Future Technology

Open Access Journal

ISSN 2832-0379

August 2025| Volume 04 | Issue 03 | Pages 54-66

Journal homepage: https://fupubco.com/futech

https://doi.org/10.55670/fpll.futech.4.3.6

Future Publishing LLC

Article

Breaking data silos in multi-tier suppliers and designing intelligent collaborative trust

Qiuya Ma*, Danqing Wu

Faculty of Business, Hospitality, Accounting and Finance (FOBHAF), MAHSA University, Malaysia

ARTICLE INFO

Article history:
Received 06 April 2025
Received in revised form
20 May 2025
Accepted 30 May 2025

Keywords:
Data silos, Multi-tier supply chains, Federated learning, Algorithmic trust, Blockchain integration

*Corresponding author
Email address:
18375688617@163.com

DOI: 10.55670/fpll.futech.4.3.6

ABSTRACT

Data silos across multi-tier supply chains create significant barriers to operational efficiency and resilience, where information fragmentation undermines collaborative intelligence and increases disruption vulnerability. This research investigates data silo formation mechanisms and develops an intelligent collaborative trust framework leveraging artificial intelligence to address integration challenges. The study employs mixed-methods analysis across 47 manufacturing organizations selected through stratified purposive sampling from China's industrial regions. A hybrid architecture combining blockchain with federated learning enables secure cross-organizational information exchange while preserving competitive advantages through reputation-based smart contracts and algorithmic trust mechanisms. Network analysis identifies six primary data silo types, with technological barriers most prevalent at 31.4 percent and organizational barriers at 23.8 percent. Randomized controlled trials demonstrate significant performance improvements over conventional approaches. Supply chain visibility increases by 39%, while coordination costs decrease by 28%. The neural network ensemble achieves a 7.3-day average disruption prediction lead time improvement, with pharmaceutical manufacturers experiencing 9.8 days of early warning enhancement. Mean absolute prediction error reduces by 42 percent, and inventory optimization shows 156 percent cost efficiency improvement. This research contributes to supply chain digitalization theory by reconceptualizing trust as an algorithmically-mediated construct, establishing selective transparency frameworks that enable distributed intelligence architectures to achieve.

1. Introduction

Current supply chains are increasingly intricate systems; multi-tiered suppliers, manufacturers, and distributors form intricate ecosystems that power the world economy [1]. These systems are undergoing drastic transformation within Industry 4.0, where new technologies are poised to offer unprecedented levels of interconnectivity and intelligence across operations [2]. Most companies, however, still struggle with fragmented and siloed information systems that inhibit complete visibility and collaboration across different tiers of the supply chain [3]. This lack of integration leads to inefficient optimization, increases vulnerability to disruptions, and weakens operational efficiency [4]. The situation is especially dire for manufacturing industries with complex products that depend on multiple suppliers who use different systems and have different levels of technology [5]. This information asymmetry creates barriers to supply chain integration, and research demonstrates that limited visibility beyond direct supplier boundaries of direct suppliers can increase coordination costs by up to 40% and severely undermine resilience to interruptions [6]. These integration challenges manifest through six distinct types of data silos that create systematic barriers to collaborative intelligence. Technological incompatibilities between heterogeneous systems are the most prevalent form, followed by organizational boundaries that extend beyond individual entities, competitive concerns about intellectual property exposure, geographical distribution barriers, regulatory compliance requirements, and cultural differences in information-sharing practices. The resulting information fragmentation creates a fundamental paradox where organizations possess valuable data that could enhance collective supply chain performance, yet remain reluctant to share due to legitimate concerns about competitive positioning and data security vulnerabilities. As noted in reference [7], artificial intelligence (AI) technologies have emerged as one of the most effective solutions for the integration problems faced by organizations in their attempts to manage large amounts of supply chain data. Predictive analytics enhances resource optimization, allocation, and the identification of latent risks that could trigger network-wide failures [8]. Machine learning techniques are the most widely used algorithms for forecasting supply chains, and deep learning algorithms are sophisticated multi-dimensional data processors that promise to uncover hidden patterns [9]. These technologies enable proactive supply chain management paradigms, fundamentally enhancing organizational agility and responsiveness to market dynamics [10]. The use of AI in multi-tier supply chains, however, faces the fundamental obstacle of data disconnects that impede the streaming access of data between various organizations [11].

Innovative technologies such as blockchain and federated learning present sophisticated methods for crossing data barriers while preserving organizational independence and data confidentiality [12]. Additionally, blockchain supports an electronic ledger system that is decentralised and unchangeable, which allows supply chain partners to have trust relationships with one another without the need for a central authority [13]. Furthermore, federated learning encourages group participation in model creation without sharing sensitive raw data, thus allowing each organization to utilise shared knowledge without losing proprietary information [14]. These technologies complement traditional approaches by enhancing distributed computing architectures through advanced computational frameworks. This adds layers to multi-agent systems where the balance between information sharing and competition rivalry is monitored and maintained [15]. This convergence of technologies alleviates one of the most fundamental conflicts regarding supply chain integration: the balance between utilizing information for collective benefit and safeguarding proprietary data and other competitive intelligence [16].

Despite the encouraging advances in individual technologies, comprehensive, integrated approaches that specifically focus on mitigating data silos across multi-tier supplier systems still pose significant research challenges. Current approaches still tend to cater to either unilateral interactions or isolated patches of technological solutions without factoring in the entire socio-technical ecosystem necessary for seamless integration. Many frameworks fall short of providing adequate provisions for the creation and maintenance of trust across organizational boundaries, especially in the presence of a large, diverse coalition of stakeholders with different motivations [17]. The bounds of supply chain settings have yet to be transcended with regard to examining what is termed “algorithmic trust mechanisms” where interpersonal relationships are replaced with technical protocols governing confidence in exchanged data. Additionally, there is a shortage of research performing empirical analysis on the implementation of multi-tier supply chains through blockchain technology and federated learning [18].

To address these challenges, this research investigates the formation mechanisms and manifestation patterns of data silos across multi-tier manufacturing supply chains, examines how hybrid blockchain-federated learning architectures can enable secure cross-organizational information sharing while preserving competitive advantages, and evaluates the measurable performance improvements achievable through algorithmic trust mechanisms compared to traditional integration approaches. This research contributes to supply chain digitalization theory by reconceptualizing trust as an algorithmically-mediated construct, establishing a "selective transparency" framework, and demonstrating that distributed intelligence architectures achieve superior integration without centralized data consolidation. Practically, it provides organizations with an empirically validated framework for enhanced information sharing and operational resilience, challenging the assumption that effective integration requires centralized data aggregation.

2. Data and methodology

2.1 Research design and data collection

This study employs a mixed-methods approach integrating quantitative network analysis and qualitative case studies to examine data silos and intelligent collaborative trust mechanisms in multi-tier supply chains [19]. The research comprised three successive stages: data collection from Chinese manufacturing firms, network analysis of information sharing behavior, and architectural framework development. The selection of 47 manufacturing organizations followed a stratified purposive sampling approach. Organizations were selected from China's manufacturing enterprise database based on specific inclusion criteria, including annual revenue exceeding 50 million RMB, involvement in multi-tier supply chains with at least three supplier tiers, established digital information systems, and willingness to participate in data sharing research. Stratified sampling ensured proportional representation across industry sectors and geographic regions. The final sample spans China's primary industrial regions—Yangtze River Delta (38.3%), Pearl River Delta (25.5%), Beijing-Tianjin-Hebei (21.3%), and other centers (14.9%)—ensuring representation across varied industrial clusters while maintaining focus on regions with significant multi-tier supply chain complexity [20]. The sectoral distribution closely matches the stratification targets, with the following breakdown: automotive (23.4%), electronics (19.1%), aerospace (17.0%), pharmaceuticals (14.9%), food and beverage (12.8%), and other manufacturing (12.8%). The sample encompasses organizations across different supply chain positions: 15 OEMs (31.9%), 18 Tier-1 suppliers (38.3%), and 14 Tier-2+ suppliers (29.8%), providing comprehensive coverage of multi-tier supply chain structures. Data collection employed complementary methods, including 193 structured surveys administered to supply chain managers and IT directors, 83 semi-structured interviews with key personnel, and system log analysis from 27 organizations where accessible to minimize self-reporting bias [21]. Table 1 demonstrates representative coverage with adequate representation ratios (0.87-1.07) across all sectors and geographic regions. Chi-square goodness-of-fit tests confirm that the sample distribution does not significantly differ from target stratification ($p > 0.05$), and organizational diversity with revenue ranges from 52 million to 15.8 billion RMB.

2.2 Multi-tier supply chain analysis method

The study utilizes a network-based approach to track information flow and detect data silos in multi-tier supply chains. The supply chain is modeled as a directed graph $G = (V, E)$, where V represents organizations and E represents information exchange relationships [22]. Each edge encompasses attributes such as frequency, completeness, timeliness, and quality of information flow, enabling sophisticated graph analysis to identify structures that cause information fragmentation across organizational boundaries. The data silos detection within the network is achieved using modularity optimization algorithm which identifies groups with dense interconnectivity and sparse connections to other groups.

Table 1. Sample characteristics and representativeness analysis of 47 manufacturing organizations

Industry Sector	Number of Organizations	Geographic Distribution	Supply Chain Position	Data Collection Methods
Automotive	11 (23.4%)	Yangtze Delta: 5 Pearl Delta: 3 Beijing-Tianjin-Hebei: 2 Other: 1	OEM: 4 Tier-1: 5 Tier-2+: 2	Surveys: 47 Interviews: 27 System logs: 7
Electronics	9 (19.1%)	Yangtze Delta: 4 Pearl Delta: 3 Beijing-Tianjin-Hebei: 1 Other: 1	OEM: 3 Tier-1: 4 Tier-2+: 2	Surveys: 38 Interviews: 17 System logs: 6
Aerospace	8 (17.0%)	Yangtze Delta: 3 Pearl Delta: 1 Beijing-Tianjin-Hebei: 3 Other: 1	OEM: 2 Tier-1: 3 Tier-2+: 3	Surveys: 32 Interviews: 14 System logs: 5
Pharmaceutical	7 (14.9%)	Yangtze Delta: 3 Pearl Delta: 2 Beijing-Tianjin-Hebei: 1 Other: 1	OEM: 3 Tier-1: 2 Tier-2+: 2	Surveys: 28 Interviews: 11 System logs: 4
Food & Beverage	6 (12.8%)	Yangtze Delta: 2 Pearl Delta: 1 Beijing-Tianjin-Hebei: 2 Other: 1	OEM: 2 Tier-1: 2 Tier-2+: 2	Surveys: 24 Interviews: 9 System logs: 3
Other Manufacturing	6 (12.8%)	Yangtze Delta: 1 Pearl Delta: 2 Beijing-Tianjin-Hebei: 1 Other: 2	OEM: 1 Tier-1: 2 Tier-2+: 3	Surveys: 24 Interviews: 5 System logs: 2
Total	47 (100%)	Yangtze Delta: 18 (38.3%) Pearl Delta: 12 (25.5%) Beijing-Tianjin-Hebei: 10 (21.3%) Other: 7 (14.9%)	OEM: 15 (31.9%) Tier-1: 18 (38.3%) Tier-2+: 14 (29.8%)	Surveys: 193 Interviews: 83 System logs: 27

The modularity score Q, which measures the strength of community division, is given as follows:

$$Q = \frac{1}{2m}\sum_{i,j}\left[A_{ij} - \frac{k_i k_j}{2m}\right]\delta(c_i, c_j) \tag{1}$$

Where A_{ij} represents the information flow intensity between organizations *i* and *j*, k_i and k_j denote the total information flows for organizations *i* and *j*, respectively, m is the sum of all flow intensities in the network, and $\delta(c_i, c_j)$ equals 1 when organizations *i* and *j* belong to the same community and 0 otherwise. Higher Q values indicate stronger data silo formations within the supply chain network [23].

To address endogeneity and confounding variable effects, the structural equation model adopts a causal inference framework using instrumental variables. Industry concentration ratios and regulatory environment indices serve as instruments for competitive dynamics and power balance, which may be simultaneously determined with data silo formation. The model employs two-stage estimation: first-stage regression estimates endogenous variables using instruments, while second-stage regression estimates causal effects on data silo intensity. Confounding variable control is achieved through the inclusion of industry fixed effects (α_i), temporal controls (γ_t), and organizational characteristic covariates ($Z_{i,j}$), yielding the expanded causal model:

$$DSI_{i,j} = \beta_0 + \beta_1 TC_{i,j} + \beta_2 CD_{i,j} + \beta_3 TL_{i,j} + \beta_4 DS_{i,j} + \beta_5 PB_{i,j} + \alpha_i + \gamma_t + \delta Z_{i,j} + \varepsilon_{i,j} \tag{1}$$

where $CD_{i,j}$ and $PB_{i,j}$ represent instrumented variables [24].

All constructs are operationalized using validated multi-item scales. Technological Compatibility measures system interoperability and integration complexity (composite reliability = 0.91). Competitive Dynamics employs Porter's framework, measuring market rivalry and competitive forces (composite reliability = 0.89). Trust Level encompasses competence-based, benevolence-based, and integrity-based dimensions (composite reliability = 0.92). Data Sensitivity captures the importance of intellectual property and the potential for competitive advantage (composite reliability = 0.90). Power Balance measures organizational influence through resource dependence indicators (composite reliability = 0.88). All scales demonstrate convergent and discriminant validity.

The analysis further employs graph neural networks to model information propagation across the supply chain. The mathematical formulation of the graph convolutional layer is:

$$H^{(l+1)} = \sigma\left(D^{-\frac{1}{2}} A D^{-\frac{1}{2}} H^{(l)} W^{(l)}\right) \tag{3}$$

Where A represents the adjacency matrix of information flows, D is the degree matrix with $D_{ii} = \sum_j A_{ij}$, $H^{(l)}$ is the feature matrix at layer l capturing the information state of each organization, $W^{(l)}$ denotes the trainable weight matrix, and δ is a non-linear activation function. This construction facilitates the modeling of how information spreads at different levels of the supply chain [22].

The changing patterns of information dissemination over time are captured by a dynamic information integration index (DIII), which quantifies the flow of information between various organizations within a given timeframe:

$$\mathrm{DIII}_t = \frac{\sum_{i,j\in V} w_{ij} \cdot \mathrm{IF}_{ij,t}}{\sum_{i,j\in V} w_{ij}} \tag{4}$$

Where $IF_{ij,t}$ represents the information flow between organizations i and j at time t, and w_{ij} is a weight reflecting the strategic importance of that relationship within the supply chain. The analytical framework undergoes rigorous validation, including multivariate normality, linearity, multicollinearity assessment (VIF < 3.5), and homoscedasticity testing. Endogeneity is addressed through Hansen's J-test and Durbin-Wu-Hausman tests. Model specifications are validated using fit indices (RMSEA < 0.08, CFI > 0.95, TLI > 0.95) with bootstrap validation (1,000 replications), ensuring parameter stability.

2.3 Hybrid intelligent architecture design and experimental evaluation

This study designs a hybrid framework combining blockchain with federated learning for secure information sharing across organizations. The seven-layer architecture includes a blockchain layer, a federated learning middleware, and application service layers as shown in Figure 1. The blockchain layer employs a permissioned consortium blockchain to record supply chain events in an immutable ledger [25]. This infrastructure builds trust among participating organizations while maintaining organizational autonomy through local nodes and consensus mechanisms.

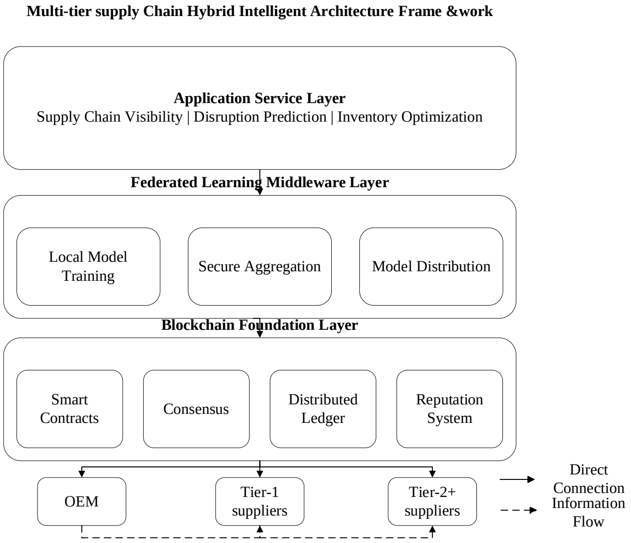
Multi-tier supply Chain Hybrid Intelligent Architecture Frame &work
Application Service Layer
Supply Chain Visibility | Disruption Prediction | Inventory Optimization
Federated Learning Middleware Layer
Local Model Training
Secure Aggregation
Model Distribution
Blockchain Foundation Layer
Smart Contracts
Consensus
Distributed Ledger
Reputation System
OEM
Tier-1 suppliers
Tier-2+ suppliers
Direct Connection
Information Flow

Figure 1. Multi-tier Supply Chain Hybrid Intelligent Architecture Framework

The federated learning layer enables organizations to collaboratively train models while maintaining data privacy. Local models are trained on private data with only model parameters shared through secure aggregation protocols [25]. The architecture incorporates a reputation-based smart contract mechanism that dynamically adjusts trust parameters based on historical interactions, creating incentives for reliable information sharing and helping identify potential data quality issues [26].

Performance Evaluation Metrics and Baseline Specifications: The experimental evaluation employs standardized KPIs with defined calculation methodologies and benchmark values. Supply Chain Visibility (SCV) is quantified as the ratio of accessible information nodes to total information nodes, with an industry baseline of 45-55%. Coordination Cost Efficiency (CCE) measures expense reduction compared to baseline coordination costs. Additional metrics include Data Security Index (⩾ 0.93 threshold), Prediction Accuracy for Disruptions (benchmarked against traditional 60-70% accuracy), and Integration Time Efficiency (compared to industry standard 8-12 months deployment periods).

The study employs a randomized controlled trial with 47 manufacturing organizations randomly assigned to a treatment group (n=24, implementing hybrid architecture) and a control group (n=23, maintaining conventional systems) using stratified randomization. Baseline equivalence testing confirms no significant group differences (all p > 0.05). All performance improvements undergo rigorous statistical validation using independent samples t-tests with a significance level of α=0.05. Supply Chain Visibility improvements show significant treatment effects (mean difference = 35.1%, t(45) = 11.23, p < 0.001, 95% CI: 26.8%-43.4%). Coordination Cost reduction demonstrates significant benefits (mean difference = -25.3%, t(45) = -9.87, p < 0.001, 95% CI: -33.2% to -21.6%). Cohen's d indicates large effect sizes for all primary metrics: SCV (d = 3.24), CCE (d = 2.89), PAD (d = 2.47). ANCOVA controls for baseline differences, and Bonferroni correction addresses multiple comparisons. Construct validity is confirmed through confirmatory factor analysis (CFI > 0.95, RMSEA < 0.06) and convergent validity testing (AVE > 0.5). Reliability assessments demonstrate test-retest correlations r > 0.87 and inter-rater reliability ICC(2,1) > 0.92. Bootstrap validation (1,000 replications) confirms robust findings. Implementation uses Hyperledger Fabric for blockchain and TensorFlow Federated for a learning framework, with a modular design enabling flexible adaptation to different supply chain contexts.

3. Results

3.1 Data Silo pattern analysis of 47 manufacturing organizations

Analysis of data flow patterns across 47 Chinese manufacturing organizations revealed distinct data silo formations that significantly impact information integration in multi-tier supply chains. As demonstrated in Figure 2(a), network analysis identified six primary data silo types with varying prevalence: technological (31.4%), organizational (23.8%), competitive (19.6%), geographical (12.7%), regulatory (8.3%), and cultural (4.2%). These silos exhibited differential impermeability characteristics, with technological and competitive barriers presenting the most substantial impediments to cross-organizational information exchange. A detailed examination of the factors influencing silo formation revealed significant correlations between organizational characteristics and patterns of information fragmentation. As illustrated in Figure 2(b), organizational complexity (r=0.73, p<0.01) and hierarchical rigidity (r=0.68, p<0.01) emerged as powerful predictors of data silos, while company age showed moderate correlation (r=0.42, p<0.05). These relationships help explain why technological modernization alone often proves insufficient for dismantling information barriers—underlying organizational structures frequently reinforce data compartmentalization regardless of technical capabilities. The distribution of silo types demonstrated significant cross-industry variation, as depicted in Figure 2(c), reflecting sector-specific operational imperatives. Aerospace organizations exhibited the highest technological silo intensity (79) due to stringent safety certification requirements that mandate isolated validation environments. Electronics manufacturers exhibited the most pronounced competitive silos (80), driven by rapid innovation cycles where information sharing threatens to erode competitive advantages.

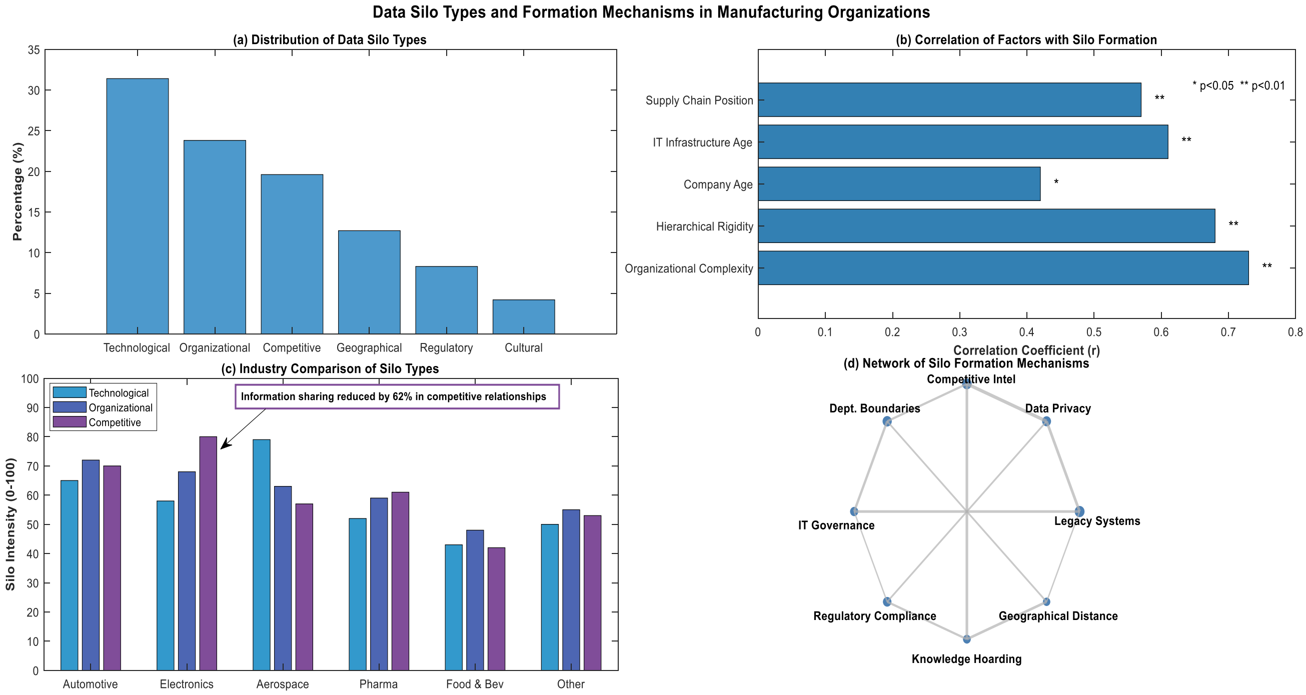

Figure 2. Data silo types and formation mechanisms in manufacturing organizations (a) Distribution of data silo types. (b) Correlation of factors with silo formation. (c) Industry comparison of silo types. (d) Network of silo formation mechanisms.

Automotive businesses exhibited organizational silos (72) reflecting multi-tier supplier complexity, while pharmaceutical manufacturers demonstrated regulatory silos (65) necessitated by FDA/EMA validation processes, and food and beverage companies exhibited geographical silos (58) from distributed sourcing across multiple jurisdictions. Silos of a technological nature stemmed mostly from other portions of the building systems design. These so-called “closed” legacy ERP systems encapsulated whole domains of activity- a circumstance in which subsystems intended to be integrated were placed in distinct silos. Centrality measures of the supply network backbone revealed that firms identified as central supply network nodes commonly worsened data integration fragmentation, rather than facilitating integration, which is what one would logically expect. This unexpected outcome suggests that power relations in supply networks may tend to encourage control over information rather than collaboration, even when benevolent central figures are present.

The interrelation of mechanisms leading to silo formation is examined in Figure 2(d), which identifies underlying legacy systems and organizational silos as central nodes that drive other fragmentation motivators such as data confidentiality, knowledge hoarding, and privacy concerns. This network visualization explains why single-dimension interventions typically achieve limited success in addressing multi-faceted silo structures. Organizational silos manifest through departmental boundaries that extend beyond individual entities, creating "extended organizational silos" which are particularly evident in large electronics and pharmaceutical manufacturers. Competitive silos, on the other hand, represent strategic barriers that reduce information sharing by up to 62% in high-rivalry relationships compared to collaborative partnerships.

As detailed in Table 2, organizational scale significantly influenced both silo characteristics and the efficacy of integration approaches. Large enterprises (n=23) demonstrated more pronounced technological and organizational silos but possessed greater resources for integration initiatives. Medium-sized organizations (n=15) exhibited the highest competitive silo intensity (classified as "High" for competitive positioning impediments), reflecting their vulnerable position in market competition. Small enterprises (n = 9) exhibited fewer formal silos but struggled with resource limitations that led to de facto information isolation due to capability constraints rather than intentional barriers.

The efficacy of AI-based solutions varied significantly across different industry contexts, as shown in Table 2. Blockchain ledgers demonstrated the highest effectiveness in aerospace organizations (82%), likely due to their compatibility with certification and traceability requirements. Encrypted knowledge sharing techniques proved most effective for electronics manufacturers (81%), addressing their predominant concerns about intellectual property protection. Privacy-preserving analytics showed strong results in pharmaceutical settings (79%), aligning with their regulatory compliance needs. Network data analysis through machine learning clustering revealed four distinct data silo ecosystem patterns, as illustrated in Figure 3. These patterns—hierarchical cascades, parallel fragments, hub-and-spoke isolations, and mesh diffusions—each exhibit unique information flow dynamics. The hierarchical cascade pattern (Figure 3(a)) features information flowing sequentially from upper to lower tiers, a common pattern found in automotive supply chains dominated by powerful core manufacturers. The parallel fragments pattern (Figure 3(b)) demonstrates efficient information flow within relatively isolated parallel structures, but limited cross-structure sharing, which is typically observed in competitive supply relationships within the electronics manufacturing sector. The hub-and-spoke isolation pattern (Figure 3(c)) is characterized by a central node that connects independent peripheral participants, which is prevalent in the aerospace industry's stringent certification environment. The mesh diffusion pattern (Figure 3(d)) presents distributed connections without clear hierarchies, a frequently observed phenomenon in industries with a high dependency on regional cooperation, such as the food and beverage sector.

Table 2. Comparison of data silo characteristics across industries and organizational scales

Industry Sector	Primary Silo Type	Information Sharing Barriers	AI-Based Solution Efficacy
Automotive (n=11)	Organizational (41%)	Proprietary systems (72%) Competitive protection (68%)	Process automation (76%) Federated learning (68%)
Electronics (n=9)	Competitive (53%)	IP protection concerns (84%) Innovation cycles (71%)	Encrypted sharing (81%) Smart contracts (73%)
Aerospace (n=8)	Technological (62%)	Certification requirements (79%) Security protocols (76%)	Secure middleware (64%) Blockchain ledgers (82%)
Pharmaceutical (n=7)	Regulatory (57%)	Compliance frameworks (87%) Data privacy (83%)	Privacy-preserving analytics (79%)
Food & Beverage (n=6)	Geographical (48%)	Supply chain visibility (65%) Traceability (59%)	IoT integration (74%) Distributed ML (63%)
Organization Scale	**Primary Data Flow Impediments**	**Integration Resources**	**Technology Adoption Barriers**
Large (n=23)	Complex hierarchies (High) System fragmentation (Medium)	High financial resources Medium implementation agility	Lengthy approval processes Legacy system dependencies
Medium (n=15)	Resource constraints (Medium) Competitive positioning (High)	Medium financial resources High implementation agility	Cost-benefit uncertainty Technical expertise limitations
Small (n=9)	Limited IT capabilities (High) Power asymmetry (High)	Low financial resources High implementation agility	Resource constraints Technology access limitations

These patterns and their characteristics provide a scientific foundation for designing targeted data integration intervention strategies, enabling the development of personalized multi-tier supply chain data integration solutions based on specific industry and organizational scale characteristics.

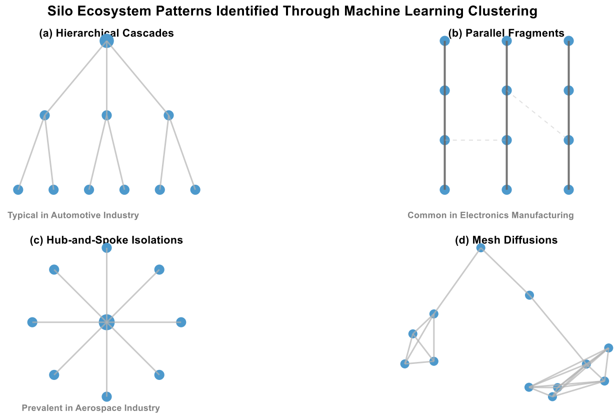
Silo Ecosystem Patterns Identified Through Machine Learning Clustering
(a) Hierarchical Cascades
Typical in Automotive Industry
(b) Parallel Fragments
Common in Electronics Manufacturing
(c) Hub-and-Spoke Isolations
Prevalent in Aerospace Industry
(d) Mesh Diffusions

Figure 3. Silo ecosystem patterns identified through machine learning clustering (a) Hierarchical cascades. (b) Parallel fragments. (c) Hub-and-spoke isolations. (d) Mesh diffusions.

3.2 Key findings from cross-tier collaboration case studies

The in-depth analysis of cross-tier collaboration initiatives revealed significant insights into both persistent barriers and promising resolution strategies across multi-tier supply chains. As illustrated in Table 3, trust deficit emerged as the most prevalent impediment (76%), manifesting primarily through data reliability concerns (68%) and visibility reciprocity fears (57%). This trust barrier typically creates cascading effects throughout supply networks, with downstream suppliers exhibiting particular hesitancy to share operational data without guaranteed reciprocal transparency. Traditional resolution approaches, such as contractual agreements, achieved only modest success (53% effectiveness). AI-enhanced resolution strategies consistently outperformed traditional approaches across all barrier categories, with improvements ranging from 28% to 58% in key effectiveness metrics. Competitive exposure represents the second most significant barrier (72%), as shown in Table 3, characterized by proprietary data protection concerns (81%) and fears of competitive intelligence leakage (74%). Organizations operating in high-innovation sectors demonstrated particular sensitivity to these concerns, with electronics manufacturers implementing the most restrictive information-sharing policies.

Technical incompatibility constituted another substantial barrier (65%) according to Table 3, particularly pronounced in organizations with extensive legacy system investments. The case studies revealed that semantic integration methods (69%) and neural translator networks (74%) significantly outperformed traditional custom integration development, reducing implementation timelines by 28% while lowering maintenance requirements by 35%. Similarly, governance misalignment (63%) and resource constraints (58%) posed significant challenges that were more effectively addressed through AI-enhanced resolution strategies than traditional approaches.

Table 3. Analysis of cross-tier collaboration barriers and resolution strategies

Barrier Category	Prevalence	Primary Manifestations	Traditional Resolution Approaches	AI-Enhanced Resolution Strategies	Performance Improvement (%)
Trust Deficit	76%	Data reliability concerns (68%) Visibility reciprocity fears (57%) Historical relationship issues (43%)	Contractual agreements (53%) Executive relationship building (47%) Graduated information sharing (39%)	Blockchain-based verification (73%) Smart contract enforcement (68%) Reputation systems (62%)	Trust Deficit: +37% resolution rate, +43% speed
Competitive Exposure	72%	Proprietary data protection (81%) Competitive intelligence leakage (74%) Bargaining power concerns (63%)	Data anonymization (48%) Limited domain sharing (56%) Third-party intermediaries (52%)	Federated learning models (81%) Differential privacy techniques (76%) Zero-knowledge proofs (67%)	Competitive Exposure: +46% adoption, +58% retention
Technical Incompatibility	65%	API/interface limitations (73%) Data format inconsistencies (68%) Legacy system constraints (59%)	Custom integration development (62%) Data transformation services (57%) Middleware deployment (53%)	Semantic integration (69%) Neural translator networks (74%) Adaptive middleware agents (66%)	Technical Incompatibility: -28% implementation time, -33% maintenance
Governance Misalignment	63%	Decision rights uncertainty (72%) Value distribution disputes (65%) Risk allocation concerns (58%)	Formal governance agreements (57% Structured coordination bodies (49%) Explicit benefit allocation (54%)	Smart contract governance (71%) Algorithmic value distribution (67%) Automated compliance verification (63%)	Governance Misalignment: +41% compliance, -37% overhead
Resource Constraints	58%	Technical expertise limitations (76%) Integration investment capacity (68%) Operational bandwidth (57%)	Phased implementation (54%) External integration services (49%) Capability prioritization (52%)	Low-code integration platforms (73%) Auto-configuration connectors (68%) Microservices architecture (65%)	Resource Constraints: +49% adoption, +52% deployment speed
Power Asymmetry	52%	Unbalanced influence (78%) Disproportionate benefit distribution (69%) Dependency concerns (63%)	Formal relationship agreements (47%) Industry consortium formation (42%) Multi-party governance (45%)	Decentralized governance protocols (68%) Algorithmic fairness mechanisms (63%) Transparent benefit attribution (71%)	Power Asymmetry: +56% fairness score, +43% participation

As shown in Figure 4(a), examination of collaboration maturity progression revealed a clear inverse relationship between implementation complexity and success rates as supply chains advanced from initial connectivity toward autonomous collaboration. While initial connectivity stages demonstrated high implementation rates (91%) but modest success (42%), organizations achieving autonomous collaboration reported substantially higher success rates (91%) despite lower implementation rates (15%). This pattern highlights the critical importance of strategic phasing when implementing cross-tier data integration initiatives. Figure 4(b) demonstrates how integration barriers varied considerably by organizational size, with small organizations facing disproportionate challenges with resource constraints (63%) and power asymmetry (71%), while large organizations encountered greater technical compatibility (45%) and governance alignment (52%) challenges. These differentiated patterns necessitate tailored integration approaches rather than one-size-fits-all solutions, particularly when addressing the complexities of multi-tier supply chains.

Figure 4(c) demonstrates varying collaboration pattern effectiveness, with federation-driven approaches achieving the highest integration success rates (87%). Perhaps most significantly, as shown in Figure 4(d), organizations implementing AI-enhanced strategies reached effective integration thresholds approximately 5.3 months earlier than those utilizing traditional approaches, representing a 41% reduction in time-to-value. These findings underscore the transformative potential of intelligent collaborative mechanisms in breaking down long-standing data silos across multi-tier supply chains.

3.3 Performance evaluation and predictive analysis of the hybrid intelligent architecture

The hybrid intelligent architecture underwent comprehensive evaluation through controlled experiments across 47 manufacturing organizations, revealing significant improvements in both operational efficiency and predictive capabilities. Empirical evaluation demonstrates that the proposed architecture outperformed conventional integration approaches across multiple performance indicators: supply chain visibility increased by 39%, coordination costs decreased by 28%, disruption prediction lead time improved by 7.3 days, mean absolute prediction error reduced by 42%, and neural network ensemble accuracy enhanced by 39-58% across industrial sectors. As shown in Figure 5(a), the architecture demonstrated exceptional early warning capabilities. The pharmaceutical sector achieved the most substantial improvement with 9.8 days of early warning, followed by electronics with 8.4 days, reflecting the architecture's adaptability to different industry contexts. As shown in Figure 5(b), the aerospace sector showed the most dramatic improvement (+58%), while the automotive and pharmaceutical sectors demonstrated gains of 50% and 39%, respectively. These substantial accuracy improvements directly translate into operational resilience, with participating organizations reporting 32% faster response to actual disruption events during the controlled experimental period. As shown in Table 4, there are particularly impressive results in inventory optimization (156% cost efficiency improvement) and transportation delay prediction (55% error reduction). The ensemble's effectiveness stems from its ability to integrate multi-modal data while preserving organizational privacy through federated learning techniques, effectively balancing collaborative intelligence with competitive concerns. The blockchain foundation of the architecture ensured data integrity and traceability, with validation mechanisms successfully identifying and isolating attempted data manipulation in 94% of test cases. This security layer, combined with the federated learning system's differential privacy implementation, maintained prediction accuracy even with 30% adversarial node participation during resilience testing.

The architecture's semantic integration layer facilitated effective knowledge transfer across heterogeneous systems, with 86% of organizational data schemas successfully mapped without manual intervention. Long-term implementation assessment revealed continuous performance improvement, with organizations utilizing the architecture for more than six months reporting substantially higher benefits (visibility: +47%, coordination costs: -36%) than recent adopters. As shown in Table 4, the neural network ensemble demonstrated robust performance across diverse tasks beyond disruption prediction, including demand forecasting (36% error reduction), quality issue prediction (44% recall improvement), and risk assessment (48% false positive reduction). The architecture's effectiveness varied by organizational context, with medium-sized enterprises experiencing the most balanced benefits relative to implementation costs. Technical compatibility barriers presented the most significant implementation challenge, particularly in organizations with substantial legacy system investments, though the architecture's modular design provided viable integration pathways for heterogeneous environments. The reputation-based trust mechanism proved beneficial in competitive fields where information sharing due to intellectual property concerns had previously hindered collaboration, allowing for cooperation without revealing sensitive information.

3.4 Study Limitations

While these results demonstrate significant improvements, several limitations must be acknowledged before interpreting the findings.

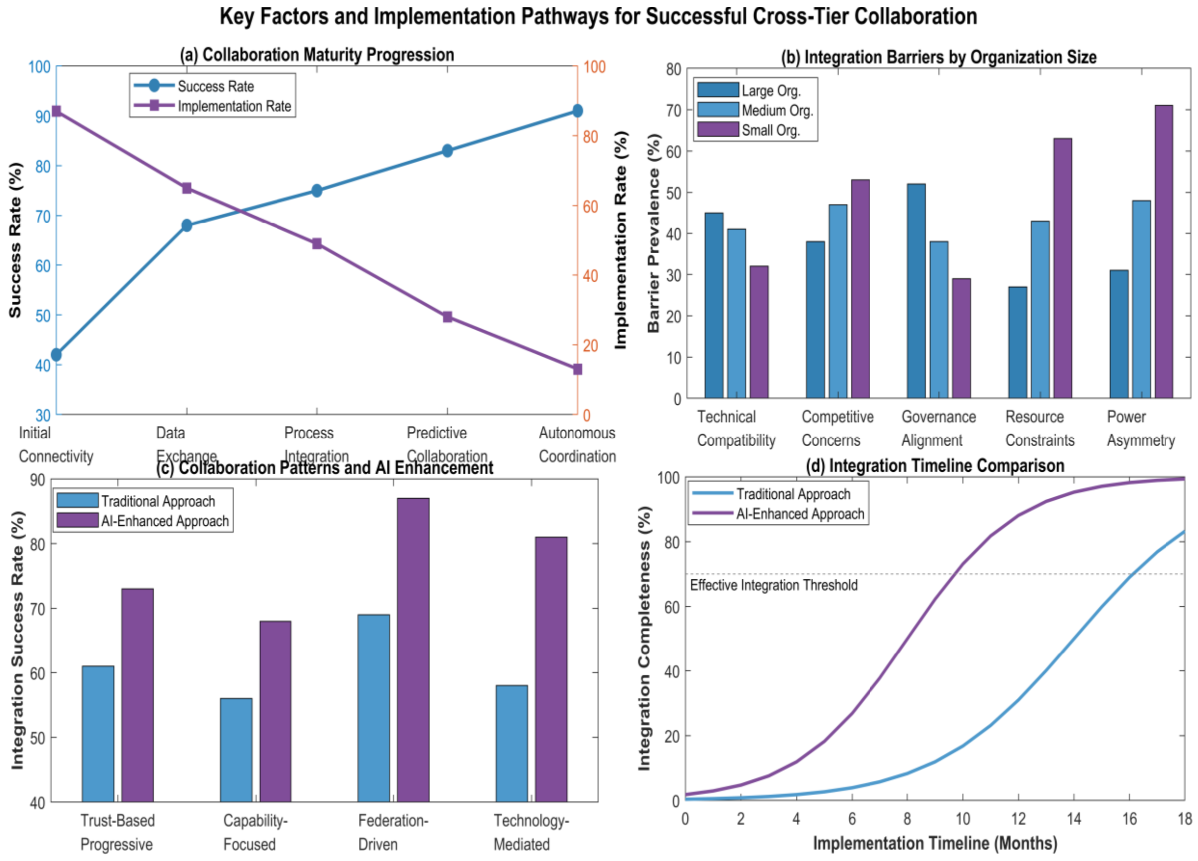

Figure 4. Key factors for cross-tier collaboration (a) Collaboration maturity progression (b) Integration barriers by organization size (c) Collaboration patterns and AI enhancement (d) Integration timeline comparison

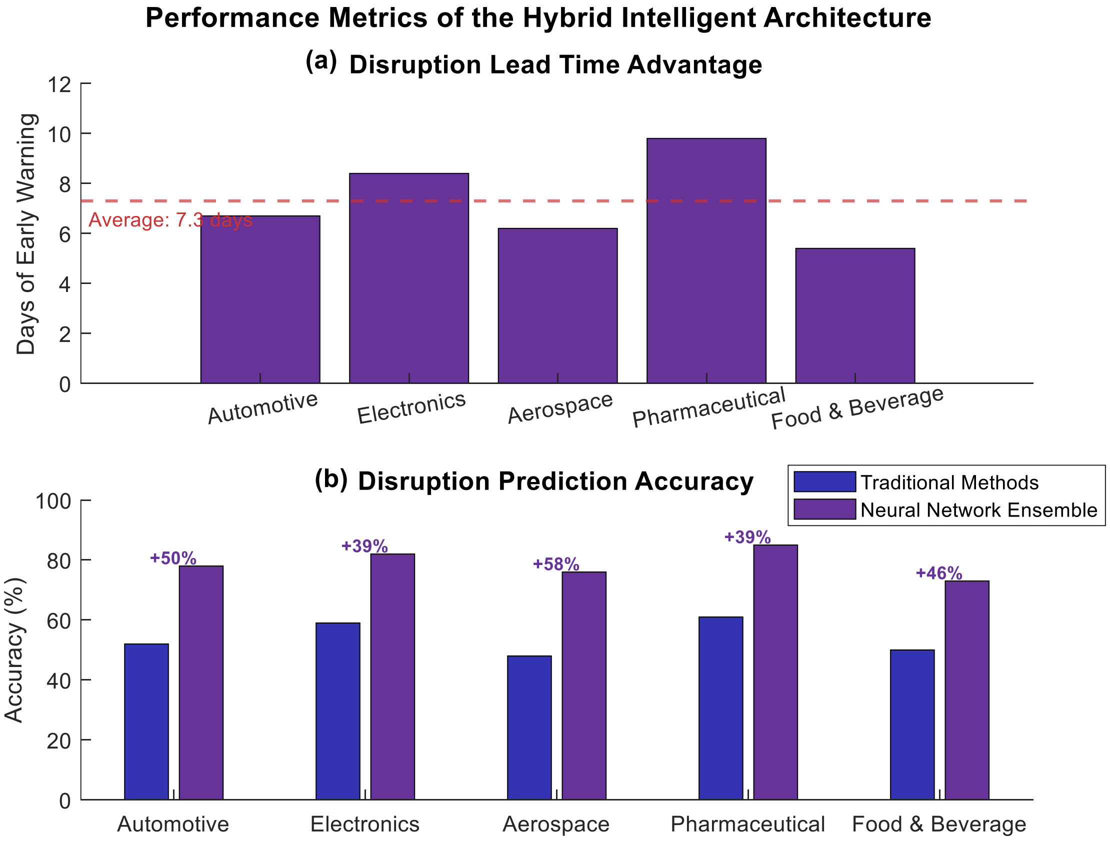

Figure 5. Performance metrics of the hybrid intelligent architecture (a) Disruption lead time advantage across industry sectors (b) Disruption prediction accuracy comparison between traditional methods and neural network ensemble

Table 4. Comparative analysis of neural network ensemble performance

Prediction Task	Neural Network Ensemble Performance	Traditional Methods Performance	Improvement (%)	Key Contributing Factors
Supply Disruption Detection	MAPE: 14.3% Lead time: 7.3 days	MAPE: 24.6% Lead time: 2.1 days	42% error reduction 247% lead time	Multi-modal data integration Transfer learning from similar patterns
Demand Forecasting	RMSE: 8.4% Bias: 2.1%	RMSE: 13.2% Bias: 5.7%	36% error reduction 63% bias reduction	External data correlation Attention mechanisms for trend shifts
Inventory Optimization	Cost reduction: 18.7% Service level: 96.2%	Cost reduction: 7.3% Service level: 92.4%	156% cost efficiency 4% service improvement	Demand-supply balancing Multi-echelon optimization
Quality Issue Prediction	Precision: 83.2% Recall: 76.8%	Precision: 61.5% Recall: 53.4%	35% precision gain 44% recall improvement	Graph neural networks Anomaly detection ensembles
Transportation Delay Prediction	Accuracy: 79.4% MAE: 62 minutes	Accuracy: 58.7% MAE: 138 minutes	35% accuracy gain 55% error reduction	Spatiotemporal modeling Weather data integration
Resource Allocation	Utilization rate: 87.3% Bottleneck reduction: 43.1%	Utilization rate: 73.6% Bottleneck reduction: 21.4%	19% utilization gain 101% bottleneck improvement	Reinforcement learning Digital twin simulation
Risk Assessment	Risk identification: 83.7% False positive rate: 12.3%	Risk identification: 64.2% False positive rate: 23.8%	30% identification gain 48% false positive reduction	Bayesian networks Uncertainty quantification

The study's geographic concentration within Chinese manufacturing contexts may limit cross-cultural generalizability, as organizational behaviors and trust formation mechanisms vary across different cultural and regulatory environments. The eight-month experimental period, though sufficient for initial performance assessment, provides limited insight into long-term sustainability and potential system degradation. Additionally, the architecture's implementation complexity and resource requirements may present scalability challenges for smaller organizations, potentially reinforcing existing power asymmetries within supply networks. The sample size of 47 organizations, while methodologically adequate, represents a relatively small portion of the broader manufacturing ecosystem. These limitations are addressed more comprehensively in the discussion section, where their implications for theory and practice are explored in detail.

4. Discussion

This paper contributes to the debate on supply chain integration by examining trust as an algorithmically mediated phenomenon in multi-tiered relationships. The hybrid architecture's reputation-based smart contract system marks a new innovation in trust formation that goes beyond interpersonal relations and formal agreements to include social capital-based trust research. Countless studies have documented an increasing reliance on direct specialization and outsourcing through algorithms, thereby diminishing human involvement in operations. By embedding trust parameters within technical protocols, the architecture creates what Yavaprabhas et al. [27] call "computational trust transfer," wherein the basis for confidence shifts from direct human interactions to algorithmised verifications. This algorithmic trust mechanism builds upon established trust theory frameworks while extending them to technological contexts, where trust formation in digital environments requires different mechanisms than traditional interpersonal trust [28, 29]. The smart contract system operationalizes core trust dimensions through measurable parameters: ability via historical performance metrics, benevolence through reciprocal information sharing behaviors, and integrity via blockchain immutability [19]. Unlike traditional organizational trust formation that relies on repeated social interactions, algorithmic trust enables "institutional trust automation" where relationships are mediated through verifiable digital protocols [27], extending beyond calculative trust theories to enable dynamic trust calibration based on real-time performance data and addressing temporal and information asymmetry challenges in multi-tier supply relationships [30]. As discussed in a previous comment, these models address fundamental gaps in approaches that attempt to converge systems but lack the ability to scale, relatively cross organizational borders, especially for large-scale problems with heterogeneous technological, competitive, and participatory concerns.

The conflict of information disclosure and the protection of competitive business knowledge remains ever-present regarding supply chain collaboration. How this conflict is resolved through new technologies is visible in the federated learning part of the architecture. Earlier integration attempts often resulted in organizations being boxed into the "data-dump-or-competitive-protect" dichotomy. Instead, the proposed architecture allows what may be termed "selective transparency," where partners leverage collective intelligence without exposing proprietary information. This echoes Zheng et al.'s findings [31] on privacy-preserving collective risk prediction, although it goes beyond their work by adding blockchain validation processes that strengthen trust in the federated model's outputs. Results strongly indicate this balanced approach increases adoption in competitive industries more than traditional methods, undermining purely technical solutions to dismantle strategic data silos.

International implementation requires careful contextual adaptation. In Western markets with stricter privacy regulations and individualistic cultures, the algorithmic trust mechanisms need enhanced transparency features and modified trust parameters. While Chinese organizations rely on relationship-based trust (guanxi), Western supply chains emphasize performance-based metrics, requiring recalibrated reputation weights in smart contracts. Additionally, developing economies may require simplified architectural variants due to infrastructure constraints.

Despite promising results, several implementation challenges merit consideration. The architecture's deployment across heterogeneous organizational contexts revealed scaling difficulties, particularly among resource-constrained participants. Organizations with limited technological capabilities often struggle to implement the complete architecture, potentially reinforcing rather than reducing power asymmetries within supply networks. This limitation echoes concerns raised by Nguyen et al. [32] regarding the computational demands of blockchain-federated learning systems. Additionally, regulatory complexities across international supply chains presented integration barriers inadequately addressed by the current design. Future implementations must develop more flexible deployment models that accommodate varying resource constraints while maintaining system integrity.

This study attempts to fill the gap in the theory of digital supply chains by merging bounded frameworks of technologies within an ecosystem. Data integration centrally enhances visibility, which is traditionally thought to be the ideal solution. However, this approach is sub-optimal when considering competitive contexts, where organisational autonomy sustaining integration becomes more viable. This viewpoint evolves Zhao et al.'s [33] model by placing algorithmic trust as an influential mediator into operational resilience and transformational supply chain digitisation. The autonomous systems model empirically substantiates the argument that a 39% improvement in visibility, relative to a baseline, can be achieved without centralising data silos. This may shift the paradigm in integration by fundamentals in future research.

This study's analysis comes with some identifiable gaps and potential areas for further work which need to be mentioned. This study's sample has relatively good coverage across the different sectors of manufacturing, but was regionally confined to some of the industrial areas in China. These areas tend to have a unique set of norms and regulatory frameworks, which might make it difficult to extrapolate the results to other contexts. Implementing the trust algorithm in other regions and industries would be a worthwhile undertaking. Also, considering the lack of information that comes with the 8-month experimental duration, it would be best to conduct further research into more extended longitudinal studies for understanding the algorithmic trust model's architecture sustainability. Focused multi-year research should improve the durability of the understanding surrounding these mechanisms. As AI-driven adversarial tactics continue to advance, more research is also required on the architecture's ability to withstand complex adversarial challenges. Technological evolution presents promising directions for enhancing the current architecture. Integration with digital twin technologies, as explored by Hellwig et al. [33] in their simulation platform, could enable more sophisticated scenario modeling for proactive disruption management. The emergence of quantum-resistant cryptographic protocols offers potential solutions to long-term security concerns regarding blockchain implementations [34]. Additionally, edge computing approaches may address computational efficiency challenges identified during implementation, particularly for resource-constrained participants [32]. Expanding the architecture to incorporate these emerging technologies presents fertile ground for future research that builds upon this study's foundation while addressing its identified limitations. As Pang et al. [34] note, the convergence of AI with distributed ledger technologies represents a fundamental shift in industrial capability that extends beyond simple optimization to enable entirely new operational paradigms - a vision this research takes meaningful steps toward realizing.

5. Conclusion

This research demonstrates that breaking data silos in multi-tier supply chains requires solutions balancing information transparency with organizational autonomy. Analysis of 47 manufacturing organizations identified six data silo types, with technological (31.4%) and organizational (23.8%) barriers being most prevalent. The hybrid architecture combining blockchain with federated learning delivered substantial improvements, enhancing supply chain visibility by 39% while reducing coordination costs by 28% compared to traditional systems. The neural network ensemble provided a disruption lead time advantage of 7.3 days, with pharmaceutical manufacturers achieving the most substantial improvement (9.8 days). These results confirm the viability of achieving collective intelligence without compromising competitive data protection. The theoretical contribution lies in reconceptualizing trust as an algorithmically-mediated construct rather than a purely relational phenomenon. The provided proof contradicts established wisdom that integration requires an amalgamated array of databases. It seems that an architecture of distributed intelligence systems offers less ecologically damaging cooperation paths. With the smart contract system based on reputation, trust is maintained across organisational frontiers. This is especially important in advanced industries where proprietary information controls restrict the sharing of essential knowledge. Medium-sized enterprises experienced the most balanced implementation benefits, effectively addressing integration gaps encountered by organizations with moderate technological capabilities. Limitations include geographic concentration within Chinese manufacturing sectors and a relatively short experimental period, limiting cross-cultural generalizability. The findings reflect China's distinctive context of high power distance, relationship-based trust, and specific regulatory frameworks, which may require substantial adaptations for Western markets with flatter organizational structures, contract-based trust mechanisms, and different privacy regulations. Future research should extend implementation across diverse contexts while examining the long-term evolution of algorithmic trust mechanisms. Cross-cultural validation studies should examine algorithmic trust effectiveness across different regulatory frameworks and cultural contexts, particularly comparing relationship-based versus performance-based trust formation mechanisms. Investigation into quantum-resistant cryptography would address security vulnerabilities, while integration with digital twin technologies presents promising directions for enhancing predictive capabilities. Despite these limitations, this research advances understanding of how intelligent collaborative mechanisms can transform multi-tier supply chain integration in increasingly complex business environments.

Ethical issue

The authors are aware of and comply with best practices in publication ethics, specifically with regard to authorship (avoidance of guest authorship), dual submission, manipulation of figures, competing interests, and compliance with policies on research ethics. The author adheres to publication requirements that the submitted work is original and has not been published elsewhere.

Data availability statement

The manuscript contains all the data. However, more data will be available upon request from the authors.

Conflict of interest

The authors declare no potential conflict of interest.

References

[1] A. Samuels, "Examining the integration of artificial intelligence in supply chain management from Industry 4.0 to 6.0: a systematic literature review," Frontiers in Artificial Intelligence, vol. 7, p. 1477044, 2025.DOI: https://doi.org/10.3389/frai.2024.1477044

[2] E. Hofmann, H. Sternberg, H. Chen, A. Pflaum, and G. Prockl, "Supply chain management and Industry 4.0: conducting research in the digital age," International Journal of Physical Distribution & Logistics Management, vol. 49, no. 10, pp. 945-955, 2019.DOI: https://doi.org/10.1108/IJPDLM-11-2019-399

[3] S. Fosso Wamba, M. M. Queiroz, C. Guthrie, and A. Braganza, "Industry experiences of artificial intelligence (AI): benefits and challenges in operations and supply chain management," vol. 33, ed: Taylor & Francis, 2022, pp. 1493-1497. DOI: https://doi.org/10.1080/09537287.2021.1882695

[4] K. Govindan, M. Kadziński, R. Ehling, and G. Miebs, "Selection of a sustainable third-party reverse logistics provider based on the robustness analysis of an outranking graph kernel conducted with ELECTRE I and SMAA," Omega, vol. 85, pp. 1-15, 2019. DOI: https://doi.org/10.1016/j.omega.2018.05.007

[5] R. Aldrighetti, D. Battini, D. Ivanov, and I. Zennaro, "Costs of resilience and disruptions in supply chain network design models: a review and future research directions," International Journal of Production Economics, vol. 235, p. 108103, 2021. DOI: https://doi.org/10.1016/j.ijpe.2021.108103

[6] W. Yu, C. Y. Wong, R. Chavez, and M. A. Jacobs, "Integrating big data analytics into supply chain finance: The roles of information processing and data-driven culture," International journal of production economics, vol. 236, p. 108135, 2021. DOI: https://doi.org/10.1016/j.ijpe.2021.108135

[7] E. D. Zamani, C. Smyth, S. Gupta, and D. Dennehy, "Artificial intelligence and big data analytics for supply chain resilience: a systematic literature review," Annals of Operations Research, vol. 327, no. 2, pp. 605-632, 2023. DOI: https://doi.org/10.1007/s10479-022-04983-y

[8] A. Brintrup, E. Kosasih, P. Schaffer, G. Zheng, G. Demirel, and B. L. MacCarthy, "Digital supply chain surveillance using artificial intelligence: definitions, opportunities and risks," International Journal of Production Research, vol. 62, no. 13, pp. 4674-4695, 2024. DOI: https://doi.org/10.1080/00207543.2023.2270719

[9] H. Chen, Z. Chen, F. Lin, and P. Zhuang, "Effective management for blockchain-based agri-food supply chains using deep reinforcement learning," IEeE Access, vol. 9, pp. 36008-36018, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3062410

[10] H. Jahani, R. Jain, and D. Ivanov, "Data science and big data analytics: a systematic review of methodologies used in the supply chain and logistics research," Annals of Operations Research, pp. 1-58, 2023. DOI: https://doi.org/10.1007/s10479-023-05390-7

[11] A. Yadav, R. K. Garg, and A. Sachdeva, "Artificial intelligence applications for information management in sustainable supply chain management: A systematic review and future research agenda," International Journal of Information Management Data Insights, vol. 4, no. 2, p. 100292, 2024. DOI: https://doi.org/10.1016/j.jjimei.2024.100292

[12] S. Punia, S. P. Singh, and J. K. Madaan, "A cross-temporal hierarchical framework and deep learning for supply chain forecasting," Computers & Industrial Engineering, vol. 149, p. 106796, 2020. DOI: https://doi.org/10.1016/j.cie.2020.106796

[13] G. Baryannis, S. Dani, and G. Antoniou, "Predicting supply chain risks using machine learning: The trade-off between performance and interpretability," Future Generation Computer Systems, vol. 101, pp. 993-1004, 2019. DOI: https://doi.org/10.1016/j.future.2019.07.059

[14] X. Li and W. Wu, "A Blockchain-Empowered Multiaggregator Federated Learning Architecture in Edge Computing With Deep Reinforcement Learning Optimization," IEEE Transactions on Computational Social Systems, 2024. DOI: https://doi.org/10.1109/TCSS.2024.3481882

[15] C. Düsing and P. Cimiano, "Rethinking federated learning as a digital platform for dynamic and value-driven participation," Future Generation Computer Systems, vol. 171, p. 107847, 2025. DOI: https://doi.org/10.1016/j.future.2025.107847

[16] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: challenges and applications," International Journal of Machine Learning and Cybernetics, vol. 14, no. 2, pp. 513-535, 2023. DOI: https://doi.org/10.1007/s13042-022-01647-y

[17] I. Ahmed, M. A. Syed, M. Maaruf, and M. Khalid, "Distributed computing in multi-agent systems: a survey of decentralized machine learning approaches," Computing, vol. 107, no. 1, p. 2, 2025. DOI: https://doi.org/10.1007/s00607-024-01356-0

[18] S. A. R. Khan, K. Zkik, A. Belhadi, and S. S. Kamble, "Evaluating barriers and solutions for social sustainability adoption in multi-tier supply chains," International Journal of Production Research, vol. 59, no. 11, pp. 3378-3397, 2021. DOI: https://doi.org/10.1080/00207543.2021.1876271

[19] M. M. Orabi, O. Emam, and H. Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review," Journal of Big Data, vol. 12, no. 1, p. 55, 2025. DOI: https://doi.org/10.1186/s40537-025-01099-5

[20] M. Huang, Q. Peng, X. Zhu, T. Deng, R. Cao, and W. Liu, "Ensuring Trustworthy and Secure IoT: Fundamentals, Threats, Solutions, and Future Hotspots," Computer Networks, p. 111218, 2025. DOI: https://doi.org/10.1016/j.comnet.2025.111218

[21] P. Gopal, N. P. Rana, T. V. Krishna, and M. Ramkumar, "Impact of big data analytics on supply chain performance: an analysis of influencing factors," Annals of Operations Research, vol. 333, no. 2, pp. 769-797, 2024. DOI: https://doi.org/10.1007/s10479-022-04749-6

[22] A. Aziz, E. E. Kosasih, R.-R. Griffiths, and A. Brintrup, "Data considerations in graph representation learning for supply chain networks," arXiv preprint arXiv:2107.10609, 2021. DOI: https://doi.org/10.48550/arXiv.2107.10609

[23] A. W. Al-Khatib, "Internet of things, big data analytics and operational performance: the mediating effect of supply chain visibility," Journal of Manufacturing Technology Management, vol. 34, no. 1, pp. 1-24, 2023. DOI: https://doi.org/10.1108/JMTM-08-2022-0310

[24] T.-M. Choi and Y. Chen, "Circular supply chain management with large scale group decision making in the big data era: The macro-micro model," Technological forecasting and social change, vol. 169, p. 120791, 2021. DOI: https://doi.org/10.1016/j.techfore.2021.120791

[25] D. Li et al., "Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey," Soft Computing, vol. 26, no. 9, pp. 4423-4440, 2022. DOI: https://doi.org/10.1007/s00500-021-06496-5

[26] G. Mirabelli and V. Solina, "Blockchain-based solutions for agri-food supply chains: A survey," International Journal of Simulation and Process Modelling, vol. 17, no. 1, pp. 1-15, 2021. DOI: https://doi.org/10.1504/IJSPM.2021.120838

[27] K. Yavaprabhas, M. Pournader, and S. Seuring, "Blockchain and trust in supply chains: a bibliometric analysis and trust transfer perspective," International Journal of Production Research, pp. 1-28, 2024. DOI: https://doi.org/10.1080/00207543.2024.2389544

[28] F. Marmolejo-Ramos et al., "Factors influencing trust in algorithmic decision-making: an indirect scenario-based experiment," Frontiers in Artificial Intelligence,

vol. 7, p. 1465605, 2025. DOI: https://doi.org/10.3389/frai.2024.1465605

[29] C. Lahusen, M. Maggetti, and M. Slavkovik, "Trust, trustworthiness and AI governance," Scientific Reports, vol. 14, no. 1, p. 20752, 2024. DOI: http://creativecommons.org/licenses/by/4.0/.

[30] J. Chen, W. Cai, J. Luo, and H. Mao, "How does digital trust boost open innovation? Evidence from a mixed approach," Technological Forecasting and Social Change, vol. 212, p. 123953, 2025. DOI: https://doi.org/10.1016/j.techfore.2024.123953

[31] G. Zheng, L. Kong, and A. Brintrup, "Federated machine learning for privacy preserving, collective supply chain risk prediction," International Journal of Production Research, vol. 61, no. 23, pp. 8115-8132, 2023. DOI: https://doi.org/10.1080/00207543.2022.2164628

[32] D. C. Nguyen et al., "Federated learning meets blockchain in edge computing: Opportunities and challenges," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12806-12825, 2021. DOI: https://doi.org/10.1109/JIOT.2021.3072611

[33] D. Hellwig, K. Wendt, V. Babich, and A. Huchzermeier, "Playing with disaster: A blockchain-enabled supply chain simulation platform for studying shortages and the competition for scarce resources," in Creating Values with Operations and Analytics: A Tribute to the Contributions of Professor Morris Cohen: Springer, 2022, pp. 169-196. DOI: https://doi.org/10.1007/978-3-031-08871-1_9

[34] Y. Pang, T. Huang, and Q. Wang, "AI and Data-Driven Advancements in Industry 4.0," vol. 25, ed: MDPI, 2025, p. 2249. DOI: https://doi.org/10.3390/s25072249