Spiral Upgrade Model: How AI Drives Continuous Cross-Domain Collaboration Among Business, Finance, and Cybersecurity (2022-2026)

Abstract

Artificial intelligence (AI) has triggered a spiral upgrade of cross-domain collaboration between digital commerce, finance, and cybersecurity, following a three-stage iterative logic: resource aggregation (integrating cross-domain data, technology, and capital through AI), risk governance (jointly mitigating cross-domain risks via AI-powered tools), and ecosystem value addition (expanding the scale and value of the cross-domain ecosystem through iterative optimization). This review synthesizes 7 key studies (2022-2026) to unpack the operational mechanism of each stage and the spiral upgrade logic: resource aggregation lays the foundation by breaking resource silos (e.g., multi-tenant infrastructure integrating SME resources, LSTM models integrating financial data); risk governance ensures sustainability by addressing cross-domain risks (e.g., privacy-enhancing technologies [PETs] mitigating privacy risks, multi-agent reinforcement learning [MARL] balancing security and financial risks); ecosystem value addition realizes iteration by amplifying cross-domain value (e.g., inclusive growth from SME participation, sustainable value from ESG integration). Findings reveal that the spiral upgrade is driven by mutual feedback—resource aggregation generates new risks that require risk governance, and risk governance optimizes resource allocation to promote ecosystem value addition; AI modularity and privacy technologies are the core drivers of spiral iteration; SMEs are the key beneficiaries and amplifiers of the spiral upgrade. This model provides a dynamic perspective on cross-domain AI collaboration, guiding researchers, practitioners, and policymakers to foster continuous value creation across sectors.

1 Introduction

The cross-domain interaction between digital commerce, finance, and cybersecurity is no longer a static collaboration but a dynamic spiral upgrade driven by AI [1][4][7]. For example, Yi's [2] multi-tenant infrastructure (digital commerce) aggregates SME resources (resource aggregation) [2], which requires Yi's [1] PETs to mitigate privacy risks (risk governance) [1], and ultimately forms an inclusive ecosystem that amplifies the value of all participants (ecosystem value addition) [7]; Zhou's [5] MARL-based vulnerability planning (cybersecurity) aggregates risk, financial, and business data (resource aggregation) [5], enables multi-stakeholder risk sharing (risk governance) [5], and optimizes resource allocation to create cost-saving and security-enhancing value (ecosystem value addition) [4]; Li and Liu's [6] LSTM model (finance) aggregates financial time-series data (resource aggregation) [6], relies on cybersecurity frameworks to protect data security (risk governance) [4], and generates improved investment returns that feed back into digital commerce and cybersecurity resource inputs (ecosystem value addition) [6]. However, existing research often views cross-domain collaboration as a linear process [2][3][6] rather than a continuous

spiral upgrade [1][5][7], overlooking the iterative feedback between resource integration, risk management, and value amplification. This review addresses this gap by synthesizing 7 key studies to construct the "resource aggregation-risk governance-ecosystem value addition" spiral upgrade model, explaining how AI enables continuous cross-domain collaboration and value escalation.

2 The Spiral Upgrade Model: Resource Aggregation, Risk Governance, Ecosystem Value Addition

2.1 Stage 1: Resource Aggregation – AI-Backed Cross-Domain Resource Integration

Resource aggregation is the starting point of the spiral, where AI breaks down domain boundaries to integrate fragmented resources (data, technology, capital) from digital commerce, finance, and cybersecurity into a shared resource pool. The core goal is to create initial value through resource complementarity, laying the foundation for subsequent risk governance and ecosystem value addition.

In digital commerce, resource aggregation focuses on **technical and data resource integration** for inclusive access. Yi [2]'s multi-tenant AI infrastructure aggregates advanced technical resources (PETs, marketing algorithms, compliance tools) into a modular platform, enabling SMEs to access resources that were previously only available to large enterprises—aggregating "scattered" SME technical needs into a "shared" resource pool. Yi [1][7]'s federated learning frameworks further aggregate cross-channel user data resources: retailers, platforms, and creators can access aggregated data insights without sharing raw data, turning "isolated" user data into "collaborative" marketing resources. This aggregation creates initial value: SMEs reduce technical costs [2], retailers improve marketing accuracy [1], and users receive personalized experiences [7].

In finance, resource aggregation centers on **data and capital resource integration** for efficiency improvement. Li and Liu [6]'s LSTM model aggregates financial time-series data resources (market trends, asset prices, historical transaction data) from multiple sources, integrating "dispersed" financial data into a "unified" prediction dataset—enabling more accurate portfolio optimization. Liu [3]'s ESG AI tools aggregate fragmented ESG data resources (energy consumption, carbon emissions, policy requirements) and capital resources (sustainable finance funds), connecting "scattered" SME ESG needs with "concentrated" financial resources—enabling SMEs to access sustainable finance support. This aggregation generates initial value: investors reduce investment risks [6], SMEs gain capital access [3], and financial institutions expand service scope [3].

In cybersecurity, resource aggregation emphasizes **risk and tool resource integration** for comprehensive protection. Zhou [4]'s hybrid SAST-DAST-SCA-IAST framework aggregates multi-dimensional security tool resources (static testing, dynamic testing, supply chain testing) into an integrated platform, integrating "single-function" security tools into a "comprehensive" risk assessment system. Zhou [5]'s MARL-based M-VP2 aggregates cross-stakeholder resource data: IT teams' vulnerability data, business units' operational

data, and financial departments' cost data—turning "isolated" stakeholder information into "collaborative" risk management resources. This aggregation creates initial value: organizations improve risk detection coverage [4], reduce resource waste [5], and align security with business objectives [5].

Notably, resource aggregation across domains is mutually reinforcing: digital commerce's aggregated user data [1] enhances finance's prediction accuracy [6]; finance's aggregated capital resources [3] supports digital commerce's SME growth [2]; cybersecurity's aggregated risk tools [4] protect the aggregated resources of both domains [1][6]. AI enables this aggregation through modular architectures [2][4], federated learning [1][7], and multi-agent data integration [5], ensuring resource complementarity without compromising security or privacy.

2.2 Stage 2: Risk Governance – AI-Powered Cross-Domain Risk Joint Management

Risk governance is the critical intermediate stage of the spiral, where AI identifies and mitigates new risks generated by resource aggregation—ensuring that the initial value created is not eroded by unmanaged risks. These risks are cross-domain: resource aggregation across digital commerce, finance, and cybersecurity creates new risk types (e.g., data privacy risks, risk-cost imbalance, ESG greenwashing) that no single domain can address alone.

In digital commerce, the core risks from resource aggregation are **privacy risks** (from data aggregation) [1][7] and **inclusive access risks** (from technical resource aggregation) [2]. AI-driven risk governance solutions include PETs and inclusive compliance tools: Yi [1][7] integrates federated learning, differential privacy, and zero-knowledge verification into data aggregation processes—ensuring that cross-channel data collaboration does not leak user privacy. Yi [2] further embeds compliance guidance modules into the multi-tenant infrastructure, helping SMEs (who lack compliance capabilities) meet privacy regulations—mitigating the risk of non-compliance penalties. This governance ensures that data and technical resource aggregation does not come at the cost of privacy violations or SME exclusion.

In finance, the key risks from resource aggregation are **prediction uncertainty risks** (from financial data aggregation) [6] and **ESG authenticity risks** (from ESG data and capital aggregation) [3]. AI-powered risk governance involves transparent prediction mechanisms and anti-greenwashing tools: Li and Liu [6]'s LSTM model includes risk disclosure modules that clearly present the limitations of AI predictions to investors—mitigating the risk of excessive reliance on AI and investment losses. Liu [3]'s ESG AI tools integrate data verification modules that cross-check SME ESG data with third-party sources—mitigating the risk of greenwashing and ensuring that sustainable finance capital flows to genuine ESG projects. This governance ensures that financial resource aggregation creates reliable rather than misleading value.

In cybersecurity, the main risks from resource aggregation are **risk assessment bias** (from multi-dimensional tool aggregation) [4] and **stakeholder conflict risks** (from cross-stakeholder data aggregation) [5]. AI-driven risk governance solutions include balanced risk-

scoring systems and multi-agent coordination: Zhou [4]'s hybrid framework integrates business and financial KPIs into risk assessment, avoiding the bias of technical-only risk scoring—mitigating the risk of over-prioritizing trivial vulnerabilities. Zhou [5]'s MARL-based framework uses AI agents to represent different stakeholders, enabling collaborative decision-making on vulnerability patch plans—mitigating conflicts between IT teams (prioritizing security), business units (prioritizing cost), and financial departments (prioritizing resource efficiency). This governance ensures that cybersecurity resource aggregation creates coordinated rather than conflicting value.

Risk governance not only mitigates existing risks but also generates feedback for resource aggregation optimization: for example, privacy governance feedback leads to improved federated learning algorithms [1], anti-greenwashing governance refines ESG data aggregation standards [3], and stakeholder coordination governance optimizes cross-stakeholder data integration [5]—paving the way for ecosystem value addition.

2.3 Stage 3: Ecosystem Value Addition – Iterative Amplification of Cross-Domain Value

Ecosystem value addition is the terminal stage of the spiral, where optimized resource aggregation (after risk governance) expands the scale and depth of the cross-domain ecosystem, creating new value that transcends single-domain and initial aggregation value. This stage completes the spiral and triggers the next round of upgrade: the new value creates new resource needs, leading to further resource aggregation, more refined risk governance, and higher-level value addition.

In digital commerce, ecosystem value addition manifests as **inclusive growth amplification** and **privacy-respecting experience enhancement**. After risk governance (privacy protection [1], SME compliance support [2]), the aggregated technical and data resources form an inclusive ecosystem: SMEs gain access to cross-channel marketing tools [1], ad targeting capabilities [7], and ESG optimization resources [3], driving their growth and expanding the digital commerce market scale. Users benefit from personalized experiences without privacy risks [7], increasing user stickiness and trust. This value addition attracts more SMEs and users to join the ecosystem, creating new resource needs (e.g., more specialized AI modules [2], broader cross-channel collaboration [1])—triggering further resource aggregation.

In finance, ecosystem value addition is reflected in **sustainable finance expansion** and **investment efficiency upgrading**. After risk governance (prediction transparency [6], anti-greenwashing [3]), the aggregated financial data and capital resources form a sustainable finance ecosystem: SMEs access low-cost ESG tools and capital [3], expanding the pool of sustainable finance participants; investors gain more accurate and reliable portfolio optimization tools [6], improving investment returns. This value addition attracts more financial institutions, investors, and SMEs to participate in sustainable finance, creating new resource needs (e.g., more granular ESG data [3], more adaptive prediction models [6])—driving the next round of resource aggregation.

In cybersecurity, ecosystem value addition takes the form of **proactive risk management upgrading** and **cross-domain security collaboration deepening**. After risk governance

(balanced risk assessment [4], stakeholder coordination [5]), the aggregated security tools and data resources form a collaborative security ecosystem: organizations achieve risk-cost balance [5], reducing unnecessary security spending and improving protection effectiveness; security vendors gain insights into cross-domain risk needs, developing more targeted products [4]. This value addition promotes cross-organizational security collaboration (e.g., shared threat intelligence [4]), creating new resource needs (e.g., more integrated security platforms [4], real-time risk data sharing [5])—initiating further resource aggregation.

The spiral upgrade logic is thus complete: resource aggregation creates initial value → risk governance protects and optimizes value → ecosystem value addition amplifies value and triggers new resource needs → the cycle repeats, driving continuous cross-domain collaboration and value escalation.

2.4 Spiral Upgrade Dynamics: Key Drivers and Feedback Mechanisms

The spiral upgrade is driven by two core factors: **AI modularity and privacy technologies** (enabling flexible resource aggregation and safe risk governance) and **SME participation** (expanding ecosystem scale and creating diverse resource needs).

AI modularity (e.g., multi-tenant modular infrastructure [2], hybrid security frameworks [4], modular LSTM models [6]) enables resources to be aggregated and disaggregated flexibly—organizations can select relevant modules based on their needs, reducing aggregation costs and improving efficiency. Privacy technologies (e.g., federated learning [1], zero-knowledge verification [7], differential privacy [1]) ensure that resource aggregation (especially data aggregation) does not compromise security, addressing the core barrier to cross-domain collaboration.

SME participation is critical because SMEs form the majority of ecosystem participants and create diverse resource needs: their demand for low-cost technical tools [2], accessible ESG resources [3], and simplified compliance support [1] drives the development of more inclusive and flexible AI solutions—expanding the ecosystem's value scope and triggering iterative upgrades.

The feedback mechanism between stages is the key to spiral continuity:

- Resource aggregation → risk governance feedback: Resource aggregation exposes new risks (e.g., data privacy [1], prediction uncertainty [6]), which drives the development of targeted risk governance tools—optimizing resource aggregation methods (e.g., adding privacy modules to data aggregation [7]).
- Risk governance → ecosystem value addition feedback: Effective risk governance builds trust among ecosystem participants, attracting more stakeholders to join and creating new value needs—driving the expansion of resource aggregation scope (e.g., including more ESG data sources [3]).
- Ecosystem value addition → resource aggregation feedback: Expanded ecosystem value creates new resource needs (e.g., more specialized AI tools [2], broader data collaboration [1]), triggering the next round of resource aggregation with higher quality and scale.

3 Spiral Upgrade Outcomes Across Domains

3.1 Digital Commerce: From Inclusive Access to Collaborative Growth Ecosystem

The spiral upgrade enables digital commerce to evolve from simple SME technical access (resource aggregation) to a collaborative growth ecosystem (ecosystem value addition). Initial resource aggregation (multi-tenant infrastructure [2], federated data tools [1]) provides SMEs with basic technical access; risk governance (privacy protection [7], compliance support [2]) ensures safe and compliant participation; ecosystem value addition amplifies this into collaborative growth: SMEs collaborate with retailers, platforms, and creators to create personalized marketing value [1][7], and the expanded ecosystem attracts more resources (e.g., sustainable finance capital [3])—driving continuous growth for all participants.

3.2 Finance: From Data-Driven Efficiency to Sustainable Inclusion Ecosystem

Finance evolves from data-driven investment efficiency (resource aggregation) to a sustainable inclusion ecosystem (ecosystem value addition) through the spiral. Initial resource aggregation (LSTM data integration [6], ESG data-capital integration [3]) improves investment and ESG efficiency; risk governance (prediction transparency [6], anti-greenwashing [3]) ensures reliable and authentic value; ecosystem value addition expands this into sustainable inclusion: SMEs gain equal access to sustainable finance [3], investors access diverse ESG investment opportunities [6], and the ecosystem drives the transformation of the entire financial sector toward sustainability—creating systemic value beyond individual transactions.

3.3 Cybersecurity: From Tool Integration to Proactive Collaboration Ecosystem

Cybersecurity evolves from security tool integration (resource aggregation) to a proactive collaboration ecosystem (ecosystem value addition). Initial resource aggregation (hybrid frameworks [4], cross-stakeholder data integration [5]) improves risk detection and management efficiency; risk governance (balanced risk assessment [4], stakeholder coordination [5]) ensures security aligns with business and financial objectives; ecosystem value addition amplifies this into proactive collaboration: organizations share threat intelligence [4], security vendors develop targeted solutions based on cross-domain needs [5], and the ecosystem enables proactive risk prevention rather than reactive patch management—protecting cross-domain value creation at scale.

4 Practical Implications

4.1 For Researchers

Design AI with spiral upgrade adaptability: Prioritize modular and privacy-preserving technologies that support flexible resource aggregation [2][7], embed risk governance modules into resource integration tools [1][5], and focus on SME needs to drive ecosystem expansion [2][3]; develop feedback collection and optimization mechanisms to enable iterative upgrades [6][4]; explore cross-domain data standards to reduce aggregation friction [1][3].

4.2 For Practitioners

Adopt spiral thinking for cross-domain collaboration: Digital commerce platforms should continuously expand resource aggregation scope (e.g., integrating ESG resources [3]) based on risk governance outcomes (e.g., privacy compliance [7]) and ecosystem needs (e.g., SME growth [2]); financial institutions should use ecosystem value addition (e.g., sustainable finance scale [3]) to guide further resource aggregation (e.g., more granular ESG data [3]) and risk governance (e.g., stricter anti-greenwashing [3]); cybersecurity teams should leverage feedback from value addition (e.g., proactive risk management [4]) to optimize resource aggregation (e.g., real-time risk data [5]) and risk governance (e.g., dynamic stakeholder coordination [5]).

4.3 For Policymakers

Support the spiral upgrade with targeted policies: Fund modular and privacy-enhancing AI technologies to lower resource aggregation barriers [1][2]; establish cross-domain risk governance standards (e.g., privacy regulations [7], ESG verification norms [3]) to ensure safe value creation; incentivize SME participation (e.g., subsidies for AI tool access [2], tax breaks for ESG improvements [3]) to expand ecosystem scale; create flexible regulatory frameworks that adapt to spiral upgrades (e.g., updating rules based on ecosystem value addition outcomes [6]).

5 Conclusion

This review synthesizes 7 key studies to propose the "resource aggregation-risk governance-ecosystem value addition" spiral upgrade model for AI-driven cross-domain collaboration among digital commerce, finance, and cybersecurity. The model reveals that sustainable cross-domain integration is a continuous iterative process: AI enables the aggregation of fragmented resources to create initial value, supports joint risk governance to protect and optimize value, and drives ecosystem value addition to amplify value and trigger further upgrades. The spiral is powered by AI modularity, privacy technologies, and SME participation, with feedback mechanisms ensuring continuity. By understanding this spiral upgrade logic, researchers, practitioners, and policymakers can foster a dynamic cross-domain ecosystem that continuously creates inclusive, secure, and sustainable value—unlocking AI’s full potential to drive mutual growth across business, finance, and cybersecurity.

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.