Applied AI Letters

WILEY

PERSPECTIVE OPEN ACCESS

Unlocking IIoT Potential: A Systematic Review of AI Applications, Adoption Drivers, and Implementation Barriers

Tinashe Magara | Mampilo Phahlane

Department of Information Systems, College of Science, Engineering, and Technology, University of South Africa, Pretoria, South Africa

Correspondence: Tinashe Magara (tinashenosh@gmail.com)

Received: 21 August 2025 | **Accepted:** 17 November 2025

Keywords: AI adoption | AI taxonomy | artificial intelligence (AI) | cybersecurity | federated learning | industrial internet of things (IIoT) | technology

ABSTRACT

Artificial Intelligence (AI) is playing an increasingly vital role in the Industrial Internet of Things (IIoT), enabling predictive analytics, real-time monitoring, and autonomous operations across industries such as manufacturing, logistics, and energy. However, widespread adoption is hindered by technological, organizational, and infrastructural challenges. This paper examines the adoption, application, and challenges of AI–IIoT environments, focusing on implementation domains, adoption drivers, enabling technologies, and key barriers. We conducted a Systematic Literature Review (SLR using PRISMA). Peer-reviewed English-language journal articles published between 2018 and 2025 were sourced from ScienceDirect, Web of Science (WoS), Scopus, IEEE Xplore, Springer, Google Scholar, Elsevier, and Taylor & Francis. After applying inclusion criteria and screening procedures, 46 relevant journal articles were included for analysis. Key AI applications identified include predictive maintenance, anomaly detection, real-time monitoring, autonomous process control, and smart supply chains. Adoption is facilitated by external enablers 5G infrastructure, regulatory support, and internal factors, organizational readiness, and workforce skills. Challenges include data quality issues, cybersecurity risks, legacy system integration, and limited model scalability. Technologies such as edge computing, cloud platforms, and federated learning are instrumental in mitigating these challenges. While adoption is growing, significant barriers remain. AI has the potential to drive operational efficiency and innovation in IIoT, provided these constraints are addressed. This paper offers a comprehensive taxonomy of AI applications and proposes a framework of adoption factors, offering valuable insights for researchers, practitioners, and policymakers involved in AI-driven industrial transformation.

1 | Introduction

The integration of the Industrial Internet of Things (IIoT) and artificial intelligence (AI) is driving a paradigm shift in industrial operations by enabling advanced automation, real-time decision-making, and predictive analytics within the broader context of digital transformation [1–3]. According to the IDC report, it is predicted that in 2025 IoT devices will produce more than 90 zettabytes of data [4]. However, [5] argued that from the generated data only a small portion of this data is being used efficiently. Kalla and Smith highlighted the application of AI, especially concatenating machine learning and deep learning with IIoT systems, help make better use of the data by improving efficiency, allowing for self-management, predicting maintenance needs, and analyzing data in real-time [6]. Lv et al. highlighted that organizations are significantly utilizing AI-enabled IIoT as a driver for competitive advantage, resilience, and sustainability, making this transition not simply technological but strategic [7].

However, despite its revolutionary potential, Hou et al. pointed out that the AI's adoption in IIoT systems is still an unequal and scattered paradigm [8]. According to [9–11] highlighted the common challenges of AI adoption in IIoT systems include cybersecurity threats, low-quality data, a shortage of qualified personnel, and troubles integrating AI with older systems. While AI and IIoT research is expanding rapidly, there are significant challenges [12, 13] hindering scalable IIoT adoption [14]. IIoT systems themselves consist of interconnected sensors, devices, and actuators that enable continuous monitoring and control of industrial processes, significantly improving efficiency, safety, and resource utilization [15]. AI enhances these capabilities by enabling applications such as predictive maintenance, anomaly detection, and intelligent supply chain management [16]. However, large-scale IIoT deployments face significant challenges in managing massive heterogeneous datasets while safeguarding sensitive operational data against increasingly sophisticated cyber-physical threats [17]. Building resilient, secure, and trustworthy AI-enabled IIoT architectures requires coordinated advancements in encryption, authentication, edge computing, and federated learning [18].

Although AI has reached considerable maturity as a discipline, its systematic integration into IIoT remains under-theorized and inconsistently executed across industries. Existing studies tend to address isolated dimensions such as algorithmic improvements, sector-specific use cases, or isolated security issues without offering a comprehensive synthesis. This leaves a critical gap for a structured review that consolidates fragmented knowledge and provides a unified analytical framework for adoption, application, and challenge dimensions.

This article conducts a Systematic Literature Review (SLR) using the PRISMA technique to fill this gap. It covers peer-reviewed English-language journal papers published between 2018 and 2025 in a variety of industrial domains, including manufacturing, logistics, energy, and agriculture. The review excludes gray literature, non-peer-reviewed sources, and studies focusing exclusively on consumer IoT or algorithmic innovation without applied context.

The main contributions of this study are as follows:

- *Comprehensive Synthesis*: Presents the most current synthesis of peer-reviewed literature on AI adoption and application in IIoT, bridging fragmented insights across technical, organizational, and sectoral dimensions.
- *Application Taxonomy*: Develops a detailed taxonomy of AI use cases in IIoT, highlighting core domains such as predictive maintenance, anomaly detection, real-time monitoring, autonomous control, and intelligent supply chain management.
- *Adoption Drivers and Barriers*: Systematically classifies adoption enablers and constraints using established frameworks, differentiating external factors from internal capabilities.
- *Enabling Technologies*: Analyzes the role of advanced technologies such as edge computing, cloud platforms, and federated learning in enabling secure, scalable, and real-time AI integration within IIoT ecosystems.
- *Integrative Framework*: Proposes a unified adoption framework that connects theoretical perspectives with actionable strategies, offering practical guidance for researchers, industry practitioners, and policymakers.

This paper aims to enhance knowledge, guide strategic industrial adoption, and pinpoint promising avenues for further study by combining and evaluating the current state of research in AI-enabled IIoT.

The remainder of this paper is organized as follows: Section 2 outlines the theoretical background underpinning the research. Section 3 details the research methodology. Section 4 presents the empirical findings. Section 5 provides a comprehensive discussion, addressing theoretical contributions and practical implications. Finally, Section 6 concludes the paper, highlighting its limitations and directions for future research.

2 | Background

2.1 | Industrial Internet of Things

Through the application of IoT technology to industrial environments, the Industrial Internet of Things (IIoT) links sensors, control systems, and machinery to facilitate constant data interchange with little assistance from humans [19]. With its ability to provide real-time monitoring, automation, and predictive analytics, IIoT, which first emerged in the early 2010s as an advancement of machine-to-machine communication, is now essential to Industry 4.0 [20]. Unlike consumer IoT, IIoT operates in mission-critical environments including industrial, energy, and transportation where security, scalability, and reliability are essential [21].

AI integration improves IIoT by enabling predictive maintenance, intelligent control, and autonomous optimization. Examples include computer vision for automated inspection and deep learning models that predict equipment breakdowns, decreasing downtime and expenses [22]. This AI–IIoT convergence, often termed AIoT, is transforming industries into adaptive, self-optimizing ecosystems [23]. Advantages of IIoT include improved operational efficiency, enhanced safety, reduced maintenance costs, and data-driven decision-making [24]. However, adoption faces barriers such as data heterogeneity, cybersecurity risks, legacy system constraints, and workforce skill gaps. Addressing these challenges is critical to realizing the full transformative potential of IIoT.

2.2 | Role of AI in IIoT

The intelligence layer of IIoT is artificial intelligence, which includes machine learning (ML), deep learning (DL), and reinforcement learning (RL). This allows for autonomous decision-making, pattern recognition, and prediction [25]. Applications range from predictive maintenance, which eliminates unplanned downtime, to deep learning-based quality inspection, which detects microscopic flaws. The merging of AI and IIoT, dubbed Artificial Intelligence of Things (AIoT), provides adaptive, self-optimizing systems with significant implications for supply chain resilience, personalization, and sustainability [26]. When paired with edge computing and 5G, AIoT enables low-latency, distributed intelligence for mission-critical operations.

Technical obstacles including data heterogeneity, model interpretability, and legacy system integration, however, continue to make adoption unequal. While cybersecurity and privacy issues necessitate strong measures, organizational challenges include talent shortfalls and unwillingness to change [27]. It's critical to strike a balance between edge and centralized cloud AI. While edge improves speed and privacy but restricts computing capacity, cloud enables scalability but adds latency. A hybrid strategy that allows for distributed model training without centralizing sensitive data is provided by federated learning [28].

AI essentially drives operational efficiency, accuracy, and adaptability as the IIoT's decision-making core. Cross-disciplinary cooperation and innovation are needed to overcome enduring organizational, technological, and regulatory obstacles in order to realize its full potential.

2.3 | Theoretical Frameworks

This paper synthesizes established models from organizational innovation and technology diffusion literature to examine the adoption of artificial intelligence (AI) in the Industrial Internet of Things (IIoT), tailoring them to the specific operational, safety, and scalability requirements of the industrial context. A macro-level structure is offered by the Technology–Organization–Environment (TOE) framework [29], which divides adoption determinants into:

- Technological context: AI–IIoT technologies' maturity and capabilities, including interoperability, cybersecurity protections, and infrastructure readiness.
- Organizational context: Internal resources and preparedness elements, including workforce competencies, digital infrastructure, leadership commitment, and an innovative culture.
- Environmental context: External factors influencing strategic adoption include industry standards, competitive dynamics, and regulatory requirements.

The Unified Theory of Acceptance and Use of Technology (UTAUT) [30] and the Technology Acceptance Model (TAM) [31] provide micro-level insights into user acceptance to supplement TOE's macro view. When evaluating workforce preparedness for AI–IIoT integration, key characteristics such as perceived utility, perceived ease of use, social influence, and behavioral intention are essential.

Although TOE, TAM, and UTAUT have been proven in fields including cloud adoption, smart cities, and healthcare, their combined use in AI–IIoT is still in its infancy. These frameworks must be modified to meet the unique needs of the IIoT, which include real-time analytics, low-latency decision-making, and safety-critical operations. Figure 1 presents the integrated theoretical framework that enables a systematic analysis of how organizational preparedness, technological capabilities, and environmental pressures interact with human acceptability factors to influence AI adoption outcomes. This method provides a comprehensive, multi-layered framework that goes beyond disjointed investigations by combining macro- and micro-level viewpoints. Additionally, it facilitates comparative sectoral analysis and aids in locating leverage areas to speed up the adoption of safe, scalable AI in industrial settings.

3 | Methodology

3.1 | Review Protocol

This study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines [32] to ensure methodological rigor, transparency, and replicability. The review was conducted according to the Systematic Literature Review (SLR) framework of [33], which defines SLR as a method for identifying, evaluating, and synthesizing existing research through a reproducible, explicit, and comprehensive approach. Four principles guided this process:

1. *Systematicity*: A structured, multi-phase protocol.
2. *Explicitness*: Transparent reporting of search, screening, and synthesis steps.
3. *Comprehensiveness*: Broad coverage of relevant literature.
4. *Reproducibility*: Sufficient documentation for independent replication.

The research was guided by three research questions that guided the review:

RQ$_1$: What are the predominant application domains of AI–IIoT across industrial sectors?

RQ$_2$: What key drivers and barriers influence AI adoption in IIoT environments?

RQ$_3$: Which enabling technologies support effective AI deployment in IIoT ecosystems?

3.2 | Search Strategy and Selection

To ensure comprehensive coverage, the literature search was conducted across seven primary databases recognized for their relevance and indexing quality:

- *IEEE Xplore*: Leading repository for IIoT and AI technical research.
- *Scopus and Web of Science*: Multidisciplinary sources with rigorous indexing standards.
- *ScienceDirect and Elsevier*: Strong in engineering and technology-focused studies.

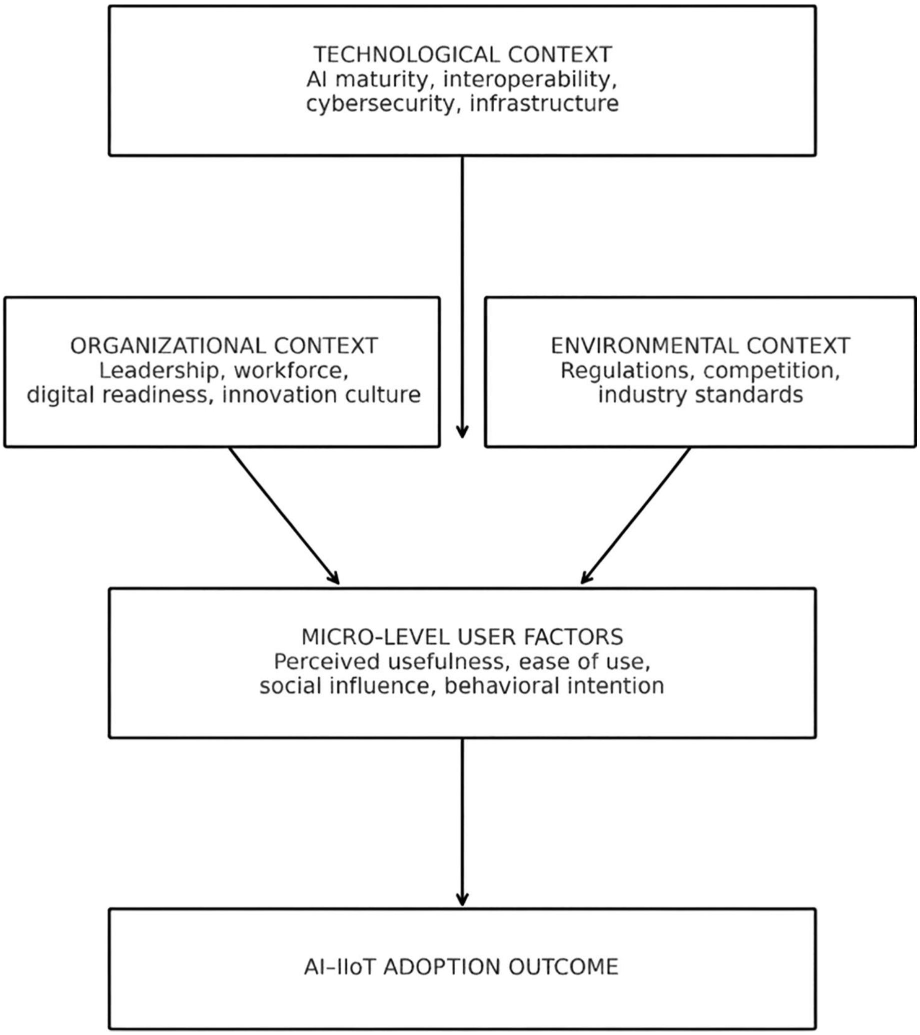

FIGURE 1 | Integrated theoretical framework for AI adoption in IIoT.

- *SpringerLink*: Rich in industrial application case studies.
- *Taylor & Francis*: Cross-sector insights into policy and implementation.

Google Scholar was employed exclusively for forward and backward citation tracking, in line with systematic review quality guidelines [34].

3.2.1 | Search Query

Boolean search strings were developed based on the study's objectives, focusing on the adoption, application, and implementation of AI in IIoT. The standardized query applied across all databases was: (“Artificial Intelligence” OR AI OR “Machine Learning” OR “Deep Learning”) AND (“Industrial Internet of Things” OR IIoT OR “Industrial IoT” OR “Industry 4.0”) AND (“Adoption” OR “Implementation” OR “Application” OR “Deployment”).

The search targeted Title, Abstract, and Keywords fields.

Preliminary Screening—Retrieved records were filtered using eligibility criteria:

- *Inclusion*: Peer-reviewed journal articles, English language, published between January 2018 and March 2025.
- *Exclusion*: Non-English works, conference proceedings, book chapters, and studies focusing solely on consumer IoT or algorithmic development without IIoT context.

Titles, abstracts, and keywords were examined to exclude irrelevant studies.

3.3 | Screening and Inclusion Criteria

Duplicate records obtained from several databases were eliminated after article identification, resulting in a more streamlined pool for screening. To assess preliminary relevance, abstracts and titles were examined separately. Studies that focused on Artificial Intelligence (AI) in Industrial Internet of Things (IIoT) contexts and satisfied the basic scope were kept for additional analysis.

Inclusion criteria were as follows:

- Empirical studies or case studies examining AI integration in IIoT.
- Technical or organizational analyses of AI adoption.
- Explicit discussion of adoption drivers, barriers, and enabling factors.

Exclusion criteria included:

- Studies focused solely on consumer IoT applications.
- Conceptual or theoretical papers without empirical validation.
- Non-English publications.

In the final inclusion stage, full-text articles were assessed to ensure methodological rigor and alignment with the study's objectives. This process resulted in a final corpus of 46 peer-reviewed journal articles published between January 2018 and March 2025. These articles collectively provided comprehensive insights into AI adoption drivers, barriers, and enabling technologies across diverse industrial sectors. PRISMA principles were followed during the stepwise screening process, guaranteeing methodological transparency and reproducibility (Figure 2).

3.4 | Data Extraction and Analysis

A structured coding scheme was used to methodically extract data from the final collection of 46 included research articles. The industrial sector, AI application, adoption drivers, barriers, and enabling technologies were all coded for each record.

3.4.1 | Analysis Techniques

Three complimentary methods of analysis were used:

- RQ_1 (application domains) thematic analysis
- RQ_2 (barriers/drivers) causal network mapping
- RQ_3 (enabling technology) technology-function matrix

4 | Results

4.1 | Trends

The literature synthesis reveals a clear surge of scholarly interest in AI within the IIoT domain, with publication activity accelerating after 2019 and reaching its peak during the 2021–2025

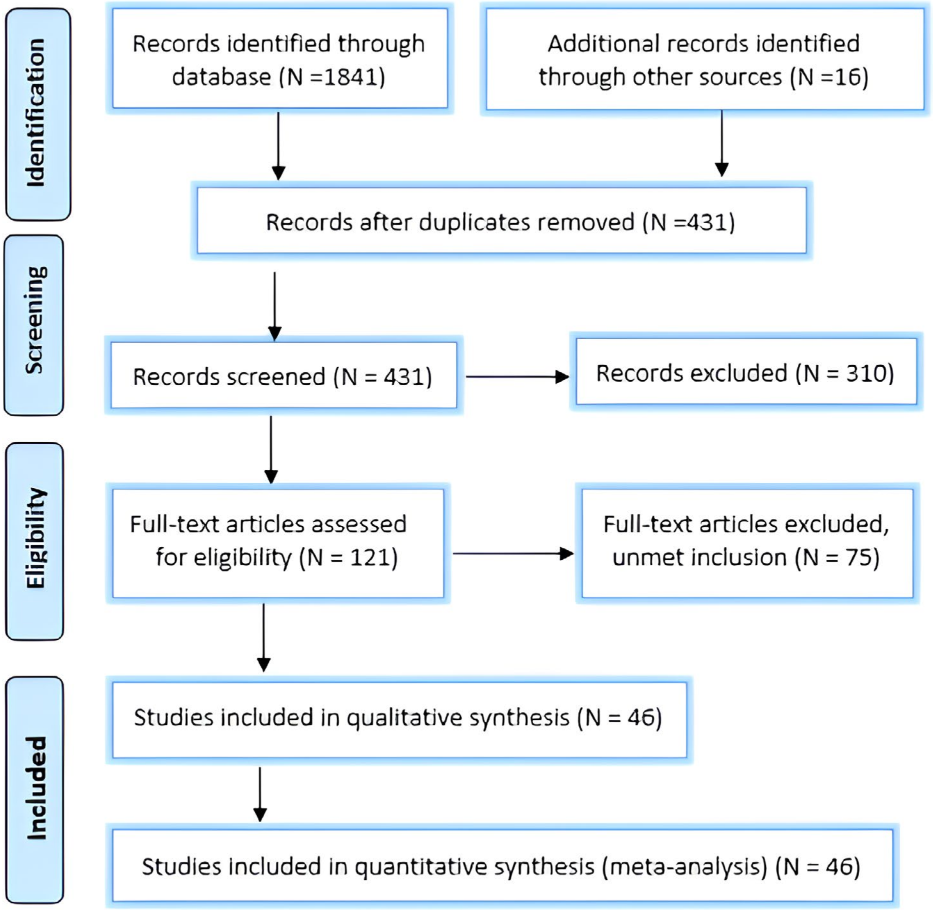

FIGURE 2 | PRISMA flow diagram of literature search and selection.

period. This trajectory aligns with the rapid maturation of Industry 4.0 and the recognition of AI as a foundational enabler of intelligent, data-driven industrial ecosystems [35, 36]. The majority of contributions appeared in high-impact journals spanning artificial intelligence, IoT, and industrial engineering, underscoring the strong interdisciplinary engagement driving this research agenda [37].

In terms of sectoral distribution, manufacturing, particularly smart factories and process industries, dominated the discourse, accounting for the largest share of reviewed studies. Logistics and energy followed as secondary domains, while applications in smart cities and urban infrastructure remained underexplored [38]. This concentration illustrates the field's production-centric orientation and reveals a gap in research addressing cross-sectoral or service-oriented IIoT contexts [39].

Methodologically, the analysis shows that deep learning techniques, especially convolutional neural networks (CNNs) and recurrent neural networks (RNNs), were the most frequently employed, alongside support vector machines (SVMs) and hybrid models [40]. These were commonly integrated with high-frequency sensor data streams to enable predictive maintenance, anomaly detection, and automated quality inspection. Recent studies, however, increasingly emphasize edge AI, reflecting the critical need for latency-sensitive, privacy-preserving analytics deployed closer to industrial devices and gateways [41].

Thematic trends highlight a growing shift toward data-intensive learning models capable of processing high-dimensional, heterogeneous IIoT datasets. At the same time, there is rising attention to the ethical, safety, and trust dimensions of AI, acknowledging the operational and economic risks inherent in safety-critical environments [42]. Collectively, these findings suggest that while research has made significant strides in technical applications, the field is gradually broadening to include socio-technical considerations essential for sustainable and trustworthy AI adoption in IIoT.

4.2 | Taxonomy of AI Applications

The systematic literature synthesis identified six dominant domains of AI applications within IIoT environments: predictive maintenance, process optimization, anomaly and fault detection, quality control and inspection, real-time monitoring and control, and supply chain and logistics (Figure 3). These categories illustrate both the breadth of industrial functions where AI is deployed and the depth of task-specific optimization achievable through machine learning, deep learning, and hybrid approaches [43, 44].

Predictive maintenance emerged as the most widely cited application, underscoring its critical role in reducing operational costs, extending equipment lifespans, and minimizing unplanned downtime [45]. Studies highlighted the superiority of AI models, particularly temporal sequence learning applied to sensor data, over rule-based systems in detecting early failure patterns. However, challenges such as class imbalance and limited labeled datasets continue to hinder predictive accuracy [46].

Process optimization represents a rapidly expanding application area, where reinforcement learning and heuristic optimization are employed to improve energy efficiency, throughput, and adaptive control [47]. Despite promising results, scalability and computational overhead in large-scale industrial systems remain major barriers [48].

Anomaly and fault detection is extensively applied in manufacturing and energy domains, enabling AI models to capture subtle deviations in production lines, machinery, and cyber-physical systems [49]. Compared to traditional threshold-based methods, AI provides higher sensitivity, yet the lack of interpretability in deep learning models limits trust in industrial decision-making [50].

Quality control and inspection, often driven by computer vision and pattern recognition, automates defect detection in processes and products. This enhances precision and reduces reliance on manual inspection, improving consistency [51]. Nonetheless, many studies note that domain-specific training data restrict cross-domain generalizability [52].

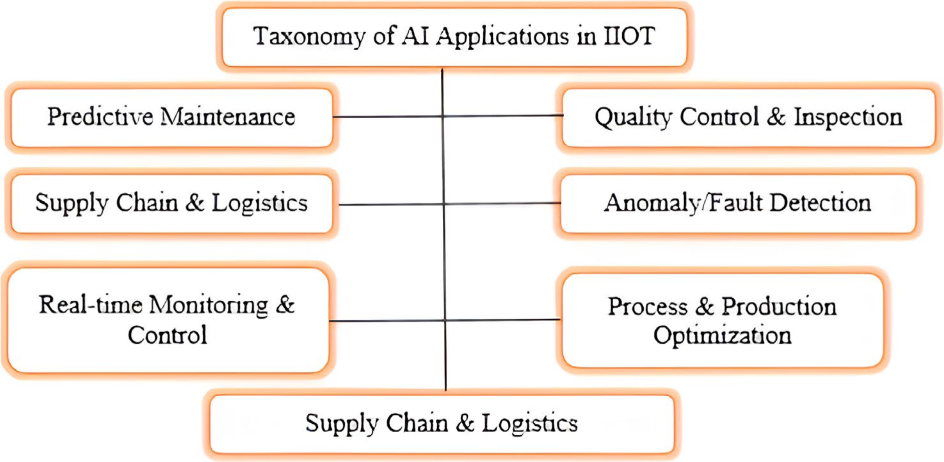

FIGURE 3 | Taxonomy of AI applications in IIoT.

Real-time monitoring and control showcases AI's capability to handle high-frequency sensor streams for dynamic operational adjustments, including adaptive scheduling, load balancing, and safety-critical monitoring [53]. Edge AI is increasingly integrated to address latency and privacy needs, though compatibility with legacy infrastructure poses persistent challenges [54].

Finally, supply chain and logistics applications demonstrate AI's capacity to optimize demand forecasting, routing, and inventory management [55]. These implementations enhance resilience and efficiency but rely heavily on harmonized, high-quality data from geographically dispersed sources, a limitation highlighted in multiple studies [56].

Collectively, the taxonomy reveals that while predictive maintenance dominates scholarly attention, emerging domains such as real-time monitoring and supply chain resilience signal a diversification of AI applications across IIoT. Figure 3 summarizes these categories, providing a structured view of how AI contributes to intelligent, adaptive, and data-driven industrial ecosystems.

4.3 | Adoption Drivers and Barriers

The synthesis of 46 peer-reviewed studies revealed that the adoption of Artificial Intelligence (AI) in the Industrial Internet of Things (IIoT) is shaped by both external and internal antecedents, each exerting enabling and inhibiting effects on implementation outcomes. These findings are summarized in Figure 4, which integrates the drivers and barriers most frequently emphasized across the reviewed literature.

From an external perspective, technological readiness was the most cited enabler, with studies highlighting the importance of edge–cloud integration, real-time analytics, interoperability, and cybersecurity maturity in supporting scalable deployment of AI solutions [57, 58]. Regulatory and standards readiness also emerged as a recurring theme, with compliance to ISO/IEC frameworks, data governance regulations, and sovereignty laws providing legitimacy and trust in industrial environments [59]. Additionally, market and ecosystem readiness, encompassing vendor maturity, data-sharing consortia, and the availability of skilled integrators, was identified as critical for fostering cross-organizational collaboration and knowledge exchange [60].

On the internal side, organizational readiness featured prominently, with leadership commitment, strategic alignment, and IT infrastructure modernization serving as key determinants of AI success [61]. Operational readiness, including the integration of AI with operational technology (OT), high-quality sensor data, and predictive maintenance workflows, was also recognized as a central adoption driver [62]. Finally, workforce readiness was widely discussed, emphasizing the role of employee upskilling, training, and trust in AI systems for predictive and prescriptive decision-making [63].

Despite these enablers, the literature consistently reported persistent barriers. Technological inhibitors include poor interoperability, heterogeneous data, and limited scalability of AI models in real-time contexts [64]. Organizational challenges such as shortages of AI talent, cultural resistance, and misalignment between AI initiatives and business priorities further slow adoption [65]. From an environmental perspective, fragmented

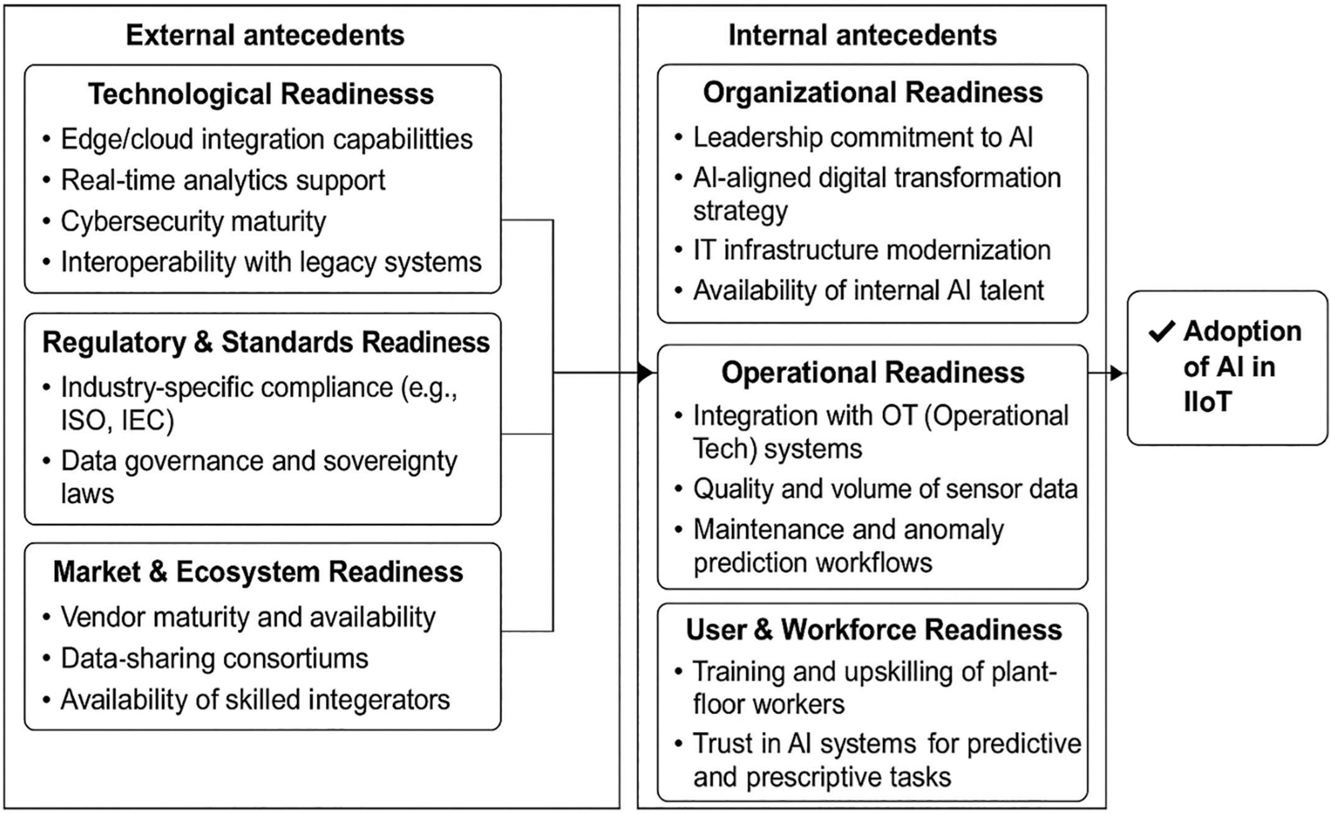

FIGURE 4 | Adoption of AI in the IIOT model. *Source:* Authors' own work.

regulatory frameworks and immature vendor ecosystems were identified as systemic barriers, creating uncertainty and risk for early adopters [66].

Overall, the results from the literature synthesis demonstrate that AI adoption in IIoT is not determined by a single dimension but by the alignment of technical, organizational, and environmental readiness with workforce acceptance. As illustrated in Figure 4, adoption success depends on mitigating structural barriers while leveraging key enablers, offering a roadmap for researchers and practitioners seeking to accelerate AI-driven industrial transformation.

4.4 | Enabling Technologies

The synthesis of the reviewed literature highlights edge computing, cloud platforms, and federated learning as pivotal enablers for effective AI deployment in IIoT environments. These technologies address fundamental challenges of latency, scalability, and privacy, which are frequently cited as barriers to industrial adoption [41, 67].

Edge computing is increasingly emphasized for its ability to perform real-time analytics at the device or gateway level, reducing reliance on centralized data centers and mitigating latency in safety-critical operations [68]. This decentralization also enhances privacy by limiting raw data transmission outside the industrial site.

Cloud platforms provide the computational scalability and storage capacity necessary for handling high-dimensional sensor data and training complex AI models. Studies show that cloud-based architectures enable flexible resource allocation, integration across distributed sites, and support for continuous model updates [69, 70]. However, concerns about data sovereignty and vendor lock-in persist.

Federated learning represents an emerging paradigm that allows collaborative model training across organizations and devices without centralizing sensitive data [71]. This approach simultaneously enhances privacy, ensures compliance with data governance regulations, and enables cross-sectoral knowledge sharing. Nonetheless, heterogeneity in data quality and communication overhead remains unresolved limitations [72].

Taken together, these enabling technologies provide the infrastructural backbone for scalable, secure, and efficient AI–IIoT integration, as summarized in Figure 5, which maps their role in addressing adoption barriers. The findings underscore that the future of AI in IIoT will increasingly depend on hybrid infrastructures that balance local responsiveness with global scalability.

5 | Discussion

5.1 | Theoretical Implications

This review systematically addressed the three guiding research questions through a structured synthesis of 46 peer-reviewed studies. In response to RQ_1, the findings reveal a diverse taxonomy of AI applications in IIoT, with predictive maintenance, process optimization, anomaly detection, quality control, and logistics emerging as dominant domains [45, 47]. Predictive maintenance, in particular, has received disproportionate attention, highlighting its potential for reducing downtime and extending equipment lifespans [73]. However, limitations such as data imbalance and poor label availability remain major obstacles, reducing predictive accuracy [46]. By explicitly linking algorithmic methods such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and reinforcement learning to these application domains, this study extends prior models of industrial AI deployment and underscores the task-specific optimization capabilities of modern machine learning techniques [3].

Addressing RQ_2, the synthesis integrates the Technology Organization Environment (TOE) framework with micro-level models of technology acceptance (TAM and UTAUT). Adoption determinants extend beyond technological maturity such as interoperability, cybersecurity, and infrastructure readiness to include organizational resources (leadership commitment, digital literacy, innovation culture) and user acceptance factors

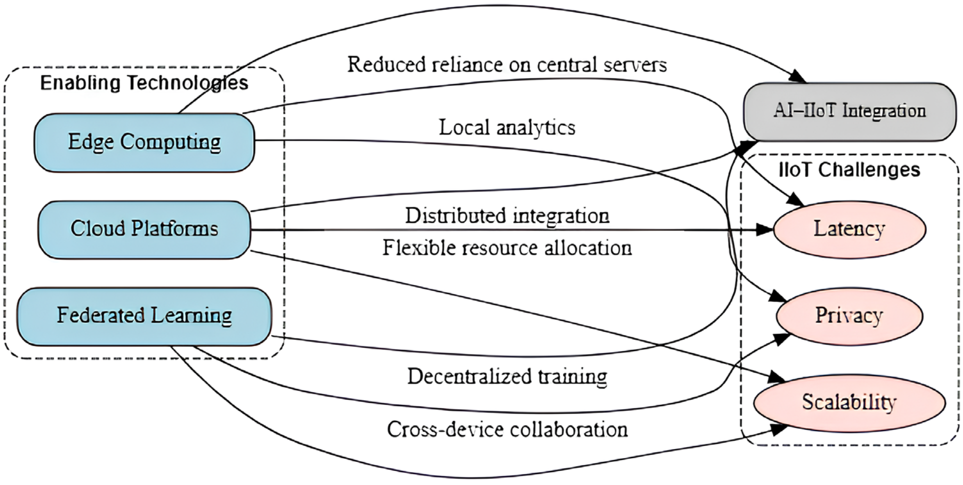

FIGURE 5 | Enabling technologies and their role in addressing IIoT challenges.

(perceived usefulness, trust, and social influence) [25]. This confirms that adoption is inherently multi-faceted, shaped by both systemic constraints and individual behavioral intentions.

For RQ_3, enabling technologies such as edge computing, cloud platforms, and federated learning emerged as critical for addressing latency, scalability, and privacy challenges [25]. Edge computing reduces communication delays for real-time control in safety-critical environments, while cloud systems facilitate scalable storage and analytics. Federated learning, though nascent, provides a promising pathway for privacy-preserving model training in distributed industrial ecosystems.

This integrated framework extends the TOE model to IIoT contexts, uniquely combining macro-level infrastructure readiness with micro-level acceptance constructs, thereby offering a more holistic theoretical lens for studying AI–IIoT adoption.

5.2 | Practical Implications

The findings have direct relevance for practitioners and policymakers. Industrial organizations seeking to unlock AI's potential in IIoT should invest in robust data infrastructures, including standardized pipelines and interoperable protocols, as AI accuracy hinges on high-quality, consistent data. Cybersecurity must be treated as foundational, with proactive measures such as intrusion detection, secure communication, and continuous system updates. Gradual integration strategies, via pilot projects and hybrid edge–cloud architectures, can minimize legacy system incompatibilities while fostering operator trust. Workforce training in AI and data analytics remains essential for bridging skill gaps and ensuring human readiness for deployment. Policymakers, meanwhile, can facilitate adoption by clarifying regulatory frameworks, incentivizing industrial AI initiatives, and mandating sector-specific safety standards.

5.3 | Ethical and Regulatory Considerations

The literature also reveals growing concern around AI ethics, interpretability, and safety in IIoT contexts. Black-box deep learning models raise interpretability challenges that complicate industrial decision-making in safety-critical sectors. Algorithmic bias and fairness issues further undermine trust, particularly when AI decisions affect operational reliability or worker safety. The adoption of explainable AI (XAI) frameworks and transparent governance mechanisms is therefore vital to maintain accountability. Regulatory oversight should evolve to address sector-specific risks, particularly in energy, manufacturing, and transportation where failures may have cascading societal and economic consequences.

In sum, the synthesis confirms that AI adoption in IIoT transcends purely technological concerns: it represents a multi-layered transformation that demands robust infrastructure, organizational alignment, user trust, and regulatory safeguards. By unifying fragmented findings across disciplines, this study provides a holistic roadmap for both scholars and practitioners, advancing understanding of how AI can be systematically and responsibly deployed in Industry 4.0 ecosystems.

6 | Conclusion

This systematic analysis looked at the applications, acceptable criteria, and implementation challenges of AI in IIoT contexts, encompassing 46 peer-reviewed publications published between 2018 and 2025. Supply chain management, anomaly detection, process optimization, quality control, real-time monitoring, and predictive maintenance are the six key application domains that the study identified to show how AI may help with data-driven industrial optimization. The external elements that influence adoption include technology and regulatory preparedness, whereas the internal factors are organizational capabilities, personnel competences, and user trust.

Deployment is nevertheless hampered by enduring issues such as data heterogeneity, cybersecurity flaws, legacy system interaction, and limited model scalability.

By lowering latency, guaranteeing scalability, and protecting data privacy, the assessment emphasizes enabling technologies like edge computing, cloud platforms, and federated learning as essential to removing these obstacles. When taken as a whole, these results provide a theoretical contribution and a useful road map for the adoption of industrial AI by incorporating user-level acceptance variables into the Technology Organization Environment paradigm.

Although AI has shown promise in revolutionizing IIoT, its long-term implementation necessitates strong data governance, hybrid infrastructure plans, and legal protections. Longitudinal studies, sector-specific comparison assessments, and empirical validation of adoption frameworks should be the focus of future research, especially when it comes to new paradigms like edge-cloud hybridization, trustworthy AI, and massive language models in IIoT. Scholars and practitioners may more fully unleash AI's potential to propel resilient, intelligent, and morally sound industrial transformation by filling in these gaps.

Funding

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

1. L. Bu, Y. Zhang, H. Liu, X. Yuan, J. Guo, and S. Han, "An IIoT-Driven and AI-Enabled Framework for Smart Manufacturing System Based on Three-Terminal Collaborative Platform," *Advanced Engineering Informatics* 50 (2021): 101370.

2. Y. Hu, Q. Jia, Y. Yao, et al., "Industrial Internet of Things Intelligence Empowering Smart Manufacturing: A Literature Review," *IEEE Internet of Things Journal* 11, no. 11 (2024): 19143–19167.

3. S. De, M. Bermudez-Edo, H. Xu, and Z. Cai, “Deep Generative Models in the Industrial Internet of Things: A Survey,” *IEEE Transactions on Industrial Informatics* 18, no. 9 (2022): 5728–5737.

4. R. David, G. John, R. John, et al., *Data Age 2025: The Digitization of the World* (IDC, 2023).

5. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” *Future Generation Computer Systems* 29, no. 7 (2013): 1645–1660.

6. D. Kalla and N. Smith, “Integrating IoT, AI, and Big Data for Enhanced Operational Efficiency in Smart Factories,” *Educational Administration: Theory and Practice* 30, no. 5 (2024): 14235–14245.

7. Z. Lv, L. Qiao, S. Verma, and V. Kavita, “AI-Enabled IoT-Edge Data Analytics for Connected Living,” *ACM Transactions on Internet Technology* 21, no. 4 (2021): 1–20.

8. K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou, and C. de Vaulx, “Trends and Challenges in AIoT/IIoT/IoT Implementation,” *Sensors* 23, no. 11 (2023): 5074.

9. A. A. Alli, K. Kalinaki, M. Fahadi, and L. Ibrahim, “Securing Industrial Internet of Things (IIoT): A Review of Technologies, Strategies, Challenges, and Future Trends,” in *Artificial Intelligence Solutions for Cyber-Physical Systems* (Auerbach Publications, 2024), 244–263.

10. A. Goknil, P. Nguyen, S. Sen, et al., “A Systematic Review of Data Quality in CPS and IoT for Industry 4.0,” *ACM Computing Surveys* 55, no. 14 (2023): 1–38.

11. A. Khanfor, “Determinants to Adopt Industrial Internet of Things in Small and Medium-Sized Enterprises,” *Future Internet* 16, no. 9 (2024): 340.

12. D. M. K. Dave and B. K. Mittapally, “Data Integration and Interoperability in IoT: Challenges, Strategies and Future Direction,” *International Journal of Computer Engineering and Technology (IJCET)* 15 (2024): 45–60.

13. G. B. Raja, “Impact of IIOT in Future Industries: Opportunities and Challenges,” in *Internet of Things*, 1st ed., ed. A. K. Rana, A. O. Salau, S. Sharma, S. Tayal, and S. Gupta (CRC Press, 2021), 101–112.

14. A. Hazra, M. Adhikari, T. Amgoth, and S. N. Srirama, “A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions,” *ACM Computing Surveys* 55, no. 1 (2021): 1–35.

15. S. F. Ahmed, M. S. B. Alam, M. Hoque, et al., “Industrial Internet of Things Enabled Technologies, Challenges, and Future Directions,” *Computers and Electrical Engineering* 110 (2023): 108847.

16. R. Ejjami and K. Boussalham, “Resilient Supply Chains in Industry 5.0: Leveraging AI for Predictive Maintenance and Risk Mitigation,” *International Journal for Multidisciplinary Research* 6, no. 4 (2024): 25116.

17. V. Demertzi, S. Demertzis, and K. Demertzis, “An Overview of Privacy Dimensions on the Industrial Internet of Things (Iiot),” *Algorithms* 16, no. 8 (2023): 378.

18. A. T. Shahad and Q. A. Al-Haija, “Fortifying Industrial IoT (IIoT): Leveraging AI for Optimizing Security,” in *Information Security Governance Using Artificial Intelligence of Things in Smart Environments* (CRC Press, 2026), 242–257.

19. H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The Industrial Internet of Things (IIoT): An Analysis Framework,” *Computers in Industry* 101 (2018): 1–12.

20. F. Qiu, A. Kumar, J. Hu, et al., “A Review on Integrating IoT, IIoT, and Industry 4.0: A Pathway to Smart Manufacturing and Digital Transformation,” *IET Information Security* 1 (2025): 9275962.

21. X. Guo, S. Han, X. S. Hu, et al., “Towards Scalable, Secure, and Smart Mission-Critical IoT Systems: Review and Vision,” in *Proceedings of the 2021 International Conference on Embedded Software* (Association for Computing Machinery, 2021), 1–10.

22. F. Banaie and M. Hashemzadeh, “Complementing IIoT Services Through AI: Feasibility and Suitability,” in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT* (Springer International Publishing, 2021), 7–19.

23. J. Kale, “Convergence of Artificial Intelligence With the Internet of Things Towards Industry 4.0,” in *Convergence of Artificial Intelligence and Internet of Things for Industrial Automation* (CRC Press, 2024), 33–48.

24. P. Mathur, “Overview of IoT and IIoT,” in *IoT Machine Learning Applications in Telecom, Energy, and Agriculture: With Raspberry Pi and Arduino Using Python* (Apress Berkeley, 2020), 19–43.

25. S. Latif, M. Driss, W. Boulila, et al., “Deep Learning for the Industrial Internet of Things (Iiot): A Comprehensive Survey of Techniques, Implementation Frameworks, Potential Applications, and Future Directions,” *Sensors* 21, no. 22 (2021): 7518.

26. D. A. Milovanovic and V. Pantovic, “5G-AIoT Artificial Intelligence of Things: Opportunity and Challenges,” in *Driving 5G Mobile Communications With Artificial Intelligence Towards 6G* (CRC Press, 2023), 253–276.

27. Y. Hoong and D. Rezania, “Balancing Talent and Technology: Navigating Cybersecurity and Privacy in SMEs,” *Telematics and Informatics Reports* 15 (2024): 100151.

28. S. Duan, D. Wang, J. Ren, et al., “Distributed Artificial Intelligence Empowered by End-Edge-Cloud Computing: A Survey,” *IEEE Communications Surveys and Tutorials* 25, no. 1 (2022): 591–624.

29. A. Mahmoudian, B. Izadi, D. Y. Pyun, et al., “Challenges of Social Media Workers in Football Clubs Using Technology–Organization–Environment (TOE) Framework,” *Future Business Journal* 11, no. 1 (2025): 188.

30. R. W. Idayani and E. W. T. Darmaningrat, “Evaluation of Factors Affecting Student Acceptance of Zedemy Using the Unified Theory of Acceptance and Use of Technology (UTAUT),” *Procedia Computer Science* 234 (2024): 1276–1287.

31. S. R. Natasia, Y. T. Wiranti, and A. Parastika, “Acceptance Analysis of NUADU as e-Learning Platform Using the Technology Acceptance Model (TAM) Approach,” *Procedia Computer Science* 197 (2022): 512–520.

32. R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, “How to Properly Use the PRISMA Statement,” *Systematic Reviews* 10, no. 1 (2021): 117.

33. B. Kitchenham and S. Charters, “Guidelines for Performing Systematic Literature Reviews in Software Engineering Version 2.3,” *Engineering* 45, no. 4 (2007): 1051.

34. M. Gusenbauer, “Beyond Google Scholar, Scopus, and Web of Science: An Evaluation of the Backward and Forward Citation Coverage of 59 Databases' Citation Indices,” *Research Synthesis Methods* 15, no. 5 (2024): 802–817.

35. R. S. Peres, X. Jia, J. Lee, et al., “Industrial Artificial Intelligence in Industry 4.0-Systematic Review, Challenges and Outlook,” *IEEE Access* 8 (2020): 220121–220139.

36. M. Javaid, A. Haleem, R. P. Singh, et al., “Artificial Intelligence Applications for Industry 4.0: A Literature-Based Study,” *Journal of Industrial Integration and Management* 7, no. 1 (2022): 83–111.

37. W. Karwowski, G. Salvendy, L. Albert, et al., “Grand Challenges in Industrial and Systems Engineering,” *International Journal of Production Research* 63, no. 4 (2025): 1538–1583.

38. S. Bibri, “On the Sustainability of Smart and Smarter Cities in the Era of Big Data: An Interdisciplinary and Transdisciplinary Literature Review,” *Journal of Big Data* 6, no. 1 (2019): 25.

39. C. Liu, Z. Su, X. Xu, and Y. Lu, “Service-Oriented Industrial Internet of Things Gateway for Cloud Manufacturing,” *Robotics and Computer-Integrated Manufacturing* 73 (2022): 102217.

40. M. Al-Smadi, O. Qawasmeh, M. Al-Ayyoub, Y. Jararweh, and B. Gupta, "Deep Recurrent Neural Network vs. Support Vector Machine for Aspect-Based Sentiment Analysis of Arabic Hotels' Reviews," *Journal of Computational Science* 27 (2018): 386–393.

41. S. S. Gill, M. Golec, J. Hu, et al., "Edge AI: A Taxonomy, Systematic Review and Future Directions," *Cluster Computing* 28, no. 1 (2025): 18.

42. N. Omrani, G. Rivieccio, U. Fiore, F. Schiavone, and S. G. Agreda, "To Trust or Not to Trust? An Assessment of Trust in AI-Based Systems: Concerns, Ethics and Contexts," *Technological Forecasting and Social Change* 181 (2022): 121763.

43. I. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," *SN Computer Science* 2, no. 6 (2021): 1–20.

44. K. Bian and R. Priyadarshi, "Machine Learning Optimization Techniques: A Survey, Classification, Challenges, and Future Research Issues," *Archives of Computational Methods in Engineering* 31, no. 7 (2024): 4209–4233.

45. Y. CA, "Integrated and Intelligent Manufacturing: Perspectives and Enablers," *Engineering* 3, no. 5 (2017): 588–595.

46. S. Yao, S. Hu, Y. Zhao, A. Zhang, and T. Abdelzaher, "Deepsense: A Unified Deep Learning Framework for Time-Series Mobile Sensing Data Processing," in *Proceedings of the 26th International Conference on World Wide Web* (Association for Computing Machinery, 2017), 351–360.

47. D. B. Raven, Y. Chikkula, K. M. Patel, et al., "Machine Learning & Conventional Approaches to Process Control & Optimization: Industrial Applications & Perspectives," *Computers & Chemical Engineering* 189 (2024): 108789.

48. L. E. Lwakatare, A. Raj, I. Crnkovic, J. Bosch, and H. H. Olsson, "Large-Scale Machine Learning Systems in Real-World Industrial Settings: A Review of Challenges and Solutions," *Information and Software Technology* 127 (2020): 106368.

49. I. Mendia, S. Gil-Lopez, I. Grau, and J. del Ser, "A Novel Approach for the Detection of Anomalous Energy Consumption Patterns in Industrial Cyber-Physical Systems," *Expert Systems* 41, no. 2 (2024): e12959.

50. Z. Teng, L. Li, Z. Xin, et al., "A Literature Review of Artificial Intelligence (AI) for Medical Image Segmentation: From AI and Explainable AI to Trustworthy AI," *Quantitative Imaging in Medicine and Surgery* 14, no. 12 (2024): 9620–9652.

51. M. Arora, "AI-Driven Industry 4.0: Advancing Quality Control Through Cutting-Edge Image Processing for Automated Defect Detection," *International Journal of Computer Science and Mobile Computing* 12, no. 8 (2023): 16–32.

52. Z. Huang, H. Wang, E. P. Xing, and D. Huang, "Self-Challenging Improves Cross-Domain Generalization," in *European Conference on Computer Vision* (Springer International Publishing, 2020), 124–140.

53. J. Lee, J. Singh, M. Azamfar, and V. Pandhare, "Industrial AI and Predictive Analytics for Smart Manufacturing Systems," in *Smart Manufacturing* (Elsevier, 2020), 213–244.

54. T. Meuser, L. Lovén, M. Bhuyan, et al., "Revisiting Edge Ai: Opportunities and Challenges," *IEEE Internet Computing* 28, no. 4 (2024): 49–59.

55. B. Singh, "Revolutionizing Supply Chains for Optimized Demand Planning, Inventory Management, and Logistics: An In-Depth Analysis of AI and ML Solutions in the Modern Era," in *Supply Chain Transformation Through Generative AI and Machine Learning* (IGI Global, 2025), 103–128.

56. N. Rane, S. Choudhary, and J. Rane, "Artificial Intelligence for Enhancing Resilience," *Journal of Applied Artificial Intelligence* 5, no. 2 (2024): 1–33.

57. S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, et al., "The Future of Enterprise Automation: Integrating AI in Cybersecurity, Cloud Operations, and Workforce Analytics," *Artificial Intelligence and Machine Learning Review* 3, no. 2 (2022): 1–15.

58. T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions," *Sensors* 25, no. 1 (2025): 213.

59. S. K. Shandilya, A. Datta, Y. Kartik, and A. Nagar, "Navigating the Regulatory Landscape," in *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy* (Springer Nature Switzerland, 2024), 127–240.

60. P. Dudczyk, J. K. Dunston, and G. V. Crosby, "Blockchain Technology for Global Supply Chain Management: A Survey of Applications, Challenges, Opportunities and Implications," *IEEE Access* 12 (2024): 70065–70088.

61. B. Shneiderman, "Bridging the Gap Between Ethics and Practice: Guidelines for Reliable, Safe, and Trustworthy Human-Centered AI Systems," *ACM Transactions on Interactive Intelligent Systems* 10, no. 4 (2020): 1–31.

62. H. Gamal, "Technological Integration and Innovative Strategies Harnessing Artificial Intelligence for Operational Excellence," in *Building Business Knowledge for Complex Modern Business Environments* (IGI Global, 2025), 237–270.

63. E. S. Tenakwah and C. Watson, "Embracing the AI/Automation Age: Preparing Your Workforce for Humans and Machines Working Together," *Strategy & Leadership* 53, no. 1 (2025): 32–48.

64. R. C. Reddy, B. Bhattacharjee, D. Mishra, and A. Mandal, "A Systematic Literature Review Towards a Conceptual Framework for Enablers and Barriers of an Enterprise Data Science Strategy," *Information Systems and e-Business Management* 20, no. 1 (2022): 223–255.

65. J. Schwaeke, C. Gerlich, H. L. Nguyen, D. K. Kanbach, and J. Gast, "Artificial Intelligence (AI) for Good? Enabling Organizational Change Towards Sustainability," *Review of Managerial Science* 19 (2025): 1–26.

66. X. Chen and A. D. Lloyd, "Understanding the Challenges of Blockchain Technology Adoption: Evidence From China's Developing Carbon Markets," *Information Technology & People* 38, no. 3 (2025): 1328–1362.

67. M. Sharma, A. Tomar, and A. Hazra, "Edge Computing for Industry 5.0: Fundamental, Applications, and Research Challenges," *IEEE Internet of Things Journal* 11, no. 11 (2024): 19070–19093.

68. M. Yazdi, "Integration of IoT and Edge Computing in Industrial Systems," in *Advances in Computational Mathematics for Industrial System Reliability and Maintainability* (Springer Nature Switzerland, 2024), 121–137.

69. G. Fylaktopoulos, M. Skolarikis, I. Papadopoulos, G. Goumas, A. Sotiropoulos, and I. Maglogiannis, "A Distributed Modular Platform for the Development of Cloud Based Applications," *Future Generation Computer Systems* 78 (2018): 127–141.

70. C. Pahl, P. Jamshidi, and O. Zimmermann, "Architectural Principles for Cloud Software," *ACM Transactions on Internet Technology* 18, no. 2 (2018): 1–23.

71. B. Farahani and A. K. Monsefi, "Smart and Collaborative Industrial IoT: A Federated Learning and Data Space Approach," *Digital Communications and Networks* 9, no. 2 (2023): 436–447.

72. B. N. Jørgensen, S. S. Gunasekaran, and Z. G. Ma, "Impact of EU Laws on AI Adoption in Smart Grids: A Review of Regulatory Barriers, Technological Challenges, and Stakeholder Benefits," *Energies* 18, no. 12 (2025): 3002.

73. J. Lee, J. Ni, J. Singh, B. Jiang, M. Azamfar, and J. Feng, "Intelligent Maintenance Systems and Predictive Manufacturing," *Journal of Manufacturing Science and Engineering* 142, no. 11 (2020): 110805.