Cross-Domain Adoption of AI: Core Challenges and Practical Solutions—A Literature Review (2022-2026)

Abstract

While artificial intelligence (AI) has demonstrated transformative potential across healthcare, quantum science, digital commerce, cybersecurity, and finance, its large-scale cross-domain adoption is hindered by multifaceted challenges. This review synthesizes 10 recent studies (2022-2026) to identify three overarching barriers: technical incompatibility with domain-specific demands, privacy and regulatory compliance risks, and resource constraints for small-to-medium enterprises (SMEs) and specialized fields. Through analyzing innovative solutions proposed in the literature—including hybrid AI architectures, privacy-enhancing technologies (PETs), and adaptive algorithmic frameworks—this paper highlights how tailored AI implementations address these challenges. The findings underscore the importance of domain-driven AI design and cross-disciplinary collaboration, providing actionable insights for researchers, practitioners, and policymakers aiming to accelerate responsible AI adoption across sectors.

1 Introduction

The proliferation of AI technologies has created unprecedented opportunities for innovation across diverse industries, from medical diagnostics to financial portfolio management [1][10]. However, the translation of AI research into real-world applications is often fragmented, with domain-specific characteristics posing unique obstacles that generic AI models cannot adequately address [3][5]. For instance, healthcare demands high precision and strict data privacy [1][9], while quantum physics requires handling complex, unstructured systems [2], and digital commerce balances user privacy with business needs [7][8]. This review examines recent literature (2022-2026) to systematically map the core challenges of cross-domain AI adoption and the novel solutions proposed to overcome them. By integrating findings from healthcare, quantum science, digital commerce, cybersecurity, and finance, this paper aims to identify common patterns and divergent strategies, offering a holistic perspective on responsible and effective AI implementation.

2 Core Challenges of Cross-Domain AI Adoption

2.1 Technical Incompatibility with Domain-Specific Demands

Many AI models struggle to adapt to the unique requirements of specialized fields. In healthcare, for example, lung nodule segmentation requires precise identification of heterogeneous, often small-sized lesions— a task where traditional algorithms fail due to inadequate feature extraction [1]. Similarly, quantum geometry modeling for fractional Chern insulators involves complex quantum states that defy conventional mathematical modeling, limiting the applicability of standard machine learning approaches [2]. In cybersecurity,

microservice architectures generate massive volumes of vulnerability data, demanding AI systems that can prioritize risks based on context-specific cost-benefit tradeoffs [4][5]. This technical mismatch between generic AI frameworks and domain-specific needs remains a primary barrier to adoption.

2.2 Privacy and Regulatory Compliance Risks

Data privacy is a universal concern across sectors, particularly in healthcare and digital commerce, where sensitive personal information is central to AI modeling [3][9]. Healthcare data—such as electronic health records (EHRs) used for HIV treatment adherence measurement [9]—is protected by strict regulations (e.g., HIPAA, GDPR), while digital commerce platforms face growing scrutiny over cross-channel data sharing [3][8]. The conflict between data accessibility (critical for AI training) and privacy protection (mandated by law) creates a "data paradox" that hinders collaborative AI development [8]. Additionally, financial sectors handling user financial data and ESG-related information must comply with regulatory requirements, adding layers of complexity to AI implementation [6][10].

2.3 Resource Constraints for SMEs and Specialized Fields

Resource limitations disproportionately affect SMEs and specialized fields, slowing AI adoption. SMEs, which lack the infrastructure of large corporations, struggle to deploy advanced AI systems for digital commerce or cybersecurity [7][4]. In financial governance, small enterprises face challenges in implementing AI-driven ESG rating improvement strategies due to financial constraints [6]. Even in specialized fields like quantum physics, the computational resources required for data-driven modeling are often prohibitive, limiting the scalability of innovative approaches [2]. This resource gap exacerbates the digital divide between large organizations and SMEs, as well as between mainstream and niche sectors.

3 Innovative Solutions from Recent Literature

3.1 Hybrid and Adaptive AI Architectures

To address technical incompatibility, researchers have developed hybrid AI architectures tailored to domain-specific demands. Chang et al. [1] proposed the PDU-Net algorithm, which integrates path aggregation and dual attention mechanisms to enhance feature extraction for lung nodule segmentation—directly addressing the precision needs of medical imaging. In cybersecurity, Zhou [5] introduced a hybrid SAST-DAST-SCA-IAST framework that combines multiple security testing methodologies, enabling AI to prioritize vulnerabilities based on microservice-specific risk profiles. For financial portfolio optimization, Li and Liu [10] leveraged LSTM’s strength in time-series data processing to create a model adapted to the dynamic nature of financial markets, demonstrating how domain-specific algorithm selection improves performance.

3.2 Privacy-Enhancing Technologies (PETs) for Compliant Collaboration

Privacy-enhancing technologies (PETs) have emerged as a key solution to the data paradox. Yi [3][8] proposed federated learning (FL) frameworks integrated with differential privacy and zero-knowledge verification, enabling cross-channel data collaboration in digital commerce without exposing sensitive user information. In healthcare, Yue et al. [9] used EHR phenotyping methods that prioritize data de-identification, ensuring compliance with privacy regulations while enabling AI-driven measurement of HIV treatment adherence. These PETs—including FL, differential privacy, and zero-knowledge proof—strike a balance between data utility and privacy, facilitating legal and ethical AI deployment [7].

3.3 Resource-Efficient and Inclusive AI Frameworks

To address resource constraints, researchers have developed lightweight and inclusive AI frameworks. Yi [7] designed a multi-tenant trusted AI infrastructure for SMEs, integrating incentive systems and standardized APIs to reduce implementation costs for digital commerce. In cybersecurity, Zhou's [4] M-VP2 method uses multi-agent reinforcement learning to optimize vulnerability patch planning, minimizing resource consumption while maximizing security outcomes. For financial ESG governance, Liu's [6] research highlights the need for resource-efficient AI tools that help cash-constrained SMEs improve their ESG ratings, suggesting that scalable, low-cost AI solutions are critical for inclusive adoption.

4 Discussion and Future Directions

The literature review reveals that cross-domain AI adoption success hinges on three key principles: domain-driven customization, privacy-by-design, and resource efficiency. Hybrid architectures (e.g., PDU-Net [1], SAST-DAST-SCA-IAST [5]) demonstrate that AI must be tailored to the unique demands of each sector, while PETs (e.g., federated learning [3][8], differential privacy [7]) address compliance risks that universalize across domains. Resource-efficient frameworks [4][7] further ensure that AI benefits are not limited to large organizations or resource-rich fields.

Future research should focus on two critical areas: first, developing interoperable AI systems that can adapt across multiple domains without compromising performance, and second, creating standardized evaluation metrics for domain-specific AI effectiveness. Additionally, policymakers should prioritize supporting SMEs through incentives for adopting low-cost, compliant AI tools, while researchers should collaborate with domain experts to co-design AI solutions that address real-world needs. By fostering cross-disciplinary collaboration and prioritizing responsible innovation, the research community can accelerate AI's transformative potential across sectors.

5 Conclusion

This review synthesizes recent literature to identify the core challenges of cross-domain AI adoption—technical incompatibility, privacy compliance risks, and resource constraints—and the innovative solutions proposed to mitigate them. From hybrid AI architectures in healthcare and cybersecurity to privacy-enhancing frameworks in digital commerce and inclusive tools for SMEs, the literature demonstrates that tailored, domain-driven AI implementations are key to overcoming these barriers. As AI continues to evolve, the

integration of domain expertise, privacy-by-design principles, and resource-efficient design will be critical to unlocking its full potential across sectors, driving inclusive, responsible, and impactful innovation.

References

[1] Chang, C., Fu, M., Chen, X., et al. (2025, November). Research on PDU-Net Lung Nodule Segmentation Algorithm Based on Path Aggregation and Dual Attention. In *2025 4th International Conference on Image Processing, Computer Vision and Machine Learning (ICICML)* (pp. 1897-1900). IEEE.

[2] Wu, A. K., Primeau, L., Zhang, J., et al. (2025). Modeling Quantum Geometry for Fractional Chern Insulators with unsupervised learning. *arXiv preprint arXiv:2510.03018*.

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

[4] 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.

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

[6] 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.

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

[8] 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.

[9] Yue, Y., Khanal, A., Lyu, T., Weissman, S., & Liang, C. (2025, May). EHR Phenotyping Methods for Measuring Treatment Adherence Among People Living With HIV in All of Us: Towards Disparities and Inequalities in HIV Care Continuum. In *AMIA Annual Symposium Proceedings* (Vol. 2024, p. 1294).

[10] 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).