Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Federated AI for Multi-Enterprise Supply Chain Collaboration

Pallab Haldar
Independent Researcher, USA
Corresponding Author: Pallab Haldar, **E-mail**: reach2pallabhaldar@gmail.com

| ABSTRACT

As global supply chains expand into complex, interdependent ecosystems, organizations face a paradox: the need to share intelligence without sharing data. Traditional centralized AI architectures, dependent on aggregated datasets, conflict with regulatory restrictions, competitive secrecy, and privacy mandates. Federated Artificial Intelligence (FAI) resolves this paradox by enabling multiple enterprises to collaboratively train and deploy AI models across distributed data sources without transferring raw data. This article proposes an Enterprise Federated AI Architecture (EFAIA) tailored for multi-enterprise supply chain optimization. It integrates data fabric layers, secure aggregation protocols, and governance mechanisms that enable AI-driven forecasting, risk management, and procurement collaboration across organizational boundaries. The framework is demonstrated through industry-relevant use cases in manufacturing, pharmaceuticals, and logistics. Key benefits—enhanced prediction accuracy, regulatory compliance, and ecosystem trust—are balanced against challenges in interoperability, latency, and model governance. The article argues that federated AI is not merely a technical innovation but an organizational catalyst for co-intelligent supply networks, aligning efficiency with ethics in the emerging era of distributed intelligence.

| KEYWORDS

Federated Learning, Supply Chain Intelligence, Distributed Data Governance, Privacy-Preserving AI, Cross-Enterprise Collaboration

| ARTICLE INFORMATION

ACCEPTED: 12 November 2025 **PUBLISHED:** 02 December 2025 **DOI:** 10.32996/jcsts.2025.7.12.34

1. Introduction and Context

Supply chain structures have dramatically shifted away from simple sequential arrangements toward intricate, interdependent networks connecting multiple enterprises. Today's supply systems function as complex webs linking component producers, transportation companies, assembly plants, and retail outlets—with each participant both creating and utilizing crucial operational information. This transformation mirrors broader trends toward integrated supply operations through collaborative planning mechanisms and joint decision processes that generate benefits beyond organizational limits [1]. Effective integration demands nuanced protocols for information exchange that properly balance operational visibility against protection of confidential data, especially as real-time information from various partners increasingly drives decisions about inventory placement, transportation routing, and numerous other operational aspects.

Digital transformation and increasing interconnectedness have created a fundamental contradiction for organizations: they must somehow extract collective insights without exposing underlying information. Regulatory developments have intensified this challenge by establishing strict limitations on data movement. Legislation such as GDPR from Europe, CCPA from California, and China's PIPL now enforce strict requirements regarding data jurisdiction and storage location. These legal frameworks profoundly affect information flows across national borders, presenting compliance obstacles that conventional centralized data analysis methods simply cannot resolve without risking legal violations or exposing competitive information [2]. The conflict

between maximizing information utility while ensuring privacy protection stands as perhaps the central challenge confronting supply chain intelligence systems today, particularly as companies implement artificial intelligence for forecasting and operational enhancements.

These limitations have necessitated a fundamental architectural shift in modern supply operations: developing collective intelligence capabilities without centralized information repositories. Traditional approaches requiring partners to upload information to shared databases create unacceptable exposures through loss of control, security vulnerabilities, and compliance risks. Industry participants increasingly require systems to maintain local information governance while still enabling network-wide learning and optimization. This architectural evolution aligns with contemporary understanding that supply networks function as adaptive complex systems requiring both individual node independence and network-level coordination to achieve stability and performance targets [1]. The technical challenge involves designing frameworks that respect organizational boundaries while enabling cross-company learning.

Enterprise Federated AI Architecture (EFAIA) specifically addresses these requirements by facilitating distributed model development across organizational information boundaries while maintaining privacy and sovereignty. Unlike traditional AI implementations, EFAIA enables multiple organizations to jointly develop and utilize machine learning models without transferring actual data between participants. This technique represents significant progress in privacy-preserving machine learning approaches, allowing organizations to benefit from shared insights while maintaining strict protection of sensitive operational information [2]. The federated learning concept fundamentally transforms supply chain collaboration from a paradigm of "share data to gain insights" to one of "share insights while protecting data," effectively separating intelligence creation from information exposure.

This article aims to define, explain, and implement a comprehensive Federated AI Architecture specifically designed for multi-enterprise supply chain collaboration. The framework emphasizes privacy-preserving learning techniques, distributed information governance mechanisms, and compatibility with existing enterprise technologies. By allowing organizations to contribute toward collective intelligence while maintaining control over sensitive information, EFAIA converts competitive, fragmented supply chains into collaborative intelligence networks where data remains distributed but insights become shared resources. This transformation addresses the strategic requirement for optimization models spanning organizational boundaries without compromising competitive position or regulatory adherence [1]. The resulting architecture establishes a new model for supply chain intelligence that balances the seemingly contradictory requirements of collaboration and competition in contemporary business ecosystems.

2. Enterprise Federated AI Architecture Framework

The Enterprise Federated AI Architecture (EFAIA) establishes a structured approach tailored specifically for supply chain networks involving multiple companies. Through a carefully layered design, this architecture permits collaborative intelligence across organizational boundaries while protecting data independence and operational autonomy. EFAIA consists of five distinct yet interconnected structural components working together to enable privacy-conscious machine learning across separate enterprises.

Local Data Processing Nodes (LDPNs) form the foundational layer of the architecture. Individual companies host and manage their own nodes containing private information sets from various operational systems - from planning platforms to shop floor controls to warehouse management applications to connected devices. A crucial feature is that original information never crosses organizational limits, thus maintaining both legal compliance and confidentiality of business-sensitive details. Inside each node, data undergoes preparatory processing, including characteristic extraction, standardization, identity removal, and aberration identification. These preparatory steps ensure subsequent algorithmic training uses consistent, high-quality inputs while establishing primary privacy safeguards. Experimental applications with major distributed systems reveal that properly designed LDPNs deploy effective privacy protection while retaining processing capacity through streamlined communication methods and independent processing structures [3]. Such developments bring federated approaches within practical reach for corporate supply applications, despite differences in technology environments and varying connectivity limitations between participating organizations.

Built on this decentralized information foundation, the Model Training Layer implements specialized learning algorithms operating independently within each participant's environment. Rather than gathering information centrally, this component distributes model development across participating entities using advanced techniques addressing specific challenges in distributed settings. These algorithms handle variations in data characteristics, communication limitations, and statistical discrepancies between participating organizations. Current optimization approaches incorporate flexible aggregation techniques accounting for environments with varied processing capabilities and differing information distributions, preventing individual participants from exerting disproportionate influence on shared models [3]. This component must additionally resolve unique

supply chain challenges, including time-series dependencies, cyclical patterns, and requirements to process both structured transaction records and unstructured contextual information within a single learning framework while preserving confidentiality assurances.

The Secure Aggregation Layer forms the essential privacy-protecting element within the architecture. A central Coordination Function combines model updates using sophisticated encryption techniques such as calculation-enabling encryption or protected multi-party computation. These approaches keep model modifications encrypted throughout the combination process, blocking inference-based attacks that might otherwise compromise sensitive details. Recent technical advances have substantially improved aggregation protocols, creating specialized cryptographic methods balancing security protections with computational performance, lessening both bandwidth requirements and processing demands that previously restricted practical implementation of privacy-preserving learning techniques in corporate environments [3]. Such innovations enable protected federated learning even for time-critical supply applications where update speed directly affects operational decisions.

Supporting these technical components, the Governance and Policy Layer defines operational guidelines, standards, and responsibility mechanisms controlling federated collaboration. This component specifies participation requirements, verification processes, model access restrictions, and performance assessment criteria. Governance structures must resolve numerous outstanding issues, including equitable treatment in multi-party environments, participation incentives, protection against harmful participants, and clarity in model development [4]. Successful frameworks implement graduated access controls, contribution evaluation systems, and automated conformity verification, ensuring all participants follow established guidelines while receiving fair benefits from collective intelligence. This element transforms technical possibilities into organizational structures, enabling continued cooperation among competing yet interdependent supply chain participants.

The Collaboration & Visualization Layer provides interaction interfaces for participants engaging with the federated ecosystem. This component delivers monitoring displays for tracking shared performance indicators like prediction accuracy, supplier stability scores, or environmental metrics without revealing underlying information. This element overcomes significant distributed analytics challenges by implementing specialized display techniques that maintain privacy protections while delivering actionable insights [4]. The visualization component applies statistical anonymization to aggregate measures, implements protected multi-party calculation for comparative analyses, and delivers customized insights based on local information contextualized by global patterns, while consistently maintaining cryptographic protection across organizational limits.

Implementing this architecture requires technical integration components, including specialized learning frameworks, protected computation libraries, and communication infrastructure for secure, efficient model updating. Modern federated systems address numerous practical challenges, including communication efficiency, participant selection methods, and update coordination protocols, accommodating real-world corporate constraints [3]. These systems balance conflicting requirements, including convergence speed, bandwidth utilization, privacy assurances, and processing efficiency. Technical advances have considerably reduced resource demands for federated learning, making these approaches feasible even for resource-limited supply chain environments [4]. The resulting framework creates both technically sound and organizationally practical methods for cross-enterprise intelligence sharing that accommodate both competitive realities and collaborative necessities in contemporary supply networks.

Architecture Layer	**Manufacturing Implementation**	**Pharmaceutical Implementation**	**Retail Implementation**
Local Data Processing	Factory telemetry, quality metrics, production schedules	Clinical trial data, temperature logs, and regulatory records	Transaction data, inventory levels, customer segments
Model Training	Predictive maintenance, defect detection	Temperature excursion prediction, shelf-life modeling	Demand forecasting, assortment planning
Secure Aggregation	Homomorphic encryption with distributed key management	Differential privacy with pharmaceutical-grade security	Secure multi-party computation with retail-specific noise addition

Table 1: Comparison of Federated AI Architecture Layers Across Implementation Domains. [3, 4]

3. Implementation Use Cases and Benefits

The practical application of Enterprise Federated AI Architecture (EFAIA) across diverse supply chain ecosystems demonstrates its transformative potential through real-world implementations. These implementations span multiple industries with distinct regulatory environments, data sensitivity concerns, and collaborative dynamics. Examining these cases provides valuable insights into both the technical deployment patterns and the tangible business benefits of federated AI in supply chain contexts.

In the automotive manufacturing sector, Original Equipment Manufacturers (OEMs) and their networks of Tier-1 and Tier-2 suppliers have implemented federated AI systems to enhance parts demand forecasting and quality control. These implementations address the inherent tension in automotive supply chains: the need for collaborative planning alongside competitive supplier relationships. A typical automotive implementation connects OEMs with multiple suppliers in a federated network where each entity maintains control of sensitive production data. Suppliers retain factory telemetry, production rates, and quality metrics locally while participating in collective model training. The federated system enables joint prediction of component demand, defect probabilities, and supply disruption risks without centralizing proprietary manufacturing data. This approach has particular significance in automotive supply chains, where intellectual property concerns have historically limited data sharing despite the clear benefits of collaborative planning. Research indicates that federated learning implementations in automotive supply chains create what has been termed "resilience through distributed intelligence," enabling more robust responses to disruption events while preserving organizational data boundaries [5]. These methods utilize vertical integration (across supply chain tiers) and horizontal collaboration (across like-tier suppliers) to produce multi-dimensional intelligence networks that deliver visibility that preserves competitive positioning instead. The distributed nature of these implementations has proven especially valuable for managing supply chain transitions during industry transformation periods, including the shift toward electric vehicles and the associated component requirement changes.

The pharmaceutical supply chain presents another compelling implementation domain for federated AI, particularly in temperature-controlled logistics (cold chain) management. Pharmaceutical manufacturers, third-party logistics providers, distributors, and pharmacies have deployed federated anomaly detection systems to monitor temperature excursions across the distribution network. This use case addresses both the critical safety requirements of pharmaceutical products and the complex regulatory landscape governing pharmaceutical data. Each supply chain node maintains local IoT sensor data within its regional jurisdiction (addressing data localization requirements in territories such as the EU, US, and China), while the federated AI model learns from collective patterns to identify potential temperature control failures before product quality is compromised. Advanced implementations integrate blockchain-verified data with federated learning systems to create immutable audit trails while preserving data sovereignty across organizational boundaries [6]. These integrated architectures enable pharmaceutical supply chains to satisfy multiple competing objectives simultaneously: regulatory compliance, product integrity, cross-border operations, and multi-stakeholder collaboration. The pharmaceutical implementations demonstrate particularly sophisticated governance frameworks that balance algorithm transparency (for regulatory validation) with model security (for competitive protection), establishing architectural patterns that have subsequently influenced federated implementations in other highly regulated industries, including medical devices, aerospace, and food safety.

Security Mechanism	Privacy Protection Level	Performance Impact	Application Domain Suitability
Differential Privacy	Moderate - Statistical guarantee against individual record disclosure	Low - Minimal computation overhead	Retail forecasting, logistics optimization
Homomorphic Encryption	High - Mathematical guarantee of computational indistinguishability	High - Substantial processing overhead	Financial transactions, strategic sourcing
Secure Multi-Party Computation	Very High - Information theoretic security	Very High - Significant latency increase	Pharmaceutical compliance, aerospace quality control

Table 2: Privacy-Performance Tradeoffs in Federated Supply Chain Applications. [5, 6]

Beyond these industry-specific implementations, EFAIA deployments consistently deliver several categories of quantifiable benefits across supply chain ecosystems. Perhaps most fundamentally, these architectures enhance data privacy protection and regulatory compliance by eliminating raw data transfer between organizations. The federated approach inherently aligns with privacy regulations, including GDPR Article 25 (data protection by design) and Article 44 (data transfer restrictions), while

enabling intelligence sharing that would otherwise be prevented by these same regulations. Advanced implementations leverage what research identifies as "digital decoupling" strategies—creating clear separation between physical data flows and logical intelligence flows through cryptographic boundaries and differential privacy mechanisms [6]. This decoupling enables organizations to maintain complete control over sensitive data assets while still participating in collaborative intelligence initiatives, fundamentally resolving the historical tension between data protection and data utilization in cross-enterprise contexts.

EFAIA implementations also demonstrate substantial improvements in collaboration efficiency across supply chain partners. By eliminating the need to establish centralized data repositories with associated legal agreements, security audits, and data transformation processes, federated architectures significantly accelerate joint intelligence initiatives. This acceleration manifests in faster joint forecasting cycles, reduced time-to-insight for collaborative analytics, and more responsive risk detection across organizational boundaries. Research confirms that properly implemented federated architectures within data fabric frameworks substantially reduce implementation time for cross-enterprise AI initiatives while simultaneously improving governance consistency and operational resilience [7]. The efficiency gains derive not only from technical streamlining but also from organizational simplification, as federated approaches reduce the governance complexity of cross-enterprise data initiatives through standardized participation protocols and automated compliance verification mechanisms.

Another consistent benefit observed across implementations is improved model generalization, particularly for smaller supply chain participants with limited historical data. The federated approach allows these organizations to benefit from collective intelligence without surrendering their data autonomy. Studies of production implementations demonstrate that federated learning architectures effectively address the "cold start" problem in supply chain forecasting by enabling new participants to immediately benefit from collective intelligence without requiring extensive historical data contribution [6]. This characteristic makes federated architectures especially valuable in dynamic supply chains with frequent partner additions or substitutions, enabling rapid intelligence integration for new participants while maintaining system-wide prediction stability. The federated approach transforms network intelligence from a barrier to entry (requiring substantial historical data) into an enabler of ecosystem flexibility (providing immediate intelligence benefits to new participants).

EFAIA implementations also enhance trust and transparency among supply chain partners through shared governance mechanisms and verifiable computation. The architecture's emphasis on explicit governance frameworks, cryptographically secured model updates, and transparent performance metrics creates new foundations for inter-organizational trust that complement traditional contractual relationships. Industry research identifies trust enhancement as a critical element in successful data fabric implementations, enabling what analysts describe as "collaborative data ecosystems" where organizations can derive mutual benefit from shared intelligence while maintaining appropriate information boundaries [7]. This trust foundation creates positive feedback loops, enabling progressively deeper intelligence sharing as confidence in the framework develops through demonstrated performance and verified privacy protection. The most mature implementations establish measurable trust metrics, including contribution balance indicators, privacy leakage assessments, and governance compliance scores that provide objective measures of ecosystem health.

Finally, federated architectures deliver measurable sustainability benefits by reducing redundant computation and data replication across the supply chain. Traditional approaches often involve multiple organizations independently developing similar models on overlapping datasets, creating unnecessary environmental impact through duplicative storage and processing. Research on sustainable computing architectures shows that a federated approach significantly reduces storage and computational overhead by eliminating redundant data copies and centralizing model-building while decentralizing execution [6]. This characteristic, with environmental sustainability objectives, is an even more significant benefit as organizations pursue responsible computing practices within a broader ESG (Environmental, Social, and Governance) framework. The world's most advanced implementations include explicit carbon accounting for computational activities, including demonstrable emission reductions, through the federated approach, relative to purely centralized or fully distributed computing processes.

4. Challenges and Mitigation Strategies

The adoption of Enterprise Federated AI Architecture in supply networks brings substantial advantages but also introduces distinct obstacles across technical, operational, and administrative domains. Recognizing these challenges and developing practical solutions represents a critical success factor for organizations seeking sustained benefits from collaborative intelligence programs.

Technical compatibility across varied computing environments stands as perhaps the most fundamental implementation barrier. Supply networks routinely connect organizations operating vastly different technology platforms—from decades-old legacy applications to modern containerized microservices. This heterogeneity complicates uniform model deployment, data preparation standards, and communication between participating systems. Companies often employ different database

technologies, maintain inconsistent data structures, apply varied feature transformation techniques, and operate with fundamentally different definitions of seemingly identical concepts like "delivery performance" or "quality standards." Medical informatics research offers instructive parallels, highlighting how structured terminology through formal concept models and implementation-independent interfaces dramatically simplifies integration across disparate systems [8]. The compatibility problem transcends mere technical connections to encompass meaning alignment—ensuring consistent interpretation of business concepts despite organizational differences in underlying representation. Successful implementations typically employ layered architectural designs separating business concept models from technical infrastructure, enabling reliable intelligence development despite back-end system variations.

Performance stability and update coordination pose substantial challenges, especially in supply contexts experiencing rapid distribution changes through cyclical patterns, market evolution, or disruptive events. Federated environments face additional complications in detecting and correcting performance degradation across organizational boundaries when direct data comparison remains impossible. Without appropriate tracking and adjustment mechanisms, distributed models may increasingly diverge from operational realities, undermining forecast accuracy and decision support reliability. Construction industry research examining blockchain-AI combinations reveals that distributed ledger systems can provide effective model synchronization mechanisms, creating independently verifiable consensus regarding model states while preserving information confidentiality [9]. These combined approaches create tamper-resistant model history trails, enabling participants to validate evolutionary changes without exposing underlying information, simultaneously addressing technical coordination and confidence establishment. Effective performance management requires continuous evaluation through indirect measurements capable of detecting degradation without requiring direct data access.

Protection overhead and response time limitations present significant practical barriers for distributed supply implementations. While cryptographic protections deliver essential confidentiality guarantees, they simultaneously introduce processing demands and communication delays, potentially affecting time-critical supply decisions. This balance between security and performance demands careful calibration based on individual application requirements. Building sector implementations combining blockchain with artificial intelligence demonstrate that statistical anonymization techniques can substantially reduce encryption demands while maintaining sufficient confidentiality protection for many supply applications, creating improved performance characteristics for time-sensitive operations [9]. These challenges extend beyond computational efficiency to include communication optimization, particularly for geographically dispersed supply networks operating across diverse connectivity infrastructures. Leading implementations typically employ graduated protection approaches matching security measures with information sensitivity and operational time requirements.

Motivation alignment among participating organizations represents a crucial organizational challenge extending beyond technical considerations. In multi-company environments, participants frequently possess unequal capabilities, information assets, and potential benefits from federated collaboration. Without specific mechanisms ensuring fair value distribution, organizations possessing valuable information assets may decline participation, producing suboptimal collective results. Construction sector research demonstrates that explicit contribution valuation models—specifically measuring different participants' impact on overall prediction accuracy—can establish sustainable motivation frameworks ensuring continued engagement [9]. These approaches transform abstract collaborative benefit concepts into measurable indicators that organizations can incorporate into partnership agreements and value-sharing arrangements. Effective implementations typically address both financial incentives and non-financial motivations, including reputation enhancement, reciprocal access benefits, and regulatory compliance advantages.

Compliance uncertainty regarding distributed AI certification presents particular challenges for highly regulated supply sectors, including pharmaceuticals, food production, aerospace, and automotive manufacturing. While federated approaches inherently address certain regulatory concerns by maintaining information within organizational boundaries, they simultaneously raise new questions regarding model validation, responsibility attribution, and compliance verification. Traditional regulatory frameworks assume centralized control and visibility into training data—assumptions that federated architectures deliberately avoid. Manufacturing technology research indicates that comprehensive audit frameworks—combining automated monitoring, distributed verification, and structured documentation—can satisfy regulatory requirements while maintaining distributed privacy boundaries [10]. These approaches generate verifiable compliance evidence without centralizing sensitive information, resolving apparent conflicts between regulatory transparency and information protection. Advanced implementations typically develop specific compliance documentation explaining how federated approaches satisfy particular regulatory requirements despite their distributed nature.

Challenge Type	Common Manifestation	Mitigation Approach	Implementation Complexity
Technical Interoperability	Incompatible data formats, conflicting API standards	Adapter-based integration layer with transformation services	Medium - Requires custom connectors but follows established patterns
Semantic Interoperability	Inconsistent business definitions, varied quality metrics	Domain-specific ontologies with formal mapping relationships	High - Requires industry consensus and ongoing maintenance
Organizational Interoperability	Misaligned update schedules, incompatible security policies	Federated governance framework with explicit policy harmonization	Very High - Demands both technical and business process alignment

Table 3: Interoperability Challenges and Solutions in Federated Supply Chain Networks. [9, 10]

In addition to these specific challenges, addressing wider concerns, such as managing technical complexity, available expertise, and integration with existing analytical processes, will also be necessary for the implementation of distributed supply. In summary, addressing these types of challenges requires all-encompassing mitigation strategies that utilize a combination of infrastructure/cross-functional governance frameworks and organizational adaptation management. Distributed supply implementation research in manufacturing environments has demonstrated that successful deployments typically follow phased implementation approaches that initially deploy easier applications and progressively begin to deal with more complex challenges as technical capabilities and organizational readiness improve [10]. The incremental approach to implementation allows organizations to accumulate expertise, further develop appropriate governance structures, and demonstrate trust through ability, not just agreement. The most effective implementations explicitly incorporate learning and adaptation mechanisms in both technical systems and administrative processes.

Several proven mitigation approaches have emerged from successful implementations. Adaptive influence mechanisms address both technical diversity and motivation alignment by dynamically adjusting different participants' influence based on data quality, contribution consistency, and model impact rather than organizational size or data volume. Structured motivation frameworks, ranging from explicit financial arrangements to reputation systems and preferential access provisions, create sustainable participation incentives and data quality improvement. Policy-based model registries provide governance foundations documenting model origins, modification history, and performance characteristics while maintaining appropriate privacy boundaries. Manufacturing technology research demonstrates these governance systems must balance structure with adaptability, providing sufficient framework for consistency while permitting evolution as both technology and organizational relationships mature [10]. The most successful implementations approach governance as a continuous process rather than a static framework, incorporating feedback mechanisms enabling ongoing refinement across both technical and organizational dimensions.

Attribution Model	Value Measurement Approach	Implementation Complexity	Ecosystem Impact
Contribution-Based	Measures the incremental accuracy gain from each participant's data	Medium - Requires counterfactual testing	Favors data-rich participants, potentially excluding smaller partners
Quality-Based	Evaluates data completeness, accuracy, and timeliness	High - Demands standardized quality metrics	Encourages data quality improvements across all participants
Outcome-Based	Quantifies business value from model predictions	Very High - Requires cross-organizational outcome tracking	Creates the strongest alignment between technical contribution and business value

Table 4: Value Attribution Models in Federated Supply Chain Intelligence. [10]

5. Conclusion and Future Directions

Enterprise Federated AI Architecture (EFAIA) represents a transformative approach for supply chain intelligence, resolving the tension between collaboration needs and data protection requirements. By enabling organizations to learn collectively without sharing raw data, this framework creates new possibilities for supply chain optimization while preserving organizational autonomy.

Successful implementations in automotive, pharmaceutical, and other industries demonstrate that EFAIA delivers significant benefits: enhanced privacy protection, accelerated collaboration, improved model performance, and strengthened trust between partners. These implementations transform fragmented supply chains into collaborative networks where insights flow freely while sensitive data remains protected.

The environmental impact of EFAIA includes reduced computational redundancy and data duplication, contributing to more sustainable digital infrastructure. Economically, federated approaches create more accessible collaboration capabilities, particularly benefiting smaller supply chain participants. Socially, the governance frameworks foster more equitable, transparent relationships between supply chain partners.

Future developments promise to extend EFAIA's impact. Cross-industry federations will connect currently siloed networks across sectors like manufacturing, logistics, and retail. Quantum-safe encryption will ensure long-term security as computational capabilities evolve. Federated reinforcement learning may enable coordinated actions across supply chain entities, not just shared analytics.

Executives should establish federation consortia within their industries, creating shared governance frameworks and standardized interfaces. Organizations should invest in privacy-preserving technologies that enable efficient implementation while maintaining security. Policymakers should create clear regulatory frameworks for federated systems, providing certainty for implementation in sensitive domains.

The ultimate vision is supply chains as distributed cognitive systems—learning locally, reasoning collectively, and acting collaboratively while respecting organizational boundaries. This approach transforms traditional supply chains from mechanical transactional systems into adaptive learning networks that continuously evolve through collective intelligence, creating supply ecosystems that simultaneously optimize for efficiency, resilience, and sustainability.

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

References

[1] Sunil Chopra, Peter Meindl, "Supply Chain Management. Strategy, Planning & Operation," ResearchGate, 2002. [Online]. Available: https://www.researchgate.net/publication/247674861_Supply_Chain_Management_Strategy_Planning_Operation
[2] Joy Nnenna Okolo et al., "Federated learning for privacy-preserving data analytics in mobile applications," World Journal of Advanced Research and Reviews, 2025. [Online]. Available: https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-1099.pdf
[3] Keith Bonawitz et al., "Towards Federated Learning at Scale: System Design," arXiv preprint arXiv:1902.01046, 2019. [Online]. Available: https://arxiv.org/abs/1902.01046
[4] Peter Kairouz et al., "Advances and Open Problems in Federated Learning," arXiv preprint arXiv:1912.04977, 2021. [Online]. Available: https://arxiv.org/abs/1912.04977
[5] Ge Zheng, "Federated machine learning for privacy preserving, collective supply chain risk prediction," International Journal of Production Research, 2023. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/00207543.2022.2164628
[6] Lise Nakache et al., "Digital Twins to improve supply chain efficiency and resilience: literature review and research potential," ScienceDirect, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S240589632501105X
[7] Justin Lavelle, Barbara Ruane, "Gartner Says Chief Supply Chain Officers Can Scale AI With Data Fabric Architecture," Gartner, 2025. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2025-10-14-gartner-says-chief-supply-chain-officers-can-scale-ai-with-data-fabric-architecture
[8] Alexandros Bousdekis, Gregoris Mentzas, "Enterprise Integration and Interoperability for Big Data-Driven Processes in the Frame of Industry 4.0," Front Big Data. 2021. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC8210777/
[9] Houljakbe Houlteurbe Dagou, Asli Pelin Gurgun, "Blockchain and AI for Sustainable Supply Chain Management in Construction," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/383455412_Blockchain_and_AI_for_Sustainable_Supply_Chain_Management_in_Construction
[10] Jiewu Leng et al., "Federated learning-empowered smart manufacturing and product lifecycle management: A review," ScienceDirect, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1474034625000722