Triadic Dynamic: Capability Alignment, Constraint Resolution, and Value Co-Creation in AI-Powered Business-Finance-Cybersecurity Synergy (2022-2026)

Abstract

Artificial intelligence (AI) has redefined cross-domain collaboration among digital commerce, finance, and cybersecurity through a triadic dynamic: capability alignment (matching domain-specific core capabilities via AI-enabled integration), constraint resolution (addressing interdomain frictions and bottlenecks with targeted AI tools), and value co-creation (generating emergent cross-domain value that transcends single-sector outcomes). This review synthesizes 7 key studies (2022-2026) to unpack the interdependent logic of the triad: capability alignment lays the groundwork by integrating complementary strengths (e.g., digital commerce's user-centric tools, finance's predictive models, cybersecurity's risk safeguards); constraint resolution removes barriers by mitigating critical frictions (e.g., SME resource scarcity, data privacy conflicts, risk-cost tradeoffs); value co-creation delivers transformative outcomes by amplifying collective potential (e.g., inclusive sustainable growth, proactive risk-resilient ecosystems). Findings reveal that: the triadic dynamic operates as a mutually reinforcing system—alignment identifies constraints, constraint resolution optimizes alignment, and both enable sustained co-creation; modular AI architectures and privacy-enhancing technologies (PETs) are the primary enablers of capability alignment; SMEs serve as the linchpin for inclusive constraint resolution and value diffusion. This framework offers a capability-centric perspective on cross-domain AI synergy, guiding researchers, practitioners, and policymakers to leverage complementary strengths for systemic value creation.

1 Introduction

Cross-domain collaboration among digital commerce, finance, and cybersecurity is no longer a matter of functional integration but a dynamic synergy driven by AI-enabled capability alignment, constraint resolution, and value co-creation [1][4][7]. For instance, Yi's [2] multi-tenant infrastructure (digital commerce) aligns SME technical capabilities with enterprise-grade AI tools (capability alignment) [2], resolves resource constraints for small businesses via modular access (constraint resolution) [2], and co-creates an inclusive ecosystem where SMEs, platforms, and users mutually benefit (value co-creation) [7]; Zhou's [5] MARL-based vulnerability planning (cybersecurity) aligns IT teams' security capabilities with business units' cost-management goals (capability alignment) [5], resolves risk-cost tradeoff constraints via collaborative decision-making (constraint resolution) [5], and co-creates a risk-resilient environment that protects financial assets and commercial operations (value co-creation) [4]; Li and Liu's [6] LSTM model (finance) aligns financial forecasting capabilities with digital commerce's demand-prediction needs (capability alignment) [6], resolves data

silo constraints via cross-domain data integration (constraint resolution) [6], and co-creates optimized investment strategies that fuel commercial growth (value co-creation) [6]. However, existing research often focuses on isolated capability application [2][3][6] or one-dimensional constraint mitigation [1][5], overlooking the triadic interdependence between alignment, resolution, and co-creation [7][4]. This review addresses this gap by synthesizing 7 key studies to construct the “capability alignment – constraint resolution – value co-creation” triadic dynamic framework, explaining how AI enables systemic synergy across business, finance, and cybersecurity.

2 The Triadic Dynamic Framework: Alignment, Resolution, Co-Creation

2.1 Dimension 1: Capability Alignment – AI-Enabled Integration of Complementary Domain Strengths

Capability alignment is the foundational dimension of the triad, where AI integrates domain-specific core capabilities—digital commerce’s user engagement and data aggregation, finance’s predictive modeling and capital allocation, cybersecurity’s risk detection and mitigation—into a cohesive system. The core objective is to leverage complementarity, ensuring that each domain’s strengths amplify the others rather than operating in isolation.

In digital commerce, capability alignment centers on **user-centric and inclusive technical capabilities**. Yi [2]’s multi-tenant AI infrastructure aligns the technical capabilities of large platforms (advanced PETs, marketing algorithms, compliance tools) with the operational needs of SMEs (low-cost access, simplified integration) [2], creating a modular system where small businesses can leverage enterprise-grade capabilities without in-house expertise. Yi [1][7]’s federated learning frameworks further align retailers’ marketing capabilities, creators’ monetization goals, and users’ privacy preferences [1][7], integrating data-driven targeting with privacy protection to form a capability bundle that serves multiple stakeholders. This alignment ensures that digital commerce’s core strength—user engagement—does not conflict with privacy or inclusivity.

In finance, capability alignment focuses on **predictive and sustainable resource allocation capabilities**. Li and Liu [6]’s LSTM model aligns financial time-series forecasting capabilities with investment decision-making needs [6], integrating market trend analysis with portfolio optimization to create a capability that benefits investors and financial institutions alike. Liu [3]’s ESG AI tools align financial institutions’ capital allocation capabilities with SMEs’ sustainability improvement needs [3], bridging the gap between sustainable finance resources and small businesses’ ESG enhancement capabilities. This alignment ensures that finance’s core strength—capital efficiency—supports rather than excludes marginalized participants.

In cybersecurity, capability alignment emphasizes **risk management and stakeholder coordination capabilities**. Zhou [4]’s hybrid SAST-DAST-SCA-IAST framework aligns technical security testing capabilities (static, dynamic, supply chain, and interactive testing) with business and financial KPIs [4], integrating risk detection with operational continuity

goals. Zhou [5]'s MARL-based M-VP2 aligns IT teams' vulnerability mitigation capabilities, business units' cost-control capabilities, and security vendors' product delivery capabilities [5], creating a multi-agent system where each stakeholder's strengths contribute to collective risk management. This alignment ensures that cybersecurity's core strength—threat protection—supports business and financial objectives rather than hindering them.

Cross-domain capability alignment is mutually reinforcing: digital commerce's user data aggregation capabilities enhance finance's predictive accuracy [1][6]; finance's capital allocation capabilities enable digital commerce's SME inclusion [3][2]; cybersecurity's risk mitigation capabilities protect the integrity of aligned business and financial systems [4][5]. AI enables this alignment through modular architectures [2][4], federated learning [1][7], and multi-agent modeling [5], ensuring that domain-specific capabilities are compatible and complementary.

2.2 Dimension 2: Constraint Resolution – AI-Powered Mitigation of Interdomain Frictions

Constraint resolution is the intermediate dimension of the triad, addressing the critical frictions that hinder effective capability alignment—resource scarcity, data privacy conflicts, risk-cost tradeoffs, and regulatory fragmentation. AI plays a targeted role in resolving these constraints, ensuring that aligned capabilities can operate seamlessly without compromise.

The primary constraints resolved across domains include:

- **Resource Scarcity Constraints**: SMEs lack the technical and financial resources to leverage advanced AI tools [2][3]. Yi [2]'s multi-tenant infrastructure resolves this by providing modular, low-cost access to PETs, marketing algorithms, and compliance tools [2], enabling small businesses to align with platform capabilities without prohibitive investments. Liu [3]'s ESG AI tools further resolve resource constraints for SMEs by simplifying ESG data collection, analysis, and reporting [3], allowing them to access sustainable finance resources previously reserved for large enterprises.
- **Data Privacy Conflicts**: Cross-domain data sharing (critical for capability alignment) conflicts with privacy regulations [1][7]. Yi [1][7] resolves this constraint via federated learning, differential privacy, and zero-knowledge verification [1][7], enabling digital commerce's data aggregation capabilities to align with finance's forecasting needs without exposing sensitive user or financial information. This resolution ensures that data-driven capabilities across domains can collaborate securely.
- **Risk-Cost Tradeoff Constraints**: Cybersecurity risk mitigation often requires excessive financial or operational costs, creating conflicts with business and financial goals [5][4]. Zhou [5]'s MARL-based framework resolves this by aligning IT teams' security capabilities with business units' cost constraints via collaborative patch planning [5], prioritizing vulnerabilities based on risk severity and financial impact. Zhou [4]'s hybrid framework further resolves this by integrating business KPIs into risk assessment [4], ensuring that security capabilities do not undermine cost-efficiency.
- **Regulatory Fragmentation Constraints**: Domain-specific regulations (e.g., GDPR for commerce, financial compliance norms) create barriers to cross-domain alignment [1][3].

Yi [1]'s compliance-by-design approach embeds regulatory requirements into federated learning frameworks [1], resolving fragmentation by ensuring that aligned capabilities across commerce and finance adhere to multiple regulatory regimes. Liu [3]'s ESG tools align with both sustainable finance standards and SME resource constraints [3], resolving regulatory barriers for small businesses' participation in sustainable finance.

Constraint resolution is not a one-time fix but an adaptive process: as new capabilities align, new constraints emerge (e.g., modular tool integration challenges [2], evolving privacy regulations [7]), requiring AI-driven solutions to continuously adapt—ensuring that alignment remains effective.

2.3 Dimension 3: Value Co-Creation – Emergent Cross-Domain Value Beyond Single-Sector Outcomes

Value co-creation is the terminal dimension of the triad, where aligned capabilities and resolved constraints generate emergent value that no single domain could achieve independently. This value is characterized by mutual benefit, inclusivity, and sustainability—amplifying the collective potential of the cross-domain ecosystem.

In digital commerce, value co-creation manifests as **inclusive, privacy-respecting growth**. Aligned capabilities (modular AI tools [2], federated data collaboration [1]) and resolved constraints (resource scarcity [2], privacy risks [7]) enable SMEs to compete with large enterprises, driving market expansion and innovation [2]. Users benefit from personalized experiences without privacy compromises [7], increasing trust and engagement. Creators gain monetization opportunities through privacy-compliant ad targeting [7], while platforms expand their user base and revenue streams [1]. This co-created value is inclusive: all stakeholders—regardless of size or resources—contribute to and benefit from the ecosystem.

In finance, value co-creation takes the form of **sustainable, efficient capital allocation**. Aligned capabilities (LSTM forecasting [6], ESG data integration [3]) and resolved constraints (resource scarcity [3], data silos [6]) enable financial institutions to direct capital toward high-potential, sustainable projects [3]. SMEs access low-cost ESG tools and funding [3], improving their sustainability ratings and market competitiveness. Investors achieve higher returns through optimized portfolios [6] and reduced risk via cybersecurity safeguards [4]. This co-created value is sustainable: capital flows support long-term environmental and social goals while delivering financial returns.

In cybersecurity, value co-creation results in **proactive, business-aligned risk resilience**. Aligned capabilities (hybrid security testing [4], multi-stakeholder coordination [5]) and resolved constraints (risk-cost tradeoffs [5], technical-business misalignment [4]) enable organizations to mitigate threats before they materialize [4]. IT teams gain actionable, cost-effective patch plans [5], business units avoid operational disruptions [5], and security vendors develop targeted products based on cross-domain needs [4]. This co-created value is resilient: the ecosystem adapts to emerging threats while supporting business and financial continuity.

Notably, value co-creation feeds back into the triad: emergent value creates new opportunities for capability alignment (e.g., expanded ESG data sharing [3], real-time threat

intelligence collaboration [4]) and identifies new constraints to resolve (e.g., scaling modular tools for global SMEs [2], harmonizing international privacy regulations [1]), driving continuous synergy.

2.4 Triadic Interdependence: How Alignment, Resolution, and Co-Creation Reinforce Each Other

The triadic dynamic operates as a self-reinforcing system with three key interdependencies:

1. **Capability Alignment → Constraint Identification**: Aligning domain capabilities exposes hidden constraints—e.g., integrating digital commerce's data aggregation with finance's forecasting reveals privacy conflicts [1], or aligning cybersecurity's risk mitigation with business operations highlights cost tradeoffs [5]. These identified constraints drive targeted resolution efforts.
2. **Constraint Resolution → Capability Optimization**: Resolving constraints refines aligned capabilities—e.g., mitigating privacy risks via PETs improves data collaboration capabilities [7], or addressing SME resource scarcity enhances modular tool accessibility [2]. Optimized capabilities enable deeper alignment across domains.
3. **Alignment + Resolution → Value Co-Creation**: Only when capabilities are aligned and constraints resolved can emergent value be co-created—e.g., aligned technical and financial capabilities, paired with resolved resource constraints, enable inclusive sustainable growth [3][2]. Co-created value then fuels further alignment and resolution.

Breakdown in any dimension disrupts the triad: misaligned capabilities lead to ineffective constraint resolution; unresolved constraints prevent meaningful value co-creation; and weak co-creation fails to sustain long-term alignment. AI acts as the glue that binds the triad, enabling flexible alignment, targeted resolution, and scalable co-creation.

3 Triadic Dynamic Outcomes Across Domains

3.1 Digital Commerce: Inclusive Ecosystems with Privacy and Growth Synergy

The triadic dynamic transforms digital commerce into an ecosystem where inclusivity, privacy, and growth coexist. Capability alignment (modular AI tools [2], federated data collaboration [1]) integrates large platforms and SMEs; constraint resolution (resource scarcity [2], privacy risks [7]) ensures equitable participation; value co-creation amplifies growth for all stakeholders—SMEs expand their reach, users gain personalized experiences, and platforms build trusted communities. The outcome is a commercial ecosystem that is both innovative and inclusive, avoiding the tradeoff between scale and equity.

3.2 Finance: Sustainable Capital Markets with Efficiency and Inclusion Synergy

Finance benefits from the triadic dynamic by forming a sustainable capital market that balances efficiency and inclusion. Capability alignment (LSTM forecasting [6], ESG data integration [3]) connects investors, financial institutions, and SMEs; constraint resolution (resource scarcity [3], data silos [6]) removes barriers for marginalized participants; value co-creation drives sustainable growth—capital flows to impactful projects, SMEs access critical funding, and investors achieve risk-adjusted returns. The outcome is a financial system that delivers both economic and societal value, transcending the tradeoff between profit and purpose.

3.3 Cybersecurity: Proactive Risk Ecosystems with Protection and Adaptability Synergy

Cybersecurity evolves into a proactive risk ecosystem that supports rather than constrains business and finance. Capability alignment (hybrid testing [4], multi-stakeholder coordination [5]) integrates technical security with business and financial goals; constraint resolution (risk-cost tradeoffs [5], misalignment [4]) ensures practicality; value co-creation delivers resilience—organizations mitigate threats efficiently, resources are allocated optimally, and the ecosystem adapts to emerging risks. The outcome is a cybersecurity system that is both robust and agile, resolving the tradeoff between protection and operational flexibility.

4 Practical Implications

4.1 For Researchers

Design AI with triadic compatibility: Develop modular, adaptable AI tools that facilitate capability alignment across domains [2][4]; embed constraint-resolution features (e.g., PETs [1], cost-balancing algorithms [5]) into cross-domain solutions; focus on emergent value metrics (e.g., SME inclusion rates [2], ESG impact [3]) rather than single-domain outcomes. Prioritize research on cross-domain capability mapping to identify hidden constraints early.

4.2 For Practitioners

Adopt triadic thinking in cross-domain collaboration: Digital commerce platforms should align SME capabilities with enterprise tools [2] and resolve privacy constraints [7] to co-create inclusive ecosystems; financial institutions should align forecasting capabilities with ESG goals [3][6] and resolve resource constraints for SMEs [3] to drive sustainable capital allocation; cybersecurity teams should align risk management with business/financial KPIs [4][5] and resolve cost tradeoffs [5] to deliver practical protection. Measure success by triadic outcomes—alignment depth, constraint resolution effectiveness, and co-created value.

4.3 For Policymakers

Support the triadic dynamic with systemic policies: Fund modular AI infrastructure to lower alignment barriers for SMEs [2]; establish cross-domain regulatory frameworks that resolve fragmentation constraints [1][3]; incentivize value co-creation via tax breaks for inclusive and

sustainable initiatives [3][7]; create feedback mechanisms to adapt policies as the triad evolves (e.g., updating privacy regulations to support secure data alignment [1]).

5 Conclusion

This review synthesizes 7 key studies to propose the “capability alignment – constraint resolution – value co-creation” triadic dynamic framework for AI-powered synergy across digital commerce, finance, and cybersecurity. The framework reveals that systemic cross-domain collaboration is not about linear integration or iterative upgrades but about leveraging AI to align complementary capabilities, resolve critical constraints, and co-create emergent value that transcends individual sectors. The triad operates as a self-reinforcing system, with each dimension reinforcing the others to drive inclusive, sustainable, and resilient outcomes. Modular AI architectures and PETs enable alignment and resolution, while SMEs act as the linchpin for inclusive value diffusion. By understanding this triadic dynamic, researchers, practitioners, and policymakers can unlock AI’s full potential to build cross-domain ecosystems that deliver mutual benefit—proving that business growth, financial efficiency, and cybersecurity resilience are not mutually exclusive but mutually reinforcing.

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.