

RESEARCH ARTICLE

Cross-Domain AI Evolution: A Framework for Capability Transformation and Value Enhancement

Minh Quang Nguyen

Department of Interdisciplinary Research Institute of Digital Innovation and Development, Vietnam

Linh Anh Tran

Department of Applied Sciences and Emerging Technologies Center for Multidisciplinary Studies, Vietnam

VOLUME: Vol.06 Issue10 2026

PAGE: 01-08

Copyright © 2026 European International Journal of Multidisciplinary Research and Management Studies, this is an open-access article distributed under the terms of the Creative Commons Attribution-Noncommercial-Share Alike 4.0 International License. Licensed under Creative Commons License a Creative Commons Attribution 4.0 International License.

Abstract

Artificial intelligence (AI) is increasingly evolving from domain-specific automation toward reusable capabilities that can be transferred, recombined, governed, and commercialized across heterogeneous application environments. However, cross-domain AI adoption is not equivalent to simply migrating an existing model from one sector to another. Effective migration requires adaptation of technical capabilities, data structures, governance mechanisms, incentives, security controls, and value-generation processes. This research develops a conceptual framework for understanding cross-domain AI evolution as a progression from capability transfer to capability transformation and ultimately to value enhancement. The framework synthesizes evidence from studies addressing AI-enabled medical image segmentation, unsupervised learning, financial forecasting, ESG-related financial analysis, privacy-preserving digital commerce, AI commercialization, and AI-driven cybersecurity. The methodology employs comparative thematic synthesis and architectural abstraction to identify reusable capability layers and transformation mechanisms across domains. The analysis indicates that cross-domain AI value depends on four interdependent dimensions: capability portability, contextual adaptation, trustworthy governance, and measurable value realization. The resulting framework positions AI evolution as a continuous process in which technical capabilities are transferred, contextualized, integrated with domain constraints, and converted into economic, operational, scientific, or social value. The study contributes a structured theoretical model for researchers and practitioners seeking to design scalable AI systems capable of operating beyond their original application boundaries.

KEY WORDS

Cross-Domain Artificial Intelligence, AI Capability Transformation, Value Enhancement, AI Framework, Capability Transfer, Intelligent Systems, AI Governance, Adaptive AI, AI Commercialization, Domain Adaptation.

1. INTRODUCTION

Artificial intelligence has moved from isolated analytical applications toward increasingly integrated systems capable of supporting decision-making, prediction, optimization,

automation, and commercialization across multiple domains. This evolution creates an important research problem: how can an AI capability developed for one domain be transformed

into a reliable and valuable capability in another? The question is more complex than model reuse because AI systems are embedded within domain-specific data structures, regulatory constraints, performance requirements, incentive mechanisms, and organizational processes.

Recent research illustrates the breadth of AI capabilities that can potentially migrate across domains. Medical image segmentation, for example, demonstrates how specialized architectures can combine path aggregation and attention mechanisms to improve the extraction of relevant information from complex visual data (Chang,C.,Fu,M.,Chen,X.,etal., 2025). Financial forecasting research demonstrates another form of specialized AI capability, where sequential learning is applied to portfolio optimization (Li,H.,&Liu,T.,2023). Similarly, unsupervised learning has been applied to computational modeling of quantum geometry, illustrating the ability of machine-learning techniques to address highly specialized scientific problems (Wu,A.K.,Primeau,L.,Zhang,J.,etal.,2025).

These examples indicate that AI capabilities are not necessarily confined to their original domains. Learning mechanisms such as representation extraction, prediction, optimization, attention, privacy preservation, and automated prioritization can potentially be abstracted and adapted to different environments. Nevertheless, direct transplantation can produce poor results when the target domain has substantially different data distributions, objectives, risk conditions, or stakeholder expectations.

The problem therefore shifts from AI capability migration to AI capability transformation. Migration refers to moving a capability from an established environment to a new environment. Transformation involves restructuring that capability so that it remains technically effective while satisfying the contextual requirements of the destination domain. Value enhancement represents the subsequent stage in which the transformed capability produces measurable benefits such as improved decision quality, operational efficiency, security, commercial performance, scientific discovery, or resource utilization.

The provided literature demonstrates this progression across several application areas. Privacy-preserving federated learning introduces mechanisms for cross-channel measurement while limiting exposure of sensitive information (Yi,X.,2026). AI commercialization research further illustrates

how technical capabilities can be integrated into multi-tenant architectures, content governance, incentives, and standardized APIs (Yi,X.,2026). Cybersecurity research similarly combines multiple security-analysis mechanisms with risk-based prioritization and reinforcement learning, demonstrating how AI capabilities can be reorganized around operational requirements (Zhou,D.,2025; Zhou,D.,2026).

This study therefore aims to develop a conceptual framework explaining the evolutionary path from capability migration → contextual transformation → system integration → value enhancement. The research addresses three objectives: first, to identify transferable AI capability dimensions; second, to determine the mechanisms through which capabilities must be transformed across domains; and third, to establish a value-oriented framework for evaluating cross-domain AI evolution.

The significance of this approach lies in its attempt to move beyond model-centric discussions of AI reuse. A cross-domain AI system should be evaluated not only according to predictive or computational performance but also according to adaptability, governance, interoperability, security, and value realization.

2. LITERATURE REVIEW

The provided literature represents multiple technological and application contexts, allowing cross-domain AI evolution to be examined through comparative synthesis rather than through a single-sector perspective.

Chang,C.,Fu,M.,Chen,X.,etal. (2025) investigate PDU-Net for lung nodule segmentation using path aggregation and dual attention. Their work demonstrates a domain-specific capability architecture in which multiple feature-extraction mechanisms are integrated to improve the identification of medically relevant patterns. The important cross-domain implication is not the specific medical application itself, but the architectural principle of combining complementary representations. Such a principle may potentially be abstracted and redesigned for other high-dimensional recognition or classification problems.

Li,H.,&Liu,T. (2023) apply an LSTM forecasting model to portfolio optimization. Their research demonstrates a different capability: temporal prediction linked directly to a decision-optimization process. This distinction is important because value is not produced merely by prediction. The forecast becomes valuable when incorporated into a downstream

decision mechanism. Thus, the study supports the proposition that AI capability transformation requires integration between analytical intelligence and domain-level action.

Liu,T. (2022) examines the impact of financial constraints on firms' ESG ratings within the Chinese stock market. Although this research does not represent the same technical architecture as the AI-focused studies, it provides an important contextual foundation for understanding how financial and institutional conditions influence evaluation outcomes. For cross-domain AI, this suggests that technical outputs cannot be interpreted independently from the constraints and measurement systems of the target environment.

Wu,A.K.,Primeau,L.,Zhang,J.,etal. (2025) demonstrate the application of unsupervised learning to modeling quantum geometry associated with fractional Chern insulators. The study is particularly relevant to cross-domain capability evolution because unsupervised learning operates without relying exclusively on conventional domain-labeled supervision. This creates conceptual potential for AI systems deployed in environments where labeled data are limited or expensive. The transferability of representation-learning principles, however, remains dependent on the compatibility between learned structures and the target domain.

The commercial literature extends this technical perspective. Yi,X. (2026) proposes a federated and differentially private framework for privacy-preserving cross-channel measurement in AI-powered digital commerce. This illustrates that AI transformation can involve not only model adaptation but also the incorporation of privacy and distributed-learning constraints. Similarly, privacy-enhanced advertising research integrates federated learning with zero-knowledge verification to support creator monetization (Yi,X.,2026). These studies indicate that trust mechanisms can become integral components of AI capability architecture rather than peripheral compliance functions.

Yi,X. (2026) further proposes a unified multi-tenant architecture integrating incentive systems, content governance, and standardized recommendation APIs for AI commercialization. This contribution is particularly important for the value-enhancement stage because it connects technical AI capabilities with organizational and commercial infrastructure.

The cybersecurity studies provide another transformation pathway. Zhou,D. (2025) presents a cost-aware vulnerability patch-planning approach based on multi-agent reinforcement learning. Zhou,D. (2026) extends cybersecurity automation through a hybrid SAST–DAST–SCA–IAST framework for risk-based vulnerability prioritization. Together, these studies illustrate how AI can progress from isolated prediction toward coordinated decision-making and risk prioritization.

Collectively, the literature reveals a research gap. Existing studies largely optimize capabilities within specific application contexts, while limited attention is given to a unified theoretical mechanism explaining how AI capabilities evolve when transferred between domains. The present research addresses this gap by conceptualizing cross-domain AI as a staged transformation process rather than simple technology reuse.

3. METHODOLOGY

3.1 Research Design

This research adopts a conceptual comparative synthesis methodology. Because the supplied literature spans medical imaging, finance, quantum science, digital commerce, AI commercialization, and cybersecurity, conventional domain-specific empirical testing would not adequately capture the common mechanisms across the studies. Instead, the methodology identifies transferable technological principles and maps them into a common analytical architecture.

The analysis consists of four stages: capability identification, abstraction, contextual transformation, and value mapping. Each reference is treated as evidence of one or more AI capabilities, such as feature extraction, temporal prediction, unsupervised representation learning, distributed learning, privacy preservation, reinforcement learning, risk prioritization, governance, or API-based commercialization.

The methodology does not claim a new empirical dataset or experimental benchmark. Rather, it develops a theoretically grounded framework from comparative analysis of the supplied studies.

3.2 Cross-Domain Capability Model

The proposed framework represents AI evolution through four layers.

Layer 1: Capability Acquisition

The first layer represents the original AI capability developed for a particular task. Examples include attention-based feature extraction in medical imaging, LSTM-based forecasting in financial applications, unsupervised learning in quantum modeling, and reinforcement learning in vulnerability patch planning.

At this stage, the capability is optimized for a defined problem and associated data environment. Its performance is therefore primarily domain-specific.

Layer 2: Capability Abstraction

The second layer identifies the underlying computational principle rather than preserving the original application-specific implementation.

For example, the underlying capability of the PDU-Net study can be abstracted as multi-level representation enhancement through feature aggregation and attention. The underlying capability of LSTM-based portfolio forecasting can be interpreted as temporal dependency modeling for predictive decision support. The unsupervised-learning study provides an example of structure discovery without complete dependence on labeled training data (Wu,A.K.,Primeau,L.,Zhang,J.,etal.,2025).

This abstraction is essential because direct transfer of application-specific architectures may fail when target-domain assumptions differ.

Layer 3: Contextual Transformation

Capability abstraction must be followed by contextual transformation. The target environment determines the acceptable data, latency, privacy, security, explainability, interoperability, and governance requirements.

For example, a capability designed for centralized learning may require federated architecture when applied to environments in which data cannot be pooled. The privacy-preserving digital-commerce research demonstrates this transformation by integrating federated learning and differential privacy into cross-channel measurement (Yi,X.,2026).

Similarly, an analytical capability intended for prediction may need to be transformed into a prioritization or optimization mechanism. The cybersecurity studies demonstrate this transition by integrating AI into vulnerability prioritization and patch-planning processes (Zhou,D.,2025; Zhou,D.,2026).

Layer 4: Value Enhancement

The final layer transforms technical capability into measurable value. Value may be scientific, operational, financial, commercial, or security-oriented.

The proposed value function can be conceptually represented as:

$$V = f(P, A, G, I, R)$$

where V represents realized value, P represents performance, A represents adaptability, G represents governance and trust, I represents interoperability, and R represents risk management.

The model emphasizes that technical accuracy alone is insufficient. A highly accurate model that cannot integrate with operational infrastructure or satisfy privacy constraints may generate limited practical value.

3.3 Transformation Mechanisms

Three mechanisms are central to the proposed framework.

First, architectural modularity enables individual capabilities to be separated from application-specific components. Standardized APIs and multi-tenant architecture illustrate how capabilities can be exposed as reusable services (Yi,X.,2026).

Second, constraint-aware adaptation allows transferred capabilities to incorporate target-domain limitations. Privacy, cost, security, and regulatory constraints should therefore be considered during transformation rather than after deployment.

Third, decision integration connects AI outputs to downstream actions. Portfolio optimization demonstrates the importance of coupling forecasting with decision processes (Li,H.,&Liu,T.,2023), while vulnerability patch planning demonstrates the same principle in cybersecurity (Zhou,D.,2025).

3.4 Illustrative Cross-Domain Transformation

Consider a hypothetical migration of an AI representation-learning capability from scientific research into industrial anomaly detection. The original capability may identify latent structures in unlabeled data. Following abstraction, the representation mechanism can be separated from the scientific assumptions of the original application. The target system can then retrain or adapt the representation using

industrial sensor data.

The final stage would integrate anomaly scores into maintenance prioritization. In this scenario, capability migration occurs when the learning mechanism is reused; transformation occurs when its representation strategy is adapted to industrial data; and value enhancement occurs when the resulting predictions reduce operational risks or maintenance inefficiencies.

The approach is consistent with the broader evidence that AI capabilities can operate at different abstraction levels. The quantum-geometry study demonstrates the potential of unsupervised learning for discovering structure in specialized scientific data (Wu,A.K.,Primeau,L.,Zhang,J.,etal.,2025), while the commercial and cybersecurity studies demonstrate how AI capabilities become valuable when integrated with broader system architectures.

3.5 Evaluation Dimensions

The framework proposes five evaluation dimensions: technical effectiveness, contextual adaptability, governance integrity, integration capability, and value realization.

Technical effectiveness measures whether the transferred capability performs its computational function. Contextual adaptability measures whether it remains effective under new domain conditions. Governance integrity considers privacy, security, transparency, and risk. Integration capability assesses interoperability with existing systems. Value realization measures whether technical improvements translate into meaningful outcomes.

This multidimensional evaluation prevents cross-domain AI from being judged exclusively through model-level metrics.

4. RESULTS

The comparative synthesis produces four principal findings concerning the evolution of AI capabilities across domains.

First, AI capabilities are more transferable at the principle level than at the implementation level. The literature shows that domain-specific architectures frequently contain reusable computational principles. Attention-based feature aggregation, temporal dependency modeling, unsupervised structure discovery, federated learning, and reinforcement learning can be understood independently from their original application contexts. However, the specific data assumptions and optimization objectives associated with each

implementation may not transfer directly. Consequently, cross-domain AI migration should occur through abstraction rather than direct replication.

Second, contextual transformation is the primary determinant of successful capability reuse. The comparison between centralized analytical systems and privacy-preserving commercial systems illustrates that the same general objective can require fundamentally different architectures under different constraints. Federated learning and differential privacy demonstrate how privacy requirements reshape system architecture rather than merely adding an external security layer (Yi,X.,2026). This finding suggests that transformation should begin by identifying target-domain constraints before selecting the final technical implementation.

Third, value enhancement requires integration of AI outputs into decision processes. Forecasting alone does not constitute portfolio value; the forecast must influence optimization decisions (Li,H.,&Liu,T.,2023). Similarly, cybersecurity intelligence becomes operationally meaningful when it informs vulnerability prioritization or patch planning (Zhou,D.,2025; Zhou,D.,2026). This indicates a progression from predictive capability toward decision intelligence. The value layer is therefore dependent on the existence of a mechanism connecting model outputs with organizational actions.

Fourth, trust and governance increasingly function as architectural capabilities. Privacy-preserving learning, zero-knowledge verification, content governance, and multi-tenant commercialization indicate that trust mechanisms are becoming integrated with AI infrastructure rather than being treated solely as external controls (Yi,X.,2026). This finding is particularly important for cross-domain migration because a capability that is technically transferable may become unusable if it violates the target domain's privacy, security, or governance requirements.

The literature also reveals that cross-domain AI evolution is nonlinear. A capability may move backward from deployment to redesign when contextual assumptions fail. Therefore, the proposed framework should be interpreted as an iterative cycle rather than a one-directional pipeline. Capability abstraction may reveal additional requirements, while deployment feedback may require architectural transformation.

The resulting conceptual sequence can be summarized as:

Domain-Specific Capability → Capability Abstraction → Contextual Adaptation → System Integration → Governed Deployment → Value Enhancement → Feedback and Reconfiguration

This sequence provides a stronger explanation of AI evolution than a simple technology-transfer model. The study concerning unsupervised learning in quantum geometry reinforces the importance of identifying reusable learning principles beneath domain-specific problems (Wu,A.K.,Primeau,L.,Zhang,J.,etal.,2025). At the same time, the commercialization and cybersecurity studies demonstrate that reusable AI must eventually interact with governance, operational, and economic structures.

The primary implication is that organizations seeking cross-domain AI adoption should evaluate capabilities as modular assets rather than isolated models. Such an approach supports more systematic reuse while reducing the risks associated with transferring inappropriate assumptions between domains.

5. DISCUSSION

The findings position cross-domain AI evolution as an architectural and organizational problem in addition to a machine-learning problem. Existing studies demonstrate strong capabilities within individual domains, but their collective interpretation indicates that sustainable AI transfer depends on the ability to separate generalizable computational principles from domain-specific assumptions.

The theoretical contribution of the proposed framework is the distinction between migration, transformation, and enhancement. Migration describes movement of an existing capability. Transformation describes adaptation to new data, constraints, objectives, and infrastructure. Enhancement describes the generation of measurable value after integration. These stages should not be treated as interchangeable. A technically successful migration may still fail to create value if the target environment lacks appropriate governance or decision integration.

The framework also challenges a purely performance-centered conception of AI maturity. Medical segmentation, forecasting, and scientific learning can produce strong computational outputs, but the value of these outputs depends on the broader system in which they operate. For example, the LSTM forecasting model becomes decision-relevant through portfolio optimization (Li,H.,&Liu,T.,2023), while cybersecurity

AI becomes operationally relevant through prioritization and patch planning (Zhou,D.,2025; Zhou,D.,2026).

A second theoretical implication concerns abstraction depth. Capability transfer becomes more feasible when systems are represented at a sufficiently general level. The unsupervised-learning study provides an example in which the underlying learning mechanism can be considered independently from the specialized scientific context (Wu,A.K.,Primeau,L.,Zhang,J.,etal.,2025). However, excessive abstraction can remove essential domain knowledge. The optimal transfer level therefore lies between rigid application specificity and overly generic technical representation.

The practical implications are significant. Organizations developing AI platforms should emphasize modular architectures, reusable APIs, configurable governance controls, and domain-adaptation mechanisms. The multi-tenant commercialization framework supports this perspective by treating AI capabilities as infrastructure that can serve multiple users and applications (Yi,X.,2026). Such architecture can reduce duplication and accelerate deployment, but it simultaneously introduces challenges concerning isolation, governance, data ownership, and performance consistency.

The literature also reveals a fundamental trade-off between reusability and specialization. Highly reusable capabilities may sacrifice domain-specific optimization, whereas highly specialized systems may provide excellent performance but limited transferability. Therefore, the objective should not be maximum reuse; it should be strategic reuse with controlled specialization.

Privacy introduces another trade-off. Federated learning can support distributed AI without requiring centralized data aggregation, while differential privacy can further constrain information leakage (Yi,X.,2026). Yet these mechanisms can impose computational, communication, or accuracy costs. Cross-domain transformation must therefore evaluate privacy as part of the value equation rather than assuming that stronger protection is cost-free.

The framework has limitations. First, it is conceptual and derived exclusively from the supplied literature rather than from a controlled experimental dataset. Second, the references represent diverse fields and therefore do not provide a standardized set of performance metrics. Third, the

proposed value function remains theoretical and requires empirical validation. Future research should test the framework using longitudinal case studies in which a single AI capability is intentionally migrated across multiple domains and evaluated using common measures of adaptability, governance, integration, and value.

A further limitation is that cross-domain transfer may be constrained by hidden dependencies in data, infrastructure, and organizational processes. A capability that appears modular at the algorithmic level may depend heavily on specialized data engineering or domain expertise. Consequently, future empirical research should measure not only model transfer but also the transferability of supporting infrastructure and knowledge.

6. CONCLUSION

This research developed a conceptual framework for understanding Cross-Domain AI Evolution as a progression from capability migration to capability transformation and ultimately to value enhancement. Comparative analysis of the supplied literature demonstrates that AI capabilities such as representation learning, forecasting, attention mechanisms, federated learning, reinforcement learning, privacy preservation, and risk prioritization can provide transferable principles across domains.

The central conclusion is that successful cross-domain AI does not result from simply moving a model from one application area to another. Instead, the capability must be abstracted, contextualized, integrated, governed, and connected to measurable outcomes. The proposed framework consequently defines five critical evaluation dimensions: technical effectiveness, contextual adaptability, governance integrity, integration capability, and value realization.

The research further establishes that value emerges when AI capabilities are embedded within decision and operational systems. Forecasting becomes valuable through optimization, cybersecurity intelligence becomes actionable through prioritization, and AI capabilities become commercially scalable through infrastructure, governance, incentives, and standardized interfaces.

The framework contributes to AI research by providing a unified conceptual vocabulary for distinguishing capability reuse from capability transformation. It also offers practitioners a structured approach for assessing whether an

AI capability is genuinely transferable and under what conditions it can generate additional value.

Future studies should empirically validate the framework across sectors, develop quantitative measures for transformation readiness, and investigate how modular AI architectures can balance generalization with domain specialization. Such work could establish cross-domain AI evolution as a measurable research discipline rather than treating AI transfer as an ad hoc deployment activity.

REFERENCES

1. Chang,C.,Fu,M.,Chen,X.,etal.(2025,November).Research onPDU-NetLungNoduleSegmentationAlgorithmBasedonPathAggregationandDualAttention.In20254thInternationalConferenceonImageProcessing,ComputerVisionandMachineLearning(ICICML)(pp.1897-1900).IEEE.
2. Li,H.,&Liu,T.(2023).PortfoliooptimizationbasedontheLSTMforecastingmodel.InProceedingsofthe2ndInternationalConferenceonFinancialTechnologyandBusinessAnalysis(Vol.48,No.1,pp.97-106).
3. Liu,T.(2022,December).FinancialConstraint'ImpactonFirm'sESGRatingBasedonChineseStockMarket.In20224thInternationalConferenceonEconomicManagementandCulturalIndustry(ICEMCI2022)(pp.1085-1095).AtlantisPress.
4. Wu,A.K.,Primeau,L.,Zhang,J.,etal.(2025).ModelingQuantumGeometryforFractionalChernInsulatorswithunsupervisedlearning.arXivpreprintarXiv:2510.03018.
5. Yi,X.(2026).AFederatedandDifferentiallyPrivateIncentive-MarketingFrameworkforPrivacy-PreservingCross-ChannelMeasurementinAI-PoweredDigitalCommerce.
6. Yi,X.(2026).Privacy-EnhancedAdTargetingforSocialE-Commerce:AFederatedLearningFrameworkwithZero-KnowledgeVerificationforCreatorMonetization.FrontiersinBusinessandFinance,3(1),102-113.
7. Yi,X.(2026).TrustedAICommercializationInfrastructureforSMBs:AUnifiedMulti-TenantArchitectureIntegratingIncentiveSystems,ContentGovernance,andStandardizedRecommendationAPIs.
8. Zhou,D.(2025,December).M-VP2:Microservice-OrientedVulnerabilityPatchPlanning-ACost-AwareApproachusingMulti-

Agent Reinforcement Learning. In 2025 55th International Conference on Computer, Internet of Things and Control Engineering (CITCE) (pp. 248-254). IEEE.

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