AI-Powered Closed-Loop Fusion: Demand-Technology-Implementation Synergy Across Business, Finance, and Cybersecurity (2022-2026)

Abstract

The cross-domain integration of artificial intelligence (AI) has formed a dynamic closed-loop ecosystem among digital commerce, finance, and cybersecurity—driven by mutually reinforcing demand pull, technical spillover, and implementation feedback. This review synthesizes 7 key studies (2022-2026) to unpack the "demand-technology-implementation" (DTI) closed-loop logic: digital commerce's demand for inclusive growth and privacy protection spurs AI technical innovation; financial sector's need for resource optimization and ESG compliance adopts and refines these technologies; cybersecurity's requirement for risk balance provides safeguards for technical 落地； and implementation outcomes from all three domains feed back to refine AI solutions. Findings reveal that: privacy-enhancing technologies (PETs) and modular AI architectures are the core technical bridges; SMEs act as the key link for inclusive value diffusion; and risk-cost balance is the common optimization target. This closed-loop framework explains how AI enables seamless fusion across business, finance, and cybersecurity, offering guidance for researchers designing cross-domain AI and practitioners building integrated ecosystems.

1 Introduction

The boundaries between digital commerce, finance, and cybersecurity are increasingly blurred by AI, forming a mutually dependent ecosystem rather than isolated sectors [1][4][6]. For example, digital commerce's demand for cross-channel marketing (business) drives the development of federated learning (AI technology) [1], which is then adapted to financial ESG data sharing (finance) [3]; cybersecurity's need to balance risk and cost (security) leads to multi-agent reinforcement learning (AI technology) [5], which optimizes business operations and financial resource allocation [4][6]; and the implementation effect of these technologies—such as SME adoption barriers [2] or regulatory compliance challenges [1]—feeds back to refine AI design. However, existing research often analyzes these domains in isolation, overlooking the closed-loop synergy of demand, technology, and implementation [2][3][5]. This review addresses this gap by synthesizing 7 key studies to construct the DTI closed-loop framework, explaining how AI drives cross-domain fusion across business, finance, and cybersecurity, and revealing the internal logic of value co-creation.

2 The DTI Closed-Loop Framework: Demand Pull, Technical Spillover, Implementation Feedback

2.1 Demand Pull: Cross-Domain Needs Driving AI Innovation Direction

Demand pull is the starting point of the closed loop, where unmet needs from digital commerce, finance, and cybersecurity define the direction of AI technical innovation. These demands are not isolated but mutually connected—solving one domain's problem often addresses another's pain point.

In digital commerce, the core demands are **inclusive growth** and **privacy-compliant collaboration**. SMEs, which form the backbone of the sector, lack access to advanced AI capabilities [2], while cross-channel marketing requires user data sharing that conflicts with privacy regulations [1]. Yi [1] identified the demand for "privacy-preserving cross-channel measurement"—retailers, platforms, and creators need to collaborate without violating user privacy; Yi [2] further pointed out the demand for "accessible AI infrastructure"—SMEs need low-cost access to PETs and marketing AI without in-house technical teams. These demands directly drive the development of federated learning frameworks [1] and multi-tenant modular architectures [2].

In finance, the core demands are **resource optimization** and **ESG compliance**. Investors need accurate market predictions to optimize portfolios [6], while SMEs face financial constraints that hinder ESG improvement [3]. Li and Liu [6] identified the demand for "high-precision financial time-series prediction"—traditional models fail to capture market volatility; Liu [3] highlighted the demand for "low-resource ESG optimization tools"—SMEs cannot afford expensive ESG consulting and data analysis. These demands align with the technical direction of AI: LSTM models for sequence prediction [6] and modular AI tools for low-cost ESG improvement [3].

In cybersecurity, the core demand is **risk-cost balance** in microservice architectures [5][4]. Organizations face a flood of vulnerabilities but limited resources to patch them, requiring AI that balances technical risk, operational continuity, and financial cost [5]. Zhou [5] identified the demand for "multi-stakeholder aligned vulnerability planning"—IT teams prioritize security, business units prioritize cost, and security vendors prioritize product adoption; Zhou [4] further demanded "integrated risk prioritization"—traditional single-dimensional testing fails to consider business impact. These demands drive the development of multi-agent reinforcement learning (MARL) [5] and hybrid security frameworks [4].

Notably, these demands are interconnected: digital commerce's SME inclusion demand [2] overlaps with finance's SME ESG resource constraint [3], and cybersecurity's risk-cost balance [5] directly affects business operations and financial resource allocation—forming a demand network that guides AI innovation.

2.2 Technical Spillover: Core AI Technologies Acting as Cross-Domain Bridges

Technical spillover is the middle link of the closed loop, where AI technologies developed to meet one domain's demand spill over to solve other domains' needs. The core technical bridges are **privacy-enhancing technologies (PETs)** and **modular AI architectures**, which have strong adaptability and compatibility across business, finance, and cybersecurity.

PETs—including federated learning, differential privacy, and zero-knowledge verification—are the most critical cross-domain technical bridge. Developed initially to address digital commerce's privacy-collaboration conflict [1], they spill over to finance and cybersecurity. Yi [1] designed a federated and differentially private framework for digital commerce cross-channel measurement—this technology spills over to finance by enabling ESG data sharing among SMEs, financial institutions, and regulators [3]: SMEs can share ESG-related data without exposing sensitive financial information, and financial institutions can use aggregated data to assess SME ESG ratings. In cybersecurity, PETs spill over to protect vulnerability data sharing—organizations can collaborate on threat intelligence without exposing internal security weaknesses [4]. Yi [6] extended PETs to social e-commerce ad targeting with zero-knowledge verification, further demonstrating their adaptability: this technology can be used in financial product marketing (e.g., personalized investment recommendations without exposing user financial data) and cybersecurity awareness campaigns (e.g., targeted risk alerts without compromising user information).

Modular AI architectures—including multi-tenant platforms and hybrid frameworks—enable inclusive technical spillover. Yi [2] developed a multi-tenant AI infrastructure for digital commerce SMEs, with standardized APIs and modular components: this architecture spills over to finance by providing low-cost ESG AI tools for SMEs [3]—SMEs can access modular ESG data analysis, report generation, and optimization modules without building custom systems. In cybersecurity, Zhou [4] designed a hybrid SAST-DAST-SCA-IAST framework with modular testing components—this architecture spills over to digital commerce and finance by allowing organizations to select relevant modules based on their size and needs: SMEs can use basic security testing modules, while large enterprises can integrate advanced risk assessment modules with business and financial data. Zhou [5]'s MARL-based M-VP2 method also adopts a modular design—agents representing different stakeholders (IT, business, finance) can be customized and reused across domains: in digital commerce, agents represent retailers, platforms, and SMEs; in finance, they represent investors, financial institutions, and regulators.

2.3 Implementation Feedback: Outcomes Refining the Closed Loop

Implementation feedback is the closing link of the loop, where the effect of AI technical 落地 in each domain provides insights to refine demand definition and technical design. This feedback ensures that AI solutions continuously adapt to cross-domain needs, forming a self-improving cycle.

From digital commerce implementation, feedback focuses on **inclusivity and usability**. Yi [2] found that while multi-tenant infrastructure lowers SME access barriers, some small businesses still face challenges with API integration and incentive understanding—this feedback leads to refined technical design: simplifying API interfaces and adding user-friendly guidance. Yi [1] observed that cross-channel measurement frameworks need to adapt to different regional privacy regulations—this feedback drives the development of flexible PETs that can be customized for GDPR, CCPA, or local data protection laws, which in turn benefits finance and cybersecurity implementations [3][4].

From finance implementation, feedback centers on **accuracy and resource efficiency**. Li and Liu [6] found that LSTM models for portfolio optimization perform well in stable markets but need adjustment for high volatility—this feedback leads to modular parameter tuning, making the model adaptable to digital commerce demand forecasting (e.g., predicting sales during promotional periods) [2]. Liu [3] noted that SME ESG AI tools need to prioritize high-impact, low-cost actions—this feedback refines the incentive systems in digital commerce's multi-tenant infrastructure [2], where SMEs can earn rewards for ESG improvements that also enhance their commercial competitiveness.

From cybersecurity implementation, feedback emphasizes **risk-business alignment**. Zhou [5] found that MARL-based patch plans need to better integrate financial cost data—this feedback leads to the integration of financial budgeting modules into the AI system, enabling direct linkage between vulnerability patching and financial resource allocation [6]. Zhou [4] observed that hybrid security frameworks need to align with business and financial KPIs—this feedback refines the risk-scoring metrics to include revenue impact and ROI, making the framework more useful for digital commerce inventory management and financial investment decisions [1][6].

This implementation feedback closes the loop: technical refinements based on one domain's outcomes better meet the demands of all three domains, driving continuous optimization of the cross-domain AI ecosystem.

3 Closed-Loop Fusion Outcomes Across Domains

3.1 Digital Commerce: Inclusive, Privacy-Respecting Growth Ecosystem

The closed loop enables digital commerce to form an inclusive ecosystem where large enterprises and SMEs coexist and collaborate. Yi [1][2][6]'s PETs and multi-tenant infrastructure—refined through feedback from finance and cybersecurity—enable SMEs to access cross-channel marketing tools [1], ad targeting capabilities [6], and ESG optimization resources [3] at low cost. Privacy compliance is guaranteed by federated learning and zero-knowledge verification [1][6], while cybersecurity safeguards from Zhou [4][5]'s frameworks protect transaction data and user information. The outcome is a growth model where SMEs are not excluded due to resource constraints, and users gain personalized experiences without privacy risks—driving overall sector growth.

3.2 Finance: Efficient, Inclusive Sustainable Finance System

Finance benefits from the closed loop by forming a sustainable finance system that balances investment efficiency and ESG inclusion. Li and Liu [6]'s LSTM models—refined through digital commerce demand forecasting feedback—improve portfolio optimization accuracy, enabling investors to achieve higher returns with lower risk. Liu [3]'s ESG AI tools—built on digital commerce's multi-tenant architecture [2] and protected by cybersecurity frameworks [4]—enable SMEs to improve ESG ratings with limited resources, expanding the pool of sustainable finance participants. The outcome is a financial system where both large institutions and SMEs can contribute to sustainability, and investment decisions are based on accurate data and robust risk safeguards.

3.3 Cybersecurity: Proactive, Business-Aligned Risk Management System

Cybersecurity completes the closed loop by developing a risk management system that aligns with business and financial objectives. Zhou [4][5]'s hybrid frameworks and MARL-based methods—refined through feedback from digital commerce and finance—enable organizations to prioritize vulnerabilities based on business impact and financial cost, not just technical risk. PETs from digital commerce [1][6] protect threat intelligence sharing, enabling proactive risk detection, while financial data integration allows for precise resource allocation to high-impact security measures. The outcome is a cybersecurity system that does not hinder business growth or financial efficiency but instead enables safe and sustainable cross-domain operations.

4 Practical Implications

4.1 For Researchers

Design AI with closed-loop adaptability: prioritize modular architectures and flexible PETs that can spill over across business, finance, and cybersecurity [1][4][6]; embed feedback collection mechanisms into technical design to enable continuous refinement [2][3][5]; and focus on SME needs as the key to inclusive value [2][3].

4.2 For Practitioners

Adopt a cross-domain mindset: digital commerce enterprises should integrate cybersecurity safeguards [4][5] and financial ESG tools [3] into their AI infrastructure [2]; financial institutions should leverage digital commerce's PETs for data sharing [1] and cybersecurity's risk models for investment protection [5]; cybersecurity teams should align risk management with business and financial KPIs [4][6]. SMEs should leverage multi-tenant platforms [2] to access integrated AI capabilities across all three domains.

4.3 For Policymakers

Support closed-loop ecosystem development: promote cross-domain data standards to facilitate technical spillover [1][6]; fund inclusive AI infrastructure for SMEs to strengthen the key link [2][3]; and develop flexible regulatory frameworks that balance innovation and risk across business, finance, and cybersecurity [1][4].

5 Conclusion

This review synthesizes 7 key studies to propose the "demand-technology-implementation" closed-loop framework for AI-powered fusion across digital commerce, finance, and cybersecurity. The framework reveals that cross-domain integration is not a one-way technical application but a dynamic cycle: demand from all three domains drives AI innovation, core technologies spill over to connect domains, and implementation feedback refines solutions. Privacy-enhancing technologies and modular architectures are the technical backbone, SMEs are the inclusive link, and risk-cost balance is the common target. By understanding this closed-loop logic, researchers, practitioners, and policymakers can unlock the full potential of AI to create an integrated ecosystem where business growth, financial efficiency, and cybersecurity are mutually reinforcing—driving sustainable and inclusive value creation across sectors.

References

[1] Yi, X. (2026). A Federated and Differentially Private Incentive–Marketing Framework for Privacy-Preserving Cross-Channel Measurement in AI-Powered Digital Commerce.

[2] Yi, X. (2026). Trusted AI Commercialization Infrastructure for SMBs: A Unified Multi-Tenant Architecture Integrating Incentive Systems, Content Governance, and Standardized Recommendation APIs.

[3] Liu, T. (2022, December). Financial Constraint'Impact on Firms' ESG Rating Based on Chinese Stock Market. In *2022 4th International Conference on Economic Management and Cultural Industry (ICEMCI 2022)* (pp. 1085-1095). Atlantis Press.

[4] Zhou, D. (2026). AI-Driven Hybrid SAST–DAST–SCA–IAST Framework for Risk-Based Vulnerability Prioritization in Microservice Architectures.

[5] Zhou, D. (2025, December). M-VP2: Microservice-Oriented Vulnerability Patch Planning-A Cost-Aware Approach using Multi-Agent Reinforcement Learning. In *2025 5th International Conference on Computer, Internet of Things and Control Engineering (CITCE)* (pp. 248-254). IEEE.

[6] Li, H., & Liu, T. (2023). Portfolio optimization based on the LSTM forecasting model. In *Proceedings of the 2nd International Conference on Financial Technology and Business Analysis* (Vol. 48, No. 1, pp. 97-106).

[7] Yi, X. (2026). Privacy-Enhanced Ad Targeting for Social E-Commerce: A Federated Learning Framework with Zero-Knowledge Verification for Creator Monetization. *Frontiers in Business and Finance*, 3(1), 102-113.