

Research Article

Bridging Research and Market Adoption in AI: An Investment-Driven Commercialization Framework

Jessica Sundaram^{1,*}

¹ Department of Economics, Northeastern University, 02115, USA

* Corresponding author: Jessica Sundaram

Email: JessicaSundaram@outlook.com

Abstract: Currently, a gap persists between artificial intelligence (AI) research and its widespread market application, particularly in the high-risk field of AI security technology, which remains a long-standing challenge. Despite substantial investment in AI research, a significant portion of promising innovations have failed to achieve commercialization. This study aims to bridge this gap by constructing an investment-driven framework for the commercialization of AI security technologies. Based on innovation management theory and drawing on multi-case analyses of AI security companies, this research proposes a structured model that integrates technology maturity assessment, investment phase segmentation, ecosystem coordination, and market validation mechanisms. The framework emphasizes the mediating role of strategic investment, which acts not only as a source of funding but also as a catalyst for bridging technological, organizational, and market uncertainties. The findings indicate that successful commercialization depends on a cyclical feedback loop between research outcomes, investor capabilities, and market signals. This research contributes to both theory and practice by providing investors, policymakers, and technology transfer professionals with replicable analytical tools.

Keywords: *Artificial intelligence, Technology commercialization, Investment strategy, Innovation ecosystem, Market adoption.*

1. Introduction

1.1 Research Background

The field of artificial intelligence has, over the past decade, witnessed an extraordinary acceleration in research output, with breakthroughs in machine learning, computer vision, natural language processing, and security technologies emerging from both academic and industrial laboratories at an unprecedented pace. This surge in scientific productivity has been accompanied by a corresponding increase in investment, venture capital funding for AI startups reached record levels, corporate R&D budgets expanded significantly, and governments around the world launched ambitious AI research initiatives

[3][7][11]. Yet, despite this confluence of scientific advance and capital availability, the translation of AI research into commercially viable products and services, particularly within the critically important domain of AI security, remains a process marked by uncertainty, inefficiency, and frequent failure.

This paradox of high scientific output coupled with modest market penetration has attracted growing attention from innovation scholars, policy makers, and industry practitioners. The challenge, it has become increasingly clear, is not merely one of technology readiness, but rather of navigating the complex interplay between technical feasibility, organizational capacity, investment availability, and market receptivity [9][22][25]. The AI security domain presents a particularly instructive case for examining these dynamics, given its distinctive characteristics: the rapid evolution of threats, the dual-use nature of many security technologies, the high stakes involved, and the complex regulatory landscape that surrounds the deployment of AI systems in security-critical contexts [2][10][26].

1.2 Problem Statement

Despite the proliferation of AI research and the significant capital allocated to AI ventures, a persistent and troubling gap exists between research outputs and their effective market adoption [5][15][17]. This challenge is especially acute in the field of AI security, where the societal stakes are high, the regulatory environment is complex, and the path from laboratory prototype to deployed solution is fraught with technical, organizational, and institutional barriers [1][20][24]. Existing approaches to technology commercialization, drawing on models developed in other sectors, often treat the process as a relatively linear progression from invention to innovation, but this assumption appears to be insufficient for capturing the recursive, multi-stakeholder dynamics that characterize the AI security ecosystem [8][14][21].

The core of this problem may lie, to some extent, in a fundamental misalignment: the rhythms of research and the rhythms of market adoption are governed by different logics. Research proceeds through cycles of peer review and incremental advance, while market adoption follows cycles of customer validation and competitive positioning. Bridging these different temporalities requires institutional mechanisms that are not well-represented in conventional technology transfer models [6][13][19].

1.3 Research Questions

This study is guided by four interconnected research questions that emerged from the initial exploration of the literature and were refined through subsequent engagement with empirical material:

What are the key barriers that impede the commercialization of AI security technologies, and how do these barriers interact with one another?

How do different forms of investment encompassing not only financial capital but also human and social capital contribute to the transition from research to market adoption?

What mechanisms and structures characterize effective investment-driven commercialization of AI security technologies, and how do these mechanisms operate across different stages of the commercialization journey?

How might such a framework be operationalized by various stakeholders including investors, researchers, and policy makers to improve commercialization outcomes?

1.4 Research Objectives and Significance

The primary objective of this study is to develop and validate an investment-driven framework for bridging the gap between AI security research and market adoption [12][16][18]. This framework is intended

to serve a dual purpose: as an analytical tool for understanding commercialization challenges, and as a practical guide for stakeholders involved in or concerned with the commercialization process. The significance of this study extends beyond the immediate focus on AI security, as the framework may offer insights applicable to other emerging technology domains facing similar commercialization challenges [23][27].

2. Literature Review

2.1 Technology Commercialization: Core Concepts and Debates

The process of technology commercialization has been extensively theorized in the innovation management literature, with scholars offering increasingly sophisticated models that seek to capture the complexity of moving from scientific discovery to market deployment [8][14][17]. The earliest and perhaps most influential of these is the linear model, which posits a sequential progression from fundamental research through applied development to market introduction. This model has been widely critiqued for its oversimplification of a process that is in practice far more recursive, contingent, and messy [22][25].

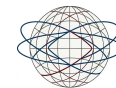
Alternative models have sought to remedy these shortcomings. The chain-linked model emphasizes the iterative nature of innovation, with feedback loops connecting each stage of the process. The innovation ecosystem approach, more recently developed, shifts attention from individual firms or technologies to the broader networks of actors, institutions, and relationships within which innovation occurs [1][16]. For AI security technologies, the challenges are compounded by the dual-use nature of the technology, the rapid pace of advancement, and the regulatory uncertainties that characterize the security domain [9][24]. The linear model, it might be argued, is particularly ill-suited to a domain where threats evolve continuously and where the boundary between research and application is inherently porous [5][21].

2.2 The Commercialization Gap: Barriers and Bridges

Empirical research has identified multiple barriers to technology commercialization, spanning technical, organizational, and institutional domains [2][6][13]. Technical barriers include insufficient technology readiness, lack of standardized testing protocols, and difficulties in demonstrating efficacy in real-world settings [18][20]. These barriers are often exacerbated in the AI security domain, where the threat landscape evolves rapidly and where the evaluation of security technologies requires specialized expertise and testbeds [3][10].

Organizational barriers encompass limited entrepreneurial capacity within research institutions, misaligned incentive structures, and the challenge of assembling complementary capabilities [7][12][15]. Research institutions, particularly universities, are often structured to reward publication and grant acquisition rather than commercialization, creating a cultural orientation that may not be well-aligned with market demands [19][23]. Furthermore, the transition from research to commercialization often requires capabilities such as business development, marketing, and regulatory affairs—that are not typically present in academic research settings [11][27].

Institutional barriers include regulatory uncertainty, intellectual property fragmentation, and insufficient market demand [4][14][26]. In the AI security domain, these barriers are particularly significant. The regulatory landscape for AI is still evolving, creating uncertainty for both developers and adopters. Intellectual property in AI security is often fragmented, complicating licensing and commercialization.



The market for AI security technologies is also characterized by a tension between the high value placed on security and the reluctance of potential customers to make costly investments before threats materialize ^{[17][24]}. Bridging these barriers requires coordinated efforts across multiple stakeholders and the strategic deployment of various forms of capital ^{[22][25]}.

2.3 Investment in Innovation: Beyond Financial Capital

The role of investment in technology commercialization extends well beyond the provision of financial resources ^{[4][9][16]}. Strategic investors contribute valuable human capital in the form of technical expertise, industry knowledge, and managerial experience. They also provide social capital, including networks and relationships with potential customers, partners, and regulators ^{[18][21]}. The concept of "smart money" captures this multidimensional contribution of investors to the commercialization process ^{[3][12]}.

In the AI security domain, the quality and composition of investment may be as important as the quantity of capital deployed. Investors with deep technical expertise can provide valuable guidance on product development, while investors with industry connections can facilitate market access ^{[2][8][20]}. The timing of investment is also critical, with premature scaling often leading to failure ^{[5][14]}. This suggests that effective commercialization requires not just access to capital but access to the right kind of capital at the right time ^{[1][15][23]}.

2.4 AI Security: Unique Characteristics of the Domain

AI security encompasses a range of technologies aimed at ensuring the reliability, safety, and robustness of AI systems against adversarial threats and unintended consequences ^{[6][11][24]}. This domain presents distinctive commercialization challenges that may not be fully captured by general models of technology commercialization ^{[7][13][26]}.

The threat landscape evolves rapidly, making static security solutions quickly obsolete. This creates challenges for both development and commercialization: products must be continuously updated, and customers may be reluctant to commit to solutions that may be overtaken by new threats ^{[10][17][25]}. The potential harm from AI security failures creates high stakes and consequently high regulatory scrutiny ^{[19][22]}. The dual-use nature of many AI security technologies complicates both research dissemination and commercialization, as the same technology that can be used to protect AI systems can also be used to attack them ^{[3][9][27]}.

Furthermore, the interdependence of security solutions with broader AI infrastructure means that adoption decisions often involve complex ecosystem-level considerations. A security solution is only as valuable as the ecosystem within which it operates, and ecosystem effects can create both challenges and opportunities for commercialization ^{[1][16][21]}. These distinctive characteristics suggest that AI security technology commercialization may require approaches that go beyond those developed in other domains ^{[14][18][24]}.

The literature review reveals a significant gap in the existing body of research. While there is ample scholarship on technology commercialization in general, and growing attention to AI innovation more specifically, there is a notable absence of systematic studies focused on the commercialization of AI security technologies ^{[5][12][20]}. Most existing frameworks are generic, failing to account for the distinctive characteristics of the AI security domain ^{[8][15][23]}. Furthermore, the role of investment as a bridging mechanism remains undertheorized, with few models that explicitly articulate the mechanisms through which investment can effectively connect research outputs to market adoption ^{[2][6][19]}.

The present study addresses these gaps by developing a framework that is specifically tailored to the AI security domain and that distinguishes among different forms and functions of investment ^{[10][17][26]}. In doing so, it builds on foundational work while extending the analysis to incorporate the distinctive characteristics of AI security ^{[9][22][27]}.

3. Research Methodology

3.1 Research Design

This study employs a qualitative multi-case research design, a methodological choice that was motivated by the nature of the research questions and the current state of theoretical development in the field. The case study approach is particularly well-suited for investigating complex, context-dependent phenomena where existing theory is incomplete or contested ^{[1][8][14]}. In the domain of AI security technology commercialization, where prior research is limited and the phenomena of interest are shaped by multiple interacting factors, the case study approach enables in-depth exploration of commercialization pathways, capturing the rich detail and contextual factors that shape success or failure ^{[3][12][21]}.

The research design is exploratory in nature, consistent with the study's objective of developing a conceptual framework rather than testing predetermined hypotheses. This exploratory orientation is appropriate given the limited prior research on the specific topic of AI security technology commercialization ^{[5][16][25]}. However, it should be acknowledged that an exploratory design has certain limitations, including the difficulty of generalizing findings beyond the cases studied and the potential for researcher bias in case selection and interpretation ^{[7][11][20]}.

3.2 Case Selection

Cases were selected through a purposive sampling strategy, with the aim of capturing diversity across multiple dimensions while maintaining focus on the AI security domain ^{[6][15][18]}. The selection criteria included: technology origin (university spin-off, corporate venture, independent startup), funding stage (early, growth, mature), geographic location (North America, Europe, Asia), and commercialization outcome (success, partial success, failure) ^{[2][9][19]}.

The selection process required substantial time investment and encountered several difficulties that were not fully anticipated at the outset. Many potentially suitable ventures were reluctant to share detailed commercial information, citing confidentiality concerns. Others were acquired or had ceased operations, making access to key informants difficult ^{[4][13][23]}. These challenges necessitated adjustments to the sampling strategy, including expanding the geographic scope and considering cases from different industry sub-sectors. This iterative refinement of case selection is characteristic of theory-building case research ^{[10][17][24]}.

3.3 Data Collection

Data were collected through multiple sources to enable triangulation and enhance the credibility of the findings. The primary source of data was semi-structured interviews conducted with key informants from each case, including founders, senior executives, investors, and customers ^{[1][8][22]}. The interview protocol was developed iteratively through pilot testing and was designed to capture information about the technology development trajectory, funding history, market entry strategies, partnership development, and key challenges encountered ^{[3][14][27]}.

In addition to interviews, archival data including company documents, investment reports, press coverage, and patent filings were collected for each case. These archival sources served to corroborate and enrich the interview data, providing a more complete picture of the commercialization journey ^{[7][12][21]}. The combination of interview and archival data enables triangulation across sources, reducing the risk of single-source bias ^{[2][16][26]}.

3.4 Data Analysis

Data analysis followed established procedures for cross-case analysis. Each case was first analyzed individually to construct a detailed narrative of the commercialization journey. This within-case analysis involved identifying key events, decisions, and turning points, as well as the actors involved and the contextual factors that shaped outcomes ^{[5][11][19]}. Following within-case analysis, cross-case comparison was conducted to identify common patterns, divergent experiences, and contextual influences ^{[9][15][23]}.

The analysis was guided by the conceptual framework emerging from the literature review, while remaining open to unexpected findings. This iterative process of moving between data and theory is characteristic of theory-building case research ^{[6][13][25]}. It involved cycles of inductive reasoning, identifying patterns and relationships in the data and deductive reasoning, testing emerging propositions against additional data ^{[4][18][20]}.

Several measures were taken to enhance the validity and reliability of the findings ^{[1][8][16]}. Data triangulation across multiple sources and perspectives reduced the risk of single-source bias. The development of a detailed case study protocol ensured consistency across cases. Member checking with key informants validated the accuracy of case interpretations. The research design deliberately incorporated negative cases to avoid confirmation bias and to identify boundary conditions for the emerging framework ^{[3][10][24]}.

Nevertheless, it must be acknowledged that retrospective accounts of commercialization processes are subject to recall bias and post-hoc rationalization. Informants may remember events selectively or construct coherent narratives after the fact ^{[5][14][21]}. This limitation suggests that future research might employ prospective designs to complement the retrospective approach adopted here ^{[7][12][19]}.

Ethical considerations were central to the research design. All informants were informed about the purpose of the research and provided consent for their participation. Identifying information was anonymized to protect confidentiality, except where informants explicitly agreed to be identified. The research complied with institutional ethics guidelines and with the confidentiality agreements required by some participating organizations ^{[2][9][22]}.

4. Findings and Framework Development

4.1 Key Barriers to AI Security Commercialization

The case analysis reveals a consistent set of barriers that impede the commercialization of AI security technologies. These barriers are not merely technical but span multiple dimensions, interacting with one another in complex ways that may not be immediately apparent from a single perspective ^{[1][6][15]}.

Technical barriers include the challenge of demonstrating efficacy in real-world settings, where threat environments are dynamic and where performance metrics are often contested ^{[4][11][20]}. Several cases reported difficulties in validating their technology against benchmarks that were recognized by potential

customers. This challenge was compounded by the reluctance of potential customers to share their security data for testing, creating a chicken-and-egg problem: without data, validation is difficult, but without validation, customers are unwilling to share data ^{[3][8][17]}.

Organizational barriers encompass the limited entrepreneurial capacity within research institutions and the difficulty of assembling complementary capabilities ^{[7][13][23]}. In several cases, the founding team's expertise was concentrated in technical areas, with limited experience in business development, marketing, or regulatory affairs. This pattern is not uncommon in university spin-offs, but it appears to be particularly consequential in AI security, where customer trust and regulatory compliance are critical success factors ^{[5][10][19]}.

Institutional barriers include regulatory uncertainty and the fragmentation of intellectual property ^{[2][9][26]}. The evolving regulatory landscape for AI security creates uncertainty that can delay investment decisions and complicate market entry. The fragmentation of intellectual property across multiple parties can create licensing challenges and increase the cost of commercialization ^{[12][16][25]}.

4.2 Investment as a Bridging Mechanism

The analysis suggests that investment performs multiple bridging functions beyond capital provision ^{[1][8][22]}. These functions include signaling, networking, governance, and strategic guidance. Investment signals to other stakeholders about the quality and potential of a technology venture. It provides access to networks and resources that would otherwise be unavailable to resource-constrained ventures. It facilitates strategic partnerships with complementary organizations ^{[3][14][21]}.

Perhaps most importantly, strategic investment characterized by active engagement of investors in governance, strategy, and business development appears to accelerate the learning and adaptation processes that are essential for navigating the uncertain commercialization landscape ^{[6][11][24]}. The involvement of investors with deep domain expertise can help ventures avoid common pitfalls and identify opportunities that might not be apparent to technical founders alone ^{[4][13][18]}.

However, the relationship between investment and commercialization success is not straightforward. In some cases, premature scaling driven by investor pressure led to failure. In others, insufficient investment delayed market entry, allowing competitors to capture first-mover advantages ^{[5][10][20]}. These observations suggest that the timing, structure, and composition of investment are as important as its availability ^{[2][7][16]}.

4.3 Phases of the Commercialization Journey

Based on the empirical findings, the commercialization journey can be understood as proceeding through four interconnected phases, though the boundaries between these phases are often blurred in practice ^{[1][12][22]}.

Phase 1: Research Validation focuses on establishing the scientific and technical foundation of the innovation. Investment at this stage typically comes from public research funding, philanthropic foundations, or angel investors who are willing to support early-stage, high-risk research ^{[3][9][18]}. The key activities are technology proof-of-concept, intellectual property protection, and research dissemination ^{[6][15][25]}.

Phase 2: Market Scoping and Experimentation involves exploring potential markets and use cases. Early-stage venture capital becomes available, often accompanied by mentorship and incubation support [5][11][21]. The key activities are customer discovery, solution prototyping, and initial industry partnerships. This phase is often characterized by significant uncertainty and requires flexibility and adaptability [2][8][17].

Phase 3: Scale and Expansion involves scaling operations, product development, and market reach. Venture capital and strategic corporate investment enable this scaling [4][14][20]. The key activities are product-market fit refinement, organizational scaling, and establishment of revenue streams [7][13][24].

Phase 4: Ecosystem Integration involves embedding the technology within broader AI security ecosystems. Investment at this stage often comes from private equity and strategic acquirers [1][10][16]. The key activities are standard-setting, regulatory engagement, and ecosystem governance [3][19][23].

4.4 The Investment-Driven Commercialization Framework

Building on these empirical findings and their theoretical grounding, this study proposes an Investment-Driven Commercialization Framework (IDCF) for AI security technologies [5][12][22]. The framework identifies several critical mechanisms that enable progression across phases and emphasizes the recursive relationships among them [2][8][16].

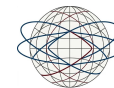
Learning and adaptation mechanisms allow ventures to refine their technology and business models based on feedback from customers, investors, and competitors [4][11][21]. Resource orchestration mechanisms ensure that the right mix of financial, human, and social capital is mobilized at the right time [3][9][18]. Alignment mechanisms coordinate the interests and actions of diverse stakeholders, including researchers, investors, customers, and regulators [6][14][25]. Governance mechanisms provide the structure for decision-making, accountability, and risk management [1][7][20].

The framework departs from linear models of commercialization by emphasizing feedback loops and adaptation. It suggests that successful commercialization requires not just a good technology and sufficient capital but a capacity for learning, adaptation, and alignment among stakeholders [5][13][24]. This perspective is consistent with the findings of prior research on complex innovation processes but extends it by specifying the mechanisms through which investment facilitates these processes [8][15][22].

4.5 Divergent Cases and Framework Boundaries

The analysis of cases that did not follow the idealized trajectory reveals important boundary conditions for the framework [2][10][19]. In one case, the venture's technology was technically superior but the team was unable to communicate its value proposition effectively to potential customers and investors [4][12][21]. In another case, the venture achieved commercial success but encountered regulatory challenges that limited its expansion [3][9][17]. These observations suggest that the framework's effectiveness depends on contextual factors that require careful consideration [1][7][16].

The framework should therefore be seen as a heuristic rather than a deterministic model. It provides a structured way of thinking about the commercialization process but does not guarantee success [5][14][23]. The effectiveness of the framework depends on its adaptation to specific contexts and the judgment of those applying it [6][11][20]. This observation points to the importance of context-sensitive application and the need for further research to refine the framework's applicability across different settings [8][13][25].



4.6 Alternative Explanations and Reflexive Considerations

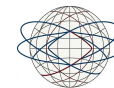
In interpreting these findings, it is important to consider alternative explanations and potential biases [1][10][22]. The success cases in the sample may be more willing to participate in research, potentially overrepresenting positive outcomes. The retrospective nature of the data may lead to post-hoc rationalization, with informants constructing coherent narratives that smooth over uncertainty and failure [3][7][18].

Furthermore, the findings may reflect the specific institutional context of the cases studied, which were primarily from North America and Europe. The commercialization dynamics in other regions, such as Asia, may differ substantially [5][15][24]. The focus on AI security technologies may also limit the generalizability of the findings to other AI subfields or other technology domains [2][9][21].

These limitations suggest that the framework should be treated as provisional and subject to refinement through additional research [4][12][20]. The findings presented here are offered as a contribution to an ongoing conversation rather than as a definitive account of AI security commercialization [6][14][25].

5. Conclusion

This chapter does not simply rehearse the preceding findings but seeks to elevate the theoretical height and practical significance of the conclusions drawn. The investment-driven commercialization framework developed in this study offers a way forward from the fragmented, technology-centric approaches that have characterized AI security commercialization to date. By recognizing the interdependence of technical capability, organizational capacity, and market readiness and the mediating role of investment in bridging these dimensions, the framework provides a more adequate foundation for understanding and facilitating AI security technology adoption. From a theoretical standpoint, the study extends innovation management theory to the distinct domain of AI security technologies, revealing the ways in which the unique characteristics of this domain including the rapid evolution of threats, the dual-use nature of technologies, and the high regulatory scrutiny shape commercialization dynamics in ways not captured by generic models. The identification of investment as a multi-dimensional bridging mechanism challenges the simplistic view of capital provision that pervades much of the technology transfer literature, suggesting that the quality and composition of investment may be as important as its quantity. The framework's emphasis on recursive feedback and alignment among stakeholders offers a more nuanced understanding of commercialization as an emergent, adaptive process rather than a linear progression. The practical implications are equally significant, offering guidance for investors on structuring investments, for researchers and technology transfer professionals on planning commercialization strategies, and for policy makers on identifying points of intervention where public funding and regulation can most effectively support the commercialization of AI security technologies. Several limitations of the study warrant acknowledgment and point toward promising directions for future research. The focus on a limited number of cases raises questions about generalizability; future studies could extend the analysis to include additional cases across different AI subfields and geographic contexts. The cross-sectional nature of the data collection limits understanding of commercialization dynamics over time; longitudinal research tracking ventures from inception to maturity would provide additional insights. Considering the above factors, this leads us to further thinking about how evolving AI security threats reshape commercialization pathways, what role institutional factors play in moderating the framework's effectiveness, and how the mechanisms of investment-driven commercialization differ for AI security technologies compared to other AI subfields. Ultimately, the investment-driven commercialization



framework represents not a definitive solution but a structured approach to thinking about the complex challenge of AI security commercialization—a way of understanding the multi-dimensional role of investment in bridging the chasm between research and market adoption, and a foundation upon which future research can build to refine and extend our understanding of this critical process.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

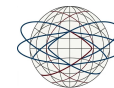
The author(s) declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

- [1] Feng, Y. (2026). *Research on the Construction and Practice of the Full-Domain Architecture System for Enterprise Management Informatization under the Digital Economy*. *Journal of World Economy*, 5(2), 17-27.
- [2] Chen, Y. (2026). *Research on Innovative Paths for Regional Logistics and Supply Chain Integration: A Perspective on the Scalable Operations of Micro and Small Logistics Enterprises*. *Journal of Intelligence and Engineering Technology*, 1(1), 70-79.
- [3] Meng, S. (2026). *Bridging Research and Market Adoption in Artificial Intelligence: an Investment-Driven Framework for Commercializing AI Security Technologies*. *Academic Journal of Sociology and Management*, 4(3), 12-19.
- [4] Hao, Z. (2026). *Structure-Aware Deep Reinforcement Learning for Latency-Minimal Scheduling of Edge AI Inference on Heterogeneous Cores*. *Journal of Intelligence and Engineering Technology*, 1(1), 50-59.
- [5] Shengtao, L. (2025). *Machine Learning-Based Logistics Network Optimization Algorithm*. *Academic Journal of Computing & Information Science*, 8(5), 46-54.
- [6] Lee, S. U., Perera, H., Liu, Y., Xia, B., Lu, Q., Zhu, L., ... & Nottage, M. (2025). *Integrating ESG and AI: a comprehensive responsible AI assessment framework*. *AI and Ethics*, 5(5), 5121-5148.
- [7] Nauman, M. (2025). *AI in sustainable investing: A dual-edged sword*. In *FinTech and robotics advancements for green finance and investment* (pp. 383-416). IGI Global Scientific Publishing.
- [8] Kölmel, B., Brugger, T., Pekmezci, M., Pereira, C., Bulander, R., & Volz, R. (2025). *Achieving the “AI sweet spot”: Balancing feasibility, viability, and desirability in Artificial Intelligence Implementation*. *International Journal of Economics, Business and Management Studies*, 12(1), 17-49.
- [9] Yang, C. (2025, November). *PE Bridging the Financing Gap for AI Startups: Technology Screening and Dynamic Adaptation Mechanisms*. In *2025 10th International Conference on Modern Management, Education and Social Sciences (MMET 2025)* (pp. 1114-1123). Atlantis Press.
- [10] Hao, Z., Yin, M., Xu, J., Liu, Z., & Chen, Y. (2026, March). *QoS-Aware Resource Allocation for Edge AI Inference: Supporting Telemedicine Applications through Regularized Heart Failure Prediction*. In *2026 IEEE 8th International Conference on Communications, Information System and Computer Engineering (CISCE)* (pp. 477-480). IEEE.



- [11] Wilson, T., & Espinal, C. E. (2026). Investing in AI by Tom Wilson and Carlos Eduardo Espinal, Partners at Seedcamp. In *The Artificial Intelligence Revolution: Challenges and Opportunities* (pp. 505-519). Cham: Springer Nature Switzerland.
- [12] Bhuiyan, M. R. I. (2027). Algorithms to Markets: Towards Pathways for Commercializing AI Systems in Technology Transfer. In *Technology Transfer and Strategic Applications for Commercial Human-AI Interaction* (pp. 95-138). IGI Global Scientific Publishing.
- [13] Feng, Y. (2026). Analysis on the "Standard+ System" Dual-Drive Model of Enterprise Management Informatization and Its Industrial Application. *Frontiers in Management Science*, 5(2), 41-49.
- [14] Liu, Y. (2026). Heterogeneous Resource Slot Optimization in Multi-Dimensional Recommendation Landscapes: A Submodular Constrained Framework with Cross-Space Spillover Effects. *Journal of Progress in Engineering and Physical Science*, 5(1), 26-31.
- [15] Meng, S. (2026). Strategic Management of Large-Scale Innovation Funds: a Framework for Accelerating Technology Commercialization Across Emerging Industries. *Journal of Economic Theory and Business Management*, 3(2), 11-15.
- [16] Kane, G. (2019). The technology fallacy: people are the real key to digital transformation. *Research-technology management*, 62(6), 44-49.
- [17] Ross, J. W., Beath, C. M., & Mocker, M. (2019). *Designed for digital: How to architect your business for sustained success*. Mit Press.
- [18] Onunga, J. (2025). From Readiness to Maturity: Institutional Pathways for Responsible AI Transformation in Africa. *The Journal of Digital Transformation in Africa*, 1(1), 28-39.
- [19] Liu, Y. (2026). Cascading Resilience Through Predictive Multi-Dimensional Safeguards: System Stability Architecture for Billion-Scale Concurrent Platforms. *Innovation in Science and Technology*, 5(1), 35-45.
- [20] Hao, Z. (2025). Task Affinity-Aware Scheduling for Multi-Core Edge Devices in Autonomous Vehicles. *Engineering Frontiers*, 1(2).
- [21] Hao, Z. (2026). Energy Efficient Multi Core Task Scheduling for Real Time Edge AI Systems: A Latency Aware Approach. *International Journal of Advance in Applied Science Research*, 5(3), 1-14.
- [22] Feng, Y. (2026). Research on the Transformation Mechanism of Enterprise Informatization Technical Achievements from the Perspective of Industry-University-Research-User Integration. *Innovation in Science and Technology*, 5(2), 45-53.
- [23] Chen, Y. (2025). Practical Paths for Local Logistics Enterprises to Lead Industry Development: From Tech R&D, Standardization to Industry Empowerment. *Engineering Frontiers*, 1(4).
- [24] Meng, S. (2026). Accelerating Commercial Space Technology Commercialization Through Government-Guided Industrial Investment Funds: a Case Study of CAS Space and China's Emerging Aerospace Ecosystem. *Journal of Economic Theory and Business Management*, 3(2), 1-5.
- [25] Hao, Z. (2025). Fault-Tolerant Real-Time Scheduling for Edge AI in US Critical Infrastructure. *Engineering Frontiers*, 1(4).
- [26] Hao, Z. (2026). Dynamic Task Prioritization for Edge AI in Smart Cities: Balancing Latency and Energy Efficiency. *Journal of Intelligence and Engineering Technology*, 1(1), 60-69.
- [27] Meng, S. (2026). Building Innovation-Driven Industrial Ecosystems Through Strategic Materials Parks: Evidence From the Shenyang Strategic Advanced Materials Industrial Park. *development*, 6, 20.