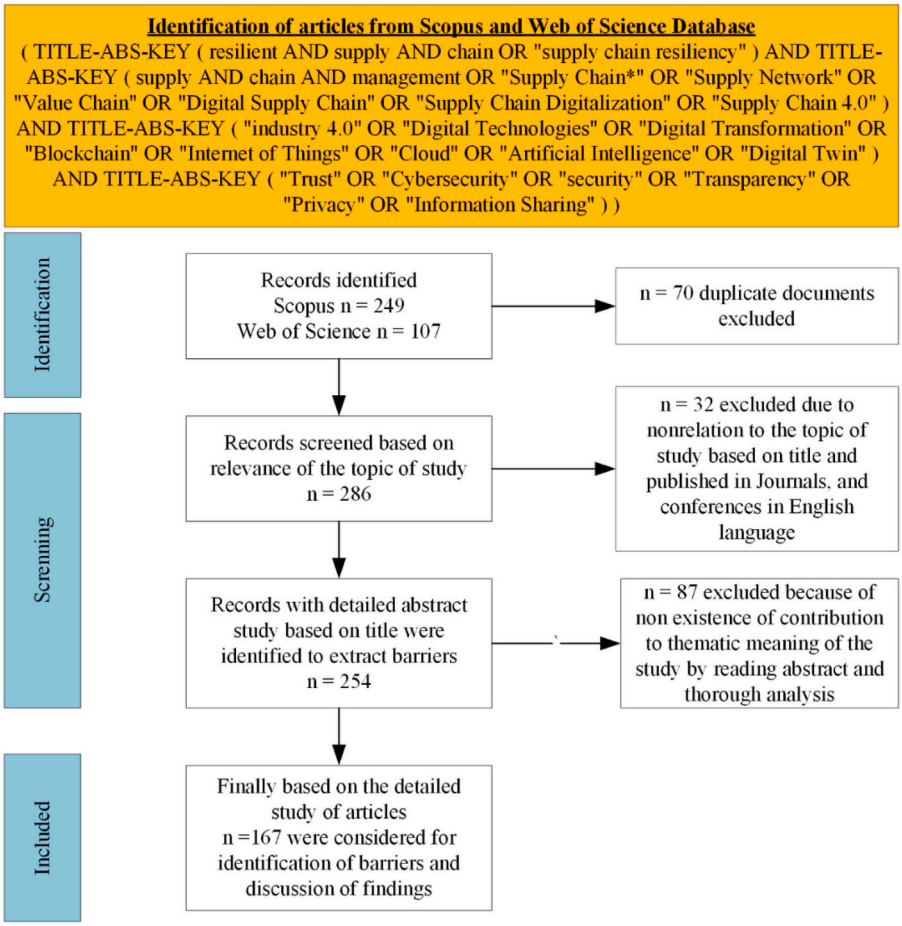

Fig. 3. Search Strategy.

Table 4
Demographics of responding organizations.

S. No.	Professional Demographics	Criteria	Number of respondents	Percentages
1	Type of Manufacturing Industry	Automobile	23	13.45
		Electrical & Electronics	21	12.28
		Healthcare device	34	19.88
		Consulting to manufacturing	65	38.01
		Others	28	16.37
2	Experience in digital technologies	4–10 years	43	25.15
		10–16 years	116	67.84
		16 & above	12	7.02
3	Experience in supply chain	5–10 years	102	59.65
		10–15 years	47	27.49
		15 & above	21	12.28
4	Designation	Top Management	10	5.85
		Senior Level Manager	37	21.64
		Middle-level manager	69	40.35
		IT professional	35	20.47
		Executive	20	11.70
5	Qualifications	Graduate	78	45.61
		Postgraduate	89	52.05
		Doctorate	4	2.34
		Total	171	100

Step 3: The difference matrix $\mathscr{D} = [d_{ij}]_{m\times m}$ where $d_{ij} = (d_{ijL}, d_{ijU})$ is calculated by finding out the difference between the lower (Eq. (2)) and upper values (Eq. (3)) of membership and non-membership functions by using the equations below.

$$d_{ijL} = \mu_{ijL}^2 - \nu_{ijL}^2 \tag{3}$$

$$d_{ijU} = \mu_{ijU}^2 - \nu_{ijU}^2 \tag{4}$$

Step 4: The interval multiplicative matrix $\mathscr{S} = [s_{ij}]_{m\times m}$ where $s_{ij} = (s_{ijL}, s_{ijU})$ is calculated using Eqs. (4) and (5).

$$s_{ijL} = \sqrt{1000^{d_{ijL}}} \tag{5}$$

$$s_{ijU} = \sqrt{1000^{d_{ijU}}} \tag{6}$$

Step 5: The indeterminacy matrix $\mathscr{T} = [\tau_{ij}]_{m\times m}$ is calculated by using Eq. (6) below.

$$\tau_{ij} = 1 - \left(\mu_{ijU}^2 - \mu_{ijL}^2\right) - \left(\nu_{ijU}^2 - \nu_{ijL}^2\right) \tag{7}$$

Step 6: The unnormalized weight matrix $U = [u_{ij}]_{m\times m}$is obtained with Eq. (7).

$$u_{ij} = \tau_{ij}\left(\frac{s_{ijL} + s_{ijU}}{2}\right) \tag{8}$$

Table 5
Exploratory Factor Analysis Results of Barriers.

Dimension	Barriers to digital trust in supply chain 4.0	Mean	Eigenvalues	Variance Explained (Cumulative)	Item Loading
Stakeholder's intent (B1)			6.741	21.925	
SB1	Unwillingness to share information digitally among SC partners	3.41			0.811
SB2	Lack in the implementation of interactive digital communications	3.12			0.838
SB3	Low understanding of Industry 4.0 implications	3.47			0.867
SB4	Understanding the importance of trust in collaborative action	3.59			0.861
SB5	User Experience and Usability for Technology	2.95			0.745
Organizational (B2)			2.357	39.514	
OB1	Unclear organizational objectives	3.69			0.744
0B2	Lack of top management support	3.60			0.682
OB3	Lack of digital culture	3.44			0.712
OB4	Lack of digital infrastructure	3.25			0.707
OB5	High investment cost of digital technologies	3.36			0.698
Technological (B3)			1.605	56.954	
TB1	Cybersecurity risks	3.12			0.849
TB2	Risk of information security and privacy	3.12			0.791
TB3	Data Ownership, Quality, and Value	3.36,			0.801
TB4	Interoperability and scalability and issues	3.26			0.822
Regulatory (B4)			1.254	70.339	
RB1	Lack of information asymmetry over the shared platforms	3.37			0.812
RB2	Lack of real-time information sharing	3.27			0.780
RB3	Distributed digital identity of SC entities	3.24			0.817

KMO: 0.865, Approx. Chi-Square: 1666.649, Cronbach's alpha = 0.897.
Barlett's test of sphericity: df: 136, Sig.0.000.
Extraction method: Principal Component Analysis, Rotation method: Varimax with Kaiser Normalization converged in 5 iterations.

Table 6
Demographics of the Expert panel.

Expert	Designation	Experience (Years)	Industry/Sector	Roles and Responsibilities
1	Chief Executive Officer	30	Manufacturing	Overall Management through AI for Quality Assurance in the SC.
2	Chief Digital Officer	25	Manufacturing	I4.0 Technologies Implementation in SC Operations
3	Head-Technology Risk and Cyber Controls	24	Consulting I4.0 technologies in SC	Handling non-financial risks like Cyber, Information security, Technology Risk, cloud security, Third Party Risk, and Operational Resilience
4	Assistant Manager	18	Manufacturing	Involved in managing the packaging, transportation, and dispatch of products.
5	Director Research	12	Robotics Manufacturing	Oversees and manages the production and distribution of the products to the customer.

Step 7: The weight of each criterion is determined by Eq. (8).

$$w_i = \frac{\sum_{i=1}^{m} w_{ij}}{\sum_{i=1}^{m}\sum_{j=1}^{m} w_{ij}} \tag{9}$$

3.5.1. Pythagorean Fuzzy-AHP implementation for weight computations

In this stage, a panel of five experts is constituted. The experts in the panel were asked to fill the pairwise comparison matrices for the main components and the barriers categorized under them per the linguistic scale in Table C.1 [95,96]. The initial pairwise matrix for the four dimensions by the five Experts is shown in Table C.2, provided in the Appendix C in the supplementary material, and their corresponding fuzzy numbers for Expert 1 are shown in Table C.3. The experts' inputs were combined in a single decision matrix, as shown in Table C.4. The sample calculation for the PF-AHP is shown in Tables C.5-C.7. The final global and local ranking of the DT dimensions and barriers with their weights is shown in Table 7.

3.5.2. Sensitivity analysis

The study has implemented a sensitivity analysis to test the robustness of ranking the barriers. Sensitivity analysis tests different configurations or combinations of weights that influence the prioritization of factors and criteria, and assesses the potential bias of the experts. We have addressed this by systematically changing the expert's weight by interchanging the weights and giving maximum weights to each expert by generating five scenarios (S1-S5), as shown in Table 8.

The weights of the barriers are obtained by interchanging the experts' weights while keeping the other main components constant. This procedure is followed with each of the five scenarios. According to Fig. 4, the weights of the barriers have not varied much from the original configuration, except for the barriers SB1, OB2, and TB1. This shows that the obtained weights are acceptable for further analysis.

3.6. Pythagorean fuzzy DEMATEL

The DEMATEL was first developed by Gabus and Fontela [97] and is a highly effective tool for identifying strengths and visualizing a causal relationship between the components in a complex system with minimum data input as compared to other MCDM techniques, such as interpretive structural modelling (ISM) and total interpretive structural modelling (TISM) [74,98,99]. Recently, studies such as [100] utilized PF-DEMATEL to identify the dependency of criteria for I4.0 sectoral prioritization. Similarly, Giri, Molla [101] utilized PF-DEMATEL for supplier selection in sustainable SC management, while Shafiee, Zare-Mehrjerdi [102] evaluated the perishable product SC risks during the COVID-19 outbreak. The steps of the PF-DEMATEL process are discussed below:

Step 1 Construction of Direct relationship matrix: The initial direct relationship matrix R_k as shown in Table C.9, is developed from k experts' inputs based on the scale in Table C.8.

Table 7
Ranking of barriers.

Main Criteria	Weight	Rank	Sub-Criteria	Local Weight	Local Rank	Global Weight	Global Rank
Stakeholder's intent (B1)	0.130	3	SB1	0.292	2	0.038	9
			SB2	0.344	1	0.045	8
			SB3	0.165	3	0.021	12
			SB4	0.133	4	0.017	13
			SB5	0.066	5	0.009	16
Organizational (B2)	0.398	1	OB1	0.140	3	0.056	7
			OB2	0.483	1	0.192	1
			OB3	0.054	4	0.022	11
			OB4	0.293	2	0.117	4
			OB5	0.029	5	0.012	15
Technological (B3)	0.371	2	TB1	0.384	2	0.143	3
			TB2	0.421	1	0.156	2
			TB3	0.155	3	0.058	6
			TB4	0.039	4	0.015	14
Regulatory (B4)	0.101	4	RB1	0.225	2	0.023	10
			RB2	0.719	1	0.072	5
			RB3	0.056	3	0.006	17

Table 8
Expert's weights scenario for sensitivity analysis.

Expert	Original	S1	S2	S3	S4	S5
E1	0.2	0.42	0.26	0.17	0.1	0.05
E2	0.2	0.05	0.42	0.26	0.17	0.1
E3	0.2	0.1	0.05	0.42	0.26	0.17
E4	0.2	0.17	0.1	0.05	0.42	0.26
E5	0.2	0.26	0.17	0.1	0.05	0.42

Step 2 Conversion of Initial direct relationship matrix: The initial direct relationship matrix R_k is converted into PF numbers with elements $r_{ij}^k = \left\langle \left(\mu_{ij}^k, \nu_{ij}^k\right)\right\rangle$ as shown in Table C.10.

Step 3 Computation of aggregated matrix: The experts' inputs are aggregated into a single aggregated matrix H with elements $h_{ij} = \left\langle \left(\mu_{ij}^{\mathrm{H}}, \nu_{ij}^{\mathrm{H}}\right)\right\rangle$.

Step 4 Computation of Average Crisp Matrix: The average crisp matrix M with elements $m_{ij} = \left(\mu_{ij}^{\mathrm{H}}\right)^2 - \left(\nu_{ij}^{\mathrm{H}}\right)^2$ is obtained.

Step 5 Calculate the normalized average crisp matrix: The normalized average crisp matrix $\mathcal{N}$ is calculated by Eq. (9).

$$\mathcal{N} = \wp \cdot M \tag{10}$$

where,

$$\wp = \frac{1}{\max \sum_{i=1}^{n} m_{ij}} \quad i,j = 1,2,3,\ldots,\ n$$

Step 6 Construct the total relationship matrix: The total relation matrix T is calculated by using Eq. (10).

$$T = \mathcal{N}(I - \mathcal{N})^{-1} \tag{11}$$

where I is an identity matrix.

Step 7 Plotting digraph: The digraph is plotted based on the threshold value. The threshold value is calculated to determine internal relations as the average of the Total relationship matrix, excluding partial relations within the matrix. A digraph is plotted for the values exceeding the threshold value only, setting zeros for the values below the threshold. The threshold found in this study was 0.04934. The adjusted total relationship matrix is shown in Table C.17.

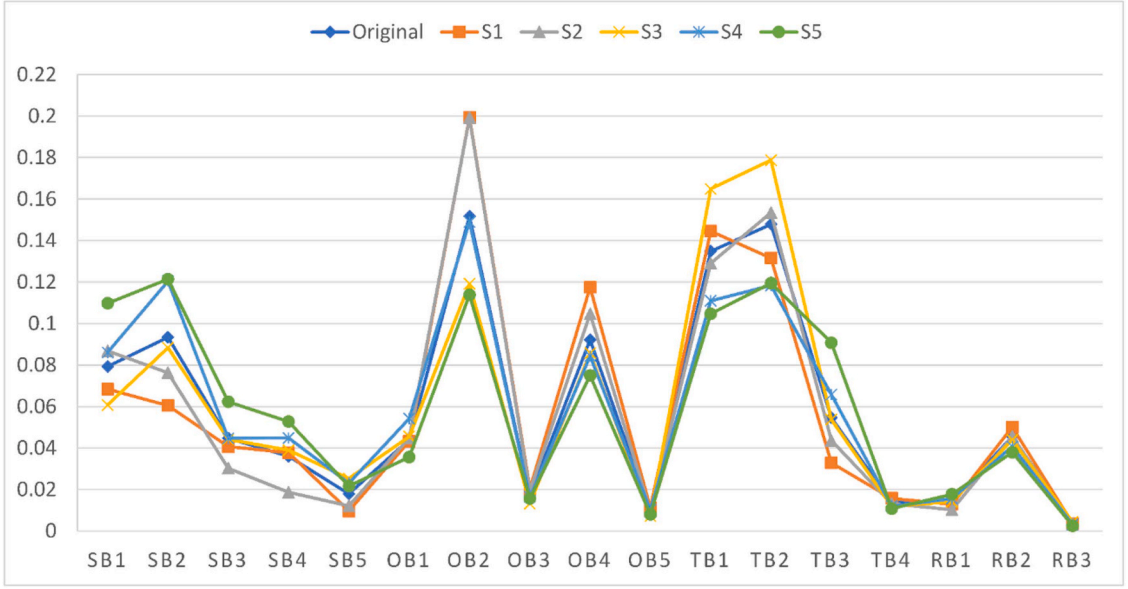

Fig. 4. Barrier weights after sensitivity analysis.

Step 8 Identify the causal relationship: The causal relationship is computed by finding the summation of rows. (R) and column (C) by using Eq. (11) and Eq. (12).

$$R_i = \sum_{j=1}^{n} t_{ij} \tag{12}$$

$$C_j = \sum_{i=1}^{n} t_{ij} \tag{13}$$

Step 9 Calculate the $(R+C)$ *and* $(R-C)$. $(R+C)$ denotes prominence effect and $(R-C)$ denotes the effect strength. The causal relation diagram is drawn by plotting $(R+C)$ on the horizontal axis and $(R-C)$ on the vertical axis. The above matrices can be found in Appendix C in the supplementary material from Table C.11-C.17.

3.6.1. Application of Pythagorean fuzzy-DEMATEL

The application of PF-AHP gives the top ten criteria for further evaluation to identify the causal relationship. The inputs were received again from the same experts as shown in Table C.9 of the Appendix C in the supplementary material, the experts were asked to provide an influence relationship between the criteria for applying PF-DEMATEL based on the scale of Table C.8. The inputs received from experts were further processed as per the steps in Section 3.3, and the calculations are presented in Table C.10-C.17. The final causal relationship is shown below in Table 9. Further, the causal diagram and interaction digraph are shown in Fig. 5.

4. Discussions

The assessment of barriers is utilized to develop the framework, which is shown in Fig. 6. The discussion on the results of the application of the methodology is discussed below in the following sections.

4.1. Discussion of findings

To develop a digitally trusted SC4.0 toward resiliency. It is imperative to identify and eliminate the critical barriers that prevent stakeholders from sharing their information on digital platforms. Based on the assessment through PF-AHP, the results are shown in Table 7, the order of priority of main dimensions is as follows: Organisational $\succ$Technological $\succ$ Stakeholder's intent $\succ$ Regulatory. Also, per Table 9 and Fig. 5, PF-DEMATEL classifies the barriers under 'Cause' and 'Effect' groups (Fig. 5(a)), with their interrelationship (Fig. 5(b)) shown. The organization's role is pertinent to building DT among the SC stakeholders to meet their obligations. Also, the 'Technological' barrier is the second important hurdle organizations must remove for a digitally trusted SC4.0. so that resiliency can be sustained, which is the result of the study by Agarwal and Seth [103] in the Indian automotive context. This points to the top management's decision-making regarding developing and deploying technologies for SC4.0. Third, an important dimension is the 'Stakeholder's intent' to share information and participate in the SC4.0 operations. The trust in SC4.0 depends on the organization's robust security and ethical responsibilities to maintain the integrity of SC stakeholders' data [104]. Fourth, 'Regulatory' concerns the oversight of the transactions of information and data, making good governance of the management leadership's actions and decisions accountable for SC4.0 sustainability. For instance, trust in BC fosters regulatory oversight with self-governance and coordination [105].

Table 9
Causal relationship of the top ten barriers.

Barriers	R_i	C_i	$R_i + C_i$	$R_i - C_i$	Causal Relationship
OB2	0.388	−0.079	0.309	0.467	Cause
TB2	−0.009	0.461	0.452	−0.470	Effect
TB1	0.150	0.675	0.825	−0.525	Effect
SB2	0.654	1.439	2.093	−0.785	Effect
OB4	1.086	0.491	1.577	0.594	Cause
SB1	1.335	1.387	2.722	−0.052	Effect
TB3	−0.148	0.673	0.525	−0.821	Effect
RB2	0.261	0.406	0.668	−0.145	Effect
RB1	0.554	−0.410	0.144	0.964	Cause
OB1	0.662	−0.110	0.552	0.773	Cause

The study reveals critically important barriers to establishing DT in SC4.0. Globally, 'Lack of top management support' (OB2) is the highest weighted factor. This underscores the integral role top management commitment in developing a digitally secure and resilient SC in the context of emerging economies, which has been emphasized by Luthra and Mangla [75]. This is also positioned within the 'Cause' group and reflects the strategic commitment at the top management level. As noted by Kalaitzi and Tsolakis [106] an organization's responsibility to protect stakeholder data fundamentally shapes trust in technology for visibility-enhancing resilience. It is essential for top executives to proactively lead digital initiatives and embed cybersecurity and data governance as regulatory measures into the core of the organizational strategies. This can be overcome through transparent performance metrics, and cross-functional trainings strengthen managerial cognition of reliability and competence building Cognition-based Trust, ensuring commitment to build DT.

The second highest-ranked barrier is the 'Risk of information security and privacy' (TB2) categorized under the 'Effect' group and most significant under 'Technological'. It emphasized the necessity for reliable, secure, and real-time information sharing among SC partners [106]. Organizations may adopt encrypted communication protocols with periodic vulnerability assessments for maintaining shared data integrity. With regular audits, encryption, access control, and real-time monitoring, reliability can be reinforced, while third-party and stakeholders' certification, regulatory adherence, and credibility. These mechanisms can institutionalize safety that enhances System-based trust.

'Cybersecurity Risks' (TB1) is ranked third globally and second among 'Technological' under the 'Effect' group. Pertaining to resilient digital systems, a majorly cybersecure SC4.0 will mitigate unintended data breaches and protect the stakeholders' data related to supply, operational, and demand risks, as suggested by Pandey, Singh [76] by conducting a case study in the Indian automobile sector. The stakeholders' primary demand for secure environments can be addressed through trust labels, data assurance certifications, and a clearly defined access control system, as has also been suggested by Wu and Zhang [86] in the Chinese coalmine context. The organizations may consider multi-layered defense frameworks and third-party certifications fostering safety, accountability, and oversight in the digital SC4.0 ecosystem. For resilient SC4.0, inadequate addressing of cybersecurity risks gives unauthorized access, makes the data of SC stakeholders vulnerable to cyber assaults, or destroys sensitive data [16]. BC-based security, strict compliance with international security standards, regular penetration testing, continuous monitoring for ensuring safety, accountability, oversight, and ensuring System-based Trust.

The fourth-ranked barrier is the 'Lack of digital infrastructure' (OB4), classified under the 'Cause' group and second within the organizational category. For a resilient I4.0 infrastructure, firms should emphasize the secure integration of software, hardware, and cyber-physical systems instead of focusing on a single technology [107]. Within the organizational level, this integrated perspective supports or impedes DT throughout the digital transformation process, as also outlined by Dixit, Malviya [16] by conducting a case study in the Indian automobile context and Strazzullo [20] by conducting a survey in the Italian Manufacturing industry. Here, the role of organizations becomes crucial to build cognition-based trust among stakeholders by developing scalable technologies leveraging cloud-based platforms, adopting an interoperable system to demonstrate measurable improvements in

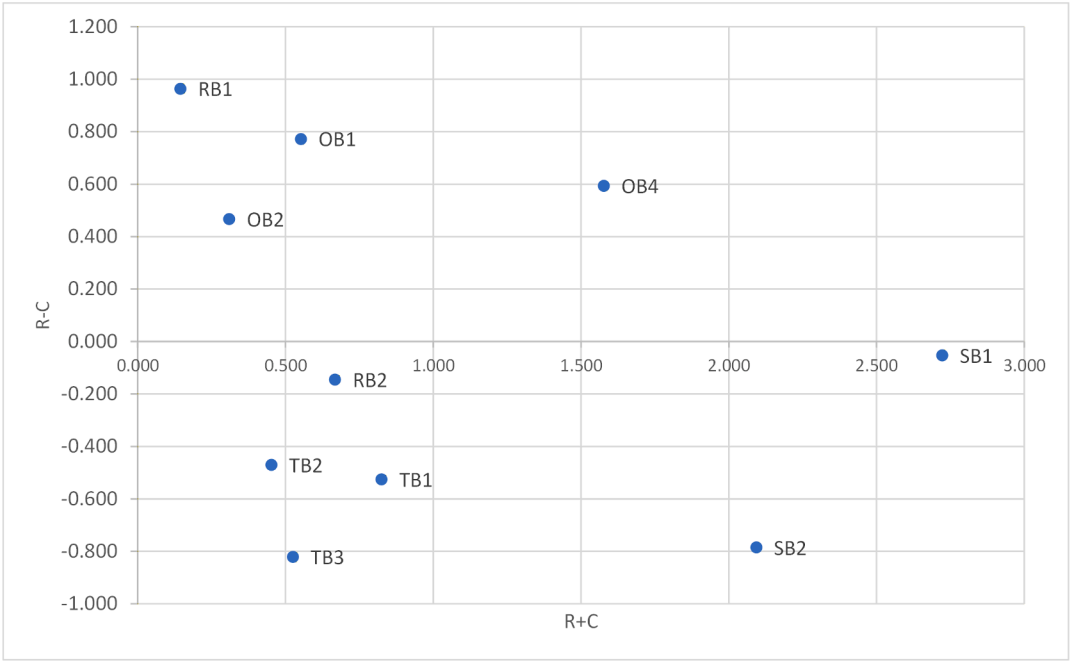

Fig. 5 (a)

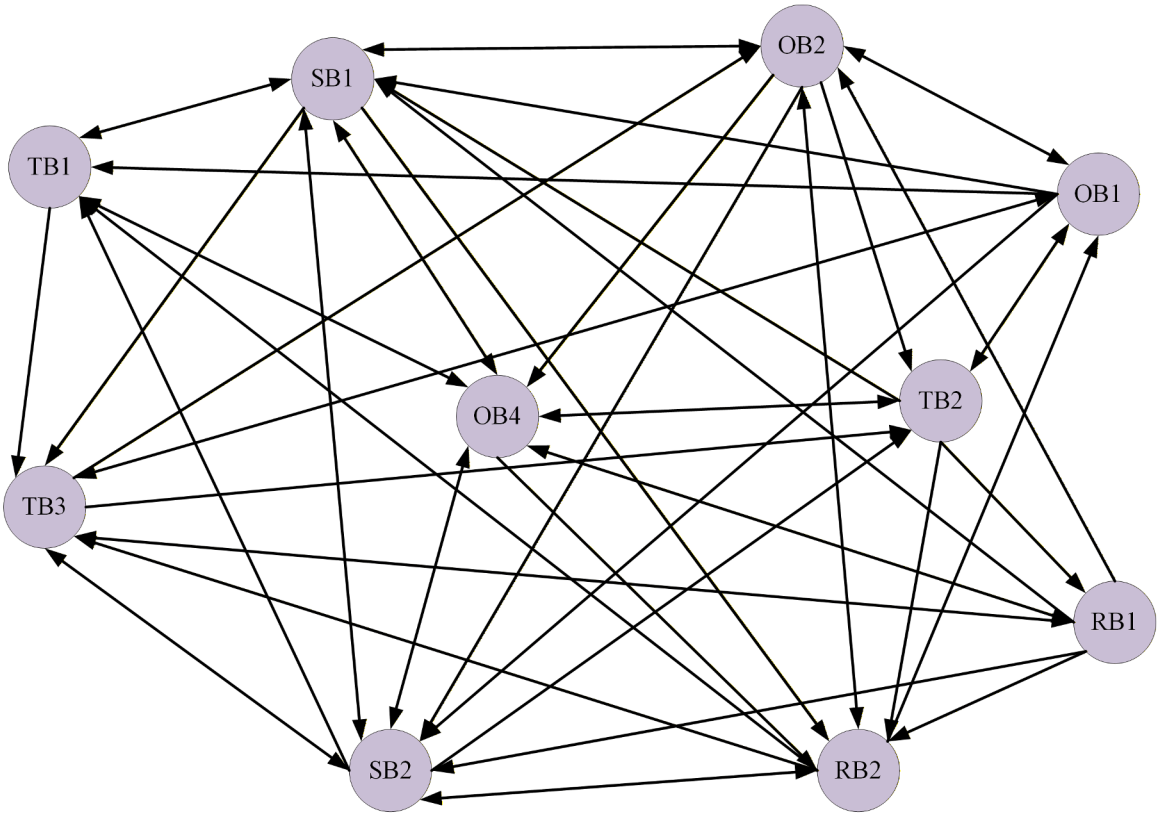

Fig. 5 (b)

Fig. 5. Causal Diagram and Interaction Digraph.

efficiency and transparency through pilot projects.

The fifth important barrier is the 'Lack of real-time information sharing' (RB2) placed under the 'Effect' group and ranked highest in the regulatory domain. Real-time, bidirectional, accurate data exchange on demand and supply is essential for SC4.0, enabling efficient logistics, inventory management, and financial transactions. This is well observed and pointed out by Wu and Zhang [86] and others Attaran [12], Pandey, Singh [76], Chaouni Benabdellah, Zekhnini [81] underline the role of IoT-based real-time information sharing in the emerging economies. This contributes to improved communication and collaboration quality among SC partners [83]. Firms may implement integrated IoT dashboards and predictive analytics tools to support just-in-time

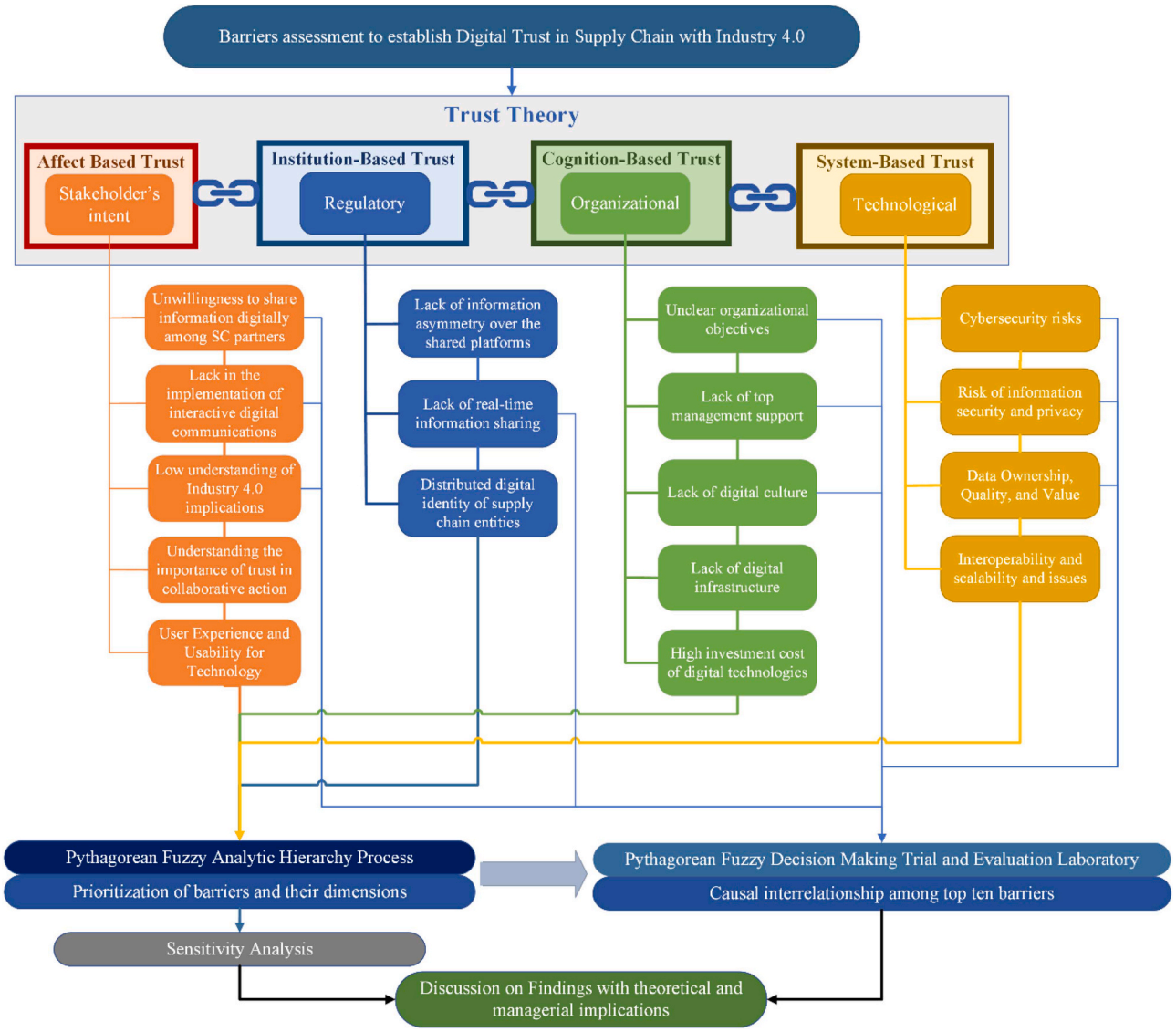

Fig. 6. Framework for Digital Trust in Supply Chain 4.0 towards Resiliency.

decision-making through improved end-to-end visibility. By instituting standardized data-sharing protocols, ensuring compliance with the regulatory framework for data transparency and accuracy, formalizing accountability and governance, fostering Institution-based trust to move towards DT.

'Data Ownership, Quality, and Value' (TB3) constitutes the sixth important barrier situated in 'Effect' group. In the interconnected SC4.0 environment, weak security practices for suppliers and contractors target cyberattacks on logistics systems and Tier-1 suppliers due to limited visibility [87]. Data ownership is crucial to building DT, as it ensures security, transparency, visibility, compliance, and trusted collaboration in BC-enabled resilient SC [86]. To establish, DT companies can establish data ownership protocols and use smart contracts to develop accountability. Transparently assigning data stewardship roles, with real-time validation mechanisms, and linking data use for measurable business outcomes, reinforces system reliability and thereby instill System-based-Trust among the stakeholders.

The seventh-ranked barrier is 'Unclear organizational objectives' (OB1), falling under the 'Cause' group. Ambiguity in goals hampers cross-functional interactions, which can be diminished by SC collaboration and competence [79]. The organization may prioritize flexibility and strategic objectives for enhancing competitiveness [17], profitability, and quality, and deliver robust operational measures to build stakeholders' confidence. Aligning digital SC initiatives with strategic goals, setting transparent performance metrics, and communicating a unified digital vision can build Cognition-based trust among stakeholders, consistent with the findings of Pandey, Daultani [2] in the Indian context and Jum'a and Bushnaq [27] in the Jordanian manufacturing context.

'Lack in the implementation of interactive digital communications' (SB2) is in eighth position as a barrier under the 'Effect' group. This has appeared due to the low level of understanding of I4.0 implications among participants [75] for digitally trusted collaborative action through data exchange for better resilient SC performance [8]. Organizations with strong leadership commitment can work on digital literacy through targeted training, fostering a culture of transparency and collaboration. Organizations can provide and deploy collaborative platforms, virtual engagement tools, and AI-driven interfaces. Frequently, empathetic interactions among SC partners are crucial for creating continuous relational communication, which nurtures mutual confidence and can establish Affect-based Trust.

The ninth-ranked barrier is the 'Unwillingness to share information digitally among SC partners' (SB1) under the 'Effect' group. The resistance to sharing critical information by SC stakeholders due to security

issues hinders partners in interactive digital communication [79]. Transitioning to a digital system in manufacturing often faces resistance to change, obsolescence, and concerns over data privacy. To overcome these challenges, comprehensive training on the functional use of technology can build participants' trust in digital technologies [20]. Cultivating innovative openness through training, transparency, nurtures mutual respect and assurance, thereby strengthening Affect-based trust. These findings align with the suggestions and findings of Dixit, Malviya [16], Chauhan, Singh [34,79], Yadav and Kumar [83] within the emerging economy context.

As for a resilient SC4.0, visibility through information sharing is crucial for businesses to adapt quickly to uncertain disruptions. This underscores the need for the involvement of top management commitment to allocate a budget for a cyber-secure digital infrastructure that can ensure trustworthy interactive digital communication for efficient SC management. Our findings align with the findings of Pandey, Daultani [2], Khan, Haleem [84]. The users' resistance to change to adapt to new digital, organizational, and process transformations often stems from a lack of training or resources. has been highlighted by Caliskan, Eryilmaz [108] in the Turkish context. Similarly, Vietnamese SC, in the early stage of I4.0 adoption, suffers from a gap between the high expected impact of these technologies and the relatively low planned investments [15], suggesting missed opportunities for competitive advantage [109]. Unwillingness to share information restricts digital communication due to the lack of sophisticated cybersecure networks, which questions the integrity of SC [66], if appropriately addressed, it can provide a competitive advantage [81] with SC collaborations, cooperation, interaction, and consistent decision-making [65,89].

'Lack of information asymmetry over the shared platforms' (RB1) is the tenth important barrier and is under 'Cause' group. Participants' concern about the level of organizational and technological capability to prevent the misuse of critical information shared through digital platforms diminishes DT. Information asymmetry creates trust asymmetry, financial cost, and reputation damage. This has also been pointed out by Brookbanks and Parry [29] and Strazzullo [20]. Establishing a unified data taxonomy creates shared benchmarks for fairness, accuracy, and accountability, reinforcing Institutional trust. SC managers should explore regulatory compliance checks on distributed digital identities to enhance transparency, control, and verification in shared digital spaces.

'Lack of digital culture' (OB3) is the eleventh important barrier. A weak digital culture in the organizations can lead to a loss of confidence among the SC stakeholders, leading to ineffective and inefficient SC operations. Here, the importance of human element I4.0 adoption has been linked to workforce management by organizations to foster a digital culture for enhancing flexibility, as suggested by Pandey, Daultani [2]. This attitude will also ensure the trustworthiness of the SC stakeholders in SC4.0 [86]. Incentivizing technology adoption to embed shared values and competencies across the organization demonstrates consistent readiness and capability, which cultivates Cognition-based trust. This has also been suggested as a counter-strategy to secure dedicated support and incentives from top management in the Turkish healthcare SC context [11]. The twelfth and thirteenth barriers, 'Low understanding of Industry 4.0 implications' (SB3) and 'Understanding the importance of trust in collaborative action' (SB4) further signify the knowledge and awareness gap among SC actors for digitally trusted collaborative action through data exchange for better SC performance [8,75]. Education and training through workshops and hands-on training can build relational connections [23], while simultaneously embedding trust and collaborative practices, allowing organizations to build affect-based trust, strengthening DT.

'Interoperability and scalability issues' (TB4) is the fourteenth important barrier. This corresponds to the lack of infrastructure, which in turn leads to interoperability and scalability issues, thereby raising security concerns and creating a lack of data trust (DT) in the infrastructure [81]. Organizations can work on adopting globally recognized standards and participating in the industry-wide standardization initiatives to overcome this barrier. These actions, utilizing modular digital architectures and cloud-based platforms, can promote System-Based Trust, enabling seamless integration and ensuring future growth. 'User Experience and Usability for Technology' (SB5) ranked sixteenth as an important barrier, creating the importance of intuitive and efficient digital platforms, as poor usability can hinder adoption and create resistance. By designing systems with a human-centric approach and integrating regular user feedback under compliance management, organizations can reinforce Affect-based trust that is vital for sustaining digital collaboration across SC networks.

Lastly, the seventeenth barrier, the 'Distributed digital identity of SC entities' (RB3), underscores the growing importance of digital identity protocols in enhancing traceability, authentication, and trust within SC4.0 environments. To address this, regulatory bodies and industrial alliances can collaborate to establish unified frameworks for verification of digital identities that ensure secure, verifiable, and permissioned access across the SC ecosystem, while being vigilant about the stakeholders' data protection regulations to build DT in the technology [20]. Such institutional safeguards formalize credibility and governance, thereby fostering Institution-based trust in SC4.0.

A digitally trusted SC4.0 instigates the requirements of data rights, which require regulatory and legal procedures. A digitally trusted and cyber-resilient platform provides a guarantee of data reliability, quality, security, safety, and credibility for transactions on an automated platform such as BC [17,83,86]. The data collection through real-time information for smarter SCM [44] with trusted BC-IoT devices [110] provides an efficient exchange of information in a trusted environment [65]. The linkage between manufacturing and logistics industry is studied by Li and Wang [64] in the Chinese context and it is highlighted that it is broken by unstable trust, which results in lagging and insecure information sharing, which can result in loss of effective collaboration. This indicates the importance of real-time information sharing to build DT in SC4.0. Its security, reliability, and quality depend on tackling barriers such as cybersecurity risks and a lack of stakeholders' DT, which, if resolved, will not hinder effective collaboration and decision-making.

4.2. Roadmap for the success of DT in SC4.0

Building DT in the SC4.0 environment requires framing digital initiatives as strategic business imperatives rather than focusing solely on technical upgrades. C-executives, i.e., the organization's senior executive, can buy-in only if a clear vision for profitability, risk mitigation, and competitiveness is secured while satisfying customers [44]. Once achieved, it can help the execution of functions in a resilient and trustworthy ecosystem. Within the SC context, this study presents a digital transformational strategy to build DT in SC4.0 in a phased roadmap from vision creation to localized pilots for the SC organizations of the emerging economies to advance their DT journey. To overcome the persistent challenges, the specific implementation roadmap is also provided in a multi-phased manner as shown in Fig. 7 and discussed below.

Phase 1. Establish a Chief Executive Suite-driven mandate

As indicated by the finding, the requirement of organizational commitment, this phase positions executive leadership to ensure board-level sponsorship to overcome barriers such as inadequate commitment, unclear objectives, and limited I4.0 understanding, indicating organizations' focus to act towards (1) Cybersecurity as a strategic Incumbent: Reframe cybersecurity from merely as a cost center to a "cornerstone of trust and motivation" with Chief Executive Officers (CEO). Chief Financial Officers (CFO) and the board are defining it as a whole business responsibility.(2) Long-term vision: Formulating a unified long-term trust strategy to stabilize SC relationships, which translates to growing investment and raised cyber budgets. (3) Cyber-risk quantification to drive investments: Demonstrate the financial strength by quantifying the high cost of breaches and linking cybersecurity risk

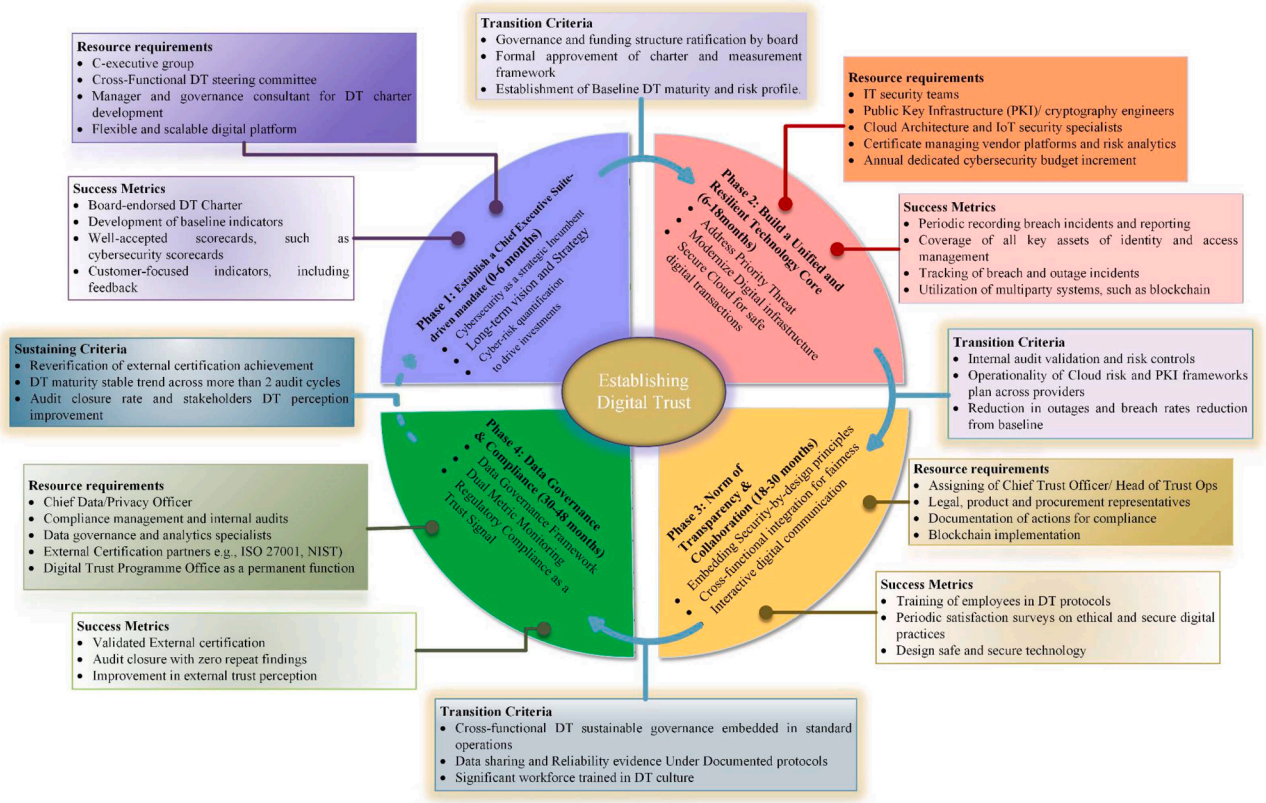

Fig. 7. Guidelines for building Digital Trust in Supply Chain 4.0.

associated with digital technologies as a compelling case for investments.

An organization's DT plans need to be executed, but they require auditing and monitoring of I4.0 technologies through a board-endorsed DT Charter with the safety and security of SC stakeholders' data as its prime and long-term goal. Here, the role of effective governance by the organization's C-suite is crucial in enabling security. Support from top leadership can take the form of executing strong governance programs that build DT among SC stakeholders. Leaders can invest more in DT factors and take measures to sustain them by aligning the organization's goals with those of improving skills and training in technology, as well as increasing understanding of DT and its dimensions. The trust measurement can be accomplished by deploying the indicator tools with cross-functional teams working together, which requires the time and effort of the executive teams. These baseline maturity indicators tools can act as a lubricant in maintaining the DT between human-human and human-machine interactions. Execution of data-driven scrutiny under governance and compliance mechanisms through user control requires a flexible and scalable digital platform that does not introduce vulnerabilities to cyberattacks and data breaches.

Organizations can track their progress through various metrics, such as the number of cyberattacks or breaches on their IoT devices and connected devices. The C-suite's responsibility is to monitor for continuous improvement regarding investment allocations, staff learning on DT initiatives, and the development of trusted relationships not only within the firm but also in business-to-business experience. Organizations can develop the DT index by continuously monitoring data governance and implementation practices to ensure security, privacy, safety, and accountability. As the monitoring of compliance management is of great concern, failure may lead to stakeholders losing confidence in the data handling authority. Well-accepted scorecards, such as cybersecurity scorecards within the internal monitoring system. Organizations can monitor delivery DT across SC stakeholders with provenance in digital rights, as well as in other spaces where the stakeholders are connected. Even customer-focused indicators, including feedback on organization data integrity practices, can be used to make them confident in the digital information exchange process. These steps can enable organizations to become capable of making strategic moves and be competitive in the dynamic market environment running on digital platforms.

The above steps lay the foundation for transitioning toward Phase 2, making their cyber space robust and breach-free from cyber-attacks. The investments to develop a strong technology core require the C-suite's formalization of budget implementation through the DT Charter. This can be executed through the approved official communication by the designated C-suite officer, allowing collective involvement of all active teams. Moreover, the organization should consider that, before deploying the DT execution, the mandate must make stakeholders confident through the baseline metrics verification, as DT connects not only with the organization but also with people and technology.

Phase 2. Build a Unified and Resilient Technology Core: Increasing cybercrime, specifically targeted attacks on devices, can cause potential damage to DT due to a lack of awareness and expertise in cyber safety. DT is an inclusive concept that indicates organizations, and their individuals must be understand the policy laid as the mission and objective of the organization with proper governance measures to become resilient to cyberattacks. These can be achieved through the following: (1) Address Priority Threats: The organizations can work on prioritising threats by responding to severe threats in time, as this could help organizations in reducing their liability and enhancing their goodwill among SC stakeholders. (2) Modern digital infrastructure: The organization can install a modern technological setup to map the functioning of the digital identities of all SC stakeholders. Implementing cryptographic keys can help in maintaining the confidentiality of shared data as they run on specific algorithms. The robust infrastructure includes

secured hardware and software for uninterrupted communication among all SC stakeholders. (3) Secure Cloud for safe digital transactions: In the modern SC4.0 operation, where data is stored on the cloud that must be secured from attacks, breaches, and unauthorized access as it is being transferred between systems. Organizations may define policies to ensure security under required regulatory compliance for devices that are cloud-oriented and exchange sensitive and crucial data.

DT establishment requires resources such as DT leaders, including technology innovators, who possess expertise in cybersecurity, privacy, and technology ethics, and have the capability to provide verification and assurance for all SC stakeholders. Despite the ubiquitous digital fabric woven into digital devices, traditional digital security remains important. For example, Public Key Infrastructure (PKI) verifies digital identities and data authentication, ensuring integrity in digital transactions. These PKIs being flexible can also be deployed in any number of environments, making them interoperable. Furthermore, DT has the capacity to unify all parties, including stakeholders and regulators, through verified certificate management vendors and the allotment of specific cybersecurity budget.

The organization can build a resilient technology core for SC4.0 by strengthening the critical information protection infrastructure against cyberattacks. This can be accomplished by periodically recording breach incidents and reporting them to the relevant cybersecurity agency. The organization can take actions to protect its users from harmful and malicious digital content. This will build confidence in the organization's stakeholders that the necessary actions regarding the safety of their data are being taken. This can also be further administered by C-executives through feedback, satisfaction surveys, and data flow analysis. Organizations can utilize multiparty systems, such as blockchain, distributed ledger, and tokenization, that mitigate the risks of security, privacy, and control.

The transition to Phase 3 requires the implementation of the actions to make a trusted technology deployment. This may be achieved by the continuous commitment of top management over concerns of data protection of all stakeholders implemented through regular auditing. These activities can build a firm's reputation and reduce data breaches and cyberattack incidents due to confidence of the SC stakeholders in the organization's technology and systems' robustness.

Phase 3. Promote a Norm of Transparency and Secure Collaboration: This phase underscores the need for transparency about the protection policies and actions taken by organizations for the stakeholders' information handling. Also, there must be informed decision-making while displaying crucial information on the SC stakeholders' common dashboard. These practices are critical to limit damage to the enterprise's reputation and build DT by (1) Embedding Security-by-design principles: While designing a technology, the established governance process with multiple supports, such as self-service, dedicated personnel for a particular digital technology. Further, while designing the data processing mechanism individual autonomy through notice and control must be maintained. (2) Empower Cross-functional integration for fairness: To make decision-making process quicker, the cross functional teams such as cybersecurity, data engineers, must work collectively rather in silos in processing data so that outcomes are equitable for all SC stakeholders. (3) Strengthen interactive digital communication: DT is not only a technology mediated solution; however, it involves people, process and technology as a two-way communication. This demands their interactive digital communication in the entire SC4.0 ecosystem.

This phase highlights the need for the assignment of Trust Officers who can execute personnel training on security and privacy through workshops to help them understand how their role affects DT. The lack of training opportunities due to misalignment of the organization's goals can create serious concerns. While the establishment of DT lies in responsible management actions that continuously utilize resources to improve the DT factors and support C-executives consisting of legal representatives, these are the main drivers of DT that ensure a clear understanding of policy and framework implementation across the SC. These actions must also be documented and distributed among all stakeholders, and their compliance must be monitored.

The improvement can be monitored through continuous assessment of the implementation of cybersecurity practices. The stakeholders must be aware and trained to take action and report threats and attacks on devices as a necessity. As the Trust Theory suggests, Trust is a collaborative approach; this suggests that each partner of the SC can contribute to the common goals of a safe and secure SC4.0 ecosystem through their feedback and monitoring system. These actions can help in understanding the importance of I4.0 implications and trust in collaborative actions for the development of digital culture among the SC stakeholders. Further, the C-executive can work on designing the technology that is safe and secure by default. However, only by deciding and acting for the establishment of DT can organizations and board members meet their obligations, which must be synthesized.

As organizations can track technology with security principles and cross-functional teams for DT governance, it enables transparent communication. The information deployed on digital technologies must be assessed periodically to ensure its safety and privacy, and provide reliable evidence to its stakeholders. Organizations can track the status of their DT workshops' deliverables through continuous monitoring, departmental tests, and the generation of report cards as a documented protocol to track improvement in DT culture. These actions can enable the organization to move to Phase 4.

Phase 4. Robust Data Governance and Anticipatory Compliance: In this Phase, organizations assess their data processing capabilities to confirm their auditable discourse. This signals an organization and its leaders' commitment to fulfilling the stakeholders' expectations through collaborative communication on data governance practices. The governance measures relate to the compliance with safety, quality, privacy, and security of digital assets. Even governance over ethics and data integrity is crucial to enable DT in SC4.0, with (1) A comprehensive data governance framework: A framework that covers each and every stakeholder of the SC for significant collaboration. This can become effective when other components, such as risk management, data quality, ownership and stewardship assurances, resilience, and ethics, are interwoven within the organization's DT strategy. (2) A Dual Metric Monitoring System: Auditability of the organization can make a long-lasting impact by drawing comparisons with previous governance measures. These metrics and monitoring systems can help prevent damage due to breaches beforehand. This monitoring can validate data accuracy, authenticity, and reliability through a secure cloud, blockchain with immutable records. (3) Regulatory Compliance as a Trust Signal: A well-structured compliance mechanism and implementation standards can help in verifiable operation, such as certificate status under NIST, ISO 27001 protocols. This enables transparency with additional details, such as where, when, and to whom to report, are provided.

The checking of governance can be conducted through the establishment of a permanent DT programme office, which checks for organization's validation of external certification such as ISO27001, NIST, etc. The office can work on sustaining the data governance mechanism that focuses on the availability of data in the right amount to the concerned stakeholders under a transparent environment. This can be achieved through defined data ownership and stewardship rights that restrict continued access to data. The C-suite can execute the cross-functional teams to make this a priority, as this directly impacts stakeholders.

Assessing the metrics, such as data quality scores, alone is insufficient for effective governance. Organizations can smartly invest in data and regular scrutiny of digital risks to demonstrate better oversight and reduce information asymmetry among SC stakeholders. In addition,

collective action can be executed only through a sense of responsibility among stakeholders when firms monitor progress by facilitating documentation for regulatory compliance. This can also assure provenance in the SC inputs to ensure data ownership and transaction records, and build valuable connections through valuable information flow to the right people. An organization's C-executive can run a risk assessment program to monitor participants, as loyal participants may not hesitate to break a relationship that compromises sensitive information.

The implementation of the four-phased framework can be converted into a sustainable execution programme by continuous monitoring. Once the governance, monitoring, and compliance structures are mature enough and validated for autonomous operation. The transition readiness is to be evaluated continuously to sustain. To ensure the readiness and operationality of the system, enforce quality rules, and ensure traceable auditability across all information exchange in the SC4.0. The dual-metric monitoring system consistently generates reliable insights, with year-on-year improvements in both internal and external indicators, thereby enhancing DT perceptions. Certification as a mandatory document and regulatory alignment have been achieved and retained across at least two audit cycles. The decision-making process for DT is institutionalized, such that governance and compliance routines are embedded within organizations as a digital culture, rather than project-driven targets. Meeting these criteria confirms the organization has transitioned from implementing to sustaining DT to build a resilient SC4.0 environment for all the stakeholders.

5. Implications

The implications for researchers, managers, and policymakers are discussed in the next subsections.

5.1. Theoretical implications

The present study contributes to the academic literature on the theoretical advancement of DT in the SC4.0 in the emerging economy context. This study utilised the Trust Theory to analyze the barriers of DT in the digitally mediated SC4.0 context. This study contributes to the theory of DT as well as to the SC4.0 by proposing a roadmap to establish DT and increase understanding of barriers through a framework and Trust theory dimensions. Studies like Strazzullo [20] explored DT within the manufacturing factory and Mubarak and Petraite [55] has explored I4.0 and DT for open innovation, lacking the empirical validation in the manufacturing SC context. This study fills this gap by exploring DT in the horizontal value chain for resiliency through an industry survey in the emerging economy context. This study has investigated seventeen barriers for their validation and discussed the findings based on the Trust Theory. The study conducted a case study to prioritize and find causal relationships of barriers utilising PF-AHP-DEMATEL, which introduces a strong methodological approach to handle uncertainty in decision-making, providing practitioners with actionable insights. These insights may be applicable to other emerging economies undergoing digital transformation to establish DT in their SCs. Further, the study contributes by discussing findings that position DT as a foundational capability to be pursued by organizations to achieve resilience in their operations. As SC is a stakeholder-operated process through collaboration, the intervention of I4.0 technologies enables communication through digital platforms, where the role of DT is inexcusable. The study has also provided a theoretical roadmap for action that organizations may adopt to build DT in their digitally mediated SCs.

5.2. Managerial implications

The present study provides a framework and roadmap for the success of DT in SC4.0. This study has investigated seventeen key barriers to DT for better SC4.0 operations in the merging economy context. Based on this, a few managerial implications can be presented. Industry managers can look upon these barriers to build a cyber-secure and resilient system for all SC stakeholders. The top management can work on revising their policies and extending them to DT establishment policies. Further, organizations can establish officials and managers responsible for monitoring the data handling practices of the organization. The discussion reveals that, to build a digitally resilient SC, DT is not an option to consider for future ventures, but rather it is a present-day need as a foundational capability. These capabilities can be developed among stakeholders in the form of digital culture through workshops/trainings for increasing awareness on disseminating data on digital platforms within a regulatory policy framework, and gathering feedback on the implemented learnings. These actions can influence improved collaboration through digital platforms, as DT is built for technology adoption. The top management's strong commitment towards budgetary allocation for building a cyber-resilient infrastructure and viewing it as a long-term strategic goal. The implications of this can be in the form of reduced risks of security attacks and help in providing transparency, safety, and accountability for stakeholders' information, which are crucial components of DT.

Manufacturing SC managers and digital consultants to manufacturing firms can consider the identified barriers and their dimensions while designing technologies for the firms. As SC4.0 operates on information sharing, the aspect of cybersecurity in the technologies developed remains a challenge for designers. Also, managers can bridge the gap between technology and people by undergoing a process of technology development that involves cross-functional teams trained for DT building. For emerging economies such as India, this study has reported the challenges and insights for DT development that are crucial in the times of digital transformation when the digital systems are in the development stage and are vulnerable to cyberattacks.

5.3. Policy implications

The present study highlights the need for policy frameworks that institutionalize DT as the core pillar in national and industrial SC initiatives. Regulatory bodies need to encourage the standardization of DT metrics in sectors that are adopting digital technologies. As evidenced in existing studies, the absence of data governance norms and interoperable frameworks affects trust building across stakeholders. Government and industry bodies need to develop clear guidelines for transparency and cybersecurity in digital SCs. Policies based on emerging global practices can help address trust-related issues in SC and help to build resilient SCs. Policy makers can pursue I4.0 technologies strategically, which can enhance trust and thereby a resilient SC through real-time visibility and proactive monitoring suggested by Hossain, Talapatra [1] in the Bangladeshi context.

Moreover, policy interventions should focus on capacity building and digital literacy. There is a need for targeted national programs to reskill manufacturing workforces in small and medium enterprises, where digital mistrust often happens from a lack of awareness and technological exposure. Apart from this, the present study also suggests that public-private collaborations are important to promote DT in supplier authentication and data exchange in SC.

This study also highlights the need for context-specific trust policies that reflect regional market realities. For emerging economies, trust in digital platforms is influenced by infrastructure readiness, institutional credibility, and socio-cultural factors. Hence, policy frameworks should not be universally imposed but instead co-created with localized inputs from industry and academia to ensure relevance, scalability, and long-term adoption.

6. Conclusion, limitations, and future research

This paper has investigated the barriers to DT in SC4.0 for resiliency by performing an SLR along with expert consultation. Through the industry-wide survey in the emerging economy context, the barriers

were critically analyzed for their significance. The study discusses the importance and implications of DT barriers by extending the Trust Theory to the digital interaction context by prioritizing them and identifying causal relationships through a framework, using an example case. Further, the study presents a roadmap to establish DT for its success in the SC4.0 context for emerging economies. The study is built on the foundation of Trust Theory, which discusses Trust as a multidimensional construct consisting of System-Based Trust, Affect-Based Trust, Institution-Based Trust, and Cognition-Based Trust. All these dimensional constructs have been utilized to discuss the implications of barriers and organizations' actions to develop DT throughout the supply network. This illustrates the applicability of the Trust Theory in the modern digital context of SC, which extends beyond organizational and interpersonal boundaries. Our findings have demonstrated the importance of stakeholders' willingness to accept vulnerability in data-driven SC4.0 operations, as well as the role of organizational compliance and policies regarding data, and the reliability of stakeholders in the organization's resilient cyberspace in the event of a breach or attack. This indicates how the establishment of DT depends on both human (SC stakeholders) and robust technical assurances. Moreover, in an emerging economy like India, challenges to SC digitalization still persist despite numerous government digital initiatives. This study presents DT at the forefront as a precautionary step that organizations may consider in their SC in I4.0 environment to sustain themselves in this digitally evolving, competitive market, which is open to any uncertain events. By applying the conventional Trust Theory in SC4.0 environments which include multi-actor data systems and automated governance architectures intrinsic to SC4.0. the study demonstrates how DT can stabilize digital interaction and reduce perceived risks and strengthen governance in digital SC settings.

The success of SC4.0 greatly depends on the reliability of data shared and trust in the technology. Previous studies have discussed the implications of the digitalization of SC, such as strategies' assessment [16], analysis of barriers to I4.0 and sustainability in SMEs [78], barriers to BC implementation in SC [84], barriers analysis of I4.0 adoption for SC competency and operational performance [34], analysis for a viable circular digital SC with BC technology [81]. The extant literature depicts a continuous lack of evaluation of barriers to DT in SC4.0. This study bridges this gap by substantiating the identified seventeen barriers through a survey in the emerging economies' manufacturing SC context for establishing DT in SC4.0. Therefore, this study contributes to the present literature by providing valuable insights and suggestions to practitioners and managers. The study's contributions are summarized below:

- This research has utilized a mixed-methods approach by utilizing EFA to group barriers into four dimensions, and further case-based evaluation through experts with PF-AHP-DEMATEL.
- The results have underlined the need for top management commitment and support with the development of robust digital infrastructure, ensuring the protection of data of all the SC stakeholders.
- With current digital transformations going on in India, the question of security, reliability, and protection rights of the data of the SC stakeholders is of great concern to the data managers and holders. The findings highlight that DT is essential as the digital SC works on real-time data, which can help managers to prevent disruptions that cause ripple effects.
- It examines the barriers and concludes that a digitally trusted SC can build a resilient SC network that can withstand shocks during disruptions, ensuring business excellence and customer satisfaction.
- This study has identified barriers for their prioritization and relationship identification through a framework. Further, presenting a detailed roadmap for the success of establishing DT in the SC4.0 environment.

The above contributions were generated from the analysis of barriers by conducting a survey within the emerging economy's manufacturing SC landscape. The findings highlight that top management commitment, risk of information security, privacy, cybersecurity risks, lack of digital infrastructure, and lack of real-time information sharing are barriers to be taken care of which can build confidence in stakeholders to share their quality data accurately for building DT, strengthening resilient SC 4.0, and fostering sustained economic growth.

6.1. Limitations and further research

This work has identified seventeen barriers to DT for SC4.0 through literature, expert inputs, and a survey-based approach integrated with expert subjective opinions for evaluating barriers in the emerging economy's manufacturing SC context. To contextualise the findings from the mixed-method analysis involving the industry survey, it is important to acknowledge that the demographics of the industry participants skewed towards respondents from consulting to manufacturing (38 %), which constitutes a limitation of the study. This perspective bias can be attributed to the Government of India's digital initiatives, e.g., Digital India, which offers advantages to companies to leverage digital technologies for improving their SC operations to be competitive in the market and further puts pressure towards digital transitions. Here, organizations that may lack digital competency often look to third-party digital consultancy for their digital execution by hiring a digital consultant to take on the role within the company. As part of our survey process, we have also reached out to experts who provide digital consulting services to manufacturing firms, as they may have a better understanding of digital technologies. However, the response rate suggests that the interest of those experts in participating in the survey skewed the demographics. While the response from other experts, such as department heads and plant managers, may provide more diverse perspectives. Therefore, this presents an opportunity for researchers to consult the experts excluded from this study and produce future research on this niche topic of DT in SC4.0.

The study utilized the PF set theory to judge the identified barriers between AHP and DEMATEL. However, the PF set theory can be integrated with other decision-making techniques such as FUCOM (Full Consistency Method), SWARA (Stepwise Weight Assessment Ratio Analysis), WASPAS (Weighted Aggregated Sum Product Assessment), CoCoSo (Combined Compromise Solution), LBWA (Level Based Weight Assessment), RAFSI (Ranking of Alternatives through Functional mapping of criterion sub-intervals into a single Interval), etc. The lack of qualitative analysis of the identified barriers can be further validated by conducting interviews with industry practitioners. We encourage future research to focus on exploring DT for sustainable buyer-supplier relationships executed through I4.0 technologies. Future studies can focus on the development of analytical and empirical models to analyze DT in different SC contexts. Also, a comparative analysis of the barriers in a specific industry across different geographical settings can be conducted. While this study contributes to the new knowledge of DT in SC4.0, it has some limitations, such as conducting a single case with a panel of five experts, underscoring the need for future studies with more case studies. This study has discussed findings on the barriers through a framework utilising the Trust Theory to generate insights and a practical, indicative roadmap for industry practitioners in emerging economies to establish the DT in SC4.0 environments and move toward resiliency. Like every study, this study also has shortcomings in the form of its basis on a single country and a single case; the findings may not be completely generalizable to all cases. However, the guiding roadmap is an indicative action plan; practical generalizability can be concretized through multi-case analysis in future works. Future studies could extend this study through longitudinal analyses employing structural equation modeling, coupled with validation of the DT measurement instruments, and taking responses from a large sample of diverse industries' SCs, such as pharmaceuticals, within a multi-country context.

Funding

The research work carried out has received no external funding from any source.

CRediT authorship contribution statement

Vaibhav Sharma: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Conceptualization. **Rajeev Agrawal:** Writing – review & editing, Validation, Supervision, Project administration, Investigation, Formal analysis. **Anbesh Jamwal:** Writing – review & editing, Visualization, Validation, Formal analysis. **Vijaya Kumar Manupati:** Writing – review & editing, Supervision, Formal analysis. **Vikas Kumar:** Writing – review & editing, Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.tbench.2025.100247.

References

[1] M.I. Hossain, et al., From theory to practice: leveraging digital twin technologies and supply chain disruption mitigation strategies for enhanced supply chain resilience with strategic fit in focus, Glob. J. Flex. Syst. Manage. (2024) 1–23.
[2] A.K. Pandey, et al., Analyzing industry 4.0 adoption enablers for supply chain flexibility: impacts on resilience and sustainability, Glob. J. Flex. Syst. Manage. (2024) 1–24.
[3] R.K. Singh, Transforming humanitarian supply chains with digital twin technology: a study on resilience and agility, Int. J. Logist. Manage. (2025).
[4] N.K. Jain, K. Chakraborty, P. Choudhary, Building supply chain resilience through industry 4.0 base technologies: role of supply chain visibility and environmental dynamism, J. Busi. Indust. Market. 39 (8) (2024) 1750–1763.
[5] B. Bhatnagar, V. Dixit, Resilient supply chains: advancing technology integration with pre-and post-disruption technology roadmap, J. Enterp. Inf. Manage. (2025).
[6] A.Z. Piprani, S.A.R. Khan, Z. Yu, Driving success through digital transformation: influence of industry 4.0 on lean, agile, resilient, green supply chain practices, J. Manuf. Tech. Manage. 35 (6) (2024) 1175–1198.
[7] A. Patidar, et al., Supply chain resilience and its key performance indicators: an evaluation under industry 4.0 and sustainability perspective, Manage. Environ. Qual. Int. J. 34 (4) (2023) 962–980.
[8] A. Ghadge, et al., The impact of industry 4.0 implementation on supply chains, J. Manuf. Tech. Manage. 31 (4) (2020) 669–686.
[9] G.F. Frederico, et al., Supply Chain 4.0: concepts, maturity and research agenda, Supp. Chain Manage. Int. J. 25 (2) (2020) 262–282.
[10] J.W. Veile, et al., The transformation of supply chain collaboration and design through industry 4.0, Int. J. Logist. Res. Appl. 27 (6) (2024) 986–1014.
[11] S. Seker, N. Aydin, Analyzing barriers and strategies in digital transformation for resilient SC in healthcare using AHP and MABAC under uncertain environment, J. Enterp. Inf. Manage. (2024) ahead-of-print(ahead-of-print).
[12] M. Attaran, Digital technology enablers and their implications for supply chain management. Supply Chain Forum: An International Journal, Taylor & Francis, 2020.
[13] C.L. Garay-Rondero, et al., Digital supply chain model in Industry 4.0, J. Manuf. Tech. Manage. 31 (5) (2020) 887–933.
[14] M. Ghobakhloo, et al., Industry 4.0 digital transformation and opportunities for supply chain resilience: a comprehensive review and a strategic roadmap, Prod. Plan. Cont. 36 (1) (2025) 61–91.
[15] A. Al Tera, A. Alzubi, K. Iyiola, Supply chain digitalization and performance: a moderated mediation of supply chain visibility and supply chain survivability, Heliyon (2024).
[16] V.K. Dixit, et al., An analysis of the strategies for overcoming digital supply chain implementation barriers, Deci. Anal. J. 10 (2024) 100389.
[17] P.C. Kandarkar, V. Ravi, Investigating the impact of smart manufacturing and interconnected emerging technologies in building smarter supply chains, J. Manuf. Tech. Manage. (2024).
[18] K.F. Cheung, M.G. Bell, J. Bhattacharjya, Cybersecurity in logistics and supply chain management: an overview and future research directions, Transp. Res. Part E Logist. Transp. Rev. 146 (2021) 102217.
[19] B. Hammi, S. Zeadally, J. Nebhen, Security threats, countermeasures, and challenges of digital supply chains, ACM Comput. Surv. 55 (14s) (2023) 1–40.
[20] S. Strazzullo, Fostering digital trust in manufacturing companies: exploring the impact of industry 4.0 technologies, J. Innov. Knowl. 9 (4) (2024) 100621.
[21] O. James, 8 Recent Cyber Attacks on the Manufacturing Industry, 2024 [cited 2025 15/03/2025]; Available from, https://wisdiam.com/publications/recent-cyber-attacks-manufacturing-industry/.
[22] PricewaterhouseCoopers, Manufacturer Cybersecurity and Supply Chain, PwC, 2022, 2022/02/24/; Available from, https://www.pwc.com/us/en/industries/industrial-products/library/cyber-supply-chain.html.
[23] A. Jena, S.K. Patel, Analysis and evaluation of Indian industrial system requirements and barriers affect during implementation of industry 4.0 technologies, Int. J. Adv. Manuf. Tech. 120 (3) (2022) 2109–2133.
[24] R. Gadekar, B. Sarkar, A. Gadekar, Model development for assessing inhibitors impacting industry 4.0 implementation in Indian manufacturing industries: an integrated ISM-Fuzzy MICMAC approach, Int. J. Syst. Assur. Eng. Manage. 15 (2) (2024) 646–671.
[25] N. Borana, T.S. Gaur, V. Yadav, Modeling of barriers to digital transformations in Indian manufacturing small and medium-sized enterprises, J. Sci. Tech. Policy Manage. (2024).
[26] S. Amoujavadi, A. Nemati, Developing sustainability, resiliency, agility, and security criteria for cloud service providers' viability assessment: a comprehensive hierarchical structure, Sustain. Fut. 7 (2024) 100219.
[27] L. Jum'a, M. Bushnaq, Investigating the role of flexibility as a moderator between supply chain integration and firm performance: the case of manufacturing sector, J. Adv. Manage. Res. 21 (2) (2024) 203–227.
[28] A. Rejeb, et al., Potentials of blockchain technologies for supply chain collaboration: a conceptual framework, Int. J. Logist. Manage. 32 (3) (2021) 973–994.
[29] M. Brookbanks, G. Parry, The impact of a blockchain platform on trust in established relationships: a case study of wine supply chains, Supp. Chain Manage. Int. J. 27 (7) (2022) 128–146.
[30] R. Kumar, et al., Prioritising elements of digitalisation for lean and green SME operations: an ISM-MICMAC study in the Indian context, J. Adv. Manage. Res. (2025).
[31] V. Sharma, R. Agrawal, V.K. Manupati, Blockchain technology as an enabler for digital trust in supply chain: evolution, issues and opportunities, Int. J. Syst. Assur. Eng. Manage. 15 (9) (2024) 4183–4209.
[32] R. D'Hauwers, J. Van Der Bank, M. Montakhabi, Trust, transparency and security in the sharing economy: what is the Government's role? Tech. Innov. Manage. Rev. 10 (5) (2020).
[33] P. Pietrzak, J. Takala, Digital Trust–Asystematic Literature Review, 2021.
[34] C. Chauhan, A. Singh, S. Luthra, Barriers to industry 4.0 adoption and its performance implications: an empirical investigation of emerging economy, J. Clean. Prod. 285 (2021) 124809.
[35] S. Kumar, M.K. Barua, Exploring the hyperledger blockchain technology disruption and barriers of blockchain adoption in petroleum supply chain, Resour. Policy 81 (2023) 103366.
[36] M. Hrouga, Towards a new conceptual digital collaborative supply chain model based on industry 4.0 technologies: a conceptual framework, Int. J. Qual. Reliab. Manage. 41 (2) (2023) 628–655.
[37] D. Ivanov, Digital supply chain management and technology to enhance resilience by building and using end-to-end visibility during the COVID-19 pandemic, IEEE Trans. Eng. Manage. (2021).
[38] H. Fatorachian, H. Kazemi, Impact of industry 4.0 on supply chain performance, Prod. Plan. Contr. 32 (1) (2021) 63–81.
[39] Global Risks Report 2024, WEF. 2024. p. 7–9.
[40] A. Patil, et al., Digital twins' Readiness and its Impacts on Supply Chain Transparency and Sustainable Performance, Industrial Management & Data Systems, 2024.
[41] L. Schilling, S. Seuring, Linking the digital and sustainable transformation with supply chain practices, Int. J. Prod. Res. 62 (3) (2024) 949–973.
[42] E. Pessot, et al., Empowering supply chains with industry 4.0 technologies to face megatrends, J. Busi. Logist. 44 (4) (2023) 609–640.
[43] Y. Lv, Y. Shang, Investigation of industry 4.0 technologies mediating effect on the supply chain performance and supply chain management practices, Environ. Sci. Poll. Res. 30 (48) (2023) 106129–106144.
[44] R. Preindl, K. Nikolopoulos, K. Litsiou, Transformation strategies for the supply chain: the impact of industry 4.0 and digital transformation, Supply Chain Forum 21 (1) (2020) 26–34.
[45] D.J. McAllister, Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations, Acad. Manage. J. 38 (1) (1995) 24–59.
[46] C.D. Duong, et al., Blockchain-based food traceability system and pro-environmental consumption: a moderated mediation model of technology anxiety and trust in organic food product, Digital Business 4 (2) (2024) 100095.
[47] K. Yavaprabhas, M. Pournader, S. Seuring, Blockchain and trust in supply chains: a bibliometric analysis and trust transfer perspective, Int. J. Prod. Res. 63 (14) (2025) 5071–5098.
[48] D.M. Rousseau, et al., Not so different after all: a cross-discipline view of trust, Acad. Manage. Rev. 23 (3) (1998) 393–404.
[49] R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust, Acad. Manage. Rev. 20 (3) (1995) 709–734.
[50] W.K. Wong, et al., A framework for trust in construction contracting, Int. J. Proj. Manage. 26 (8) (2008) 821–829.

[51] Jason Challender, P. F, Peter McDermott, The theory of trust: concept, components, and characteristics. Building Collaborative Trust in Construction Procurement Strategies, 2019, pp. 37–54.
[52] C. Lin, M. Lin, The determinants of using cloud supply chain adoption, Indust. Manage. Data Syst. 119 (2) (2019) 351–366.
[53] R.M. Morgan, S.D. Hunt, The commitment-trust theory of relationship marketing, J. Mark. 58 (3) (1994) 20–38.
[54] D.H. McKnight, L.L. Cummings, N.L. Chervany, Initial trust formation in new organizational relationships, Acad. Manage. Rev. 23 (3) (1998) 473–490.
[55] M.F. Mubarak, M. Petraite, Industry 4.0 technologies, digital trust and technological orientation: what matters in open innovation? Technol. Forecast. Soc. Change 161 (2020) 120332.
[56] D. Dobrygowski, in: A.M. Assaf Ben-Atar, Amanda Stanhaus (Eds.), Earning Digital Trust: Decision-Making for Trustworthy Technologies, World Economic Forum, 2022.
[57] A.B.A. Daniel Dobrygowski, Augustinus Mohn, Amanda Stanhaus, Earning digital trust: decision-making for trustworthy technologies, World Economic Forum (2022).
[58] D. Treat, How to Build Trust in a New Digital World, Accenture, 2021.
[59] E. Boehm, Digital Trust in a Connected World: Navigating the State of IoT Security, KEYFACTOR, 2023. https://www.keyfactor.com/state-of-iot-security-report-2023/.
[60] ISACA, Digital Trust: A-Modern-Day-Imperative, 2022. https://www.isaca.org/resources/white-papers/digital-trust-a-modern-day-imperative.
[61] S.K. Sivarama Krishnan, Manu Dwivedi, The C-suite playbook: Putting security at the Epicentre of Innovation, PwC India, 2024.
[62] Y. Guo, Digital Trust and the reconstruction of trust in the Digital society: an integrated model based on trust theory and expectation confirmation theory, Digit. Govern. Res. Pract. 3 (4) (2022) 1–19.
[63] S. Han, J.P. Ulhøi, H. Song, Digital trust in supply chain finance: the role of innovative fintech service provision, J. Enterp. Inf. Manage. (2024) ahead-of-print(ahead-of-print).
[64] Q. Li, L. Wang, Research on the information sharing in the linkage between manufacturing and logistics industry based on blockchain, in: Journal of Physics: Conference Series, IOP Publishing, 2021.
[65] Y.M. Pfaff, H. Birkel, E. Hartmann, Supply chain governance in the context of industry 4.0: investigating implications of real-life implementations from a multi-tier perspective, Int. J. Prod. Econ. 260 (2023).
[66] R.K. Ray, F.R. Chowdhury, M.R. Hasan, Blockchain applications in retail cybersecurity: enhancing supply chain integrity, secure transactions, and data protection, J. Busi. Manage. Stud. 6 (1) (2024) 206–214.
[67] D. Ivanov, A. Dolgui, A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0, Prod. Plan. Contr. 32 (9) (2021) 775–788.
[68] A.E. Meafa, et al., Driving resiliency and digitalization in the sourcing process: integration of blockchain technology and smart contracts, Benchmark. Int. J. (2024).
[69] R. Raj, V. Kumar, B. Shah, Big data analytics adaptive prospects in sustainable manufacturing supply chain, Benchmark. Int. J. 31 (9) (2023) 3373–3397.
[70] R. Manzoor, B. Sahay, S.K. Singh, Examining the factors that facilitate or hinder the use of blockchain technology to enhance the resilience of supply chains, IEEE Trans. Eng. Manage. 71 (2024) 10626–10649.
[71] P. Roozkhosh, A. Pooya, R. Agarwal, Blockchain acceptance rate prediction in the resilient supply chain with hybrid system dynamics and machine learning approach, Oper. Manag. Res. (2022) 1–21.
[72] S. Yadav, S.P. Singh, Blockchain critical success factors for sustainable supply chain, Resour. Conserv. Recycl. 152 (2020) 104505.
[73] M. Shayganmehr, et al., Assessing the role of industry 4.0 for enhancing swift trust and coordination in humanitarian supply chain, Ann. Oper. Res. (2021).
[74] S. Lahane, R. Kant, Evaluating the circular supply chain implementation barriers using Pythagorean fuzzy AHP-DEMATEL approach, Clean. Logist. Supp. Chain 2 (2021) 100014.
[75] S. Luthra, S.K. Mangla, Evaluating challenges to industry 4.0 initiatives for supply chain sustainability in emerging economies, Process Saf. Environ. Prot. 117 (2018) 168–179.
[76] S. Pandey, et al., Cyber security risks in globalized supply chains: conceptual framework, J. Glob. Oper. Strat. Sour. 13 (1) (2020) 103–128.
[77] R. Agrawal, et al., Opportunities for disruptive digital technologies to ensure circularity in supply Chain: a critical review of drivers, barriers and challenges, Comput. Ind. Eng. (2023) 109140.
[78] S. Kumar, et al., Barriers to adoption of industry 4.0 and sustainability: a case study with SMEs, Int. J. Comput. Integr. Manuf. 36 (5) (2023) 657–677.
[79] D. T.S, V. Ravi, An ISM-MICMAC approach for analyzing dependencies among barriers of supply chain digitalization, J. Model. Manage. (2022).
[80] A. Mohammed, et al., Blockchain Adoption in Food Supply Chains: A Systematic Literature Review on Enablers, Benefits, and Barriers, IEEE Access, 2023.
[81] A. Chaouni Benabdellah, et al., Blockchain technology for viable circular digital supplychains: an integrated approach for evaluating the implementation barriers, Benchmarking (2023).
[82] O. Bak, A. Braganza, W. Chen, Exploring blockchain implementation challenges in the context of healthcare supply chain (HCSC), Int. J. Prod. Res. (2023) 1–16.
[83] A.K. Yadav, D. Kumar, Blockchain technology and vaccine supply chain: exploration and analysis of the adoption barriers in the Indian context, Int. J. Prod. Econ. 255 (2023) 108716.
[84] S. Khan, et al., Barriers to blockchain technology adoption in supply chains: the case of India, Oper. Manage. Res. (2023).
[85] P. Bottoni, et al., Intelligent smart contracts for innovative supply chain management, Front. Blockchain 3 (2020) 52.
[86] Y. Wu, Y. Zhang, An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing, Adv. Eng. Inform. 51 (2022) 101522.
[87] C. Colicchia, A. Creazza, D.A. Menachof, Managing cyber and information risks in supply chains: insights from an exploratory analysis, Supp. Chain Manage. Int. J. 24 (2) (2019) 215–240.
[88] V. Naumov, et al., Methodological principles of forming multichannel digital communication in the supply chains, in: E3S Web of Conferences, EDP Sciences, 2020.
[89] F.F. Rad, et al., Industry 4.0 and supply chain performance: a systematic literature review of the benefits, challenges, and critical success factors of 11 core technologies, Indust. Market. Manage. 105 (2022) 268–293.
[90] A. Jamwal, R. Agrawal, M. Sharma, Challenges and opportunities for manufacturing SMEs in adopting industry 4.0 technologies for achieving sustainability: empirical evidence from an emerging economy, Oper. Manage. Res. (2023) 1–26.
[91] V. Jain, P. Ajmera, J.P. Davim, SWOT analysis of industry 4.0 variables using AHP methodology and structural equation modelling, Benchmark. Int. J. 29 (7) (2022) 2147–2176.
[92] J.F. Hair, W.C. Black, B.J. Babin, RE Anderson Multivariate Data Analysis: A Global Perspective, Pearson Prentice Hall, New Jersey, 2010.
[93] J. Nunnally, Psychometric Methods, 1978.
[94] T.L. Saaty, The analytic hierarchy process (AHP), J. Oper. Res. Soc. 41 (11) (1980) 1073–1076.
[95] I. Otay, M. Jaller, A novel pythagorean fuzzy AHP and TOPSIS method for the wind power farm location selection problem, J. Intel. Fuzz. Syst. 39 (5) (2020) 6193–6204.
[96] E. Ilbahar, et al., A novel approach to risk assessment for occupational health and safety using Pythagorean fuzzy AHP & fuzzy inference system, Saf. Sci. 103 (2018) 124–136.
[97] A. Gabus, E. Fontela, World problems, an invitation to further thought within the framework of DEMATEL, 1, Battelle Geneva Research Center, Geneva, Switzerland, 1972, pp. 12–14.
[98] S.L. Si, et al., DEMATEL technique: a systematic review of the state-of-the-art literature on methodologies and applications, Math. Probl. Eng. 2018 (1) (2018) 3696457.
[99] M.H.H. Hemal, F. Parvin, A. Aziz, Analyzing the obstacles to the establishment of sustainable supply chain in the textile industry of Bangladesh, Bench Coun. Trans. Benchm. Stand. Eval. 4 (3) (2024) 100185.
[100] İ. Kaya, et al., An integrated Pythagorean fuzzy-based methodology for sectoral prioritization of industry 4.0 with lean supply chain perspective, Int. J. Comput. Integr. Manuf. (2024) 1–30.
[101] B.C. Giri, M.U. Molla, P. Biswas, Pythagorean fuzzy DEMATEL method for supplier selection in sustainable supply chain management, Expert. Syst. Appl. 193 (2022) 116396.
[102] M. Shafiee, et al., A causality analysis of risks to perishable product supply chain networks during the COVID-19 outbreak era: an extended DEMATEL method under pythagorean fuzzy environment, Transp. Res. Part E Logist. Transp. Rev. 163 (2022) 102759.
[103] N. Agarwal, N. Seth, Analysis of supply chain resilience barriers in Indian automotive company using total interpretive structural modelling, J. Adv. Manage. Res. 18 (5) (2021) 758–781.
[104] G.M. Razak, L.C. Hendry, M. Stevenson, Supply chain traceability: a review of the benefits and its relationship with supply chain resilience, Prod. Plan. Cont. 34 (11) (2023) 1114–1134.
[105] J. Rahman, et al., Regulatory landscape of blockchain assets: analyzing the drivers of NFT and cryptocurrency regulation, Bench Coun. Trans. Benchmark. Stand. Eval. (2025) 100214.
[106] D. Kalaitzi, N. Tsolakis, Supply chain analytics adoption: determinants and impacts on organisational performance and competitive advantage, Int. J. Prod. Econ. 248 (2022) 108466.
[107] K. Huang, et al., The impact of industry 4.0 on supply chain capability and supply chain resilience: a dynamic resource-based view, Int. J. Prod. Econ. 262 (2023) 108913.
[108] A. Caliskan, S. Eryilmaz, Y. Ozturkoglu, Investigating the effects of barriers and challenges on Logistics 4.0 in the era of evolving digital technology, J. Model. Manage. 20 (3) (2025) 949–973.
[109] M. Akbari, J.L. Hopkins, Digital technologies as enablers of supply chain sustainability in an emerging economy, Oper. Manage. Res. 15 (3) (2022) 689–710.
[110] W. Viriyasitavat, et al., Building trust of blockchain-based internet-of-thing services using public key infrastructure, Enterp. Inf. Syst. 16 (12) (2022) 2037162.