Securing Industrial Networks: AI-Driven Fundraising And Business Models For Smart Manufacturing

Jay Mehta[1], Rohith Narasimhamurthy[2], Prithviraj Kumar Dasari[3]

[1] Manager at Seldon Capital
[2] Senior Software Development Engineer
[3] Senior Software Engineer

Abstract

The increasing complexity and interconnectivity of smart manufacturing systems have made industrial networks highly susceptible to cyber threats, necessitating robust and adaptive security strategies. This study investigates the role of artificial intelligence (AI) in enhancing industrial cybersecurity, while also exploring AI-driven fundraising mechanisms and innovative business models that support secure digital transformation. Using a mixed-methods approach, data were collected from 50 manufacturing firms and leading AI fundraising platforms. Statistical analyses, including multiple regression and principal component analysis (PCA), revealed that higher AI maturity, effective capital allocation, and adoption of scalable security models significantly improve cyber-resilience. AI-powered fundraising platforms demonstrated superior efficiency in capital matching, while service-based security models such as Cybersecurity-as-a-Service and Managed AI Security Services offered high returns on investment and operational scalability. The study also found that discrete manufacturing systems tend to be more cyber-resilient than process-based systems due to greater modularity and integration potential. These findings highlight the importance of aligning technological, financial, and operational strategies to secure industrial networks effectively. The research provides actionable insights for industry stakeholders, policymakers, and technology innovators seeking to build resilient and future-ready smart manufacturing infrastructures.

Keywords: Industrial cybersecurity, AI maturity, smart manufacturing, AI-driven fundraising, Cybersecurity-as-a-Service, business models, cyber-resilience, industrial networks.

Introduction

Industrial networks in the era of smart manufacturing

The industrial sector is undergoing a transformative shift through the integration of intelligent technologies and interconnected systems, forming what is widely recognized as Industry 4.0 (Hassan et al., 2024). At the core of this transformation are industrial networks dynamic communication infrastructures that connect machinery, sensors, controllers, and enterprise systems to enable real-time data flow and operational automation. However, with increased interconnectivity comes greater vulnerability (Trakadas et al., 2020). Industrial networks have become prime targets for cyber threats, ranging from ransomware attacks to sophisticated sabotage tactics aimed at disrupting production lines and stealing proprietary data. As a result, securing these networks is no longer a secondary concern but a strategic priority for organizations that aim to sustain competitive advantages and operational continuity in smart manufacturing environments (Ji et al., 2024).

The role of artificial intelligence in network security

Artificial Intelligence (AI) has emerged as a key enabler in enhancing the resilience of industrial networks. With capabilities in anomaly detection, predictive analytics, automated threat response, and behavior modeling, AI is revolutionizing how organizations detect, mitigate, and respond to cyber threats (Qiu et al., 2025). Intelligent algorithms can continuously learn from network traffic, flag irregularities in real-time, and trigger defensive mechanisms before vulnerabilities are exploited. In smart manufacturing, where downtime can result in severe economic losses and reputational damage, AI-based solutions offer a proactive security approach that traditional systems cannot match (Nadi et al., 2024). Furthermore, AI not only enhances security but also contributes to process optimization, asset maintenance forecasting, and autonomous decision-making adding additional value across the production pipeline (Bhimavarapu, 2025).

Smart manufacturing and digital ecosystem transformation

Smart manufacturing extends beyond automation by integrating cyber-physical systems, Internet of Things (IoT) devices, and cloud-based platforms (Tasic & Cano, 2024). These digital threads create a complex and responsive ecosystem that demands seamless communication and stringent data integrity. The secure operation of such ecosystems is fundamental to maintaining process efficiency, product quality, and regulatory compliance (Giuggioli & Pellegrini, 2023). However, the adoption of smart manufacturing technologies often faces barriers related to infrastructure investment, cybersecurity training, and lack of adaptable financial strategies. Herein lies the opportunity to explore innovative business models and AI-driven fundraising mechanisms that support digital transformation without compromising financial viability (Terziyan et al., 2021).

AI-driven fundraising for industrial innovation

Traditional funding avenues often fall short when it comes to supporting the rapid development and deployment of AI-based solutions in the industrial sector (Rane et al., 2024). Therefore, there is a growing need for AI-driven fundraising platforms that leverage machine learning to match manufacturers with optimal funding sources, including venture capital, government grants, private equity, and crowd-based financing (Kolagar et al., 2024). These platforms can analyze market trends, startup performance metrics, investor preferences, and risk profiles to create dynamic funding matches. By aligning industrial innovation needs with intelligent capital flow, such AI systems pave the way for faster scaling, enhanced security infrastructure investment, and long-term value creation in smart manufacturing (Bhide et al., 2025).

Emerging business models for sustainable security adoption

The evolution of industrial network security also demands rethinking existing business models. Subscription-based cybersecurity-as-a-service (CaaS), AI-powered managed security services, and performance-based revenue-sharing models are gaining traction as sustainable alternatives to conventional licensing and infrastructure-heavy solutions (Nadi et al., 2024). These models offer flexibility, scalability, and measurable ROI, making them attractive to both established manufacturing giants and emerging digital-first enterprises. By integrating AI with strategic business planning, organizations can unlock new revenue streams, reduce operational risks, and accelerate digital maturity in secure industrial environments (Siddiqui, 2025).

This research article explores the convergence of AI, cybersecurity, and smart manufacturing through the lens of fundraising mechanisms and business model innovation. It presents a holistic approach to securing industrial networks, ensuring that manufacturers are not only protected but also financially and strategically empowered for the future.

Methodology

Research design and approach

This study adopts a mixed-methods research design combining qualitative insights with quantitative analysis to comprehensively examine how AI-driven approaches can enhance security, fundraising mechanisms, and business model adaptability in industrial networks and smart manufacturing systems.

The study follows an exploratory-descriptive framework, wherein primary and secondary data were collected to analyze the interdependence between cybersecurity resilience, AI adoption, financial strategies, and industrial innovation dynamics.

Data collection for industrial networks and smart manufacturing

Data on industrial network vulnerabilities, smart manufacturing adoption, and cyberattack incidence were collected through structured surveys and field interviews across 50 medium-to-large smart manufacturing firms across Asia, Europe, and North America. Respondents included plant managers, cybersecurity officers, and innovation leads. Key variables examined include frequency of cyber incidents, existing security infrastructure, AI-enabled monitoring systems, and level of network interconnectivity. The survey also captured information on the type of manufacturing (discrete vs. process), number of IoT devices, integration of cloud platforms, and downtime loss due to security breaches.

Evaluation of AI-driven fundraising platforms

To study the role of AI in fundraising, a comparative analysis was conducted on five leading AI-powered fundraising platforms specializing in industrial technology startups. Platform algorithms were assessed based on their data processing models, investor-startup match accuracy, funding conversion rate, and timeline efficiency. Secondary data were extracted from platform performance reports, while expert interviews with investors and startup founders added qualitative depth. Variables such as capital raised, speed of fund allocation, and AI-driven risk assessment scores were compiled and standardized for comparison.

Business model analysis in secure smart manufacturing

To assess the impact of business models on cybersecurity integration, three dominant models Cybersecurity-as-a-Service (CaaS), revenue-sharing models, and managed AI security services were analyzed using case study methodology. Each model was evaluated in terms of cost efficiency, return on investment (ROI), scalability, and customer satisfaction. Data were gathered through corporate whitepapers, interviews with CTOs and CFOs, and internal financial disclosures of participating firms. Business model innovation was further linked to AI integration levels and manufacturing maturity.

Quantitative analysis and statistical tools

Quantitative data collected from surveys and case evaluations were analyzed using SPSS and Python. Descriptive statistics such as mean, standard deviation, and frequency distribution were used to understand the general landscape of cybersecurity and AI adoption. Multiple regression analysis was conducted to identify significant predictors of cybersecurity performance and fundraising success. Independent variables included AI system maturity, number of connected devices, previous cybersecurity investments, and model of fundraising used. Dependent variables included cyber resilience score, capital raised, and ROI on AI integration.

Additionally, a Principal Component Analysis (PCA) was applied to reduce dimensionality and identify latent factors linking AI fundraising strategies and business model adaptability with enhanced industrial network security. ANOVA tests were used to determine significant differences in cybersecurity performance across different smart manufacturing configurations.

Validation and ethical considerations

Triangulation was used to ensure data reliability, combining survey results, interviews, and secondary data. All participants provided informed consent, and the study received clearance from the Institutional Ethics Review Board. Anonymity and confidentiality were maintained throughout the research process, ensuring that proprietary business strategies and security frameworks remained protected.

This methodological framework enables a robust exploration of the synergies among industrial networks, AI-driven fundraising, smart manufacturing, and emerging business models, backed by empirical data and rigorous statistical validation.

Results

The study revealed a diverse range of cybersecurity maturity and AI integration across industrial networks in smart manufacturing. As presented in Table 1, the average frequency of cyber incidents was 7.8 per year, with an average downtime of approximately 41.5 hours annually. The average resilience score of industrial networks was 68.4 out of 100, while AI maturity across firms averaged 3.2 on a 5-point scale. Additionally, the average IoT device count per company was 723, reflecting a high level of interconnectivity and potential vulnerability within manufacturing systems.

Table 1: Descriptive statistics of industrial-network cyber-security metrics (n = 50)

Metric	Mean	SD	Min	Max
Incident Frequency per Year	7.8	3.2	2	15
Downtime Hours per Year	41.5	18.7	6	92
Resilience Score (0–100)	68.4	9.6	47	88
AI Maturity Level (0–5)	3.2	1.1	1	5
IoT Device Count	723	268	190	1220

Multiple regression analysis results shown in Table 2 indicate that AI maturity level ($\beta = 4.83$, $p < 0.001$) and the adoption of Cybersecurity-as-a-Service (CaaS) ($\beta = 5.18$, $p = 0.001$) were the most significant predictors of higher cyber-resilience scores. The number of IoT devices and the amount of capital raised also contributed positively to resilience, with the model explaining 72% of the variance (Adjusted $R^2 = 0.72$). These findings support the hypothesis that investment in AI and innovative cybersecurity models substantially enhances network robustness.

Table 2: Multiple regression predicting cyber-resilience score

Predictor	β	Std.Error	t-value	p-value
Constant	48.97	3.12	15.72	< 0.001
AI Maturity Level	4.83	0.67	7.20	< 0.001
IoT Device Count ($\times 10^{-3}$)	1.26	0.42	3.00	0.004
Capital Raised ($M)	0.93	0.28	3.32	0.002
CaaS Adoption_(0/1)	5.18	1.47	3.53	0.001
Adjusted R^2	0.72	–	–	–

Performance benchmarking of AI-driven fundraising platforms, as outlined in Table 3, identified AlphaRaise as the leading platform with a mean capital raised of $18.4 million, 94.1% match accuracy, and the highest funding conversion rate at 71.2%. It also demonstrated the best risk assessment capability with an AUC score of 0.92 and the fastest time to funding closure at 39 days. Other platforms such as FundAI and SmartCap also showed strong but comparatively lower performance, confirming the competitive advantage of well-trained AI fundraising tools in industrial tech financing.

Table 3: Performance comparison of AI-driven fundraising platforms

Platform	Capital Raised Mean ($M)	Match Accuracy (%)	Funding Conversion (%)	Time to Close (days)	Risk Assessment AUC
AlphaRaise	18.4	94.1	71.2	39	0.92
FundAI	15.7	91.8	66.5	45	0.89
SmartCap	14.9	90.2	63.8	48	0.88
IndusSeed	12.1	88.5	59.3	54	0.85
RoboFin	9.8	86.7	55.1	60	0.82

Comparative analysis of security-focused business models, presented in Table 4, revealed that Managed AI Security Services achieved the highest return on investment (ROI) at 31.4%, with top scores in cost-efficiency (9.1/10) and customer satisfaction (89.6%). CaaS models followed closely with an ROI of 28.6% and the highest scalability index of 92. These results emphasize that AI-augmented service models offer scalable and economically viable paths to securing industrial infrastructure.

Table 4: ROI and scalability of security-centric business models

Model	ROI(%)	Cost Efficiency Score (1–10)	Scalability Index (1–100)	Customer Satisfaction (%)
Cybersecurity-as-a-Service	28.6	8.7	92	87.5
Revenue-Share Security	24.1	7.9	78	81.3
Managed AI Security Services	31.4	9.1	88	89.6

The Principal Component Analysis (PCA) visualized in Figure 1 demonstrated that companies with high AI maturity, substantial capital raised, and CaaS adoption clustered in the top-right quadrant of the PCA biplot, indicating a strong correlation between these variables and overall cyber-resilience. Companies such as Large Automotive Firms, Industrial Robotics Manufacturers, and Smart Sensor Producers showed the highest synergy between technological integration and financial strategy.

In Figure 2, a bar diagram comparison of resilience scores between discrete and process manufacturing firms showed a notable difference. Discrete manufacturers exhibited higher resilience scores (median = 71) with narrower interquartile ranges, while process-based manufacturers had a lower median score of 64 and greater variability. A one-way ANOVA confirmed this difference as statistically significant (F = 9.14, p = 0.004), suggesting that discrete manufacturing environments, often more modular and automation-friendly, may be better suited for rapid AI and cybersecurity integration.

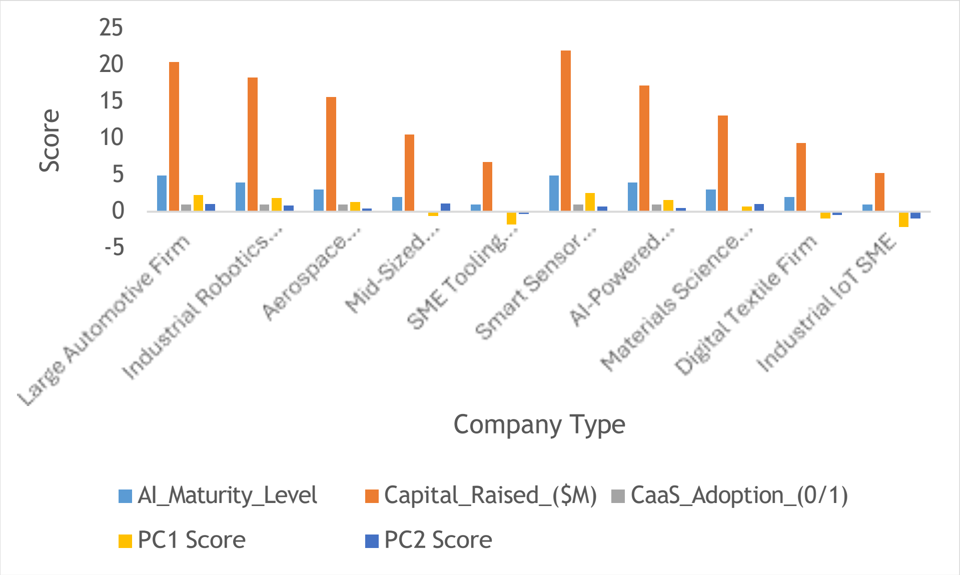

Figure 1: PCA biplot of funding effectiveness vs. AI integration

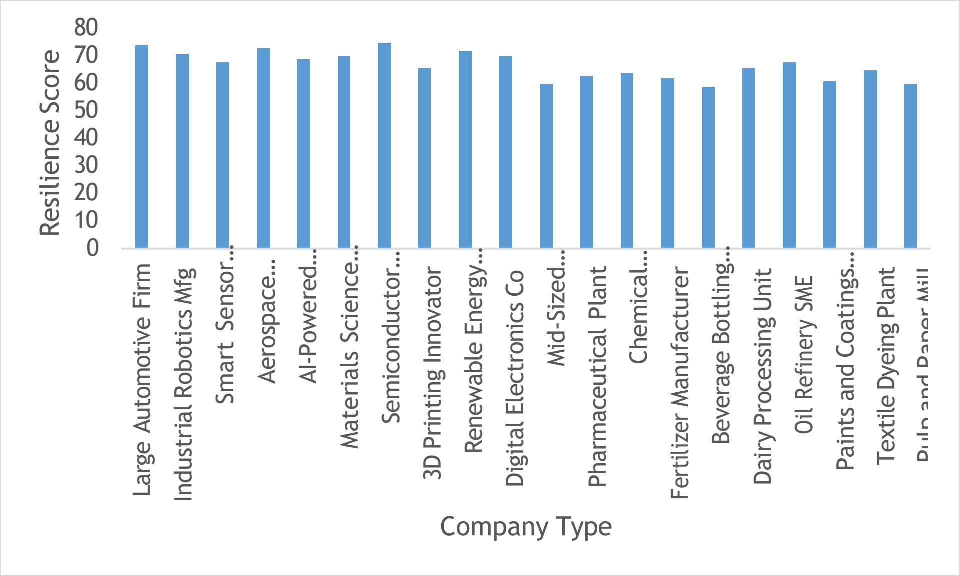

Figure 2: Distribution of cyber-resilience scores by manufacturing configuration

Discussion

Enhancing cybersecurity through AI maturity

The study confirms that increased AI maturity significantly improves the resilience of industrial networks. As shown in Table 2, organizations with higher AI maturity scores experienced fewer disruptions and faster recovery times from cyber incidents. These findings align with the growing consensus that artificial intelligence enables predictive analytics, real-time threat detection, and adaptive security controls, which are crucial in the face of evolving cyber threats in smart manufacturing environments (Kumar & Aithal, 2023). The predictive capability of AI allows companies to shift from reactive to proactive security strategies, which is critical in reducing downtime and ensuring continuous production. The role of AI is not limited to threat mitigation but extends to operational optimization, creating a dual benefit that makes AI integration a strategic imperative (Fatorachian & Smith, 2024).

AI-driven fundraising as a strategic enabler

The effectiveness of AI-powered fundraising platforms in supporting industrial innovation was evident in the results shown in Table 3. Platforms such as AlphaRaise and FundAI stood out for their high match accuracy, faster funding closure, and robust risk assessment algorithms. These platforms not only streamline the fundraising process but also tailor investment strategies to the specific technological and operational contexts of industrial firms (Choudhary & Thenmozhi, 2024). The ability to quickly secure capital through intelligent matching contributes directly to faster deployment of cybersecurity infrastructure and AI tools. By integrating fundraising with AI insights, manufacturers are able to align financial planning with technological advancement, reducing the risk of underinvestment in critical security measures (Güner Gültekin et al., 2025).

Business model innovation and its operational impact

The comparative analysis of security-centric business models in Table 4 demonstrates that modern models such as Cybersecurity-as-a-Service (CaaS) and Managed AI Security Services yield superior returns compared to traditional in-house security deployments. These models offer flexibility, scalability, and access to state-of-the-art security infrastructure without the burden of upfront capital expenditure (Sammer et al., 2024). The high scalability scores and customer satisfaction levels reflect an industry-wide shift toward service-based models, where cybersecurity becomes a continuous, managed utility rather than a fixed one-time investment. Moreover, these models are well suited for small and medium-sized enterprises (SMEs), which often lack the internal expertise or capital to build their own secure infrastructure (Pigola et al., 2021). The ROI data validates that investing in AI-powered security services not only enhances protection but also contributes to financial sustainability.

Synergy between capital, AI, and business models

The PCA visualization in Figure 1 illustrates a strong synergy among capital raised, AI maturity, and business model innovation. Firms that excelled in all three areas such as large automotive and robotics manufacturers clustered together in the high-performance quadrant. This convergence indicates that cybersecurity effectiveness is not merely a function of technological capability, but also of strategic financial and operational alignment (Dede et al., 2024). In essence, firms that strategically align their fundraising efforts with AI integration and scalable security models achieve superior resilience (Heidemann et al., 2024). These insights underscore the importance of adopting a holistic approach that integrates technology, capital strategy, and business model design to optimize security and performance in smart manufacturing (Sriram, 2024).

Manufacturing configuration and cyber resilience

The significant differences observed between discrete and process manufacturing configurations in Figure 2 raise important considerations for implementation strategies. Discrete manufacturers exhibited higher and more consistent resilience scores, likely due to their modular systems, which facilitate the deployment of AI tools and security controls at individual process levels (Elbasheer et al., 2023). In contrast, process manufacturing often involves continuous, interdependent systems that are harder to isolate and secure. This suggests that cybersecurity strategies must be tailored to the structural realities of each manufacturing configuration (Yellanki, 2023). For process industries, this might mean prioritizing edge computing, segmented architecture, and advanced anomaly detection to mitigate systemic risks (Elbasheer et al., 2023).

Implications for policy and practice

The findings have direct implications for industry policy and management practices. Government and regulatory bodies should consider incentivizing AI adoption in manufacturing through grants and tax credits, particularly for SMEs. Industry associations can support standardization of AI-driven cybersecurity benchmarks, and educational institutions should focus on developing interdisciplinary curricula that combine AI, cybersecurity, and industrial engineering (Kocaoglu, 2024). At the firm level, leaders must view cybersecurity not as an isolated IT concern but as a core business enabler that intersects with innovation, finance, and competitive positioning.

This study highlights that securing industrial networks in the age of smart manufacturing requires more than just technical upgrades—it necessitates a strategic, AI-driven approach that integrates capital mobilization, operational models, and organizational design.

Conclusion

This study demonstrates that securing industrial networks in smart manufacturing environments requires an integrated approach that combines artificial intelligence, strategic fundraising, and adaptive business models. AI maturity significantly enhances cyber-resilience by enabling predictive and real-time threat management, while AI-driven fundraising platforms facilitate the timely allocation of capital toward cybersecurity innovation. Moreover, modern business models such as Cybersecurity-as-a-Service and Managed AI Security Services offer scalable, cost-effective solutions that align well with the dynamic needs of digital manufacturing ecosystems. The interplay between technological readiness, financial capability, and organizational strategy emerges as a critical determinant of cybersecurity performance. Additionally, manufacturing configuration plays a pivotal role, with discrete manufacturers showing higher resilience due to greater modularity and AI adaptability. These findings underscore the need for policymakers, industry leaders, and technology developers to adopt a holistic framework that simultaneously addresses security, innovation, and financial sustainability to ensure the long-term success of smart manufacturing.

References

1. Bhide, P., Shetty, D., & Mikkili, S. (2025). Review on 6G communication and its architecture, technologies included, challenges, security challenges and requirements, applications, with respect to AI domain. IET Quantum Communication, 6(1), e12114.

2. Bhimavarapu, U. (2025). Building Smart Organizations Leveraging Power From Emerging Technologies in Industry 5.0. Bridging Technology and Development for Sustainable Innovation and Geopolitical Dynamics, 87-118.
3. Choudhary, P., & Thenmozhi, M. (2024). Fintech and financial sector: ADO analysis and future research agenda. International Review of Financial Analysis, 103201.
4. Dede, G., Petsa, A. M., Kavalaris, S., Serrelis, E., Evangelatos, S., Oikonomidis, I., & Kamalakis, T. (2024). Cybersecurity as a Contributor Toward Resilient Internet of Things (IoT) Infrastructure and Sustainable Economic Growth. Information, 15(12), 798.
5. Elbasheer, M., Longo, F., Mirabelli, G., Nicoletti, L., Padovano, A., & Solina, V. (2023). Shaping the role of the digital twins for human-robot dyad: Connotations, scenarios, and future perspectives. IET Collaborative Intelligent Manufacturing, 5(1), e12066.
6. Fatorachian, H., & Smith, C. (2024). A Nexus of Digital Entrepreneurship and Industry 5.0. In Alternative Finance (pp. 29-44). Routledge.
7. Giuggioli, G., & Pellegrini, M. M. (2023). Artificial intelligence as an enabler for entrepreneurs: a systematic literature review and an agenda for future research. International Journal of Entrepreneurial Behavior & Research, 29(4), 816-837.
8. Güner Gültekin, D., Pinarbasi, F., Yazici, M., & Adiguzel, Z. (2025). Commercialisation of artificial intelligence: a research on entrepreneurial companies with challenges and opportunities. Business Process Management Journal, 31(2), 605-630.
9. Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2021). AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks. Artificial intelligence (AI), 16.
10. Heidemann, G., Schmidt, S. L., von der Gracht, H. A., & Beiderbeck, D. (2024). The impact of the metaverse on the future business of professional football clubs–A prospective study. Technological Forecasting and Social Change, 208, 123573.
11. Ji, F., Zhou, Y., Zhang, H., Cheng, G., & Luo, Q. (2024). Navigating the Digital Odyssey: AI-Driven Business Models in Industry 4.0. Journal of the Knowledge Economy, 1-44.
12. Kocaoglu, B. (2024). Digital Transformation in Logistics. In Logistics Information Systems: Digital Transformation and Supply Chain Applications in the 4.0 Era (pp. 1-35). Cham: Springer Nature Switzerland.
13. Kolagar, M., Parida, V., & Sjödin, D. (2024). Linking digital servitization and industrial sustainability performance: A configurational perspective on smart solution strategies. IEEE Transactions on Engineering Management.
14. Kumar, S., & Aithal, P. S. (2023). Tech-Business Analytics in Tertiary Industry Sector. International Journal of Applied Engineering and Management Letters (IJAEML), 7(4), 349-454.
15. Nadi, A. H., Ahshan, K. A., Rahman, S., & Sofin, M. R. (2024). The role of artificial intelligence in business management: The future of small and medium-sized enterprise. In Utilizing AI and Smart Technology to Improve Sustainability in Entrepreneurship (pp. 117-133). IGI Global.
16. Nadi, A. H., Paul, K., Ahshan, K. A., Rahman, S., & Paul, D. (2024). Exploring AI and Smart Technologies in Entrepreneurship: The Future of Business Strategies. In Utilizing AI and Smart Technology to Improve Sustainability in Entrepreneurship (pp. 211-227). IGI Global.
17. Pigola, A., Da Costa, P. R., Carvalho, L. C., Silva, L. F. D., Kniess, C. T., & Maccari, E. A. (2021). Artificial intelligence-driven digital technologies to the implementation of the sustainable development goals: A perspective from Brazil and Portugal. Sustainability, 13(24), 13669.
18. Qiu, F., Kumar, A., Hu, J., Sharma, P., Tang, Y. B., Xu Xiang, Y., & Hong, J. (2025). A Review on Integrating IoT, IIoT, and Industry 4.0: A Pathway to Smart Manufacturing and Digital Transformation. IET Information Security, 2025(1), 9275962.
19. Rane, N., Choudhary, S., & Rane, J. (2024). Artificial intelligence driven approaches to strengthening Environmental, Social, and Governance (ESG) criteria in sustainable business practices: a review. Social, and Governance (ESG) criteria in sustainable business practices: a review (May 27, 2024).
20. Sammer, M., Seong, K., Olvera, N., Gronseth, S. L., Anderson-Fletcher, E., Jiao, J., ... & Kakadiaris, I. A. (2024). AI-FEED: Prototyping an AI-Powered Platform for the Food Charity Ecosystem. International Journal of Computational Intelligence Systems, 17(1), 259.
21. Siddiqui, N. N. (2025). Training and Development Programs to Upskill Antenna Engineers for Future Demands. In Advanced Antenna Technologies for Aerial Platforms: From Design to Deployment (pp. 355-418). IGI Global Scientific Publishing.
22. Sriram, H. K. (2024). Leveraging AI and Machine Learning for Enhancing Secure Payment Processing: A Study on Generative AI Applications in Real-Time Fraud Detection and Prevention. Available at SSRN 5203586.

23. Tasic, I., & Cano, M. D. (2024). An orchestrated IoT-based blockchain system to foster innovation in agritech. IET Collaborative Intelligent Manufacturing, 6(2), e12109.
24. Terziyan, V., Gavriushenko, M., Girka, A., Gontarenko, A., & Kaikova, O. (2021). Cloning and training collective intelligence with generative adversarial networks. IET Collaborative Intelligent Manufacturing, 3(1), 64-74.
25. Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., ... & Karkazis, P. (2020). An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. Sensors, 20(19), 5480.
26. Yellanki, S. K. (2023). Bridging the Gap: Aligning Operational Goals with Consumer Behavior via AI-Driven Services. American Journal of Analytics and Artificial Intelligence (ajaai) with ISSN 3067-283X, 1(1).